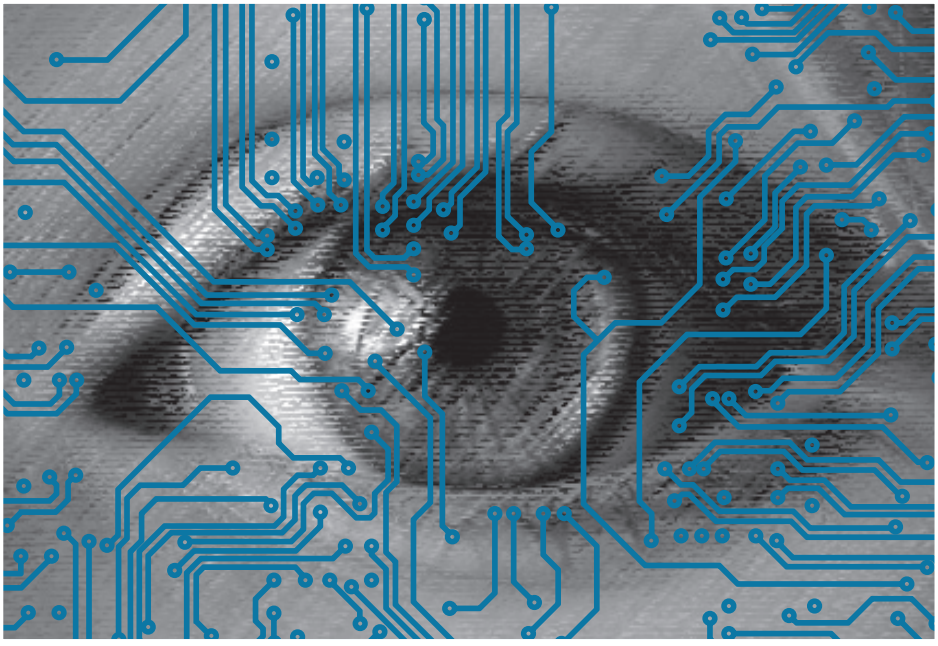
SSM

Scuola Superiore della Magistratura

IDENTITÀ DIGITALE, PROCESSO E RAPPORTI TRA PRIVATI



Giuffrè

Giuffrè Francis Lefebvre

SSM

SCUOLA SUPERIORE DELLA MAGISTRATURA

IDENTITÀ DIGITALE, PROCESSO E RAPPORTI TRA PRIVATI

GIUFFRÈ
GIUFFRÈ FRANCIS LEFEBVRE

ISBN 9788828842484

Volume a cura di Antonella Ciriello e Marisaria Maugeri

Contributo redazionale: Antonella Licheri, funzionario giudiziario
Scuola superiore della magistratura, e Ivana Petrone, nell'ambito del tirocinio
curriculare presso la Scuola superiore della magistratura, a seguito
della convenzione sottoscritta con l'Università degli Studi Federico II di Napoli

Pubblicazione della Scuola superiore della magistratura.

Giuffrè Francis Lefebvre S.p.A. Milano - 2024
Via Monte Rosa, 91 - 20149 MILANO - www.giuffrefrancislefebvre.it

---

Stampato da Tipografia Galli & C. S.r.l. - Varese

Abstract dell'intera opera

Di fronte all'evolversi vertiginoso della tecnologia e alla imponente azione normativa e di soft law europea, questo studio della Scuola Superiore della Magistratura, affronta il tema del domicilio e della identità in maniera trasversale, per sollecitare negli interpreti riflessioni adeguate e una corretta ricollocazione degli istituti.

I contributi sono aggiornati alla data del 29 marzo 2024.

INDICE SOMMARIO

PARTE I
INTRODUZIONE AL TEMA

I.
IL CONCETTO DI DOMICILIO E IDENTITÀ DIGITALI NEL QUADRO GENERALE TRA NORMATIVA INTERNA ED EUROPEA (CAD, EIDAS, NORME SPECIALI)

di *Antonella Ciriello*

II.
LE TIPOLOGIE DI DOMICILIO DIGITALE IN TERMINI GENERALI E IL LORO RECEPIMENTO NELLE NORME PROCESSUALI

di *Antonella Ciriello*

III.

RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E IDENTITÀ E DOMICILIO DIGITALI

di *Nicola Bardino*

IV.

IDENTIFICAZIONE IN RETE: IDENTITÀ DIGITALE E IDENTITÀ PERSONALE

di *Antonino Mazzeo* e *Michele Nastri*

PARTE II

LA RILEVANZA NEL PROCESSO CIVILE DELL'IDENTITÀ E DEL DOMICILIO DIGITALE

Sezione I

IL PROCESSO DI COGNIZIONE

I.

LE TIPOLOGIE DI DOMICILIO DIGITALE NEL PROCESSO CIVILE

di *Antonella Ciriello*

II.

IL DOMICILIO DIGITALE NELLA NOTIFICA TELEMATICA. I PUBBLICI ELENCHI O REGISTRI AI FINI DELLA COMUNICAZIONE E DELLA NOTIFICA

di *Antonella Ciriello*

III.

IL DOMICILIO DIGITALE NELLE COMUNICAZIONI DI CANCELLERIA

di *Ileana Fedele*

IV.

IL DOMICILIO DIGITALE NEL DEPOSITO TELEMATICO (CENNI)

di *Antonella Ciriello*

V.

IL DOMICILIO DIGITALE DELLE PUBBLICHE AMMINISTRAZIONI. LE PECULIARITÀ DELL'AVVOCATURA DELLO STATO

di *Marco La Greca*

VI.

LE PATOLOGIE DERIVANTI DALL'IMPIEGO NON CORRETTO DI IDENTITÀ O DOMICILIO DIGITALI

di *Roberto Arcella* e *Giovanni Rocchi*

Sezione II

IL PROCESSO DI ESECUZIONE

I.

I DOMICILI DIGITALI ESECUTIVI

di *Rinaldo d'Alonzo*

Sezione III
LA VOLONTARIA GIURISDIZIONE

I.
NOTE SUL DOMICILIO DIGITALE DEL NOTAIO
di *Michele Nastri*

II.
IL DOMICILIO DIGITALE NELLA VOLONTARIA GIURISDIZIONE: APPLICAZIONE DEL DOMICILIO DI PIATTAFORMA NELLA GIUSTIZIA CIVILE
di *Antonella Ciriello*

Sezione IV
IL DOMICILIO DIGITALE NELLA CRISI D'IMPRESA

I.
CODICE DELLA CRISI E DIGITALIZZAZIONE: UN PERCORSO QUASI COMPIUTO?
di *Lorenza Calcagno*

II.
IL DOMICILIO DIGITALE NEL CODICE DELLA CRISI
di *Giuseppe Fichera*

PARTE III
IDENTITÀ E DOMICILIO DIGITALI NEI GIUDIZI CIVILI DI REGNO UNITO, SPAGNA, GERMANIA E FRANCIA

I.
DIGITAL IDENTITY AND DOMICILE IN ENGLAND AND WALES
di *James Henderson* e *Renato Nazzini*

II.
LES PRINCIPES DIRECTEURS DU PROCÈS AU SERVICE DE LA NUMÉRISATION DE LA PROCÉDURE
di *Samir Merabet*

III.
DIGITALE IDENTIFIZIERUNG UND ELEKTRONISCHE KOMMUNIKATION IM DEUTSCHEN ZIVILPROZESS
di *Jonathan Hager* e *Wolfgang Hau*

PARTE IV
IDENTITÀ E DIRITTI DEI PRIVATI

I.
IDENTITÀ DIGITALE TRA DATI PERSONALI E RELAZIONI FUNZIONALI
di *Giuseppe Corasaniti*

II.
L'IDENTITÀ PERSONALE DEL MINORE DI ETÀ NEL *CYBERSPAZIO* TRA AUTODETERMINAZIONE E *PARENTAL CONTROL SYSTEM*
di *Roberto Senigaglia*

III.

IDENTITÀ DIGITALE E SUCCESSIONI PER CAUSA DI MORTE

di *Francesca Bartolini*

IV.

L'"OBLIO DIGITALE": STRUMENTI DI TUTELA DINANZI AL GIUDICE CIVILE

di *Martina Flamini*

V.

IDENTITÀ DIGITALE DELL'IMPRESA: RICOSTRUZIONE CONCETTUALE, FORME E TECNICHE DI PROTEZIONE

di *Luca Boggio*

VI.

DA OPERAIO AD AVATAR?
IDENTITÀ DIGITALE E PRIVACY DEL LAVORATORE

di *Giuseppe Sigillò Massara*

VII.

IDENTITÀ DIGITALE E RISERVATEZZA

di *Marco Rossetti*

PARTE V
DOMICILIO DIGITALE NEL PROCESSO PENALE

I.

LE CATEGORIE GENERALI DI DOMICILIO E IL PROCESSO PENALE.
IL DOMICILIO PER I DEPOSITI

di *Antonella Ciriello*

II.

LA NOTIFICA TELEMATICA NELLA DISCIPLINA DEL PROCESSO PENALE
E IL DOMICILIO DIGITALE

di *Roberto Patscot*

PARTE VI
CONCLUSIONI

I.
LE PROSPETTIVE EUROPEE NEL FUTURO PROSSIMO

di *Stefano Nativi*

APPENDICE

I.

IDENTITÀ E DOMICILIO DIGITALE IN INGHILTERRA E GALLES

di *James Henderson* e *Renato Nazzini*

II.

I PRINCIPI GUIDA DEL PROCESSO DI DIGITALIZZAZIONE DELLA PRATICA PROCESSUALE

di *Samir Merabet*

III.

IDENTITÀ DIGITALE E COMUNICAZIONE ELETTRONICA NELLA PROCEDURA CIVILE TEDESCA

di *Jonathan Hager* e *Wolfgang Hau*

I CURATORI

Antonella Ciriello - Consigliere di Cassazione, consulente del Ministro della giustizia, già Componente del Comitato direttivo della SSM

Marisaria Maugeri - Professoressa ordinaria di diritto privato, Università degli Studi di Catania, già Componente del Comitato direttivo della SSM

I COORDINATORI

Ferruccio Auletta - Professore ordinario di Diritto processuale civile, Università LUISS Guido Carli di Roma

Simona Caporusso - Professoressa associata di Diritto processuale civile, Università telematica E-Campus

Enzo Vincenti - Magistrato, Corte di cassazione

Roberto Patscot - Sostituto Procuratore della Repubblica, Procura della Repubblica presso il Tribunale di Napoli

Massimo Proto - Professore ordinario di Diritto privato, Link Campus University di Roma

GLI AUTORI

Roberto Arcella - Avvocato, foro di Napoli

Nicola Bardino - Magistrato amministrativo, responsabile vicario del Servizio per l'informatica della Giustizia Amministrativa

Francesca Bartolini - Professoressa associata di Diritto privato, Link Campus University di Roma

Luca Boggio - Professore associato di Diritto commerciale, Link Campus University di Roma

Lorenza Calcagno - già Componente del Comitato direttivo della SSM

Antonella Ciriello - già Componente del Comitato direttivo della SSM

Giuseppe Corasaniti - Professore ordinario di filosofia del diritto, Universitas Mercatorum di Roma

Rinaldo d'Alonzo - Magistrato, Tribunale di Larino

Ileana Fedele - Magistrato, Corte di cassazione

Giuseppe Fichera - Vice Capo Dipartimento per la transizione digitale della giustizia

Martina Flamini - Magistrato, Corte di cassazione

Jonathan Hager - Wissenschaftlicher Mitarbeiter, Ludwig-Maximilians-Universität München

Wolfgang Hau - Richter am Oberlandesgericht Professor, Ludwig-Maximilians-Universität München

James Henderson - Barrister, England and Wales

Marco La Greca - Avvocato dello Stato

Antonino Mazzeo - Professore Emerito di sistemi di elaborazione delle informazioni, Università degli Studi di Napoli

Samir Merabet - Agrégé des facultés, Professeur de droit privé, Université des Antilles

Michele Nastri - Notaio, distretto di Napoli, Torre Annunziata e Nola

Stefano Nativi - Scientific attaché - Telecommunications and Information Society (Digital and Cyber-security) - Permanent Representation of Italy to the European Union

Renato Nazzini - Professor of Law and Director of the Centre of Construction Law and Dispute Resolution, King's College London

Roberto Patscot - Sostituto Procuratore, Procura della Repubblica presso il Tribunale di Napoli

Giovanni Rocchi - Presidente del Consiglio dell'Ordine degli Avvocati di Brescia

Marco Rossetti - Magistrato, Corte di cassazione

Roberto Senigaglia - Professore ordinario di Diritto privato, Università degli Studi Ca' Foscari di Venezia

Giuseppe Sigillò Massara - Professore associato di Diritto del Lavoro, Link Campus University di Roma

Parte I
INTRODUZIONE AL TEMA

I.

IL CONCETTO DI DOMICILIO E IDENTITÀ DIGITALI NEL QUADRO GENERALE TRA NORMATIVA INTERNA ED EUROPEA (CAD, EIDAS, NORME SPECIALI)

di *Antonella Ciriello*

Sommario: 1.1. Introduzione. — 1.1.1. La specialità delle norme processuali (ossia Il valore delle norme del CAD, tra diritto sostanziale, rapporti con la PA e discipline processuali speciali e le regole generali su domicilio e identità digitali). — 1.2. Le definizioni di domicilio e identità digitali e la disciplina del CAD. — 1.2.1. La posta elettronica certificata e il recapito certificato qualificato (cenni), rapporti con il concetto di domicilio digitale. — 1.3. Le varie forme di domicilio digitale nel contesto generale. — 1.3.1. L'art. 3-*bis* del CAD ed i soggetti obbligati al domicilio digitale. — 1.3.2. L'identità e il domicilio digitali tra diritto, dovere e facoltà. — 1.4. Il quadro europeo (cenni). — 1.5. Altri dati normativi nazionali che contemplano il domicilio digitale (cenni).

1.1. Introduzione

Il domicilio digitale e la identità digitale costituiscono il fulcro della digitalizzazione della pubblica amministrazione, della giustizia e dei traffici commerciali, quanto ai soggetti.

È superfluo sottolineare, infatti, che ogni transazione sociale e atto giuridicamente rilevante, da chiunque provenga, debba riferirsi, per essere tale, ad una identità digitale collegata ad una persona fisica individuale o rappresentante di una persona giuridica, autore o destinatario o partecipe del procedimento.

Questa consapevolezza è molto chiara a livello europeo, tanto che l'UE ha intrapreso, nel 2021, con il cd. Decennio digitale, una produzione normativa e di "*soft law*" per garantire che la transizione al digitale sia sicura, equa e conforme ai valori europei, riconoscendo l'importanza di mantenere e ampliare i diritti dei cittadini nel contesto digitale [1].

Sul piano europeo, Il Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione

---

[1] Il PNRR italiano prevede l'integrazione del domicilio digitale con l'ANPR entro il secondo quadrimestre del 2025 (PNRR.pdf (governo.it) investimento 1.2.).

elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (eIDAS è l'acronimo di "Electronic Identification, Authentication and Trust Services", da qui in poi, per semplicità regolamento eIDAS) ha rappresentato un passo significativo nell'ambito dell'identità digitale e dei servizi fiduciari all'interno dell'Unione Europea. Il regolamento ha definito un quadro normativo per i servizi di identificazione elettronica (eID), autenticazione, servizi fiduciari (2).

All'esito di una consultazione pubblica del 2020, che ha evidenziato alcune carenze nella realizzazione degli obiettivi del regolamento (ossia la sua limitata attuazione, la necessità di interventi di aggiornamento in relazione all'evoluzione tecnologica, si è avviata, su proposta del Consiglio, la revisione del quadro eIDAS, per promuovere un sistema di identità digitale europeo più integrato e sicuro. La Commissione Europea ha presentato la proposta di Regolamento sull'identità digitale europea (European eID) il 3 giugno 2021, per aggiornare il regolamento eIDAS del 2014, introducendo il concetto di portafoglio di identità digitale europea, che faciliterà l'accesso ai servizi digitali pubblici e privati, tanto a livello nazionale quanto transfrontaliero.

Come si vedrà più approfonditamente (3), l'accordo per la revisione eIDAS è stato raggiunto nel giugno 2023 e verrà nel corso di questo anno 2024 pubblicato.

Sul piano nazionale, poi, i più importanti riferimenti normativi per i temi oggetto di questo studio, devono necessariamente essere individuati nella normativa generale, contenuta nel Codice dell'Amministrazione Digitale (da qui in poi, semplicemente, CAD), d.lgs. 7 marzo 2005, n. 82, peraltro costantemente in linea con la normativa europea alla quale è stato più volte adeguato, che tratteggia gli istituti giuridici della transizione digitale.

Il CAD, infatti, non è solo il "testo unico" che "riunisce e organizza le norme riguardanti l'informatizzazione della Pubblica Amministrazione nei rapporti con i cittadini e le imprese" (4), ma regola anche i rapporti tra privati per le norme più importanti, elencate nell'art. 2, comma 3.

---

(2) Il fondamento del regolamento eIDAS è l'articolo 114 del Trattato sul Funzionamento dell'Unione Europea (TFUE), che si propone di facilitare il funzionamento del mercato interno attraverso l'armonizzazione delle legislazioni nazionali.

(3) Cfr. S. Nativi (Parte VI), che osserva come "Nel giugno 2023 il Consiglio dell'Unione e il Parlamento europeo raggiungono un accordo sul testo della proposta di regolamento per un'identità digitale europea (eID), al fine di modificare il testo della normativa eIDAS del 2014. Il regolamento rivisto (alias eIDAS 2) costituisce un chiaro cambiamento di paradigma per l'identità digitale in Europa, con l'obiettivo di garantire a persone e imprese l'accesso universale a un'identificazione e a un'autenticazione elettronica sicura e affidabile tramite un portafoglio digitale personale su telefono cellulare".

(4) In termini la definizione si legge sul sito dell'Agenzia per l'Italia Digitale https://www.agid.gov.it/it/agenzia/strategia-quadro-normativo/codice-amministrazione digitale#:~:tex

Tra quelle norme del CAD che si applicano ai privati (ove non diversamente previsto) compaiono proprio quelle in materia di domicilio e identità digitali (rispettivamente di cui all'articolo 3-*bis* di cui agli articoli 3-*bis* e 64). Si applicano, ancora, anche ai privati, le importanti norme relative al documento informatico, alle firme elettroniche e ai servizi fiduciari di cui al Capo II, alla riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, alle comunicazioni elettroniche di cui all'art. 3-*bis* e al Capo IV.

Il CAD è stato oggetto di molteplici modifiche e integrazioni, tra l'altro, ad opera del d.lgs. 22 agosto 2016, n. 179 e poi del d.lgs. 13 dicembre 2017, n. 217 (a sua volta modificato successivamente, in seguito alla sferzata di innovazione conseguente alla Pandemia), sempre per essere progressivamente adeguato al Regolamento europeo eIDAS. È corredato da un corpo di linee guida, che sostituiscono le precedenti regole tecniche e che, a differenza di queste ultime, statiche e pubblicate con d.p.c.m., sono invece più dinamiche e curate dall'AgID secondo una procedura disciplinata dagli artt. 14-*bis* e 71 del Codice [5].

1.1.1. *La specialità delle norme processuali (ossia Il valore delle norme del CAD, tra diritto sostanziale, rapporti con la PA e discipline processuali speciali e le regole generali su domicilio e identità digitali)*

Di particolare importanza, ai fini di questo studio, per la parte relativa al processo, il dispositivo dell'art. 2, comma 6, del CAD [6] che stabilisce: « *Le disposizioni del presente Codice si applicano ((...)) al processo civile, penale, amministrativo, contabile e tributario, in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico* ».

La norma (introdotta nel 2016) era stata già anticipata, tramite l'interpretazione, dalla giurisprudenza di legittimità che, con sentenza della Sez. III, 10 novembre 2015, n. 22871, aveva chiarito come nell'art. 4 del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010, n. 24, intitolato "misure urgenti per la digitalizzazione della giustizia" erano stati estesi al processo civile i principi previsti dal decreto legislativo 7 marzo 2005, n. 82 (CAD) e successive modificazioni.

---

t=Il%20Codice%20dell'Amministrazione%20Digitale,legislativo%207%20marzo%202005%2C%20n.

[5] https://www.agid.gov.it/sites/default/files/repository_files/regolamento-adozione-linee-guida-attuazione- CAD.pdf.

[6] Le disposizioni del presente Codice si applicano ((...)) al processo civile, penale, amministrativo, contabile e tributario, in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico.

Correttamente, la corte di legittimità considera il CAD "*l'apparato legislativo di riferimento qualora gli atti processuali di cui agli artt. 121 e seg. cod. proc. civ., ed in specie i provvedimenti del giudice, siano contenuti in documenti informatici. Quest'ultima eventualità è consentita, appunto, dal testo del menzionato art. 4 laddove presuppone « l'adozione nel processo civile [_] delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005 n. 82, e successive modificazioni ». Quindi i principi generali del CAD sono applicabili anche in ambito processuale e le relative disposizioni costituiscono le norme con valore di legge ordinaria che, per il tramite dell'art. 4 del d.l. 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010, n. 24, disciplinano gli atti del processo civile redatti in forma di documento informatico (cfr. art. 1 lett.* p) *e art. 20 CAD) e sottoscritti con firma digitale (cfr. art. 1 lett.* s)) *e art. 21 CAD)*".

A fronte di tale disciplina generale, poi, i testi normativi succedutisi nel tempo sul versante della giustizia soprattutto civile (poiché sul versante penale la digitalizzazione è giunta in ritardo e non può dirsi ancora compiutamente concretamente realizzata, se non a livello normativo con le disposizioni codicistiche e la individuazione di una serie di "step" e scadenze, da ultimo ad opera del decreto ministeriale reso ai sensi dell'art. 87 della legge 10 ottobre 2022, n. 150 (7)) hanno dettato discipline che hanno valorizzato gli strumenti tecnologici esistenti, evolvendosi mano a mano che il quadro normativo si completava.

In forza di tali disposizioni, allora, ogni volta che sul versante processuale (civile, penale, amministrativo, contabile e tributario) si tratta di applicare uno degli istituti del digitale, regolati dal Codice, occorre svolgere prima una verifica di esistenza di norme speciali dettate appositamente per lo specifico processo.

In caso di vuoto normativo "speciale" occorre svolgere una verifica di compatibilità delle disposizioni del CAD prima di poterle applicare direttamente.

Si tratta di una verifica delicata e importante, che comporta, in caso di applicazione delle norme del CAD, anche la valutazione dell'applicazione

(7) Il decreto 29 dicembre 2023, n. 217 Regolamento recante: « Decreto ai sensi dell'articolo 87, commi 1 e 3 del decreto legislativo 10 ottobre 2022, n. 150 e dell'articolo 4, comma 1 del decreto-legge 29 dicembre 2009, n. 193, convertito con modificazioni dalla legge 22 febbraio 2010, n. 24, recante modifiche al decreto del Ministro della giustizia di concerto con il Ministro per la pubblica amministrazione e l'innovazione 21 febbraio 2011, n. 44 » è pubblicato nella GU Serie Generale del 30 dicembre 2023, n. 303, entra in vigore il 14 gennaio 2024 e contiene non solo le disposizioni relative al processo penale telematico ma anche tutte le modifiche introdotte in ragione della digitalizzazione conseguente alla riforma del processo civile e penale, alle regole tecniche del PCT (regolamento n. 44/2011).

delle relative linee guida, oppure delle regole tecniche del processo di volta in volta in evidenza (per esempio, nel caso del processo civile e penale, quelle regole recentemente innovate con il cit. Decreto del Ministro della Giustizia 29 dicembre 2023, n. 217 che ha modificato il regolamento contenuto nel d.m. 21 febbraio 2011, n. 44 "Regolamento concernente le regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione, in attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, convertito nella legge 22 febbraio 2010 n. 24. (G.U., Serie Generale, 18 aprile 2011, n. 89)". Pertanto la ricostruzione delle regole di volta in volta applicabili costituisce un vero e proprio ginepraio normativo, complesso da ricostruire, non solo perché le norme stesse sono in continua evoluzione in ciascun contesto, anche europeo, ma pure perché le scelte tecnologiche influenzano profondamente gli istituti e le applicazioni giurisprudenziali e spesso, i diversi contesti (amministrativo, processuale tra le varie forme di giurisdizione), si muovono in maniera eterogenea e — talvolta — incoerente.

È dunque indispensabile il confronto continuo con le regole generali per una corretta ricostruzione di ciascun istituto, nel quadro della richiesta interoperabilità dei sistemi, auspicata dall'UE per proporre una razionalizzazione che giovi al dialogo tra i paesi dell'Unione, evitare soluzioni eterogenee e fare in modo che il digitale e l'innovazione non costituisca un ostacolo per realizzazione di diritti e traffici, ma un valore aggiunto.

1.2. Le definizioni di domicilio e identità digitali e la disciplina del CAD

Il CAD delinea, in seguito ai molteplici rimaneggiamenti, un quadro abbastanza completo, pur se ancora in evoluzione come si vedrà, dell'identità e del domicilio digitali e dei possibili utilizzi.

La definizione generale del domicilio digitale fornita dal CAD, contenuta nell'art. 1 lett. *n-ter*) [8], lo descrive come un "*indirizzo elettronico eletto presso un servizio di posta elettronica certificata* [9] *o un servizio elettronico di recapito certificato qualificato, come disciplinato dal citato Regolamento eIDAS, valido ai fini delle comunicazioni elettroniche aventi valore legale*".

---

[8] La norma viene inserita dall'articolo 1, comma 1, lettera *c*), del d.lgs. 26 agosto 2016, n. 179, che detta le prime cogenti norme sulla giustizia digitale, e successivamente sostituita dall'articolo 1, comma 1, lettera *a*), numero 2), del d.lgs. 13 dicembre 2017, n. 217, che interviene per adeguare il CAD al regolamento eIDAS.

[9] La disciplina generale della posta elettronica certificata, da qui in poi semplicemente PEC, è contenuta principalmente nel Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68 e nel CAD.

La identità digitale, invece, è definita nella lettera *u-quater*) come: "l*a rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64* (infra)" (10).

Allo stato nel paese convivono i seguenti sistemi:

— « SPID »: il Sistema Pubblico di Identità Digitale, disciplinato dall'articolo 64 del CAD;

— « CIE »: Carta di identità il documento d'identità munito di elementi per l'identificazione fisica del titolare, di cui all'articolo 66 del decreto legislativo 7 marzo 2005, n. 82;

— CNS: (decreto 9 dicembre 2004 Mef- Interno e Innovazione) Carta Nazionale dei Servizi (CNS) è uno strumento di identificazione in rete che consente la fruizione dei servizi delle amministrazioni pubbliche (11).

La CNS non contiene la foto del titolare e non richiede particolari requisiti di sicurezza per il supporto plastico. La completa corrispondenza informatica tra CNS e Carta d'Identità Elettronica (CIE) assicura l'interoperabilità tra le due carte (12).

L'art. 64 del CAD, poi, riveste particolare importanza ai fini dell'identità e del domicilio digitali, poiché disciplina il "Sistema pubblico per la gestione delle identità digitali e modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni regolando la carta d'identità elettronica, la carta nazionale dei servizi e lo SPID che costituiscono strumenti per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni per i quali sia necessaria l'identificazione informatica.

Lo SPID, specificamente, "sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (comma 2-*ter*) è costituito come "insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, secondo modalità definite con il decreto di cui al comma 2-*sexies*", identificano gli utenti per consentire loro il compimento di attività e l'accesso ai servizi in rete.

---

(10) Concetto diverso dall'identità, è l'identificazione informatica [*u-ter*) è definita dal CAD come: *la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso. In genere, l'identificazione è indispensabile per l'attribuzione dell'identità del soggetto-*

(11) Nel d.m. 9 dicembre 2004 https://www.agid.gov.it/sites/default/files/repository_files/documentazione_trasparenza/decreto_9_dicembre_2004.pdf è definita come "Documento informatico, rilasciato da una Pubblica Amministrazione, con la finalità di identificare in rete il titolare della carta" Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete.

(12) https://www.agid.gov.it/it/piattaforme/carta-nazionale-servizi.

Di particolare interesse il comma 2-*septies* dell'art. 64 che, dopo aver previsto che "Un *atto giuridico può essere posto in essere da un soggetto identificato mediante SPID, nell'ambito di un sistema informatico avente i requisiti fissati nelle regole tecniche adottate ai sensi dell'articolo 71, attraverso processi idonei a garantire, in maniera manifesta e inequivoca, l'acquisizione della sua volontà*" stabilisce, poi, che "r*estano ferme le disposizioni concernenti il deposito degli atti e dei documenti in via telematica secondo la normativa anche regolamentare in materia di processo telematico*". Per garantire l'affidabilità del sistema, poi, la norma prevede che i gestori dell'identità digitale accreditati sono iscritti in un apposito elenco pubblico, tenuto da AgID, consultabile anche in via telematica.

Il comma 2-*duodecies*, del medesimo articolo, che si occupa della "verifica dell'identità digitale con livello di garanzia almeno significativo, ai sensi dell'articolo 8, paragrafo 2, del Regolamento" eIDAS, stabilisce che tale verifica produce, nelle transazioni elettroniche o per l'accesso ai servizi in rete, gli effetti del documento di riconoscimento equipollente, di cui all'articolo 35 del testo unico di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.

La disposizione si applica altresì in caso di identificazione elettronica ai fini dell'accesso ai servizi erogati dalle pubbliche amministrazioni e dai soggetti privati tramite canali fisici (13).

Al fine di verificare l'identità digitale il comma 3-ter individua un sistema di verifiche e controlli. In particolare "*I gestori dell'identità digitale accreditati, in qualità di gestori di pubblico servizio, prima del rilascio dell'identità digitale a una persona fisica, verificano i dati identificativi del richiedente, ivi inclusi l'indirizzo di residenza e, ove disponibili, il domicilio digitale o altro indirizzo di contatto, mediante consultazione gratuita dei dati disponibili presso l'ANPR di cui all'articolo 62, anche tramite la piattaforma prevista dall'articolo 50*-ter. *Tali verifiche sono svolte anche successivamente al rilascio dell'identità digitale, con cadenza almeno annuale, anche ai fini della verifica dell'esistenza in vita. Il direttore dell'AgID, previo accertamento dell'operatività delle funzionalità necessarie, fissa la data a decorrere dalla quale i gestori dell'identità*

(13) Si tratta dei presupposti di verifica dell'identità digitale, che assumeranno estremo rilievo nel contesto dell'EUWALLET; per fornire in relazione a specifiche esigenze, gli attributi qualificati dell'utente, "ivi compresi i dati relativi al possesso di abilitazioni o autorizzazioni richieste dalla legge ovvero stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche, ovvero gli altri dati, fatti e informazioni funzionali alla fruizione di un servizio attestati da un gestore di attributi qualificati, secondo le modalità stabilite da AgID con Linee guida" (testualmente nell'art. 64 cit.).

digitale accreditati sono tenuti ad effettuare le verifiche di cui ai precedenti periodi".

L'articolo 65 del CAD, inoltre, disciplina in via generale le modalità per la trasmissione valida di istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica.

Oltre alla sottoscrizione con le firme di cui all'art. 20 del medesimo CAD (che contiene la presunzione di riferibilità al titolare della forma digitale in caso di sottoscrizione di un documento), si valorizza l'utilizzo di uno dei tre sistemi di identificazione prima descritti (CNS; CIE; SPID), nonché la trasmissione dal proprio domicilio digitale iscritto in pubblici elenchi o da un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, conforme al Regolamento eIDAS.

1.2.1. *La posta elettronica certificata e il recapito certificato qualificato (cenni), rapporti con il concetto di domicilio digitale*

La posta elettronica certificata (già regolata, in generale, dal Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3), richiamata, nella prospettiva sempre generale, dall'art. 48 del CAD, è associata al recapito certificato qualificato nella definizione sopra richiamata che il CAD fornisce del domicilio digitale e costituisce allo stato anche lo strumento per inviare comunicazioni elettroniche a valore legale.

Sebbene la normativa europea da tempo abbia richiesto che la PEC sia adeguata a determinati attributi, il processo di adeguamento è ancora in corso, e se ne prevede il completamento in tempi brevi.

In particolare il decreto legge 14 dicembre 2018, n. 135, prevede che con d.p.c.m., sentita l'AgID e il Garante per la protezione dei dati personali, siano adottate le misure necessarie a garantire la conformità dei servizi di posta elettronica certificata (PEC), di cui agli articoli 29 e 48 del decreto legislativo 7 marzo 2005, n. 82, al regolamento (UE) n. 910 del Parlamento europeo e del Consiglio del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (14). A far data dall'entrata in

(14) https://www.agid.gov.it/sites/default/files/repository_files/documento_finale_gdl_rem_versione_1.2_28.07.2022_1.pdf

vigore del suindicato d.p.c.m., l'articolo 48 del decreto legislativo n. 82 del 2005 sarà abrogato (15).

In attesa che questo procedimento (annunziato per la fine del 2024) si compia e che la PEC italiana si trasformi in REM (16), convivono (non sempre felicemente) nel CAD, sia l'art. 48 che stabilisce che la PEC è lo strumento per la trasmissione telematica di comunicazioni che necessitano di una ricevuta di invio e di una ricevuta di consegna (e che equivale alla notificazione per mezzo della posta "analogica"), sia l'art. 6 (17) che, con espressioni simili, attribuisce il medesimo valore alle comunicazioni tra domicili digitali (ossia la PEC — ma a norma di eIDAS — e il SERCQ, di cui all'art. 1 lettera *n-ter*) (18).

Pertanto, in termini generali, nel nostro paese, fino a quando tutti gli indirizzi PEC rilasciati non saranno adeguati, non si può dire, in assoluto, che la PEC costituisca un domicilio digitale conforme al regolamento eIDAS

---

(15) Il d.lgs. 13 dicembre 2017, n. 217, come modificato dal d.l. 14 dicembre 2018, n. 135, convertito con modificazioni dalla l. 11 febbraio 2019, n. 12, ha disposto (con l'art. 65, comma 7) che "Con decreto del Presidente del Consiglio dei ministri, sentiti l'Agenzia per l'Italia digitale e il Garante per la protezione dei dati personali, sono adottate le misure necessarie a garantire la conformità dei servizi di posta elettronica certificata di cui agli articoli 29 e 48 del decreto legislativo del 7 marzo 2005, n. 82, al regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. A far data dall'entrata in vigore del decreto di cui al primo periodo, l'articolo 48 del decreto legislativo n. 82 del 2005 è abrogato".

(16) REM è l'acronimo di *Registered Electronic Mail*: in sostanza un servizio di "posta elettronica certificata europea" con valore legale su tutto il territorio dell'Unione conforme agli standard emessi da ETSI (European Telecommunications Standards Institute).

(17) L'art. 6 prevede che "Le comunicazioni tramite i domicili digitali sono effettuate agli indirizzi inseriti negli elenchi di cui agli articoli 6-*bis*, 6-*ter* e 6-*quater*, o a quello eletto come domicilio speciale per determinati atti o affari ai sensi dell'articolo 3-*bis*, comma 4-*quinquies*. Le comunicazioni elettroniche trasmesse ad uno dei domicili digitali di cui all'articolo 3-*bis* producono, quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno ed equivalgono alla notificazione per mezzo della posta salvo che la legge disponga diversamente. Le suddette comunicazioni si intendono spedite dal mittente se inviate al proprio gestore e si intendono consegnate se rese disponibili al domicilio digitale del destinatario, salva la prova che la mancata consegna sia dovuta a fatto non imputabile al destinatario medesimo. La data e l'ora di trasmissione e ricezione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.

(18) V. Massella, *Gli strumenti di AgID per supportare la trasformazione digitale* (scuolamagistratura.it), incontro di studi P22085 nonché incontro di studi P24002, la quale evidenzia che "la PEC non soddisfa appieno i requisiti previsti dal Regolamento eIDAS: non è prevista la verifica certa dell'identità del richiedente della casella di PEC il gestore non è obbligato a sottoporsi alle verifiche di conformità da parte degli organismi di valutazione accreditati da Accredia".

(che, come visto richiede la identificazione del mittente e altre caratteristiche).

La PEC può essere considerata un domicilio digitale o all'esito dell'adeguamento volontario (ed infatti, recentemente, i gestori stanno provvedendo ad invitare tutti i titolari a provvedervi, per il momento ancora facoltativamente) oppure attraverso la iscrizione dell'indirizzo PEC a uno degli elenchi previsti dallo stesso art. 3-*bis* del CAD (o quale conseguenza di un obbligo per determinate categorie di soggetti o quale esercizio di una facoltà) poiché tale iscrizione, in genere, si accompagna alla verifica dell'identità "qualificata" del suo titolare (19).

Questo spiega perché, nell'attuale situazione, ove il soggetto non sia titolare di domicilio digitale iscritto (perché non obbligato e per non aver esercitato la relativa facoltà), si prevede che, nei rapporti con la PA, la mera trasmissione da una PEC costituisca "*elezione di domicilio digitale (speciale, ai sensi dell'articolo 3*-bis*, comma 4*-quinquies*, per gli atti e le comunicazioni a cui è riferita l'istanza o la dichiarazione).*

La norma, esplicitamente, si pone in termini di sussidiarietà rispetto *a* "l*e disposizioni normative che prevedono l'uso di specifici sistemi di trasmissione telematica nel settore tributario*". Per gli aspetti, processuali, invece, come vedremo, la disciplina del CAD è solo generale, derogata dalle specifiche disposizioni ai sensi dell'art. 2 comma 6, tra cui quelle specifiche del processo civile e penale telematico.

In particolare, sul piano processuale, come si vedrà negli appositi capitoli dedicati al processo ordinario, benché sia previsto dalle norme anche il recapito certificato qualificato (SERCQ), la PEC rimane centrale sia nel settore civile che in quello penale. Nel primo, costituisce sia lo strumento della notifica e comunicazione di cancelleria, che di deposito in attesa dell'evoluzione (programmata dalle norme, ma non realizzata) verso l'upload. Nel settore penale, invece, è strumento di notifica, ma non di deposito, se non per effetto della normativa emergenziale, in via transitoria.

1.3. Le varie forme di domicilio digitale nel contesto generale

L'art. 3-*bis* del CAD, come accennato, è intitolato "Identità digitale e Domicilio digitale". La norma va letta in stretta correlazione con altre norme di cui costituisce punto di riferimento generale, tra cui le norme dei singoli processi telematici.

---

(19) L'identificazione informatica [*u-ter*) è definita dal CAD come: *la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.*

Sempre sul piano generale, assumono rilievo, per le definizioni in esso contenute e per i rinvii all'art. 3-*bis*, le disposizioni del d.l. 16 luglio 2020, n. 76 e successive modifiche che regola all'art. 26 la "Piattaforma per la notificazione digitale degli atti della pubblica amministrazione" e il relativo domicilio di piattaforma stabilendo al comma 5 le relative disposizioni, nonché dal regolamento attuativo introdotto con Decreto della Presidenza del Consiglio dei Ministri - Dipartimento Per La Trasformazione Digitale 8 febbraio 2022, n. 58 (in G.U., 6 giugno 2022, n. 130).

Si tratta di disposizioni che operano un riordino dopo la frettolosa creazione, durante la crisi della Pandemia, delle indispensabili piattaforme per gestire le certificazioni "vaccinali" dei cittadini e che disciplinano la definizione di « domicilio digitale di piattaforma » facendosi carico di una risistemazione dei concetti di domicilio digitale con riflessi sulla generale nozione del CAD, con la quale si armonizzano.

Il sistema che emerge, per quanto qui rileva, prevede tre forme di domicilio digitale ([20]):

1) « domicilio digitale generale »: l'indirizzo di posta elettronica certificata o di un servizio elettronico di recapito certificato qualificato inserito in uno degli elenchi di cui agli articoli 6-*bis*, 6-*ter* e 6-*quater* del CAD e previsto dall'articolo 26, comma 5, lettera *a*), del decreto-legge 76 del 2020;

2) « domicilio digitale speciale »: l'indirizzo di posta elettronica certificata o di un servizio elettronico di recapito certificato qualificato, eletto ai sensi dell'articolo 3-*bis*, comma 4-*quinquies*, del decreto legislativo n. 82 del 2005 o di altre disposizioni di legge, come domicilio speciale per determinati atti o affari, se a tali atti o affari è riferita la notificazione, di cui all'articolo 26, comma 5, lettera *b*), del decreto-legge;

3) « domicilio digitale di piattaforma »: l'indirizzo di posta elettronica certificata o di un servizio elettronico di recapito certificato qualificato,

---

([20]) Cosa diversa dal domicilio digitale è il recapito digitale, definito dal regolamento di cui al decreto 8 febbraio 2022, n. 58 come "il canale di comunicazione, diverso dal domicilio digitale, indicato dal destinatario ai fini del ricevimento degli avvisi di cortesia". Una applicazione di tale forma di recapito si rinviene nel processo penale.

L'art. 349 c.p.p. dispone che" Quando procede alla identificazione, la polizia giudiziaria invita la persona nei cui confronti vengono svolte le indagini a dichiarare o a eleggere il domicilio per le notificazioni a norma dell'articolo 161, nonché ad indicare il recapito della casa di abitazione, del luogo in cui esercita abitualmente l'attività lavorativa e dei luoghi in cui ha temporanea dimora o domicilio, oltre che ad indicare i recapiti telefonici o gli indirizzi di posta elettronica nella sua disponibilità" (analogamente dispone l'art. 161 c.p.p. rispetto al difensore). Si legge nella relazione introduttiva al d.lgs. n. 150 del 2022 che tale indicazione è conforme alla delega che imponeva di prevedere che, ai soli fini del rintraccio o delle comunicazioni di cortesia, il destinatario possa fornire anche un semplice indirizzo di posta elettronica, non certificato (appunto, un mero recapito digitale).

appositamente eletto per la ricezione delle notificazioni delle pubbliche amministrazioni effettuate tramite piattaforma, di cui all'articolo 26, comma 5, lettera *c*), del decreto-legge [n.d.r. n. 76 del 2020].

Tali definizioni, che tradiscono l'intento di "sistematizzare" la disciplina risultano già armonizzate con il CAD, e possono costituire il punto di partenza dello studio dell'istituto anche rispetto agli aspetti processuali, in ragione del valore generale delle norme del CAD per i processi telematici.

Ed infatti, come si vedrà nelle pagine che seguono, le tre tipologie di domicilio risultano già recepite ed esistenti nel settore della giustizia ordinaria, civile e penale.

1.3.1. *L'art. 3*-bis *del CAD ed i soggetti obbligati al domicilio digitale*

Il citato art. 3-*bis* del Codice dell'Amministrazione Digitale, oltre a predicare il diritto per tutti all'accesso ai Servizi Online (tramite l'identità digitale dell'individuo o tramite un punto di accesso telematico specificato nell'articolo 64-*bis*), stabilisce l'obbligo di Domicilio Digitale per alcuni soggetti specifici, indicati nell'articolo 2, comma 2 (professionisti registrati in elenchi ufficiali, soggetti iscritti nel registro delle imprese, pubbliche amministrazioni). La norma rimanda agli elenchi indicati negli articoli 6-*bis* o 6-*ter*.

Per tutti gli altri soggetti, il domicilio digitale è solo facoltativo, come domicilio generale. In particolare, le persone fisiche hanno la facoltà di eleggere o modificare il Domicilio Digitale che verrà registrato nell'elenco dell'articolo 6-*quater*. Se un domicilio eletto non è più attivo, viene automaticamente cancellato da tale elenco seguendo le procedure stabilite nelle Linee guida.

La norma prosegue dettando una serie di indicazioni sulle modalità di scelta e gestione dei domicili digitali e sui doveri cui i titolari sono tenuti.

I domicili digitali devono essere scelti seguendo le procedure descritte nelle Linee guida. Le persone fisiche possono anche selezionare il proprio domicilio digitale utilizzando il servizio dell'articolo 64-*bis*, quello fornito online dall'Anagrafe nazionale della popolazione residente (ANPR), o recandosi personalmente all'ufficio anagrafe del proprio comune di residenza.

Chi possiede un domicilio digitale è tenuto a utilizzarlo con attenzione e deve comunicare eventuali cambiamenti dello stesso secondo le modalità descritte nelle Linee guida. Le medesime stabiliscono anche come gestire e aggiornare l'elenco dei domicili digitali, regolando pure i i casi in cui il proprietario del domicilio digitale sia deceduto o non possa più utilizzarlo.

Sempre nell'art. 3-*bis* si legge del Domicilio Digitale speciale, che è un domicilio elettivo scelto specificamente per certi atti o procedimenti. Il soggetto che lo sceglie non può sollevare obiezioni riguardo alla forma o alla

data di spedizione e ricezione delle comunicazioni o notificazioni inoltrate a tale domicilio. Come vedremo, di questa forma di domicilio, sia il processo civile che quello penale conoscono delle specifiche applicazioni.

1.3.2. *L'identità e il domicilio digitali tra diritto, dovere e facoltà*

Come accennato, il CAD per espressa disposizione dell'art. 2 si applica anche ai rapporti tra privati, quanto alle disposizioni e linee guida riguardanti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-*bis* e al Capo IV, l'identità digitale di cui agli articoli 3-*bis* e 64.

Rispetto ai privati, peraltro, gli istituti in esame, sono concepiti sia come un diritto che come una facoltà.

In particolare, nei confronti della PA, l'identità e il domicilio digitale sono un diritto.

Ed infatti l'art. 2 (intitolato diritto all'uso delle tecnologie, in vigore dal 27 gennaio 2018) prevede al comma 1-*quinquies* che "Tutti i cittadini e le imprese hanno il diritto all'assegnazione di un'identità digitale attraverso la quale accedere e utilizzare i servizi erogati in rete dai soggetti di cui all'articolo 2, comma 2, alle condizioni di cui all'articolo 64".

E il successivo comma 1-*sexies* stabilisce che "Tutti gli iscritti all'Anagrafe nazionale della popolazione residente (ANPR) hanno il diritto di essere identificati dalle pubbliche amministrazioni tramite l'identità digitale di cui al comma 1-*quinquies*, nonché di inviare comunicazioni e documenti alle pubbliche amministrazioni e di riceverne dalle stesse tramite un domicilio digitale, alle condizioni di cui all'articolo 3-*bis*".

Di particolare importanza l'art. 3-*bis* del CAD, intitolato: Identità digitale e Domicilio digitale, in vigore dal 30 giugno 2022.

Tale norma invero, stabilisce che "chiunque ha il diritto di accedere ai servizi on-line offerti dai soggetti di cui all'articolo 2, comma 2, tramite la propria identità digitale (*omissis*)" ma poi precisa subito che per determinate categorie di soggetti l'identità digitale è obbligatoria (costituisce quindi un dovere).

Si tratta di tutti i soggetti pubblici (ossia le Pubbliche amministrazioni in senso stretto, i gestori di servizi pubblici le società a controllo pubblico, di cui all'art. 2 del CAD), dei professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese. Costoro hanno l'obbligo di dotarsi anche di un domicilio digitale iscritto nell'elenco di cui agli articoli 6-*bis* (Indice nazionale dei domicili digitali delle imprese e dei professionisti INIPEC) o 6-*ter* (Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi IPA).

Per i soggetti non obbligati, pertanto, nel quadro attuale, dotarsi di un domicilio digitale resta una facoltà, che si può esercitare eleggendo domicilio digitale nell'elenco di cui all'articolo 6-*quater* (l'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese; INAD) (21).

Che si tratti di un cammino in evoluzione volto a superare il cd. "divario digitale", lo si evince chiaramente dall'art. 3-*bis* che demanda ad un decreto del Presidente del Consiglio dei ministri o del Ministro delegato per la semplificazione e la pubblica amministrazione, sentiti l'AgID e il Garante per la protezione dei dati personali e acquisito il parere della Conferenza unificata, di stabilire la data a decorrere dalla quale le comunicazioni tra le pubbliche amministrazioni e i cittadini non forniti di domicilio digitale avvengono esclusivamente in forma elettronica. Si prevede, in sostanza, che sia attribuito a questi soggetti direttamente dallo stato un domicilio digitale o siano studiate modalità per poter effettuare a loro la consegna e consentire loro la consultazione di documenti digitali.

In particolare, l'articolo 6-*quater*, comma 2 del CAD prevede che il domicilio digitale dei professionisti iscritti nell'INI-PEC sia inserito anche nell'INAD quale domicilio digitale in qualità di persone fisiche, fermo restando il diritto di eleggerne uno diverso o di cancellarlo.

Ed infatti anche a tali professionisti, che ai sensi della norma citata, si trovano automaticamente iscritti nell'INAD, anche come privati cittadini, deve essere garantita (tramite non solo la sostituzione ma la cancellazione dell'indirizzo professionale da tale elenco) la possibilità di non figurare nell'elenco come, almeno per il momento, possibile per tutti i privati).

La relativa previsione è contemplata nelle linee guida aggiornate, rilasciate dall'AgID, in relazione a tale elenco (22).

---

(21) È previsto che le persone fisiche possano altresì eleggere il domicilio digitale avvalendosi del servizio di cui all'articolo 64-*bis*, di quello reso disponibile on-line dall'Anagrafe nazionale della popolazione residente (ANPR) di cui all'articolo 62, ovvero recandosi presso l'ufficio anagrafe del proprio comune di residenza.

(22) Si legge nelle linee guida pubblicate dall'AgID, al paragrafo 3, che, qualora, entro 30 giorni dall'inserimento provvisorio di cui al precedente punto 2, il professionista non abbia usufruito della propria facoltà di modifica del domicilio digitale trasmesso dall'INI-PEC, il Gestore INAD provvede alla pubblicazione di quanto al richiamato punto 2. Qualora il professionista abbia optato per la modifica del domicilio digitale, al fine di eleggerne uno personale in INAD diverso da quello presente in INI-PEC, il Gestore INAD procede alla cancellazione del domicilio digitale inizialmente Linee Guida dell'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese Versione 2.1

1.4. Il quadro europeo (cenni)

Il domicilio digitale, dunque è, per esplicita previsione dell'art. 1 lett. *n-ter*) del d.lgs. 7 marzo 2005, n. 82 (codice dell'amministrazione digitale di qui in poi, semplicemente il CAD), l'unico utilizzabile e valido per comunicazioni elettroniche a valore legale (v. *infra*).

Eppure, non si può dire che il perimetro normativo dell'istituto sia netto, poiché risulta da mille rivoli normativi e risente, per molti versi, dell'evoluzione ancora incompiuta del "fenomeno" della digitalizzazione. Un cammino ancora incompleto, proprio perché, come visto, il domicilio digitale è obbligatorio per alcune categorie di soggetti, ma non per altri, cosicché la possibilità di gestire comunicazioni, servizi, traffici in maniera completamente digitale è direttamente proporzionale alla diffusione delle identità e dei domicili digitali e — pertanto — esclusa in determinate situazioni.

Ma questo stato di cose, che si è protratto per anni, è destinato ad un cambiamento in tempi brevi. Il momento storico che viviamo, infatti, rispetto al passato, mostra una maturazione generale e multilivello di tecnologie e consapevolezze, soprattutto sul piano europeo.

Del resto, proprio su tale versante, il concetto di domicilio e identità digitali sono oggetto di nuove regole, la cui pubblicazione è attesa tra pochi mesi: si tratta dell'aggiornamento del più volte citato Regolamento eIDAS), frutto di una consultazione avviata dall'UE nel 2020 ([23]). Il suo testo è ancora riservato e pure, da quanto già annunziato dalle autorità europee, è noto che verrà ampliata e semplificata la possibilità per i comuni cittadini di dotarsi di una identità digitale, utilizzabile in tutta l'UE, e profilabile in relazione all'utilizzo che se ne debba fare (con il cd. EU-Wallet un portafoglio di identità digitali).

Scopo del regolamento, infatti, è garantire "che le persone e le imprese possano utilizzare i propri sistemi nazionali di identificazione elettronica (eID) per accedere ai servizi pubblici disponibili online in altri paesi dell'UE, creare un mercato interno europeo dei servizi fiduciari garantendo che essi funzionino a livello transfrontaliero e abbiano lo stesso status giuridico dei loro equivalenti cartacei tradizionali."

Il portafoglio europeo di identità digitale (EDIW) dovrebbe sostenere la mobilità transfrontaliera dei cittadini e delle imprese in tutta l'Unione e

---

- 8 agosto 2023, pag. 14 di 16 trasmesso dall'INI-PEC e alla pubblicazione del domicilio scelto. Successivamente alla pubblicazione, qualora il professionista opti per la cessazione del domicilio digitale in INAD, il Gestore procede alla cessazione del domicilio digitale inizialmente trasmesso dall'INI-PEC o di quello modificato, nei modi indicati dal paragrafo 2.3.1.

([23]) https://digital-strategy.ec.europa.eu/en/news/digital-identity-and-trust-commission-launches-public-consultation.

promuovere lo sviluppo di servizi di e-government interoperabili in tutta l'Unione.

Ma gli interventi normativi europei non sono isolati, poiché la Commissione Europea ha intrapreso un vero e proprio programma strategico per il decennio digitale, già dal 2021, stabilendo interventi legislativi e concrete attività a pioggia fino al 2030, così da indirizzare la trasformazione digitale dell'Europa.

Si parla di una vera e propria "onda" di digitalizzazione che impone agli interpreti uno sforzo di ricostruzione e razionalizzazione con la normativa interna.

Proprio mentre questo studio viene alla luce, per esempio, è pubblicato il Regolamento (UE) 2023/2844, che mira a modernizzare e digitalizzare la cooperazione giudiziaria e l'accesso alla giustizia in materia civile, commerciale e penale a livello transfrontaliero nell'Unione Europea e segue il principio del "digitale per *default*" ([24]), ovvero l'idea che la digitalizzazione debba essere l'opzione standard nelle comunicazioni giudiziarie transfrontaliere (e anche interne), auspicando che ciò agevoli l'accesso alla giustizia, la sua efficienza, e la tutela dei diritti.

Tale ultimo regolamento richiama più volte, regolando i flussi telematici e le udienze a distanza, le regole dettate dal già citato regolamento (UE) n. 910/2014, cd. eIDAS, e gli strumenti utilizzati per l'identificazione elettronica dell'utente al livello di garanzia elevato quale precisato all'articolo 8, paragrafo 2, lettera *c*), del medesimo regolamento nonché il periodo di conservazione delle informazioni e dei documenti.

1.5. Altri dati normativi nazionali che contemplano il domicilio digitale (cenni)

Se è il CAD il punto di riferimento principale occorre evidenziare l'adeguamento di altri importanti corpi normativi, in un percorso, ancora in itinere, che dovrebbe consentire l'accesso ai servizi pubblici e la comunicazione tra pA e privati, oltre che tra privati, attraverso strumenti digitali.

Nonostante per il cittadino il domicilio digitale, come detto, non sia obbligatorio, sono intervenute modifiche nel Decreto del Presidente della Repubblica del 30 maggio 1989, n. 223, recante il REGOLAMENTO anagrafico della popolazione residente. L'art. 20 stabilisce che a "*ciascuna persona residente nel comune deve essere intestata una scheda individuale*"

([24]) L'espressione si legge nel primo considerando della direttiva (UE) 2023/2843 del parlamento europeo e del consiglio del 13 dicembre 2023, sulla digitalizzazione della cooperazione giudiziaria.

sulla quale devono essere obbligatoriamente indicati "t*ra tutti gli attributi che identificano la persona (come il cognome, il nome, il sesso, la data e il luogo di nascita, il codice fiscale, la cittadinanza, l'indirizzo dell'abitazione etc.) anche gli estremi della carta d'identità e il domicilio digitale*" (comma così modificato dall'articolo 3, comma 1, lettera *c*), punto 1), del d.lgs. 19 gennaio 2017, n. 5).

Adeguamenti sono poi intervenuti in altri corpi normativi, come la legge 7 agosto 1990, n. 241 sulla Trasparenza atti amministrativi) che stabilisce, a proposito del responsabile del procedimento, che a chiunque vi abbia interesse o faccia accesso sono comunicati tra gli altri dati, il domicilio digitale del responsabile del procedimento.

La norma generale che disciplina i concorsi pubblici, poi, Decreto del Presidente della Repubblica 9 maggio 1994, n. 487 (in Suppl. ordinario alla G.U., 9 agosto, n. 185). - Regolamento recante norme sull'accesso agli impieghi nelle pubbliche amministrazioni e le modalità di svolgimento dei concorsi, dei concorsi unici e delle altre forme di assunzione nei pubblici impieghi, recentemente integrata, prevede all'art. 1 che alle procedure di concorso si partecipa esclusivamente previa registrazione nel Portale unico del reclutamento di cui all'art. 35-*ter* del decreto legislativo del 30 marzo 2001, n. 165, G.U. 9 maggio 2001, n. 106 cui si accede attraverso le forme accreditate di identità digitali.

II.

LE TIPOLOGIE DI DOMICILIO DIGITALE IN TERMINI GENERALI E IL LORO RECEPIMENTO NELLE NORME PROCESSUALI

di *Antonella Ciriello*

2.1. Le tipologie di domicilio digitale in termini generali e il loro recepimento nelle norme processuali

Anche sul piano processuale, limitando per ora l'indagine al solo processo ordinario (civile e penale), risultano individuabili i concetti generali sopra declinati (ancora in evoluzione per effetto della nuova normativa in corso di introduzione (cd. Decreto correttivo), ai sensi dell'articolo 1, comma 3, della legge 26 novembre 2021, n. 206 [1].

Le norme processuali specificamente dettate in materia di digitale, che assumono un connotato di specialità, come visto, in relazione al disposto dell'art. 2 comma 6 del CAD, regolano il domicilio digitale generale, e prevedono già a certi fini anche la figura del domicilio digitale speciale (sistematizzata ed estesa con il correttivo in corso di emanazione), oltre che una forma di domicilio digitale di piattaforma.

In particolare, sia pure solo per la comunicazione e la notifica, va segnalato l'art. 16-*ter* del d.l. n. 179 del 2012 che, occupandosi del domicilio generale a tali fini, richiama i pubblici elenchi generali del CAD (come visto INIPEC, IPA e INAD), per aggiungervi ulteriori elenchi specifici, quali il registro delle PA e il ReGIndE, gestiti dal Ministero della Giustizia [2].

---

[1] È attualmente all'esame della Camera il testo del decreto legislativo concernente disposizioni integrative e correttive al decreto legislativo 10 ottobre 2022, n. 149, recante attuazione della legge 26 novembre 2021, n. 206, leggibile sul sito istituzionale https://temi.camera.it/leg19/dossier/OCD18-19766/disposizioni-integrative-e-correttive-al-d-lgs-149-2022-riforma-del-processo-civile.html

[2] L'art. 16-*ter* è una norma centrale anche per la giustizia amministrativa e così dispone: 1. Pubblici elenchi per notificazioni e comunicazioni ". A decorrere dal 15 dicembre 2013, ai fini della notificazione e comunicazione degli atti in materia civile, penale, amministrativa, contabile e stragiudiziale si intendono per pubblici elenchi quelli previsti dagli articoli 6-*bis*, 6-*quater* e 62 del decreto legislativo 7 marzo 2005, n. 82, dall'articolo 16, comma 12, del

L'iscrizione a tali elenchi, così come a quelli generali del CAD, per i soggetti che sono obbligati, o che esercitino una facoltà, conduce a parere di chi scrive, come già accennato — in maniera indiretta a ritenere la conformità di tali indirizzi PEC alla normativa eIDAS (per il tramite cioè della specifica normativa che consente il popolamento di tali elenchi previa identificazione del titolare) (3).

Accanto a tali forme di domicilio digitale generale, poi, sia il processo civile che quello penale attribuiscono rilevanza al domicilio digitale speciale (considerato, come visto, dall'art. 3-*bis*, comma 4-*quinquies* e art. 65 del CAD, nonché, tra gli altri, dall'art. 1 lett. *h*), del Decreto della Presidenza del Consiglio dei Ministri - Dipartimento Per La Trasformazione Digitale 8 febbraio 2022, n. 58).

In particolare, tale domicilio rileva, a titolo esemplificativo, nella comunicazione telematica civile, in ragione delle previsioni dell'art. 16, comma 7, d.l. n. 179 del 2012, che, nello stabilire come "*Nei procedimenti civili nei quali sta in giudizio personalmente la parte il cui indirizzo di posta elettronica certificata non risulta da pubblici elenchi, può indicare l'indirizzo di posta elettronica cer-*

---

presente decreto, dall'articolo 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, convertito con modificazioni dalla legge 28 gennaio 2009, n. 2, nonché il registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia.

1-*bis*. Le disposizioni dei commi 1 e 1-*ter* si applicano anche alla giustizia amministrativa. -1-*ter*. Fermo restando quanto previsto dal regio decreto 30 ottobre 1933, n. 1611, in materia di rappresentanza e difesa in giudizio dello Stato, in caso di mancata indicazione nell'elenco di cui all'articolo 16, comma 12, la notificazione alle pubbliche amministrazioni degli atti in materia civile, penale, amministrativa, contabile e stragiudiziale è validamente effettuata, a tutti gli effetti, al domicilio digitale indicato nell'elenco previsto dall'articolo 6-ter del decreto legislativo 7 marzo 2005, n. 82, e, ove nel predetto elenco risultino indicati, per la stessa amministrazione pubblica, più domicili digitali, la notificazione è effettuata presso l'indirizzo di posta elettronica certificata primario indicato, secondo le previsioni delle Linee guida di AgID, nella sezione ente dell'amministrazione pubblica destinataria. Nel caso in cui sussista l'obbligo di notifica degli atti introduttivi di giudizio in relazione a specifiche materie presso organi o articolazioni, anche territoriali, delle pubbliche amministrazioni, la notificazione può essere eseguita all'indirizzo di posta elettronica certificata espressamente indicato nell'elenco di cui all'articolo 6-*ter* del decreto legislativo 7 marzo 2005, n. 82, per detti organi o articolazioni.

(3) In linea con tale disciplina l'art. articolo 16-*sexies*, l. n. 179 del 2012 Domicilio digitale (come mod. da decreto legislativo del 10 ottobre 2022, n. 149) che prevede: "*Salvo quanto previsto dall'articolo 366 del codice di procedura civile, che prevede come, quando la legge prevede che le notificazioni degli atti in materia civile al difensore siano eseguite, ad istanza di parte, presso la cancelleria dell'ufficio giudiziario, alla notificazione con le predette modalità può procedersi esclusivamente quando non sia possibile, per causa imputabile al destinatario, la notificazione presso l'indirizzo di posta elettronica certificata, risultante dagli elenchi di cui all' articolo 6-bis6del decreto legislativo 7 marzo 2005, n. 82, nonché dal registro generale degli indirizzi elettronici, gestito dal ministero della giustizia".*

tificata al quale vuole ricevere le comunicazioni e notificazioni relative al procedimento. In tale caso le comunicazioni e notificazioni a cura della cancelleria, si effettuano ai sensi del comma 4 e si applicano i commi 6 e 8".

Questa ricostruzione, come accennato, risulta sistematizzata dall'intervento normativo in corso di approvazione, che contiene numerose disposizioni che introducono la facoltà delle parti di indicare, in luogo della residenza o dell'elezione di domicilio, l'indirizzo di posta elettronica certificata (PEC) risultante da pubblici elenchi o di eleggere un domicilio digitale speciale (4).

Sul versante penale, per il domicilio digitale speciale, analoga disposizione risulta introdotta dall'art. 16 cit. comma 7-*bis*, con gli opportuni adattamenti richiesti in quel contesto per la notifica all'imputato. La specificazione di tale disciplina si rinviene, nel codice di rito (sempre quale forma di domicilio digitale speciale) nell'articolo 161 c.p.p.: comma 1, in base al quale "*Il giudice, il pubblico ministero o la polizia giudiziaria, nel primo atto compiuto con l'intervento della persona sottoposta alle indagini o dell'imputato non detenuti o internati, li invitano a dichiarare uno dei luoghi indicati nell'articolo 157, comma 1, o un indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato, ovvero a eleggere domicilio per le notificazioni dell'avviso di fissazione dell'udienza preliminare, degli atti di citazione in giudizio ai sensi degli articoli 450, comma 2, 456, 552 e 601, nonché del decreto penale di condanna. Contestualmente la persona sottoposta alle indagini o l'imputato sono avvertiti che hanno l'obbligo di comunicare ogni mutamento del domicilio dichiarato o eletto e che in mancanza di tale comunicazione o nel caso di rifiuto di dichiarare o eleggere domicilio, nonché nel caso in cui il domicilio sia o divenga inidoneo, le notificazioni degli atti indicati verranno eseguite mediante consegna al difensore, già nominato o che è contestualmente nominato, anche d'ufficio. comma 1*-bis. *Della dichiarazione o della elezione di domicilio, ovvero del rifiuto di compierla, nonché degli avvertimenti indicati nei commi 1 e 2, è fatta menzione nel verbale*".

Altro esempio di domicilio digitale, speciale, con la caratteristica ulteriore di essere fornito dall'amministrazione a privati, è contemplato dal Codice della crisi di impresa, con l'art. 199 del decreto legislativo 12 gennaio 2019, n. 14 (intitolato Fascicolo della procedura) che stabilisce come "Con la pubblicazione della sentenza di liquidazione giudiziale viene assegnato il domicilio digitale e viene formato il fascicolo informatico della procedura, nel quale devono essere contenuti tutti gli atti, i provvedimenti e i ricorsi attinenti al procedimento, opportunamente suddivisi in sezioni, esclusi quelli

(4) *Loc. cit.* (si vedano in particolare, i comma 2, lett. *c*), n. 2; comma 5, lett. *d*); comma 7, lett. *c*); comma 8, lett. *b*), *g*), n. 1, *o*), *p*), *q*), *z*), n. 2).

che, per ragioni di riservatezza, debbono essere custoditi nel fascicolo riservato" (...*omissis*).

Si può ritenere che anche una sorta di domicilio di piattaforma sia prevista nella recente normativa introdotta dal decreto-legge 24 febbraio 2023, n. 13, che all'art. 36 disciplina il deposito telematico nei procedimenti di volontaria giurisdizione su un apposito portale direttamente da parte delle persone fisiche che (in tali procedimenti) possono stare in giudizio personalmente.

Il secondo comma prevede, infatti che, "Quando si avvale del portale di cui al comma 1 per il deposito in modalità telematiche di atti processuali e documenti, la parte il cui indirizzo di posta elettronica certificata non risulta da pubblici elenchi può altresì manifestare la volontà di ricevere le comunicazioni e notificazioni relative al procedimento, ai fini e per gli effetti di cui all'articolo 16, comma 7, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, tramite il portale stesso (v. *infra* domicilio digitale nella volontaria giurisdizione).

Invece, quanto ai sistemi di deposito, tramite upload, viene in evidenza il concetto di identità e identificazione digitale.

Per esempio, con riguardo al PDP (portale dei depositi telematici) l'identificazione informatica dei difensori per l'accesso all'Area Riservata avviene mediante SPID o Smart Card, anche se i difensori abilitati sono gli avvocati iscritti al ReGinDE (5).

Del pari, per il tribunale on line, l'accesso avviene per i cittadini interessati tramite SPID (6).

---

(5) Stabiliscono poi le specifiche tecniche del PPT; https://pst.giustizia.it/PST/resources/cms/documents/SPECifiche_Tecniche_PPT_11.07.2023_post_DM_2023_signed.pdf, dettate con Provvedimento del Direttore Generale dei sistemi Informativi Automatizzati del 11 luglio 2023, relative al deposito con modalità telematica degli atti individuati dall'articolo 1 del Decreto del Ministro della Giustizia del 4 luglio 2023 Portale deposito atti penali. *L'accesso al PDP è consentito unicamente ai soggetti iscritti nel ReGIndE con ruolo avvocato, praticante abilitato, nonché avvocato ente pubblico e funzionario ente pubblico, questi ultimi limitatamente agli appartenenti all'Avvocatura dello Stato.*

(6) (https://smart.giustizia.it/to?id=to_faq_01&kb_category=d0a6445087ca35502a1e20ee8bbb3522. Gli istanti, poi, possono acquisire o consultare la documentazione richiesta nell'area riservata.

III.

RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE E IDENTITÀ E DOMICILIO DIGITALI

di *Nicola Bardino*

Sommario: 3.1. La trasformazione degli apparati amministrativi a seguito dell'introduzione delle tecnologie digitali. — 3.2. L'attività amministrativa digitalizzata come modulo procedimentale. — 3.3. *Segue*: la digitalizzazione e l'assetto organizzativo. — 3.4. L'identità digitale come correlato necessario dell'innovazione tecnologico-organizzativa dell'Amministrazione e come proiezione della cittadinanza amministrativa dell'individuo. Cenni sull'identità digitale pubblica nella prospettiva europea. — 3.5. *Segue*: il domicilio digitale e i canali di comunicazione telematici con la pubblica amministrazione (cenni).

3.1. La trasformazione degli apparati amministrativi a seguito dell'introduzione delle tecnologie digitali

L'innovazione che negli ultimi decenni ha attraversato l'Amministrazione pubblica, manifestatasi sotto il profilo culturale a partire dalle riforme degli Anni '90, e materiale grazie all'apporto delle tecnologie informatiche, si è sin qui innestata su un quadro organizzativo concreto pressoché immutato, plasmato assecondando le molteplici declinazioni dei tradizionali principi di buon andamento e imparzialità (art. 97, 2° comma, Cost.), e strutturato in senso verticale e orizzontale, in accordo con principi, di matrice europea, di sussidiarietà, differenziazione e adeguatezza (art. 118, 1° comma, Cost.).

Il Codice dell'Amministrazione Digitale (d.lgs. 7 marzo 2005, n. 82, in seguito anche CAD) all'interno di questa cornice ha operato la trasposizione dei principi di economicità, imparzialità, pubblicità e trasparenza portati dall'art. 1 della legge sul procedimento amministrativo (l. 7 agosto 1990, n. 241), all'ambito della tecnologia applicata allo svolgimento dell'attività amministrativa

Si è autorevolmente constatato che, con l'introduzione di questi principi, le riforme degli Anni '90, a partire dalla citata legge sul procedimento

amministrativo, avevano "*inteso cambiare le amministrazioni in astratto*" (1) senza però incidere sulla loro operatività materiale e, in definitiva, sull'organizzazione dei poteri pubblici. La progressiva trasposizione tecnologica dei medesimi principi, mediata dal CAD, anche grazie alle modifiche normative di cui si darà cenno nel prosieguo, è divenuta negli ultimi anni il principale fattore di innovazione capace di intervenire sull'organizzazione concreta dell'Amministrazione.

A giustificazione e chiarimento di questo recente fenomeno, è significativo osservare che l'innovazione tecnologica tende in effetti a plasmare le coordinate dello spazio giuridico entro cui si svolge tradizionalmente la cura degli interessi pubblici, rispetto ai quali il CAD ha promosso l'impiego di strumenti informatici via via più sofisticati, armonizzati con i principi del procedimento, così da trasformare lo sviluppo digitale in una caratteristica intrinseca del potere pubblico (2).

L'Amministrazione è giunta, quindi, ad acquisire una dimensione organizzativa digitale, all'interno della quale emerge una modalità (alternativa e, in certi casi, esclusiva) di eseguire prestazioni potenziate da automatismi e da canali di comunicazione elettronici, basati su procedure di acquisizione e manipolazione dei dati sempre più sofisticate (si pensi all'impiego della c.d. intelligenza artificiale).

Lo scenario nel quale si situa la trasformazione dell'Amministrazione corrisponde ad una ancor più significativa e persino inattesa declinazione del potere pubblico e dello Stato, qualificato ora come digitale, ossia inteso come "*Stato che regola i processi di digitalizzazione, sia come Stato che digitalizza se stesso*" (3), in modo da definire una generale proiezione dell'ordinamento verso la sfera digitale e una corrispondente costruzione dello Stato digitale, intesa come dimensione in cui si esplicano i tradizionali poteri (in particolare il potere giudiziario e quello amministrativo).

Entrambe le accezioni preludono ad un riassetto organizzativo le cui linee di sviluppo procedono di pari passo con la ridefinizione delle regole (non solo tecniche) di esercizio dei poteri pubblici e delle relative modalità di controllo (4).

Nella sfera dell'Amministrazione pubblica, una testimonianza di tale riassetto e dei riflessi che esso produce sull'attività e sugli apparati, può essere

---

(1) R. Cavallo Perin-D.U. Galetta (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino 2020, XIX.

(2) L. Torchia, *Lo Stato digitale*, Bologna, 2023, 17.

(3) V. Bontempi, in Aa.Vv., *Lo Stato digitale nel piano nazionale di ripresa e resilienza*, Roma, 2022, 18.

(4) L. Torchia, *Lo Stato digitale*, cit., p. 18.

rinvenuta a partire da interventi normativi tutto sommato datati. Si pensi, al riguardo all'art. 1, comma 162, l. 27 dicembre 2006, n. 296, che, obbedendo ad un'evidente logica semplificatrice, ha consentito di sostituire con una firma a stampa la sottoscrizione autografa del funzionario responsabile apposta sugli avvisi di accertamento dei tributi locali o regionali (5), quando gli atti impositivi siano stati interamente elaborati mediante sistemi informatici. In tale evenienza, il nominativo del funzionario istruttore e le fonti da cui sono desunti i dati oggetto di elaborazione devono essere individuati in un apposito atto dirigenziale, e indicati nel provvedimento impositivo (6).

In questa fattispecie si coglie, pur a un livello embrionale, l'interconnessione tra i principali aspetti ancor oggi coinvolti dallo svolgimento dell'attività amministrativa mediante gli strumenti informatici.

Il potere si manifesta attraverso una procedura che culmina nell'emissione di una decisione finale automatizzata che a sua volta presuppone la compresenza di due indefettibili contrappesi: il primo è dato dal doveroso esercizio della funzione organizzatrice (consistente, in questo caso, nell'individuazione formale del funzionario responsabile), il cui scopo consiste nel permettere l'imputazione del provvedimento assunto in forma di decisione automatizzata, come tale privo della sottoscrizione autografa, all'organo che per *fictio iuris* ne assume la paternità per conto dell'Amministrazione, consentendo ai suoi effetti costitutivi di manifestarsi nel mondo giuridico; il secondo riguarda la trasparenza della decisione, la quale si realizza mediante l'indicazione dei dati oggetto di elaborazione, così da garantire l'effettività del controllo e la pienezza del diritto di difesa da parte del destinatario finale.

3.2. L'attività amministrativa digitalizzata come modulo procedimentale

Negli ultimi anni, gli approfondimenti della giurisprudenza amministrativa si sono concentrati attorno ad alcune tra le principali questioni poste dalla crescente diffusione delle decisioni automatizzate. Pronunciandosi sul tema dell'ammissibilità dell'utilizzo di metodi algoritmici all'interno del procedimento amministrativo, il Consiglio di Stato ne ha inquadrato l'impiego come "*modulo organizzativo*", ossia come "*strumento procedimentale ed istruttorio, soggetto alle verifiche tipiche di ogni procedimento amministrativo, il quale resta il* modus operandi *della scelta autoritativa, da svolgersi sulla scorta delle legislazione attributiva del potere e delle finalità dalla stessa attribuite all'organo pubblico*".

Muovendo da tale piano concettuale, ossia dall'identificazione dell'automatismo algoritmico come una delle plausibili modalità di formazione del

(5) V. art. 3, d.lgs. n. 12 febbraio 1993, n. 39.

(6) V. Cass., Sez. VI, 29 dicembre 2012, n. 29820.

contenuto della decisione amministrativa, questa stessa giurisprudenza ha quindi soffermato l'attenzione sulla "*necessità che la 'formula tecnica', che di fatto rappresenta l'algoritmo, sia corredata da spiegazioni che la traducano nella 'regola giuridica' ad essa sottesa e che la rendano leggibile e comprensibile*" (7), ponendo così l'accento su quell'esigenza di trasparenza — finalisticamente orientata a garantire il controllo sull'attività amministrativa — che era già rinvenibile a partire dalle prime forme di regolazione degli automatismi provvedimentali sottesi alle cosiddette *decisioni robotiche* (8).

3.3. *Segue*: la digitalizzazione e l'assetto organizzativo

Ricondurre l'utilizzo degli strumenti informatici al campo del procedimento amministrativo e ai suoi principi, contribuisce all'edificazione di un modello generale di svolgimento dei poteri pubblici contraddistinto dall'applicazione di regole trasparenti e verificabili, come tale ritenuto ammissibile proprio perché pienamente suscettibile di controllo (9).

Vi è, poi, un ulteriore aspetto inevitabilmente sotteso all'appropriazione da parte dell'ordinamento e dei poteri pubblici del territorio digitale. Questo salto dimensionale richiede l'istituzione e l'organizzazione di un canale di comunicazione e di accesso tra il cittadino e l'apparato pubblico, necessario per garantire il rafforzamento dell'uso di apparati e procedure informatiche nel procedimento amministrativo, dando prosecuzione attuativa al principio generale, oggi riconducibile all'art. 12, d.l. 16 luglio 2020, n. 76, (c.d. *decreto semplificazioni*), secondo il quale la Amministrazioni pubbliche agiscono mediante strumenti informatici e telematici, e sono obbligate a comunicare ai soggetti interessati il domicilio digitale del responsabile del procedimento. (comma 1, lett. *b*), *c*) e *d*)).

Non può sfuggire come, intervenendo sul versante organizzativo, la disposizione in esame imponga all'Amministrazione di assolvere un onere aggiuntivo rispetto all'identificazione del responsabile del procedimento nel contesto di atti esternati in forma cartacea benché redatti con modalità informatizzate.

---

(7) Cons. Stato, Sez. VI, 13 dicembre 2019, n. 8472.

(8) F. Patroni Griffi, *La decisione robotica e il giudice amministrativo*, in *www.giustizia-amministrativa.it*, sezione Studi e approfondimenti, 28 agosto 2018, 4-5, intervento al convegno sulla Decisione robotica, organizzato nell'ambito dei "Seminari Leibniz per la teoria e la logica del diritto", svoltosi a Roma il 5 luglio 2018 (ora pubblicato in A. Carleo (a cura di), *Decisione robotica*, Bologna, 2019.

(9) Anche se con esso, tuttavia, sul giudice verrebbe scaricato quel "*ruolo di 'mediazione' degli interessi, di valutazione e talvolta di accertamento del fatto*" il quale, a ben guardare, costituisce il nucleo essenziale della discrezionalità amministrativa (v. F. Patroni Griffi, *op. cit*.).

Il decreto semplificazioni richiede infatti all'Amministrazione di manifestarsi verso l'esterno in forma digitale, attraverso la predisposizione di un percorso diretto di comunicazione tra gli interessati al provvedimento finale e il responsabile del procedimento. Questi, a tal fine, è dunque tenuto ad assumere un domicilio digitale (10), vale a dire un indirizzo elettronico presso un servizio di posta elettronica certificata ovvero un servizio elettronico di recapito certificato, come tuttora definito dal Regolamento UE n. 910/2014 (eIDAS).

Si tratta di un passaggio significativo e ineludibile, per il cui tramite, da un lato, trova trasposizione e, nel contempo, amplificazione (11) la facoltà di partecipazione al procedimento amministrativo da parte dell'interessato (artt. 7, 8 e 10-*bis*, l. n. 241 del 1990). Dall'altro, emerge un connesso profilo organizzativo: attraverso l'assunzione di un domicilio digitale (o di un equivalente servizio elettronico di recapito beneficiario di certificazione eIDAS), sono le singole unità organizzative, immedesimate nel responsabile del procedimento, a operare nello spazio digitale e a manifestarsi all'interno di esso come articolazioni dell'Amministrazione.

In questo senso e in conclusione, l'attribuzione obbligatoria di un domicilio digitale al responsabile del procedimento e all'unità organizzativa competente rappresenta così, oltre ad uno strumento di partecipazione interno al procedimento stesso, un criterio giuridico di imputazione delle informazioni e dell'attività all'Amministrazione.

3.4. L'identità digitale come correlato necessario dell'innovazione tecnologico-organizzativa dell'Amministrazione e come proiezione della cittadinanza amministrativa dell'individuo. Cenni sull'identità digitale pubblica nella prospettiva europea

A tale espansione dell'organizzazione amministrativa nello spazio digitale, attraverso la rete *internet*, corrisponde la costruzione giuridica di un'identità digitale degli amministrati, intesa come declinazione della soggettività indispensabile per conferire l'accesso ai canali di comunicazione e di informazione degli apparati burocratici. L'identificazione digitale del cittadino opera come un'estensione originaria della soggettività giuridica, funzio-

(10) Incluso nell'indice previsto dall'art. 6-*ter* del CAD.

(11) Le facoltà partecipative trovano poi ulteriore ampliamento e consacrazione nell'art. 7, comma 1, del CAD, secondo cui "*chiunque ha diritto di fruire dei servizi erogati dai soggetti di cui all'articolo 2, comma 2, in forma digitale e in modo integrato, tramite gli strumenti telematici messi a disposizione dalle pubbliche amministrazioni e il punto di accesso di cui all'articolo 64*-bis*, anche attraverso dispositivi mobili*".

nale ad un'imputazione univoca dell'accesso ai servizi dell'Amministrazione tramite canali telematici.

L'identità digitale (12), nell'accezione esaminata e a differenza dell'analoga nozione predicata nell'ambito penalistico (13), costituisce quindi un attributo dell'individuo oggetto di validazione e riconoscimento da parte dell'apparato pubblico, che ne assicura la piena fruibilità sia nei rapporti con l'Amministrazione sia all'interno del mercato sempre più orientato — secondo le linee di sviluppo dettate dall'Unione Europea — all'utilizzo di sistemi di identificazione digitali omogenei, interconnessi e valevoli senza soluzione di continuità a livello transfrontaliero (14).

Va qui notato che l'attuale sistema di rilascio dell'identità digitale funziona ancora con due distinte modalità: tramite carta d'identità elettronica e tramite accesso al sistema pubblico di identità digitale. Quest'ultimo opera sulla base del concetto di identità digitale c.d. *federata*, fondato sulla cooperazione applicativa da parte di più operatori che forniscono il servizio all'utenza registrata (allo stato le società fornitrici sono 11, di cui nove private e due pubbliche).

3.5. *Segue*: il domicilio digitale e i canali di comunicazione telematici con la pubblica amministrazione (cenni)

A corollario e completamento dell'attributo dell'identità digitale, il domicilio digitale, facoltativamente attivabile da parte dei cittadini, ma pur sempre obbligatorio per professionisti e imprese (oltreché, come visto, per le Amministrazioni), è diretto ad agevolare l'inoltro agli apparati amministrativi, in luogo delle forme tradizionali, delle comunicazioni o delle notifica-

---

(12) L'identità digitale è ottenuta mediante accesso al Sistema Pubblico di Identità Digitale (SPID), ovvero tramite l'impiego della Carta d'Identità Elettronica (CIE).

(13) Dove si rinviene una nozione di "*identità digitale*" assai più lata, riferita all'aggravante di cui all'art. 640-*ter*, comma 3, c.p., l'accertamento della quale "*non presuppone una procedura di validazione adottata dalla Pubblica amministrazione, ma trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici gestiti da privati*" (Cass. pen., Sez. II, 8 settembre 2023, n. 38027).

(14) Dev'essere ricordato come la Commissione Europea abbia da tempo allo studio l'istituzione di un portafoglio di identità digitale denominato EUDI, diretto alla fruizione dei servizi e all'utilizzo nel mercato in tutti i casi in cui sia renda necessario disporre di informazioni depositate ed elaborate presso le amministrazioni. Con Risoluzione del Parlamento europeo del 18 aprile 2023 sull'accelerazione mediante l'eGovernment dei servizi pubblici digitali che sostengono il funzionamento del mercato unico (2022/2036(INI)) (C/2023/444) è stato inoltre recentemente ribadito che "*un'identità digitale sicura e in grado di rafforzare la tutela della vita privata è importante affinché i cittadini possano interagire con le pubbliche amministrazioni e le imprese in tutto il mercato unico europeo*".

zioni agli interessati, come stabilito in via prioritaria dal CAD (15), secondo le modalità previste dall'art. 64 (cfr. in particolare i commi da 2-*ter* a 2-*quinquies*).

In particolare, ai sensi dell'art. 3-*bis* del CAD, l'accesso ai servizi *on-line* è garantito tramite l'identità digitale e anche attraverso il punto di accesso telematico attivato presso la Presidenza del Consiglio dei ministri, di cui all'articolo 64-*bis*. Riassumendo brevemente i tratti salienti della disciplina, basti ricordare come la norma richiamata preveda la facoltà di eleggere o modificare il proprio domicilio digitale, fermi gli obblighi di farne un uso diligente e di comunicare ogni modifica o variazione. Sin dal 1° gennaio 2013, le amministrazioni pubbliche e i gestori o esercenti di pubblici servizi comunicano con il cittadino (qui da intendersi nel senso di "*persona fisica*") esclusivamente tramite il domicilio digitale dallo stesso dichiarato (l'invio di una copia analogica degli atti con firma a stampa rimane ammesso in via residuale soltanto in mancanza di un domicilio digitale).

Il successivo art. 5-*bis* regola le modalità di comunicazione previste per la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche, i quali possono avvenire esclusivamente attraverso canali telematici, rafforzando, anche in questo caso, l'impiego delle tecnologie digitali.

Infine, deve essere ricordato che analoghi canali telematici di comunicazione sono stati da tempo introdotti nell'ambito degli appalti pubblici (a partire dalla disciplina contenuta nel d. lgs. 18 aprile 2016, n. 50), la cui filiera è stata recentemente rivisitata nel senso di un'ulteriore massiva digitalizzazione, ad opera del nuovo codice dei contratti pubblici, approvato con d. lgs. 31 marzo 2023, n. 36.

(15) Ai sensi degli artt. 6-*bis* e ss. del CAD, sono istituiti appositi registri, riuniti sotto la denominazione di Indice Nazionale dei Domicili Digitale (INAD).

IV.
IDENTIFICAZIONE IN RETE: IDENTITÀ DIGITALE E IDENTITÀ PERSONALE

di *Antonino Mazzeo* e *Michele Nastri*

Sommario: 4.1. Premessa. — 4.2. Aspetti giuridici dell'identificazione. — 4.3. Identificazione in rete dei cittadini. — 4.4. Certificazione di ruoli e attributi. — 4.5. eIDAS 2.0 e il wallet europeo dei cittadini. — 4.6. Conclusioni. - Allegato 1.

4.1. Premessa

I servizi di identificazione e autenticazione sono oggi ampiamenti utilizzati in Internet dai cittadini di tutto il mondo, spesso gestiti da operatori privati internazionali, quali Amazon, Facebook, Google, Microsoft o direttamente da enti quale, ad esempio, quelli bancari. Tali servizi, usati anche per forme di mutua identificazione fra operatori diversi (un utente può autenticarsi ad un servizio mediante le credenziali di un altro provider), rappresentano uno standard de facto in ambito internazionale e al di sopra dei sistemi nazionali. Essi sono gestiti da soggetti privati che operano prevalentemente con finalità di tipo commerciale e non nascono per gestire servizi di natura istituzionale, quali quelli offerti dalle PP.AA., e regolamentati per soddisfare le specifiche esigenze dei governi nazionali, pertanto, possono presentare debolezze rispetto a garanzie identificative, sicurezza, privacy e protezione dei dati.

Oggi, stante le vigenti normative nazionali, lo scenario dei sistemi di identificazione utilizzati nella Comunità Europea si presenta disomogeneo, con sistemi specifici nazionali, spesso fra loro poco o del tutto non interoperabili, seppur basati su tecnologie industriali di base che sono ormai standard de facto, quali ad esempio quelle di SAML, *auth0*, *Openid*. Da un'analisi condotta dalla Commissione Europea, gli Stati Membri hanno notificato alla Commissione stessa 19 sistemi di identificazione per 14 Membri, al maggio 2021 (1).

(1) Dalla Relazione alla *Proposta di Regolamento del Parlamento Europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per*

Tali sistemi implementano solo alcune funzionalità dell'identificazione e al di fuori di un protocollo comune standard condiviso e che vincola gli Stati Membri nello sviluppo e implementazione dei propri sistemi di identificazione nazionali.

Per far fronte alle esigenze di necessità di disporre di servizi identificativi digitali comuni e interoperabili, ad elevata sicurezza e in grado di limitare i furti di identità e soddisfare i vincoli di privacy, garantendo lo sviluppo di un mercato unico digitale, promuovendo lo sviluppo di servizi pubblici transfrontalieri fondamentali, incentivando e rafforzando la concorrenza nel mercato unico, migliorando la facilità d'impiego (per cittadini e imprese), il 3 giugno 2021 la Commissione Europea ha presentato una proposta sull'Identità Digitale Europea basata sul quadro eIDAS regolato nel 2014 (che per brevità indichiamo con eIDAS 2.0), con l'obiettivo di offrire ad almeno l'80% dei cittadini la possibilità di utilizzare un'identità digitale per accedere ai principali servizi pubblici entro il 2030 e di farlo oltre i confini dell'UE.

Nel passato recente, in concomitanza con le restrizioni legate al Covid-19, per far fronte all'impossibilità di incontrarsi in presenza nei luoghi di lavoro, si sono velocemente sviluppate e sono comparse nel mercato nuove piattaforme tecnologiche industriali per consentire forme di collaborazione a distanza (ad esempio, Teams Microsoft, Meet di Google, Zoom, Jabber di Cisco, etc.). Piattaforme specializzate sia negli aspetti di gestione testi e documenti (tipiche applicazioni collaborativa a distanza di applicazioni di Office) sia in quelli legati a forme avanzate di videoconferenze in grado di far connettere un numero rilevante di partecipanti (ad esempio, aule didattiche virtuali, seminari e conferenze a distanza, etc.).

Sotto la spinta dell'esperienza dei servizi di collaborazione a distanza, sono stati fatti anche i primi tentativi di gestione a distanza di attività lavorative proprie degli enti pubblici e, quindi, assoggettate a vincoli di norma e regolate da specifici processi burocratici. Fra le prime applicazioni in tal senso annoveriamo, oltre alle lezioni a distanza di scuole e università già avviate anche prima del Covid-19, anche lo svolgimento formale delle sedute d'esame (queste fatte con la partecipazione di membri delle commissioni e candidati tutti a distanza), l'espletamento di concorsi pubblici, di processi del mondo della giustizia, degli atti notarili a distanza (è stata in tal senso

---

un'identità digitale europea si evince infatti che dall'entrata in vigore del Regolamento eIDAS sono stati notificati (come legalmente adottati) 19 sistemi di identificazione elettronica da 14 Stati membri.

espressamente approvata una norma che abilita i notai a stipulare la costituzione di società s.r.l. a distanza (2)), etc.

Come detto gli aspetti critici di tali applicazioni, richiedenti lo sviluppo di specifiche piattaforme tecnologiche in grado di supportare in modo integrato tutte le funzionalità e le garanzie di sicurezza necessarie a soddisfare i vincoli di norma, interessano prevalentemente gli aspetti del tracciamento delle sessioni e dell'identificazione forte delle persone a distanza e non di "avatar digitali" e dell'eventuale accertamento delle volontà dei soggetti coinvolti.

Nel presente lavoro il paragrafo 2 affronta tale tematica prevalentemente dal punto di vista giuridico, mentre nei paragrafi seguenti si evidenziano gli aspetti tecnologici e di processo allo stato percorribili in base alla normativa nazionale ed europea (eIDAS) vigente e considerando anche taluni aspetti in discussione nella evoluzione di eIDAS del 2014 in eIDAS 2.

4.2. Aspetti giuridici dell'identificazione

L'ordinamento nazionale italiano si occupa dell'identificazione principalmente in ambito pubblicistico, e particolarmente in diritto penale e amministrativo.

Non è scopo di questo lavoro indagare il complesso problema del rapporto tra identità personale, identità digitale e identificazione (3), in

---

(2) Con il d.lgs. 8 novembre 2021, n. 183 che recepisce la direttiva (UE) 2019/1151 del Parlamento europeo e del Consiglio del 20 giugno 2019, che modifica la direttiva (UE) 2017/1132 per quanto concerne l'uso di strumenti e processi digitali nel diritto societario.

(3) La locuzione identità personale allo stato non può più essere considerata univoca dal punto di vista giuridico, ma può avere diverse accezioni (G. Resta, *Identità personale e identità digitale*, in *Il Diritto dell'Informazione e dell'Informatica*, 2007, 511 ss.; V. Zeno-Zencovich, voce *Identità personale*, in *Dig. disc. priv., sez. civ.*, IX, Torino, 1993, 294; Giusel. Finocchiaro, voce *Identità personale*, in *Dig. disc. priv., Sez. civ.*, Aggiorn. 5, 2010, 724 ss.): da una parte la nozione tradizionale di complesso delle risultanze anagrafiche, che servono ad identificare il soggetto nei suoi rapporti con i poteri pubblici e a distinguerlo dagli altri consociati (F. Messineo, *Problemi dell'identità delle cose e delle persone nel diritto privato*, in *Annali del seminario giuridico dell'Università di Catania*, IV, Napoli, 1950, 64 ss., 66.); dall'altra, in una visione più moderna, rispetto all'individuo, anche la "*sintesi ideale della sua "biografia"* (G. Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003, 43; G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impresa*, 2017, 724 s.; M. Tampieri, *L'identità personale: il nostro documento esistenziale*, in *Europa e Diritto Privato*, 2019, 1195 s.), in una prospettiva accolta dall'ordinamento, come "*diritto all'identità personale*", espressione utilizzata dall'art. 1 della legge 31 dicembre 1996, n. 675 e poi dall'art. 2, d.lgs. 30 luglio 2003, n. 196 (Codice in materia di protezione dei dati personali). La definizione di identità personale non si ritrova in ogni caso nei testi normativi, ma nella giurisprudenza, che la rappresenta come "*bene-valore*

continua evoluzione dal punto di vista normativo e interpretativo e che attiene tematiche relative soprattutto ai diritti della persona: ci limiteremo quindi al solo tema dell'identificazione, salvo qualche indispensabile cenno.

In diritto privato la norma di riferimento è l'art. 49, legge 16 febbraio 1913, n. 89 (legge notarile): anch'essa però, pur con le diverse finalità proprie del settore (tutela dei singoli rapporti tra privati), trova la sua ragione nella tutela pubblicistica delle contrattazioni, che è uno dei compiti e ragione fondante dell'attività notarile, ed è presidiata da un sistema sanzionatorio nei confronti del notaio in sede disciplinare (e quindi amministrativa) e penale (4).

---

costituito dalla proiezione sociale della personalità dell'individuo, cui si correla un interesse del soggetto ad essere rappresentato, nella vita di relazione, con la sua vera identità, e non vedere travisato il proprio patrimonio intellettuale, ideologico, etico, religioso, professionale (Cass., 7 febbraio 1996, n. 978, in *Foro it*., 1996, I, 1253; cfr. anche Corte cost., 3 febbraio 1994, n. 13, in *Foro it.*, 1994, I, 1668, che configura il diritto all'identità personale come « *diritto ad essere sé stesso, inteso come rispetto dell'immagine di partecipe alla vita associata, con le acquisizioni di idee ed esperienze, con le convinzioni ideologiche, religiose, morali e sociali che differenziano, ed al tempo stesso qualificano, l'individuo* »).

(4) Annoso è il tema della responsabilità del notaio per falso ideologico nell'accertamento dell'identità personale: tuttavia anche la giurisprudenza più liberale ritiene necessaria quanto meno una verifica sommaria dell'autenticità del documento di riconoscimento esibito, il che comporta, anche in relazione a quanto precisato in prosieguo nel testo, l'uso di tutte le tecnologie disponibili. Cass. pen. 26 aprile 2006, n. 16497, in *Banca dati CED Cassazione*, 2006, non ha ritenuto responsabile il notaio per falsità dell'attestazione di certezza dell'identità personale qualora abbia proceduto all'l'identificazione utilizzando un documento di identità falso esibito dall'interessato, in quanto il reato di falsità ideologica può sussistere solo ove, in punto di fatto, siano accertate caratteristiche proprie del documento o altre circostanze idonee a far sorgere quantomeno il sospetto che si trattasse di documento falso; conforme G. Sicchiero, *Notaio e responsabilità professionale - "della cui identità personale io notaio sono certo": chiose sull'art. 49 l.n.*, nota a sentenza Cass. civ. 29 maggio 2018, n. 13362, in *Giur. it*., 2019, 1324. Secondo un orientamento più restrittivo il testo dell'art. 49 l.n. dopo la modifica del 1976, non richiede più una conoscenza personale in quanto anteriore all'attestazione ma esclude che sia "sufficiente un accertamento compiuto sulla base di un semplice documento d'identità apparentemente genuino e poi rivelatosi falso, essendo necessario che esso sia accompagnato da altre diligenti indagini" Cass. pen. 13 gennaio 1981, in *Vita Notar*., 1982, 860; Cass. pen. 30 gennaio 1985, in *Vita Notar*., 1986, 391; Cass. pen. 30 aprile 1992, in *Giur. it*., 1994, 2; contrario a tale orientamento P. Boero, *La legge notarile commentata*, Torino, 1993, 285, il quale lo critica in quanto così si tende a *"sopravvalutare l'importanza della funzione di accertamento dell'identità, pretendendo dal notaio ciò che talora questi non può conseguire nemmeno con la massima diligenza; e finisce col ridurre grandemente la portata innovativa (o chiarificatrice) della legge del 1976, poiché si ha quasi l'impressione che l'unico mezzo reputato sicuramente idoneo per l'accertamento continui ad essere, paradossalmente, la conoscenza pregressa"*. Va rilevato tuttavia che tale giurisprudenza presenta continue oscillazioni in ordine al concreto atteggiarsi del regime di responsabilità: da ultimo particolarmente rigida Cass. civ., ordinanza 1° giugno 2023, n. 15490, reperibile in CED Cassazione di cui si

Partendo quindi dalla rilevanza essenzialmente pubblicistica dell'identificazione, l'approccio ordinamentale del legislatore italiano è tradizionalmente pragmatico e graduale: la regolazione, riguardo all'intensità dei controlli, è sempre stata rapportata all'importanza dell'attività rispetto alla quale è propedeutica. Pertanto, al di fuori dell'ambito informatico e telematico (e del terreno accidentato che sta percorrendo la relativa normazione), le modalità dell'identificazione sono graduate dalla legge in ragione di tali principi: ad esempio ai fini della presentazione di istanze alla pubblica amministrazione o della redazione di dichiarazioni sostitutive dell'atto di notorietà (art. 38, d.p.r. 28 dicembre 2000, n. 445) per l'identificazione è sufficiente l'esibizione della fotocopia del documento di riconoscimento (ed il rischio riceve un contrappeso dalla prevista attività di controllo successivo); per l'identificazione ai fini della costituzione delle parti negli atti notarili il citato art. 49 legge notarile prevede che il notaio debba "essere certo dell'identità personale delle parti", con ciò prevedendosi un'attività di accertamento e verifica (5).

Resta fermo però in tutte le ipotesi lo schema di fondo dell'identificazione che, salva la graduazione delle attività volte all'accertamento o alla

---

riporta la massima "*L'art. 49 della l.n. (nel testo fissato dall'art. 1 della l. n. 333 del 1976) secondo il quale il notaio deve essere certo dell'identità personale delle parti e può raggiungere tale certezza, anche al momento dell'attestazione, con la valutazione di "tutti gli elementi" atti a formare il suo convincimento, contemplando, in caso contrario, il ricorso a due fidefacienti da lui conosciuti, va interpretato nel senso che il professionista, nell'attestare l'identità personale delle parti, deve trovarsi in uno stato soggettivo di certezza introno a tale identità, conseguibile, senza la necessaria pregressa conoscenza personale delle parti stesse, attraverso le regole di diligenza, prudenza e perizia professionale e sulla base di qualsiasi elemento astrattamente idoneo a formare tale convincimento, anche di natura presuntiva, purché, in quest'ultimo caso, si tratti di presunzioni gravi, precise e concordanti; l'accertamento relativo è demandato al giudice del merito, il cui giudizio è incensurabile in cassazione se motivato in maniera congrua e logica. (Nel caso di specie il notaio ha identificato le parti sulla base delle carte di identità — successivamente risultate non autentiche —, che ha fotocopiato, dell'esistenza di una procura speciale a vendere — la cui sottoscrizione poi è risultata apocrifa — e facendo affidamento sulla presenza all'atto dei funzionari bancari e di intermediazione con i quali le parti avevano intrattenuto pregressi rapporti. A giudizio della Corte territoriale, il notaio non ha assolto all'obbligo di adeguata diligenza professionale sancito dall'art. 49 l.n. poiché la sua certezza soggettiva della identità delle parti, raggiunta al momento dell'attestazione, non è stata conseguita attraverso elementi presuntivi gravi, precisi e concordanti. Tanto più che la semplice richiesta alle parti di mostrare un certificato anagrafico avrebbe consentito al notaio di accorgersi della falsità dei documenti d'identità esibiti dai contraenti)*".

(5) Per una disamina della tematica tra gli altri G. Casu, *Sub* artt. 48-50, in *La legge notarile commentata,* a cura di G. Casu e G. Sicchiero, Torino, 2010, 258; P. Ferrero, *Commento all'art. 49 della legge notarile*, in *La legge notarile,* a cura di P. Boero, M. Ieva, Milano, 2014, 329; P. Boero, *La legge notarile commentata con la giurisprudenza*, Torino, 1993, 287.

verifica dell'identità dichiarata, è il risultato dell'attività di accertamento, consistente in un giudizio che consegue all'acquisizione di dati (6).

Il paradigma normativo cui far riferimento in materia di identificazione (prima di addentrarsi nelle problematiche dell'identificazione elettronica) è contenuto negli artt. 1, lett. *c*) e *d*) e 35 del d.p.r. n. 445 del 2000, che individuano i documenti di identità e riconoscimento idonei per l'identificazione personale e quindi, in linea generale, quelli muniti di fotografia del titolare e rilasciati dallo Stato. L'identificazione personale con tali documenti è generalmente reputata sufficiente nell'ambito dell'attività amministrativa (7), e la norma dell'ordinamento del notariato che richiede un'attività ulteriore costituisce un'eccezione.

Da tale paradigma è lecito trarre principi generali, utili anche in un sistema normativo, quale quello dei regolamenti e delle Direttive comunitarie in materia di identificazione elettronica, che astrae da tali principi, di competenza del legislatore nazionale.

L'accertamento dell'identità in rete pone infatti ulteriori problemi, rendendo necessaria una disciplina che si aggiunge, e in buona parte non sostituisce, quanto previsto dalla normativa nazionale previgente, peraltro non molto estesa ed attuata attraverso una prassi ormai secolare (8).

La principale fonte normativa in materia di accertamento dell'identità e identificazione nell'ambito delle reti telematiche (Internet o altro) è infatti di fonte comunitaria: si tratta del Regolamento eIDAS (electronic IDentification Authentication and Signature) Regolamento UE n. 910/2014, che definisce l'identificazione elettronica, i mezzi di identificazione elettronica, i dati di identificazione personale e il regime di identificazione elettronica all'art. 3, nn. 1, 2, 3 e 4). L'identificazione elettronica è prima di tutto considerata un processo il che, al netto della diversa terminologia, corrisponde perfettamente alla tradizionale definizione di accertamento dell'identità, nell'accezione classica di tipo pubblicistico. Tale processo consiste

---

(6) G. Casu, *Sub* artt. 48-50, in *La legge notarile commentata*, cit., 258.

(7) Cfr. anche Testo Unico delle leggi in materia di Pubblica sicurezza (T.U.L.P.S.) r.d. n. 773/1931 in materia di pubblica sicurezza art. 144: "L'autorità di pubblica sicurezza ha facoltà di invitare, in ogni tempo, lo straniero ad esibire i documenti di identificazione di cui è provvisto, e a dare contezza di sé. Qualora vi sia motivo di dubitare della identità personale dello straniero, questi può essere sottoposto a rilievi segnaletici".

(8) Basti pensare che l'introduzione della Carta di identità in Italia come obbligatoria per tutti i cittadini ed i residenti avviene in Italia solo nel 1931 con il T.U.L.P.S. a seguito di un lungo dibattito sulle limitazioni alla libertà personale che ne potevano conseguire, il cui esito risente ovviamente del regime che governava l'Italia in quegli anni. L'obbligo della carta di identità venne quindi abrogato nel dopoguerra, pur permanendo ad altri fini l'obbligo di identificarsi alle autorità di pubblica sicurezza. Nei paesi di *Common Law* abbiamo strumenti di identificazione e tutela dell'identità molto meno invasivi.

nell'uso di dati di identificazione personale, che rappresentano una persona, in forma elettronica.

Tale Regolamento, come vedremo nel prosieguo, è in corso di revisione attraverso la Proposta di Regolamento del Parlamento Europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea (2021/0136/COD).

Nel quadro normativo europeo il collegamento alla persona si ha attraverso il processo di identificazione elettronica, e si differenzia dall'identità digitale che è la rappresentazione informatica di tale collegamento, e ne è quindi lo strumento tecnologico. Tale normativa è stata attuata con diverse norme di recepimento nella normativa nazionale ed in particolare nel CAD, tra le quali da ultimo (unitamente ad interventi alla identificazione per il rilascio di firme elettroniche ed a fini antiriciclaggio (9)) quelle contenute nel d.l. n. 76/2020. Queste ultime ridefiniscono in modo sostanziale ipotesi e modalità di identificazione elettronica quale sistema di accertamento dell'identità personale, al netto di alcune incertezze lessicali (10). In particolare, il sistema è delineato nella nuova formulazione dell'art. 64 del CAD, in funzione sia di un necessario allineamento alla normativa comunitaria, sia di un ampliamento degli strumenti e dei casi d'uso della identità digitale.

A seguito delle modifiche, il CAD nel suo complesso definisce per la

---

(9) Per le quali si rinvia, per una disamina approfondita di novità e criticità a G. Arcella, L. Piffaretti, M. Manente, *L'identificazione non in presenza fisica nel contrasto al riciclaggio ed al terrorismo internazionale*, Studio n. 2-2020/*bis* del Consiglio Nazionale del Notariato.

(10) La novella al CAD, ed in particolare all'art. 64 contenuta nell'art. 24 del d.l. semplificazioni 2020 (d.l. 16 luglio 2020, n. 76, convertito in legge con modificazioni con l. 11 settembre 2020 n. 120), utilizza costantemente la terminologia "identità digitale" anche quale sinonimo di "regime di identificazione elettronica" e "verifica dell'identità digitale" quale sinonimo di "identificazione elettronica" come più correttamente avrebbe dovuto essere per adeguarsi alla terminologia comunitaria del regolamento eIDAS (electronic IDentification Authentication and Signature) Regolamento UE n. 910/2014, intendendosi con tale ultima locuzione non solo lo strumento tecnologico utilizzato per l'accertamento dell'identità in rete e la connessione al titolare, ma anche l'intero processo che di identificazione che solo nella sua interezza conferisce certezze all'accertamento dell'identità: ciò si spiega con la originaria funzionalità del dettato normativo del CAD alla volontà di favorire il Sistema Pubblico per la gestione dell'Identità Digitale di cittadini e imprese (SPID), anteriore al Regolamento eIDAS, al quale ultimo si sono dovuti adeguare non solo l'ordinamento nazionale, ma l'intera organizzazione dei servizi interessati dalla normativa. In particolare, l'uso promiscuo della locuzione identità digitale, con accezione prevalentemente tecnica nelle definizioni del CAD, e come quasi sinonimo di identificazione elettronica nell'articolato, può facilmente indurre in errore l'interprete. Solo un attento lavoro di adeguamento interpretativo consente di conservare coerenza al sistema.

prima volta organicamente modalità ed effetti dell'identificazione delle persone in rete, il che è sicuramente un dato positivo. Tuttavia, non va sottovalutata, e non può essere del tutto apprezzata, la scelta legislativa di abbassare indiscriminatamente i livelli di sicurezza, senza considerare gli scenari di utilizzo in cui l'identificazione viene effettuata per determinarne le modalità, ponendosi con ciò in controtendenza con l'atteggiamento tradizionale del nostro ordinamento. Tale scelta, come vedremo in prosieguo, rischia di essere seriamente messa in crisi dagli sviluppi della normativa comunitaria.

L'obiettivo di incentivare le relazioni giuridiche in rete è stato perseguito dalla normativa nazionale del 2020 semplificando l'identificazione attraverso tre modalità principali:

— aumento del numero degli strumenti utilizzabili;

— equiparazione del riconoscimento in rete al riconoscimento personale;

— abbassamento dei regimi di garanzia delle identità digitali (o meglio dei sistemi di identificazione digitale) utilizzabili.

Una breve disamina delle norme in materia di identificazione elettronica consente qualche considerazione sistematica. Il principale (e sicuramente opportuno) intervento normativo è consistito nel riconoscimento generalizzato dell'utilizzabilità della Carta d'Identità Elettronica (CIE) (11) per l'accesso in modo indifferenziato ai servizi in rete, in particolare della P.A., con ciò rendendo obbligatoria l'accettazione di tale strumento di identificazione da parte di tutte le Pubbliche Amministrazioni, ed in prospettiva dai gestori di servizi pubblici e dagli altri soggetti di interesse pubblico. Si tratta sicuramente di un passo in avanti, considerando le caratteristiche di sicurezza della CIE.

La modifica più incisiva però è contenuta nel nuovo comma 2-*duodecies* dell'art. 64, in quanto per la prima volta la verifica dell'identità digitale (o meglio dell'identificazione elettronica se si rispetta la terminologia del Regolamento UE) è equiparata all'accertamento dell'identità personale tramite

(11) La cornice normativa della CIE deriva dalle norme generali sul rilascio della carta di identità ed in particolare dal testo unico delle leggi in materia di pubblica sicurezza (T.U.L.P.S.) r.d. n. 773/1931, art. 3, e dalla normativa che fin dagli anni '90 si è succeduta, per confluire nel CAD e nelle relative disposizioni attuative (l. 16 giugno 1998, n. 191, art. 2 comma 4, d.p.c.m. 22 ottobre 1999, n. 437, d.lgs. 7 marzo 2005, n. 82, CAD, art. 64, art. 65, decreto 23 dicembre 2015). Da tenere presente, da ultimo, il riconoscimento della CIE come documento di identità avente valore su tutto il territorio dell'Unione Europea (con conseguente standardizzazione) di cui al Regolamento (UE) 2019/1157 del Parlamento Europeo e del Consiglio del 20 giugno 2019 sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione.

controllo del documento di riconoscimento. Viene infatti richiamato l'art. 35 del d.p.r. n. 445/2000, che individua i documenti di riconoscimento utilizzabili per l'accertamento dell'identità.

Il risultato di questo primo rinvio normativo consiste nell'equiparazione dell'utilizzo di "identità digitale con livello di garanzia almeno significativo" (*rectius* "regimi di garanzia dell'identificazione elettronica" secondo l'art. 8 del Regolamento eIDAS) alla identificazione mediante documento cartaceo di identità o di riconoscimento.

Si è trattato di una novità assoluta, in quanto l'utilizzo dell'identità digitale era riconosciuto solo per finalità volta per volta determinate (art. 64 CAD, art. 19, d.lgs. 21 novembre 2007, n. 231).

In precedenza, l'identità digitale era infatti utilizzabile (e tendenzialmente obbligatoria) per l'accesso ai servizi in rete della P.A., ma senza che il suo uso comportasse esplicitamente il riconoscimento personale del soggetto che la utilizza. Il furto di identità digitale diventa così esplicitamente sostituzione di persona (12).

Questo sembra essere a tutti gli effetti l'approdo normativo dell'evoluzione che ha portato alla completa assimilazione (mediante inclusione) dell'identità digitale all'identità personale. La necessità di trovare un centro di imputazione degli effetti giuridici dell'attività in rete da una parte, e la stretta connessione dei dati dell'identità digitale alla persona fisica dall'altra, conducono a tale conclusione obbligata.

Se si considera l'obbligatorietà ormai acquisita (almeno come punto di arrivo cui tendere (13)) dell'utilizzo dell'identità digitale per l'uso dei servizi

---

(12) In verità già secondo Cass. pen. 22 giugno 2018, n. 42572, in *Dir. e giust*., 2018, 320, integra il reato di sostituzione di persona chi utilizza l'identità digitale di un altro soggetto, o chi crea un profilo Facebook utilizzando abusivamente l'immagine di altra persona. In dottrina cfr. G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, cit., in particolare sul reg. Ue 679/2016; M. F. Cocuccio, *Il diritto all'identità personale e l'identità "digitale"*, cit.; S. Landini, *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Riv. dir. industriale*, 2017, 180; F. Cristiani, *Il diritto alla protezione dei dati personali oltre la vita nell'era digitale*, in *Resp. civ. e prev*., 2015, 2031; F. Delfini, *Gli approcci di Unione europea, Stati Uniti d'America e Cina nella gestione dell'identità digitale*, in *Riv. dir. priv*., 2015, 335.

(13) In questo senso la norma del d.l. 31 maggio 2021 n. 77, convertito in l. 29 luglio 2021, n. 108, che all'art. 38 lettera *c*) aggiunge al CAD un nuovo articolo, il 64-*ter,* che istituisce un "Sistema di Gestione Deleghe" per consentire a chiunque di delegare a terzi l'accesso a servizi, così genericamente individuato, attraverso un meccanismo che prevede il preventivo rilascio di accreditamenti al servizio per delegante e delegato, la conservazione delle deleghe all'interno del sistema, e l'utilizzo degli attributi qualificati (già previsti per lo SPID) per individuare i delegati e l'esercizio della delega. Il tutto attraverso l'uso di SPID di qualunque livello e della CIE. Valgono anche qui le riflessioni fatte nel testo circa l'inoppor-

in rete della P.A. la portata di questo intervento appare in tutta la sua rilevanza.

Qualche perplessità è scaturita sin da subito dalla scelta del livello di garanzia significativo dell'identificazione elettronica perché sia raggiunto il risultato dell'identificazione, che non è il più sicuro livello di garanzia degli strumenti di identificazione elettronica, ma quello intermedio.

L'art. 8 del Regolamento eIDAS definisce infatti tre livelli di garanzia dei regimi di identificazione elettronica:

— "basso" riduce il rischio di uso abusivo o alterazione dell'identità;

— "significativo" (*substantial*) riduce significativamente il rischio di uso abusivo o alterazione dell'identità;

— "elevato" (*high*) ha lo scopo di impedire l'uso abusivo o l'alterazione di identità.

I requisiti che corrispondono a tali livelli di garanzia sono contenuti nel Regolamento di Esecuzione (UE) 2015/1502 della Commissione dell'8 settembre 2015 (emanato in attuazione del suddetto art. 8) che definisce i vari livelli dal punto vista funzionale sia in sede di rilascio, sia in sede di uso. Senza entrare nel merito delle singole specifiche va rilevato come esempio che solo il livello di garanzia elevato prevede in sede di rilascio il riconoscimento tramite la fotografia dell'utente (si veda il documento di identità munito di fotografia che costituisce, ai sensi dell'art. 35 del d.p.r. n. 445/2000 un requisito essenziale per il riconoscimento personale) o comunque tramite caratteristiche biometriche. Il livello "significativo" non prevede tale forma di sicurezza. Analogamente, in sede di utilizzo dell'identità digitale, la protezione da attacchi informatici è "moderata" per il livello significativo, "elevata" per il livello elevato.

La procedura per l'utilizzo a livello europeo degli strumenti di identificazione elettronica prevede la notifica da parte degli Stati membri alla Commissione da parte dei singoli Stati (art. 9 Regolamento eIDAS).

L'Italia al momento ha notificato sia lo SPID (14) (per ciascuno dei tre livelli di garanzia "basso, significativo e elevato)" sia la CIE (per il livello

---

tunità di attribuire il medesimo valore a tutti i tipi di identificazione elettronica (o anche solo alle identificazioni di livello "significativo" rispetto a quello "elevato") con l'aggiunta che, in relazione alla delegabilità in genere, una norma recante misure esclusivamente operative non può di certo superare i limiti formali e sostanziali previsti dall'ordinamento per l'effettuazione in nome altrui di attività di rilevanza giuridica.

(14) L'emissione dell'identità SPID prevede tre livelli di sicurezza all'art. 6 del d.p.c.m. 24 ottobre 2014, che solo in via di fatto e con un certo grado di approssimazione possiamo ritenere sovrapponibili ai livelli di garanzia previsti dalla normativa europea: infatti per quanto riguarda gli standard tecnologici il riferimento è a precise norme tecniche che tuttavia non trovano esatto riscontro nel regolamento di esecuzione 1502/2015. Per quanto riguarda l'identificazione al rilascio sono invece previste (art. 7, d.p.c.m. 24 ottobre 2014) modalità che

elevato) (15). Quasi tutti gli altri paesi dell'Unione si sono limitati a notificare le rispettive carte di identità elettroniche, e ciò rende impossibile, al momento, che un'identità digitale di livello "significativo", non basata su un preventivo riconoscimento personale tramite documento di riconoscimento, possa essere utilizzata a pieno titolo in Italia solo perché proveniente da altro Stato dell'Unione.

L'equiparazione della identificazione elettronica di livello di garanzia significativo all'esibizione del documento di riconoscimento cartaceo, in modo generalizzato e non per applicazioni predeterminate ha destato, quindi, qualche preoccupazione. Si consente, infatti, l'uso di strumenti di identificazione elettronica il cui rilascio ed uso non sono tutelati al massimo livello possibile senza alcuna graduazione degli scenari di uso, secondo quello che è stato sempre il comportamento del legislatore non solo con riferimento alle applicazioni in rete, ma anche in ambiente tradizionale.

Una notazione a parte deve essere fatta in relazione all'uso del passaporto elettronico per l'identificazione a distanza: tale strumento è suscettibile per sua stessa natura di essere utilizzato per verifiche informatiche anche a distanza in quanto provvisto, come la CIE, di microchip leggibili con tecnologia NFC (16), non è espressamente incluso tra gli strumenti di identificazione elettronica ammessi per l'identificazione a distanza dal CAD, né tra quelli notificati ai sensi della normativa eIDAS, ma è previsto da un articolato e distinto quadro normativo (17), e solo un'interpretazione irrazionale potrebbe portare ad escluderlo dal novero degli strumenti sicuri per l'identificazione elettronica. Si può ritenere che, anche in mancanza di un espresso riconoscimento, i passaporti elettronici siano equiparabili ai regimi di identificazione elettronica di livello elevato quanto ad efficacia.

Collegata alla questione della sicurezza relativa alle singole applicazioni è la questione della sicurezza in sede di utilizzo. Se infatti elevati livelli di sicurezza possono essere garantiti in sede di rilascio, e la tecnologia può

---

richiedono (anche per il primo e secondo livello) l'esibizione di un documento di riconoscimento (anche in via indiretta) o l'utilizzo di strumenti, come la firma elettronica qualificata, che presumono il controllo di un documento di riconoscimento in fase di rilascio. Da questo punto di vista quindi la normativa nazionale si caratterizza come in parte più rigorosa rispetto a quella europea. Per un'attenta disamina dal punto di vista giuridico dello SPID v. G. LEVANTE, *Il sistema pubblico di identità digitale*, Studio di Diritto dell'Informatica n. 1-2020/DI del Consiglio Nazionale del Notariato.

(15) Gazzetta Ufficiale dell'Unione Europea C 309 del 13 settembre 2019.

(16) Acronimo che sta per *Near field communication*. Tale tecnologia è disponibile su tutti i più recenti smartphone e tablet.

(17) Senza pretesa di completezza si citano: Regolamento (CE) n. 2252/2004 del Consiglio del 13 dicembre 2004; l. 13 luglio 1966, n. 559; l. 21 novembre 1967, n. 1185; l. 31 marzo 2005, n. 43.

ridurre o impedire (livello significativo o elevato) gli attacchi di tipo informatico, l'uso personale dello strumento di identificazione non può prescindere, almeno allo stato attuale della tecnologia, da qualche forma di controllo umano. In altre parole, non è possibile verificare con certezza, ed impedire, l'uso abusivo dell'identità digitale da parte di soggetti diversi dal titolare, e tale rischio non può essere accettato in determinate attività.

Tali considerazioni sembra siano sul punto di essere fatte proprie dal legislatore comunitario, che con la Proposta di Regolamento 2021/0136 intende perseguire una vasta serie di obiettivi, per i quali le condizioni di sicurezza del sistema sono da ritenersi fondamentali ed in particolare:

— fornire soluzioni di identità digitale transfrontaliere affidabili e sicure;

— garantire che i servizi pubblici e privati possano fare affidamento su un'identità digitale affidabile e sicura transfrontaliera;

— fornire ai cittadini il pieno controllo dei propri dati personali e garantirne la sicurezza qualora utilizzino soluzioni di identità digitale;

— garantire condizioni paritarie per la fornitura di servizi fiduciari qualificati nell'UE e la loro accettazione;

— estendere pienamente al settore privato l'utilizzo dei servizi fiduciari eIDAS.

In ragione di questo ambizioso programma il tema della sicurezza dei servizi utilizzati si è posto subito all'attenzione nel corso della procedura legislativa: ad una prima proposta (art. 24 della proposta di Regolamento) della Commissione, in cui era previsto l'utilizzo di servizi di livello "significativo" o "elevato" si è affiancata la più rigorosa proposta del Parlamento che prevede l'utilizzo esclusivamente di servizi di livello "elevato".

Si sono già esposte le ragioni che fanno propendere, in linea di principio, per la soluzione adottata dal Parlamento Europeo: in sintesi in un sistema in cui l'identità digitale e l'identità personale finiscono per riunirsi e sovrapporsi a livello normativo e operativo, la certezza dell'identificazione assume un rilevo fondamentale.

Tuttavia, la scarsa diffusione nell'Unione, nonché la qualità dei sistemi di identificazione elettronica (solo cinque paesi utilizzano sistemi considerati maturi secondo i rilevamenti fatti in sede di preparazione della proposta) la problematica degli stretti tempi di introduzione dei nuovi sistemi (solo dodici mesi secondo l'originaria proposta di regolamento) e molti altri fattori fanno ritenere che ci troviamo di fronte ad una vera criticità.

In particolare, l'Italia avrebbe la seria difficoltà di dover sostituire in un tempo brevissimo tutte le identità digitali SPID, in massima parte di livello "intermedio" o "basso", in un momento in cui la diffusione della Carta d'identità elettronica (per definizione di livello "elevato") presenta proble-

matiche di tipo strutturale (approvvigionamento, disponibilità di personale, etc.). Ciò senza contare l'impatto sul sistema delle industrie che hanno prodotto e commercializzato lo SPID.

Il rischio è quello di dover sostituire in fretta e in modo oneroso un sistema che ha dato buoni risultati nella modernizzazione dei rapporti tra cittadini e Pubblica Amministrazione.

La soluzione potrebbe consistere nell'introduzione di una maggiore gradualità e l'ammissione di soluzioni ponte, ma è chiaro che ciò comporta una l'adozione di una normativa più elastica, che lasci autonomia per un periodo sufficiente ai legislatori nazionali.

Altra possibilità che richiederebbe adeguato approfondimento per l'applicazione nel contesto europeo è quella della graduazione dei livelli di sicurezza minimi rispetto alla tipologia ed al contesto di uso: questa sarebbe ovviamente la soluzione preferibile, ma richiederebbe un notevolissimo sforzo per la definizione normativa dei contesti, o la rinuncia parziale all'uniformità a livello europeo, lasciando spazio residuo alla normazione nazionale.

4.3. Identificazione in rete dei cittadini

L'identificazione dei cittadini (nelle forme medie e forti) e i meccanismi autorizzativi per accesso a funzioni e dati nelle applicazioni a distanza, rappresentano l'aspetto più critico per le garanzie da esse richieste. In Europa, con il regolamento eIDAS nella sua prima versione del 2014 e con quello in corso di approvazione, denominato per semplicità eIDAS 2.0, si stanno ponendo le basi per lo sviluppo di standard e norme in grado di garantire che le forme di cooperazione, interoperabilità e di identificazione possano valere nell'intera comunità europea, favorendo in tal modo lo sviluppo di nuove tecnologie e applicazioni di utilità per i cittadini e di opportunità di sviluppo per le imprese.

In Europa, l'Italia è una delle nazioni più avanzate nel ricorso a forme di identificazione digitali. In essa da anni è in uso SPID (Sistema Pubblico di Identità Digitale), una soluzione identificazione rispondente ai requisiti di eIDAS, che consente ai cittadini di accedere ai servizi online della pubblica amministrazione con un'unica identità digitale (a partire da username e password, fino a modalità di più alto livello, con forme di identificazione a due fattori) utilizzabile da computer, tablet e smartphone. Lo SPID, diffusosi specialmente in concomitanza con l'emergenza del Covid-19, prevede tre livelli di sicurezza identificativi, di cui sono stati implementati dai provider solo i primi due (salvo alcune eccezioni poco diffuse). Parecchi provider in Italia offrono ormai questo servizio che ha già rilasciato in forma gratuita

milioni di identità digitali ai cittadini. Il servizio SPID opera allo stato al livello di sicurezza medio, per cui l'identità, non associata ad un attributo fisico del soggetto di essa titolare, risulta essere di fatto cedibile o delegabile al possessore fisico delle credenziali. Il livello di sicurezza più alto (High) non è stato praticato dai provider, se non in casi limitati, richiedendo esso maggiori costi di investimento nelle infrastrutture tecnologiche, più complesse procedure di "*on boarding*" verso i cittadini e, sempre per problemi di costi non facilmente utilizzabile gratuitamente.

I dati che caratterizzano l'uso di SPID rilevati dal sito di AGID e aggiornati a settembre 2023, indicano che sono state rilasciate 36.052.347 identità SPID da 12 gestori (provider) privati; 14.166 amministrazioni consentono l'accesso ai loro servizi con SPID; 174 fornitori di servizi privati lo usano.

Da essi si evince chiaramente sia il significativo rilascio di identità SPID ai cittadini sia la forte crescita del numero di amministrazioni pubbliche che vi ricorrono per consentire l'accesso ai servizi in internet da esse erogati. A favorire il successo di SPID in Italia, nonostante le iniziali difficoltà d'uso, è stata anche la sua gratuità per un uso a livello di sicurezza medio, con autenticazione a due fattori. Tale livello è certamente adeguato a gran parte delle transazioni in internet dei vari enti.

Differentemente dallo SPID, la CIE (Carta di Identità Elettronica) opera a livello di sicurezza "high". La CIE è rilasciata dai comuni ed è dotata della foto anche digitale del soggetto titolare, non ha raggiunto i livelli di distribuzione massiva quale quello dello SPID, rilasciato anche da soggetti privati, e presenta delle modalità di utilizzo meno semplici. Per semplificarne l'uso, di recente nella CIE è stato introdotto un meccanismo di identificazione a due fattori analogo a quello utilizzato da SPID, in modo da assicurare e semplificare le procedure di accesso ai servizi, autenticando il soggetto anche a livello di sicurezza indicato in EU come "significativo". Con tali modifiche presumibilmente la CIE sostituirà nel futuro prossimo lo SPID non appena tutti i cittadini potranno usufruire di tale carta di identità.

4.4. Certificazione di ruoli e attributi

Per l'accesso ai servizi sia pubblici sia privati e al trattamento dei dati informatici, occorre aggiungere ai meccanismi di identificazione a vari livelli di sicurezza di un soggetto, anche meccanismi autorizzativi basati sul possesso di specifici "attributi" (ad es. un titolo di studio, una carica istituzionale o professionale, etc.). Tali attributi personali sono posti in un "certificato d'attributo" collegato all'identità digitale del soggetto da esso profilato. Gli attributi di un soggetto spesso sono generati da entità terze che ne detengono

i poteri di attribuzione. Esse sono, quindi, in grado di definire e registrare e aggiornare gli attributi depositandoli in un "certificato di attributo" consultabile in modo aperto dai possibili utilizzatori in seno a processi autenticativi di un soggetto titolare.

Un certificato di attributo è gestito secondo standard consolidati da un'autorità di attributo (che opera in modo analogo a una CA che pubblicizza i certificati di firma digitale).

Un attributo qualificato descrive così come gli attributi una specifica proprietà di un'identità di una persona, esso si definisce qualificato perché è attestato da un soggetto (spesso un'istituzione) a cui la legge conferisce il potere di attribuzione. Di solito gli attributi qualificati non cambiano frequentemente nel tempo e il numero di operazioni fatte in lettura è molto maggiore di quelle in scrittura. Gli attributi possono essere statici, come il semplice possesso di un titolo generico, o dinamici, quando un titolo è suscettibile di sospensione o revoca o è assegnato per intervalli di tempo limitati, anche piccoli (ad esempio, l'appartenenza ad una professione per gli iscritti a un albo o l'assegnazione momentanea, per periodo anche brevissimi, di un ruolo a un soggetto delle PP.AA., ad esempio direttore generale ASL, presidente CDA, presidente di una commissione, etc.).

L'attributo, dal punto di vista della normativa, viene in rilievo sotto almeno due profili: quello delle firme elettroniche qualificate e dei sigilli elettronici da una parte, e quello dell'identità digitale (in senso lato), dall'altra.

Per quanto riguarda il primo aspetto va detto che non vi è stata sinora alcuna realizzazione che consenta di collegare correttamente e con procedure informatiche un attributo (intendendosi per tale l'enunciazione di funzioni, qualifiche, poteri e altre prerogative in genere) alla firma elettronica. Vi è menzione della possibilità di aggiungere attributi specifici nel Regolamento eIDAS (910/2014) e precisamente all'art. 24, ove è prevista la possibilità per i prestatori di servizi fiduciari qualificati di inserire nel certificato tali attributi previa verifica al momento del rilascio, e agli articoli 28 (relativo ai certificati di firma qualificata) e 38 (relativo ai certificati dei sigilli elettronici qualificati), dove, nel prevedersi la possibilità di inserire attributi volontari all'interno dei certificati, si precisa che questi non devono pregiudicare l'interoperabilità e il riconoscimento di tali firme e sigilli.

Il CAD prevede invece gli attributi in relazione alle firme nel regolare il certificati di firma elettronica qualificati (art. 28) al terzo comma lettera *a)* ove è sancito che il certificato qualificato può contenere *le qualifiche specifiche del titolare di firma elettronica, quali l'appartenenza ad ordini o collegi professionali la qualifica di pubblico ufficiale, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza*, ed al successivo

comma 3-*bis*, ove è previsto che tali informazioni possano essere contenute anche in un separato certificato.

Nessuno dei provvedimenti di attuazione in materia di firma ha però specificato le modalità di esplicazione degli attributi in conformità al regolamento eIDAS nell'ambito di procedure automatizzate.

Qualche accenno si ritrova nelle Linee Guida AGID contenenti le *Regole Tecniche e Raccomandazioni afferenti alla generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate* (18).

Resta pertanto aperta la sola possibilità di indicare gli attributi nel certificato di firma secondo le modalità di cui sopra, ma la verifica (o anche la sola possibilità di accorgersi dell'esistenza degli attributi) resta affidata al controllo manuale.

Il CAD prende in considerazione gli attributi in relazione anche ad altri specifici aspetti e, in particolare, in relazione ai domicili digitali (art. 6-*bis*) e all'identità digitale in relazione alla quale l'art. 64 così statuisce al comma 2-*duodecies*: "*L'identità digitale, verificata ai sensi del presente articolo e con livello di sicurezza almeno significativo, attesta gli attributi qualificati dell'utente, ivi compresi i dati relativi al possesso di abilitazioni o autorizzazioni richieste dalla legge ovvero stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche, ovvero gli altri dati, fatti e informazioni funzionali alla fruizione di un servizio attestati da un gestore di attributi qualificati, secondo le modalità stabilite da AgID con Linee guida*".

In materia vi sono stati poi ulteriori sviluppi della normazione secondaria con riferimento alla sola identità digitale.

In nota (19) si riportano le definizioni di attributi riportate nel d.p.c.m. 24 ottobre 2014.

---

(18) Pubblicate il 13 febbraio 2020. Al punto 4.1 si legge infatti b. *L'organizationName* (2.5.4.1017) dei certificati di firma elettronica, eventualmente utilizzato per indicare l'appartenenza o l'affiliazione del titolare all'organizzazione e esclusivamente nel caso in cui il prestatore di servizi fiduciari abbia avuto e conservi prova della volontà dell'organizzazione medesima a tale uso e che la stessa si assuma l'obbligo di richiedere la revoca del certificato nel caso in cui il titolare del certificato lasci l'organizzazione. Nel caso in cui l'*organizationName* sia presente, i medesimi vincoli si applicano anche all'eventuale codifica dell'attributo *title.* L'attributo *title*, se presente, contiene il ruolo del titolare in linguaggio naturale e, facoltativamente, una seconda parte costituita da un codice numerico derivato dai codici delle professioni pubblicati da ISTAT. Nel caso in cui sia presente, il codice ISTAT della professione è preceduto dalla stringa: (esadecimale 0x3A3A, e title=descrizioneInLinguaggi oNaturale::codiceNumerico). L'*organizationName* non è utilizzato nel caso in cui il titolare sia un semplice cliente dell'organizzazione.

(19) Si riportano di seguito le definizioni di attributi presenti nel d.p.c.m. 24 ottobre 2014:

Nel maggio del 2021, AGID ha pubblicato le linee guida per "Regole tecniche dei gestori di attributi qualificati *ex* art. 1, comma 1, lettera *m*) del d.p.c.m. 24 ottobre 2014". Con esse è possibile creare dei certificati di attributo da parte di un soggetto denominato "Attribute Authority" che consentono l'attribuzione di specifiche qualifiche a persone fisiche con l'obiettivo di fornire delle funzioni autorizzative assegnate a un particolare soggetto.

In materia di identità digitale il percorso normativo è quindi più avanzato.

Sebbene sia possibile ricorrere all'uso del certificato d'attributo per certificare il possesso di un titolo professionale, allo stato, stante anche la carenza di standard di interoperabilità e di diffusione e utilizzo delle tecnologie abilitanti presso gli enti potenzialmente interessati, il certificato d'attributo, di fatto, è scarsamente utilizzato in Italia e in Europa con riferimento a servizi delle PP.AA. Si ricorre spesso a soluzioni non del tutto appropriate per realizzare una firma di certificazione (ad esempio, spesso si usa il campo descrittivo Titolo del certificato di firma X509, come in precedenza segnalato, ma con utilità limitata ad un dominio chiuso che riesce a utilizzarne il valore, peraltro, non codificato in modo standard e interpretabile, quindi, *erga omnes*).

Lo SPID prevede anche qualcosa per certificare il titolo professionale, in particolare, le Linee Guida SPID sulle identità digitali per professionisti ([20]),

---

b) attributi: informazioni o qualità di un utente utilizzate per rappresentare la sua identità, il suo stato, la sua forma giuridica o altre caratteristiche peculiari;

c) attributi identificativi: nome, cognome, luogo e data di nascita, sesso, ovvero ragione o denominazione sociale, sede legale, nonché il codice fiscale o la partita IVA e gli estremi del documento d'identità utilizzato ai fini dell'identificazione;

d) attributi secondari: il numero di telefonia fissa o mobile, l'indirizzo di posta elettronica, il domicilio fisico e digitale, nonché eventuali altri attributi individuati dall'Agenzia, funzionali alle comunicazioni;

e) attributi qualificati: le qualifiche, le abilitazioni professionali e i poteri di rappresentanza e qualsiasi altro tipo di attributo attestato da un gestore di attributi qualificati;

f) autenticazione informatica: verifica effettuata dal gestore dell'identità digitale, su richiesta del fornitore di servizi, della validità delle credenziali di accesso presentate dall'utente allo stesso gestore, al fine di convalidarne l'identificazione informatica;

m) gestori di attributi qualificati: i soggetti accreditati ai sensi dell'art. 16 che hanno il potere di attestare il possesso e la validità di attributi qualificati, su richiesta dei fornitori di servizi;

o) identità digitale: la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi.

([20]) Linee guida per il rilascio dell'identità digitale per uso professionale del 20 aprile 2020.

indicano le modalità di rilascio delle identità digitali SPID per "uso professionale" intese come quelle utili a provare l'appartenenza di una persona fisica all'organizzazione di una persona giuridica e/o la sua qualità di professionista, iscritto all'Albo unico di cui al d.p.r. 7 agosto 2012, n. 137. Tali qualità sono espresse tramite attributi abbinati all'identità digitale e gestiti da un'apposita autorità di attributi avente i dovuti poteri (ad esempio un ordine professionale). Ma tale meccanismo è quasi del tutto non utilizzato in modo "aperto".

4.5. eIDAS 2.0 e il wallet europeo dei cittadini

Il regolamento eIDAS n. 910/2014 sull'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche nel mercato interno è stato il primo atto legislativo in materia di identità digitale a fornire la base per l'identificazione elettronica transfrontaliera, l'autenticazione e la certificazione dei siti web in tutta l'UE.

Il 3 giugno 2021 la Commissione ha presentato una proposta basata sul quadro eIDAS del 2014, con l'obiettivo di offrire ad almeno l'80% dei cittadini la possibilità di utilizzare un'identità digitale per accedere ai principali servizi pubblici entro il 2030 e di farlo oltre i confini dell'UE.

La necessità di tale regolamento si rileva da alcune circostanze che si rinvengono nei documenti associati alla bozza del regolamento eIDAS 2.0 e dalle riscontrate carenze del regolamento eIDAS, riassumibili in:

— sistemi di identificazione nazionali con differenti standard e notevoli discrepanze;

— il regolamento eIDAS regola solo alcuni aspetti dell'identificazione e i sistemi esistenti non sono interoperabili;

— non c'è e non è prevista, in virtù dei principi basilari del Diritto dell'Unione, alcuna richiesta da parte della Commissione nei confronti degli Stati membri di sviluppare ed implementare un sistema di identificazione nazionale;

— gli Stati Membri hanno informato la Commissione dell'esistenza di 19 sistemi di identificazione per 14 Stati membri, tuttavia sembra siano di più;

— il regolamento non prevede disposizioni in termini dell'uso fatto dai privati o dai terminali mobili circa i dati dell'identificazione (The General Data Protection Regulation (EU) GDPR creata nel 2016 ed entrata in vigore solamente il 25 maggio 2018);

— gli attuali servizi di autenticazione ed identificazione come Google e Facebook navigano un mondo privato non totalmente regolamentato e dunque lascia spazio a lacune inerenti a privacy e data protection.

Con la proposta di modifiche al regolamento eIDAS finalizzate alla definizione di un framework per la Identità Digitale Europea, l'Unione Europea cerca di imprimere un'ulteriore accelerazione al processo di digitalizzazione dei servizi (pubblici e privati), ampliando le possibilità effettive del loro utilizzo in ambito transfrontaliero per:

— fornire accesso a soluzioni di identità elettronica altamente sicure e affidabili;

— assicurare che i servizi pubblici e privati possano contare su soluzioni affidabili e sicure di identità digitale;

— assicurare che le persone fisiche e giuridiche abbiano la facoltà di utilizzare soluzioni di identità digitale;

— assicurare che tali soluzioni siano legate a una serie di attributi e consentano la condivisione mirata di dati di identità limitati alle esigenze del servizio specifico richiesto;

— assicurare l'accettazione di servizi fiduciari qualificati nell'UE nonché parità di condizioni per la loro prestazione.

Si registra una crescente domanda di soluzioni di identità elettronica in grado di fornire tali funzionalità, con guadagni in termini di efficienza e un livello elevato di fiducia in tutta l'UE, tanto nel settore privato quanto in quello pubblico, basandosi sulla necessità di identificare e autenticare gli utenti con un livello elevato di garanzia.

Al fine di raccogliere tutti gli attributi associati ad un'identità di un cittadino, il nuovo regolamento eIDAS 2.0 propone la realizzazione del portafoglio delle identità (*european digital identity wallet*) un contenitore standard di attributi che consente ad un cittadino europeo di conservare dati di identificazione, credenziali ed attributi collegati alla sua identità e sotto il suo pieno controllo, al fine di esibirli alle parti richiedenti e di utilizzarlo come strumenti di autenticazione (*online* e *offline*).

Il compito di dotare i cittadini del *wallet* spetta a ciascuno Stato membro (ed è previsto che sia rilasciato gratuitamente) che potrà provvedervi direttamente oppure delegando un soggetto al rilascio o, infine, riconoscendo il *wallet* rilasciato da soggetti terzi.

Il *wallet* deve consentire la gestione degli attributi, qualificati e no, del titolare dello stesso, la validazione dei dati identificativi, la presentazione dei dati ed attributi anche in modalità offline ed assicurare un livello di sicurezza almeno "elevato" secondo la classificazione contenuta nell'art. 8 del Regolamento. Ciò, come si è visto in precedenza, comporterà la necessità che l'Italia riveda in modo significativo il proprio sistema di identità digitali e, in particolare, lo SPID.

Grande attenzione è posta in tema di tutela dei dati personali in quanto è fatto divieto sia di raccogliere informazioni circa l'uso del *wallet* da parte

degli utenti sia di condividere dati ulteriori, salvo consenso dell'interessato, rispetto a quelli necessari alla gestione del *wallet* stesso.

Il *wallet* è lo strumento naturale in cui andranno a confluire gli "attestati elettronici di attributi" che sono disciplinati nella nuova Sezione 9 del regolamento. Si tratta della trasposizione del concetto di "*Verifiable Credentials*" le quali, con la proposta in esame, entrano a pieno titolo nella disciplina giuridica europea.

Così come per gli altri servizi fiduciari anche gli attestati di attributi potranno essere qualificati o non qualificati (ossia emessi da un prestatore di servizi qualificato o da altro soggetto) con una differenza di effetti disciplinata dall'art. 45a della proposta (21). Infine, secondo l'*Annex* VI, gli Stati membri devono garantire a un emittente di attestati elettronici qualificati di poter verificare tramite fonti pubbliche sicure almeno un insieme minimale di attributi di una persona (22).

Si tratta, pertanto, di un'ulteriore spinta verso l'accesso ai dati pubblici che richiederà un notevole sforzo, dal punto di vista organizzativo ed informatico, da parte della pubblica amministrazione per poter rendere effettiva la previsione.

Ulteriore incentivo alla diffusione e utilizzo dell'*European digital identity wallet* sono dati dall'art. 12b.2, in cui viene stabilito che in tutti i casi in cui un provider privato rilascia servizi sulla base di un meccanismo di "strong user authentication" deve accettare anche l'utilizzo del *wallet* a tale scopo. Il riferimento, anche se indiretto, va ai sistemi di strong authentication già introdotti dalla PSD2 per i servizi di pagamento che quindi dovranno essere affiancati con il nuovo sistema introdotto dalla proposta regolamentare in esame.

Il *Wallet* mira a conservare dati e attributi di identificazione personale per l'uso di procedure online private e pubbliche e per facilitare notevolmente l'identificazione elettronica. Esso sarà utilizzato principalmente per l'identificazione sicura in caso di servizi online. Sono attentamente da analizzare i livelli di sicurezza adottati dalle varie nazioni per l'accesso ai servizi online che richiesti ai fini dell'identificazione.

Si ritiene utile al fine di meglio inquadrare lo stato di avanzamento della proposta eIDAS 2.0 per la sua approvazione, di riportare in allegato 1,

---

(21) Gli attributi qualificati devono avere pari valenza giuridica di quelli rilasciati "su carta" mentre a quelli non qualificati non possono essere negati effetti giuridici per il solo fatto di essere emessi in forma elettronica.

(22) L'insieme minimo di attributi comprende: indirizzo, età, sesso, stato civile, stato di famiglia, nazionalità, diplomi, titoli e abilitazioni relative al percorso scolastico, qualifiche, titoli e abilitazioni professionali, permessi pubblici e licenze, dati societari e finanziari.

traducendoli in italiano e sintetizzandoli, alcuni punti di un rapporto prelevato dal sito della Comunità sull'argomento del 29 giugno 2023 ([23]), data in cui il Parlamento e il Consiglio hanno raggiunto un accordo provvisorio sul regolamento eIDAS.

4.6. Conclusioni

Nel presente lavoro sono stati sinteticamente esposti gli aspetti funzionali, tecnologici e giuridici legati alla rilevante tematica dell' identificazione dei soggetti in rete e, in particolare, quelli legati all'identità digitale e personale e all'uso di attributi, ad essa associati, inseriti come detto nel *wallet* del cittadino previsto in eIDAS 2.0, contenitore in cui inserire, sotto il diretto controllo del titolare, un insieme di attributi personali e professionali, qualificati o meno, collegati alla sua identità digitale.

Il tema dell'identità digitale è oggi ritenuto un elemento critico per avviare tutti i processi/progetti di trasformazione digitale su larga scala (nazionale e transfrontaliera). Le normative dei vari governi nazionali conformi ai dettami di eIDAS 2.0 e le soluzioni tecnologiche sviluppate dal mondo industriale in ambito europeo, giocheranno un ruolo centrale per avviare concretamente tali trasformazioni, semplificandone i processi burocratici e abilitando lo sviluppo di nuovi e più efficienti servizi ai cittadini europei anche in logica transfrontaliera.

Il dominio della giustizia è certamente centrale e interessato a seguire tali innovazioni e a guidare la trasformazione digitale dei propri processi. Il notariato, in tal senso, seguendo attivamente l'evoluzione della normativa nazionale ed europea, ha da tempo investito e continua a investire nella digitalizzazione. In particolare, esso sta investendo nello sviluppo di un sistema tecnologico per creare un'autorità di attributo in grado di certificare il possesso del titolo professionale di notaio (e quindi lo stato del ruolo attivo, sospeso e revocato). La PKI-attributo si affianca alla PKI di firma già operativa da anni per esporre in modo standard (X509) i certificati d'attributo dei notai e che, unitamente al certificato di firma, perfezionerà il processo di firma a norma di un atto digitale, separando gli aspetti di attribuzione del ruolo da quelli del rilascio delle firme digitali. Tale modello, certamente è replicabile ad altri domini. Si pensi soltanto ai vantaggi che si potrebbero ottenere certificando i ruoli degli operatori di giustizia (magistrati, cancellieri, etc.), con rilascio di attributi anche limitati a finestre temporali di poche ore.

([23]) https://digital-strategy.ec.europa.eu/it/policies/electronic-identification.

Allegato 1

"...

Si è portata al tavolo dei negoziati un'agenda molto ambiziosa composta da undici punti. A causa del gran numero di punti, non è stato possibile raggiungere un accordo su testi concreti. Si è deciso, invece, di redigere conclusioni per il trilogo, che specificano in dettaglio ciò che è stato concordato a livello politico. Si cercherà, pertanto, di tradurre queste conclusioni in testi concreti.

Tutte le priorità del Parlamento si riflettono nell'accordo provvisorio che garantirà elevati livelli di protezione dei dati, cybersicurezza e interoperabilità del nuovo quadro.

Attualmente sono in corso trilogie tecniche con l'obiettivo di finalizzare tutte le questioni in sospeso nel mese di ottobre

I principali elementi dell'accordo provvisorio del 29 giugno sono di seguito elencati:

1. Identificatore univoco e persistente (UPI)

Fin dall'inizio, questo si è rivelato l'elemento più delicato dell'intera proposta per il Parlamento dal punto di vista della protezione dei dati. Molti gruppi temevano che l'UPI, che secondo la proposta della Commissione sarebbe stata utilizzata per la corrispondenza dei documenti di identità nelle transazioni transfrontaliere per stabilire un legame univoco tra una persona e un numero nazionale unico, portasse con sé troppe implicazioni negative per la privacy. Alla fine, la Commissione ha suggerito una soppressione di questa disposizione, accettata da entrambi i colegislatori. Poiché l'uso delle UPI solleva anche questioni costituzionali in alcuni Stati membri, il Consiglio è stato lieto di sostenere la soppressione. La soppressione della disposizione sull'UPI è una grande vittoria per la privacy e per il Parlamento.

2. *Onboarding* nel *Wallet* e nei servizi fiduciari

Al fine di rispondere alle preoccupazioni specifiche di paesi come l'Italia e la Danimarca, si è concordato di disporre di procedure speciali per l'*onboarding* remoto sul portafoglio per quegli Stati membri che attualmente utilizzano un livello di garanzia "sostanziale". In base al compromesso raggiunto, tali Stati membri potranno utilizzare le loro attuali procedure di *onboarding* per la verifica dell'identità durante l'*onboarding*, anche mediante procedure a distanza.

3. Certificazione del *Wallet.*

Si è discusso se la certificazione GDPR del *Wallet* dovesse essere obbligatoria o meno. Il compromesso trovato è stato che la certificazione GDPR del *Wallet* sarebbe rimasta su base volontaria. Inoltre, è stata aggiunta una clausola di revisione che verificherà la maturità del GDPR per la certificazione della protezione dei dati, incluso se la certificazione GDPR debba diventare obbligatoria.

4. Sanzioni

Le sanzioni, anch'esse approvate dal Parlamento, devono essere allineate al metodo delineato nella direttiva NIS2. I valori concreti delle sanzioni devono ancora essere confermati. Nell'ambito del compromesso, abbiamo anche preso in considerazione le esigenze specifiche di quegli Stati membri che non dispongono di un sistema di sanzioni amministrative pecuniarie, come la Danimarca, ma in cui i tribunali nazionali sono responsabili dell'imposizione delle ammende.

5. Accesso degli emittenti del *Wallet* alle funzionalità hardware e software

Si è concordato l'obbligo per i produttori di telefoni di garantire l'accesso alle funzionalità hardware e software proprietarie su cui il *Wallet* farà affidamento, in linea con i requisiti DMA.

6. Funzionalità estese del portafoglio

Il Parlamento ha introdotto una serie di funzionalità di base che il portafoglio dovrebbe fornire per impostazione predefinita, tra cui la possibilità di utilizzare la firma elettronica per firmare i documenti, di controllare le impostazioni sulla privacy tramite la dashboard sulla privacy, di generare pseudonimi, ecc. Il Consiglio ha affermato che ciò sarà costoso e rallenterebbe il lancio dei portafogli. Alla fine, nell'ambito del pacchetto più ampio, il Consiglio ha accettato le funzionalità proposte dal Parlamento.

7. Firme elettroniche gratuite

Il Parlamento ha suggerito che le firme elettroniche dovrebbero essere gratuite per l'uso da parte di tutti gli utenti del portafoglio. Il compromesso raggiunto limita l'uso gratuito delle firme alle sole persone fisiche, il che rappresenta un grande risultato per rendere le firme elettroniche più disponibili.

8. Libri mastri elettronici

Il Parlamento ha soppresso la disposizione sui registri elettronici, che era stata proposta come uno dei nuovi servizi fiduciari nella riforma dell'eIDAS. Nell'ambito del più ampio pacchetto di compromesso, il Parlamento ha accettato di reinserire i registri elettronici nel testo, in quanto ciò era importante per molti Stati membri.

9. Governance

Il Parlamento ha inoltre proposto un approccio olistico alla governance al fine di garantire una governance del nuovo ecosistema adeguata alle esigenze future. Il Consiglio ha accettato il principio alla base del nostro approccio e il testo concreto sarà concordato a livello tecnico. Tra le altre cose, è stato chiarito che il Comitato per l'identità digitale avrà principalmente un ruolo consultivo.

10. QWACS - certificati di autenticazione di siti *Web* qualificati

Abbiamo discusso se i browser *Web* dovrebbero o meno essere autorizzati a adottare misure di sicurezza precauzionali una volta identificato un potenziale problema di sicurezza con un certificato di autenticazione del sito *Web* qualificato. Nell'ambito del compromesso, il Consiglio ha accettato la proposta del Parlamento secondo cui i navigatori dovrebbero essere in grado di adottare misure precauzionali.

11. Tempistica per l'emissione del *Wallet*

Si è discusso delle tempistiche per l'emissione del *Wallet*. La Commissione ha proposto 12 mesi dopo l'adozione per l'entrata in vigore, il Parlamento ha chiesto 18 mesi, mentre il Consiglio ha chiesto 24 mesi dopo l'entrata in vigore degli atti di esecuzione. Nell'ambito del pacchetto più ampio, il Parlamento ha accettato che il punto di partenza sia 24 mesi dopo l'entrata in vigore degli atti di esecuzione.

...".

PARTE II
LA RILEVANZA NEL PROCESSO CIVILE DELL'IDENTITÀ E DEL DOMICILIO DIGITALE

Sezione I
IL PROCESSO DI COGNIZIONE

I.
LE TIPOLOGIE DI DOMICILIO DIGITALE NEL PROCESSO CIVILE

di *Antonella Ciriello*

1.1. Le tipologie di domicilio digitale nel processo civile

Come visto nel capitolo introduttivo, dalla normativa generale si evincono i concetti di domicilio generale, speciale e di piattaforma (v. *supra* cap. 1).

Tali istituti trovano una propria declinazione nelle regole processuali civili e penali, con delle differenze significative tra settori della giurisdizione e tipologie di atti processuali.

In particolare, ai fini delle comunicazioni e delle notifiche, la norma rilevante (valida non solo nel processo civile ordinario ma anche in quello penale e in altre giurisdizioni) è stata, sino ad oggi l'art. 16-*ter* del decreto-legge 18 ottobre 2012, n. 179 [1] (v. *infra* cap. 1 e, più specificamente, in questo capitolo, paragrafo 2).

Mentre questo scritto è realizzato, tuttavia, risulta in corso di approvazione il decreto legislativo concernente disposizioni integrative e correttive al decreto legislativo 10 ottobre 2022, n. 149, sottoposto al parere del Parlamento Tale corpo normativo, come emerge dal testo all'esame del parlamento, ha adeguato numerose norme prevedendo, accanto al domicilio digitale risultante da pubblici elenchi, la possibilità di eleggere un domicilio digitale speciale e dettando una specifica disposizione per il domicilio digitale ai fini delle comunicazioni e delle notifiche, contenuta nell'art. 196-*septies*.1 disp. Att. C.p.c. [2].

---

[1] Tale decreto-legge, ripetutamente rimaneggiato negli anni, dettava "misure per favorire la crescita, lo sviluppo dell'economia e della cultura digitali, attuare politiche di incentivo alla domanda di servizi digitali e promuovere l'alfabetizzazione informatica, nonché per dare impulso alla ricerca e alle innovazioni tecnologiche, quali fattori essenziali di progresso e opportunità di arricchimento economico, culturale e civile e, nel contempo, di rilancio della competitività delle imprese". La sua sezione Giustizia Digitale, ha costituito per anni il testo unico dei processi telematici e contiene ancora norme di grande rilevanza, nonostante la razionalizzazione e la codificazione realizzata con le due riforme Cartabia (d.lgs. nn. 149 e 150 del 2022).

[2] Il testo del decreto legislativo correttivo è leggibile sul sito del Parlamento italiano https://temi.camera.it/leg19/dossier/OCD18-19766/disposizioni-integrative-e-correttive-al-d-lgs-149-2022-riforma-del-processo-civile.html

Per i depositi telematici, invece, le discipline si differenziano tra processo civile e penale (per non parlare degli altri processi, aspetto che — necessariamente — dovrà essere oggetto di rimeditazioni in ottica europea, essendo necessaria una progressiva integrazione delle differenze, ove non strettamente imposte dalla natura dell'attività processuale da compiersi).

Per il deposito telematico, pertanto, mentre nel processo civile fino ad oggi lo strumento utilizzato resta la posta elettronica certificata (pur risultandone previsto il superamento da parte della normativa primaria, per questa parte ancora inattuata), nell'ancora neonato processo penale telematico (e limitatamente ai casi in cui il deposito telematico stesso è ammesso) lo strumento è differenziato: accanto all'*upload* presso il portale dei depositi telematici, PDP [3] è tutt'ora ammessa (in proroga) quella tipologia di deposito tramite messaggio PEC, introdotto durante il periodo emergenziale, [4] nonché il deposito cartaceo.

Di seguito il testo del novello (in corso di emanazione), art. 196-*septies*.1 (Domicilio digitale). — Salvo che la legge preveda diversamente, le comunicazioni e notificazioni al difensore o alla parte presso il difensore sono effettuate tramite posta elettronica certificata all'indirizzo risultante da pubblici elenchi o dal registro generale degli indirizzi elettronici gestito dal Ministero della giustizia. Quando la parte sta in giudizio personalmente, ai soggetti dotati di domicilio digitale eletto ai sensi dell'articolo 3-*bis*, commi 1 e 1-*bis*, del codice dell'amministrazione digitale di cui al decreto legislativo 7 marzo 2005, n. 82, o che hanno indicato un domicilio digitale speciale ai sensi dell'articolo 3-*bis*, comma 4-*quinquies*, dello stesso codice le comunicazioni e le notificazioni sono effettuate tramite posta elettronica certificata o servizio elettronico di recapito certificato qualificato e si applicano le disposizioni previste dal settimo comma dell'articolo 149-*bis* del codice di procedura civile, salvo che la legge non preveda diversamente. Le comunicazioni e le notificazioni alle pubbliche amministrazioni che stanno in giudizio avvalendosi direttamente di propri dipendenti sono effettuate agli indirizzi di posta elettronica comunicati a norma dell'articolo 16, comma 12 del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221. In caso di mancata comunicazione, la notifica è effettuata ai sensi dell'articolo 16-*ter*, comma 1-*ter* del decreto-legge n. 179 del 2012. I pubblici elenchi degli indirizzi di posta elettronica certificata sono quelli previsti dagli articoli 6-*bis*, 6-*ter* e 6-*quater* del codice dell'amministrazione digitale.

[3] Nelle specifiche tecniche del DGSIA, recentemente aggiornate e pubblicate in consultazione sul sito https://pst.giustizia.it/PST/resources/cms/documents/ SPECIFICHE_TECNICHE_DM_44_2011REV_04.01.24.pdf si legge all'art. 18 che l'accesso al PDP è consentito unicamente ai soggetti iscritti nel ReGIndE con ruolo avvocato, praticante abilitato, nonché avvocato ente pubblico e funzionario ente pubblico, questi ultimi limitatamente agli appartenenti all'Avvocatura dello Stato.

[4] Prevede l'art. 3 del d.m. 217 cit. comma 8, che "*Rimane consentito il deposito mediante posta elettronica certificata come disciplinato dall'articolo 87*-bis *del decreto legislativo 10 ottobre 2022, n. 150 per tutti i casi in cui il deposito può avere luogo anche con modalità non telematiche*". L'art. 87-*bis* prevede poi: "*1. Sino al quindicesimo giorno successivo alla pubblicazione dei regolamenti di cui ai commi 1 e 3 dell'articolo 87, ovvero sino al diverso termine previsto dal*

Nel caso di deposito "emergenziale prorogato", il domicilio digitale del mittente, ai sensi dell'art. 87-*bis*7 del decreto legislativo 10 ottobre 2022, n. 150, è quello che si evince dal ReGinDe. Per gli uffici destinatari, invece, è previsto che "gli indirizzi di posta elettronica certificata degli uffici giudiziari destinatari" siano indicati "in apposito provvedimento del Direttore generale per i sistemi informativi automatizzati, pubblicato nel portale dei servizi telematici del Ministero della giustizia".

Si tratta, ovviamente, di una soluzione tampone, nata nell'emergenza e prorogata nelle more dell'adeguamento degli applicativi del PPT: infatti la PEC autonoma, che rappresenta un flusso non integrato direttamente con gli applicativi del fascicolo informatico (a loro volta ancora in evoluzione), comporta ovvie attività ulteriori foriere di criticità e appesantimenti del lavoro.

Tornando sul versante civile, nei paragrafi che seguono saranno affrontati gli aspetti rilevanti tenendo conto delle ultime modifiche normative.

---

regolamento di cui al comma 3 del medesimo articolo per gli uffici giudiziari e le tipologie di atti in esso indicati, per tutti gli atti, i documenti e le istanze comunque denominati diversi da quelli previsti nell'articolo 87, comma 6-bis*, e da quelli individuati ai sensi del comma* 6-ter *del medesimo articolo, è consentito il deposito con valore legale mediante invio dall'indirizzo di posta elettronica certificata inserito nel registro generale degli indirizzi elettronici di cui all'articolo 7 del regolamento di cui al decreto del Ministro della giustizia 21 febbraio 2011, n. 44. Il deposito con le modalità di cui al periodo precedente deve essere effettuato presso gli indirizzi di posta elettronica certificata degli uffici giudiziari destinatari, indicati in apposito provvedimento del Direttore generale per i sistemi informativi automatizzati, pubblicato nel portale dei servizi telematici del Ministero della giustizia. Con il medesimo provvedimento sono indicate le specifiche tecniche relative ai formati degli atti e alla sottoscrizione digitale e le ulteriori modalità di invio. Quando il messaggio di posta elettronica certificata eccede la dimensione massima stabilita nel provvedimento del Direttore generale per i sistemi informativi automatizzati di cui al presente comma, il deposito può essere eseguito mediante l'invio di più messaggi di posta elettronica certificata. Il deposito è tempestivo quando è eseguito entro le ore 24 del giorno di scadenza*".

II.

IL DOMICILIO DIGITALE NELLA NOTIFICA TELEMATICA. I PUBBLICI ELENCHI O REGISTRI AI FINI DELLA COMUNICAZIONE E DELLA NOTIFICA

di *Antonella Ciriello*

Sommario: 2.1. I pubblici elenchi o registri rilevanti a fini della comunicazione e della notifica. — 2.1.1. Le modifiche introdotte dallo schema di decreto legislativo all'esame del parlamento. — 2.2. L'impervio cammino della notifica telematica intrecciato con le evoluzioni del domicilio digitale. — 2.3. Il registro INAD e la notifica telematica obbligatoria della legge Cartabia.

2.1. I pubblici elenchi o registri rilevanti a fini della comunicazione e della notifica

Il domicilio digitale rilevante per le comunicazioni e le notifiche nel processo civile, nonché lo strumento concreto utilizzato per le medesime, è stato fino ad oggi la Posta elettronica certificata (PEC).

La riforma introdotta con il d.lgs. 10 ottobre 2022, n. 149, tuttavia, seguendo le indicazioni della legge delega, alla tradizionale PEC (che riesce ad essere adeguata ai requisiti europei come visto [1]), solo indirettamente, nel contesto processuale, attraverso il "censimento" di tutti soggetti obbligati a dotarsene, nei rispettivi pubblici elenchi), ha affiancato in tutti i dati normativi [2] il riferimento al servizio elettronico qualificato certificato, che ad oggi

---

[1] V. Cap. 1 ove si osserva che l'iscrizione agli elenchi di cui all'art. 16-*ter*, d.l. 18 ottobre 2012, n. 179, e 16-*sexies* del medesimo decreto, così come a quelli generali del CAD, per i soggetti che sono obbligati, o che esercitino una facoltà, conduce — in maniera indiretta — a ritenere la conformità di tali indirizzi PEC alla normativa eIDAS (solo indirettamente, in alter parole, per il tramite cioè della specifica normativa che consente il popolamento di tali elenchi previa identificazione qualificata del titolare).

[2] Il riferimento al SERCQ compare, da ultimo, anche nel decreto del Ministro della Giustizia 21 febbraio 2011, n. 44 come modificato dal Decreto del Ministro della Giustizia 29 dicembre 2023, n. 217, ove all'art. 1 compare l'ulteriore lettera *e-bis*) che definisce il "*il servizio elettronico di recapito certificato qualificato" rinviando al Regolamento (UE) n. 910/2014 (eIDAS).*

non è ancora attivo nel paese (3). Nelle more, la PEC, come visto nel primo capitolo, dovrà adeguarsi agli standard europei.

Ad oggi, dunque, il domicilio digitale rilevante ai fini della notificazione (e non solo nella giustizia ordinaria, sia civile che penale, ma anche in quella amministrativa, contabile e nella materia stragiudiziale) è quello risultante dai pubblici elenchi indicati dall'art. 16-*ter*, del d.l. 18 ottobre 2012, n. 179, di seguito riportati..

1) l'elenco di cui all'art. 6-*bis* del CAD (Indice Nazionale della Posta Elettronica Certificata - ossia **INIPEC**);

2) l'elenco di dui all'articolo 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2 (**Registro delle Imprese**);

3) l'elenco di cui all'art. 6-*ter* del CAD (**indice PA, IPA**), a certe condizioni indicate dal medesimo art. 16-*ter*;

4) il registro generale degli indirizzi elettronici gestito dal Ministero della Giustizia (**ReGinDE** art. 7, d.m. 21 febbraio 2011, n. 44);

5) l'elenco di cui all'art. 16 comma 12, d.l. n. 179 del 2012 (**Registro delle PA**) gestito dal Ministero della Giustizia;

6) l'elenco di cui all'art. 6-*quater* del CAD (l'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese **INAD**);

7) l'elenco di cui all'art. 62 del CAD (l'Anagrafe nazionale della popolazione residente **ANPR**).

Ciascuno di questi elenchi è disciplinato da regole specifiche. I primi tre (INIPEC, registro delle Imprese e IPA) oltre che l'ANPR (4) e l'INAD, assumono rilevanza generale, anche al di fuori del contesto processuale (5).

---

(3) Sul punto, osserva V. MASSELLA, loc. cit. "*Il servizio in questione, ancora non attivo sul territorio nazionale, risponde ai seguenti requisiti: è un servizio fornito da prestatore di servizi fiduciari qualificati; garantisce un alto livello di sicurezza nell'identificazione del mittente; garantisce l'identificazione del destinatario prima dell'invio dei dati; invio e ricezione sono garantiti da firma elettronica avanzata o sigillo elettronico avanzato apposto da un prestatore di servizi fiduciari qualificato; il mittente e il destinatario sono al corrente di qualsiasi modifica dei dati inviati; ora e data d'invio e ricezione vengono collegate ai dati attraverso una validazione temporale elettronica qualificata La PEC non soddisfa appieno i requisiti previsti dal Regolamento eIDAS: non è prevista la verifica certa dell'identità del richiedente della casella di PEC il gestore non è obbligato a sottoporsi alle verifiche di conformità da parte degli organismi di valutazione accreditati da Accredia*".

(4) L'ANPR è l'anagrafe nazionale di tutti i residenti del Paese, una evoluzione complessa dei registri anagrafici tradizionali che dovrà integrarsi nei prossimi anni con il domicilio digitale dei residenti stessi.

(5) V. sul punto M. REALE, Lezione tenuta nel corso P23030 della Scuola Superiore della Magistratura in ea9b2439-a655-0c80-6d9a-895626d68c44 (scuolamagistratura.it).

Il Registro delle PA e il ReGinDE, invece, gestiti dal Ministero della Giustizia, assumono la qualità di pubblici elenchi rilevanti ai fini della comunicazione e della notifica (proprio in virtù dell'art. 16-*ter* in commento) in materia civile, penale, amministrativa, contabile e stragiudiziale.

In particolare, il Registro Generale degli Indirizzi Elettronici (ReGIndE), è disciplinato dall'art. 7 del d.m. 21 febbraio 2011, n. 44, (recentemente innovato dal d.m. 15 novembre 2023, n. 217) e contiene i dati identificativi e l'indirizzo di posta elettronica certificata dei soggetti abilitati. Si alimenta, per i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato, mediante i dati contenuti negli elenchi riservati di cui all'articolo 16, comma 7, del decreto-legge 29 novembre 2008, n. 185, convertito nella legge del 28 gennaio 2009 n. 2, inviati al Ministero della Giustizia secondo le specifiche tecniche di cui all'articolo 34 (6). Dalle medesime specifiche è regolata la accessibilità del registro stesso ai soggetti abilitati (7).

In seguito alla evoluzione recente della normativa è stato stabilito un allineamento tra il ReGinDE e l'INAD, per i soggetti abilitati esterni non iscritti in albi (modifiche inserite con d.m. 29 dicembre 2023, n. 217).

Del pari il Registro delle Amministrazioni Pubbliche è gestito dal Ministero della Giustizia, ai sensi dell'art 16, comma 12, del d.l. n. 179 del 2012, e risulta consultabile esclusivamente dagli utenti abilitati all'interno degli uffici giudiziari, nonché degli uffici notificazioni, esecuzioni e protesti, e dagli avvocati.

Si tratta, tuttavia, di un elenco incompleto, poiché nel termine originariamente assegnato alle PPAA per l'iscrizione (il 30 novembre 2014) (8) e poi rimosso nel 2020, solo alcune delle pubbliche amministrazioni risultavano iscritte (circostanza che, comprensibilmente, ha frustrato per molti anni la possibilità realizzare il contraddittorio telematico verso moltissimi enti pubblici).

Per tale ragione la disciplina è stata modificata con la valorizzazione dell'indice delle PA e il rimaneggiamento sia dell'art. 16 comma 12 del d.l. n.

---

(6) La norma in questione stabilisce che "*I professionisti iscritti in albi ed elenchi istituiti con legge dello Stato comunicano ai rispettivi ordini o collegi il proprio domicilio digitale di cui all'articolo 1, comma 1, lettera* n-ter *del decreto-legislativo 7 marzo 2005, n. 82. Gli ordini e i collegi pubblicano in un elenco riservato, consultabile in via telematica esclusivamente dalle pubbliche amministrazioni, i dati identificativi degli iscritti e il relativo domicilio digitale. ...*".

(7) Ossia sia tramite funzionalità disponibili nei Punti di Accesso (PDA) privati sia tramite l'area riservata del Portale dei Servizi Telematici del Ministero della Giustizia.

(8) Il termine fu inserito nel comma 12 dall'art. 47, n. 1, decreto-legge 24 giugno 2014, n. 90, convertito con la legge 11 agosto 2014, n. 114 pubblicata in G.U. il 18 agosto 2014 ed in vigore dal 19 agosto 2014) per essere poi soppresso con il decreto-legge 16 luglio 2020, n. 76, art. 28.

179 del 2012 che dell'art. 16-*ter*, per stabilire che, ove la Pubblica Amministrazione non abbia comunicato il proprio domicilio digitale, le comunicazioni e notificazioni di cancelleria si eseguono mediante consegna in cancelleria, considerandosi dunque la mancata comunicazione una ipotesi legislativamente predeterminata di imputabilità della impossibilità di notificare telematicamente, e le notifiche su istanza di parte si eseguono ai sensi dell'art. 16-*ter*, comma 1-*ter* (v. *infra* capitolo successivo) (9). Il registro è consultabile, per i soggetti abilitati, previa autenticazione, nell'area riservata del Portale dei Servizi Telematici del Ministero della Giustizia.

L'INAD, infine, di nuovissima istituzione (giugno 2023) (10) costituisce la vera svolta per la concreta attuazione della notifica telematica, poiché è il domicilio digitale per i privati. Il suo limite, ad oggi, risiede nella facoltatività che — però — è destinata ad assottigliarsi con il tempo, anche in ragione della disciplina europea in arrivo (11).

Possono eleggere il proprio domicilio digitale mediante registrazione nell'INAD: *a*) le persone fisiche che abbiano compiuto il diciottesimo anno di età e che abbiano la capacità di agire; *b*) i professionisti che svolgono una professione non organizzata in ordini, albi o collegi ai sensi della legge 14 gennaio 2013, n. 4); *c*) gli enti di diritto privato non tenuti all'iscrizione nell'INI-PEC.

Il CAD, nell'art. 6-*quater*, ne affida la realizzazione e la gestione dell'INAD all'AgID (Agenzia per l'Italia Digitale), stabilendo che vi provveda avvalendosi delle strutture informatiche delle Camere di commercio già deputate alla gestione dell'elenco di cui all'articolo 6-*bis* (INI-PEC).

Mentre per i professionisti non iscritti in albi, registri o elenchi professionali (di cui all'articolo 6-*bis*), è prevista la possibilità di eleggere presso

---

(9) Il comma 1-*ter* dell'art. 16-*ter* del d.l. n. 179 del 2012 prevede: "*Fermo restando quanto previsto dal regio decreto 30 ottobre 1933, n. 1611, in materia di rappresentanza e difesa in giudizio dello Stato, in caso di mancata indicazione nell' elenco di cui all'articolo 16, comma 12, la notificazione alle pubbliche amministrazioni degli atti in materia civile, penale, amministrativa, contabile e stragiudiziale è validamente effettuata, a tutti gli effetti, al domicilio digitale indicato nell'elenco previsto dall'articolo* 6-ter *del decreto legislativo 7 marzo 2005, n. 82, e, ove nel predetto elenco risultino indicati, per la stessa amministrazione pubblica, più domicili digitali, la notificazione è effettuata presso l'indirizzo di posta elettronica certificata primario indicato, secondo le previsioni delle Linee guida di AgID, nella sezione ente dell'amministrazione pubblica destinataria. Nel caso in cui sussista l'obbligo di notifica degli atti introduttivi di giudizio in relazione a specifiche materie presso organi o articolazioni, anche territoriali, delle pubbliche amministrazioni, la notificazione può essere eseguita all'indirizzo di posta elettronica certificata espressamente indicato nell'elenco di cui all'articolo 6-ter del decreto legislativo 7 marzo 2005, n. 82, per detti organi o articolazioni*".

(10) https://domiciliodigitale.gov.it/dgit/home/public/#!/home.

(11) Il CAD prevede un costante allineamento tra INAD e ANPR.

l'INAD un domicilio digitale professionale e un domicilio digitale personale diverso dal primo, per i professionisti iscritti in albi ed elenchi il domicilio digitale INAD è il medesimo indirizzo inserito nell'elenco di cui all'articolo 6-*bis* (12) (fermo restando il diritto di eleggerne uno diverso ai sensi dell'articolo 3-*bis*, comma 1-*bis*, oppure, come già evidenziato *supra* di cancellarlo, per poter fruire della facoltatività di tale iscrizione come tutti gli altri privati) (13).

I soggetti che vogliano attivarlo devono accedere al servizio messo a disposizione dall'AgID, tramite la propria identità digitale. L'AgID ha pubblicato sul proprio sito istituzionale le relative Linee Guida, aggiornate l'8 agosto 2023 (14).

Alla data di completamento dell'Anagrafe Nazionale della Popolazione Residente (ANPR), i domicili digitali eletti dalle persone fisiche e iscritti nell'INAD saranno trasferiti al Ministero competente, come previsto all'articolo 6-*quater*, comma 3 del CAD, unitamente a tutti i dati oggetto di tracciamento, al fine di consentire l'accesso alle informazioni relative all'elezione, alla modifica o alla cessazione di ciascun domicilio digitale.

---

(12) Si prevede, ancora, nell'art. 6-*quater* che "Ai fini dell'inserimento dei domicili dei professionisti nel predetto elenco il Ministero dello sviluppo economico rende disponibili all'AgID, tramite servizi informatici individuati nelle Linee guida, i relativi indirizzi già contenuti nell'elenco di cui all'articolo 6-*bis*".

(13) In altre parole, per i professionisti iscritti nell'INI-PEC, l'indirizzo sarà inserito anche nell'INAD anche quale domicilio digitale "personale", salvo che il soggetto non decida di eleggerne uno diverso, quale persona fisica o scelga di volerlo cancellare. Sul punto infatti le linee guida rilasciate dall'AgID prevedono: qualora, entro 30 giorni dall'inserimento provvisorio di cui al precedente punto 2, il professionista non abbia usufruito della propria facoltà di modifica del domicilio digitale trasmesso dall'INI-PEC, il Gestore INAD provvede alla pubblicazione di quanto al richiamato punto 2. Qualora il professionista abbia optato per la modifica del domicilio digitale, al fine di eleggerne uno personale in INAD diverso da quello presente in INI-PEC, il Gestore INAD procede alla cancellazione del domicilio digitale inizialmente Linee Guida dell'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese Versione 2.1 - 08 agosto 2023 trasmesso dall'INI-PEC e alla pubblicazione del domicilio scelto. Successivamente alla pubblicazione, qualora il professionista opti per la cessazione del domicilio digitale in INAD, il Gestore procede alla cessazione del domicilio digitale inizialmente trasmesso dall'INI-PEC o di quello modificato, nei modi indicati dal paragrafo 2.3.1.

(14) https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_inad_ex_art._6quater_ CAD_0.pdf.

2.1.1. *Le modifiche introdotte dallo schema di decreto legislativo all'esame del parlamento* (15)

La ricostruzione fornita nel paragrafo precedente, risulta confermata dalle modifiche (volte ad un mero riordino) introdotte dallo schema di decreto correttivo già approvato dal Governo il 15 febbraio 2024 e, al momento di pubblicazione di questo contributo, all'esame delle Camere per il prescritto parere, ai sensi dell'articolo 1, comma 3, della legge 26 novembre 2021, n. 206.

Pur non trattandosi del testo definitivo, appare opportuno confrontarsi con lo schema di d.lgs. in discorso, poiché, per questa parte, risulta sostanzialmente ricognitivo e di risistemazione della normativa previgente. Ed infatti, in generale, (come si legge nella relazione di accompagnamento mutuata dalle "schede di lettura" corredate al testo in esame alla Camera dei deputati), "numerose disposizioni dello schema in commento "sono volte ad adeguare la formulazione del codice di rito al processo telematico" (16).

In particolare, proprio con riferimento al tema oggetto di questo volume, sono state adeguate in più punti le norme che introducono la facoltà delle parti di indicare, in luogo della residenza o dell'elezione di domicilio, l'indirizzo di posta elettronica certificata (PEC) risultante da pubblici elenchi o di eleggere un domicilio digitale speciale (comma 2, lett. *c*), n. 2; comma 5, lett. *d*); comma 7, lett. *c*); comma 8, lett. *b*), *g*), n. 1, *o*), *p*), *q*), *z*), n. 2).

Il novello art. 179-*septies*.1, in particolare, nella rubrica intitolata domicilio digitale, costituisce l'applicazione e specificazione dei concetti enucleati nel paragrafo che precede (17), ma va salutata con favore per il riordino che

---

(15) Lo schema del Decreto correttivo alla Riforma del processo civile, contenuta nel Decreto Legislativo n. 149 del 10 ottobre 2022 (Riforma Cartabia) trasmesso alle Camere per il prescritto parere, è leggibile sul sito della Camera https://temi.camera.it/leg19/dossier/OCD18-19766/disposizioni-integrative-e-correttive-al-d-lgs-149-2022-riforma-del-processo-civile.html

(16) "Espungendo i riferimenti al deposito in cancelleria di atti, alla nota di iscrizione a ruolo e alla stesura di provvedimenti in calce agli atti (si tratta, in particolare, delle disposizioni di cui al comma 1, lett. *c*), *e*), *l*) e *m*); comma 2, lett. *c*), n. 1, *l*), *p*), *q*), *r*), *s*), *z*), *bb*), *cc*), *dd*), *ee*), *mm*), n. 2, *nn*), n. 2, *oo*); comma 4, lett. *l*), *m*), *n*) e *o*); comma 5, lett. *b*), *c*), n. 2, *e*), *f*), *g*), *h*), n. 2, e *i*); comma 7, lett. *d*), *h*), n. 2, *l*), *m*), *n*), *o*), n. 2, *p*); comma 8, lett. *e*), *g*), n. 3, *h*), *i*), *m*), *n*), *r*), *t*), *u*), *z*)) nonché le previsioni relative all'obbligo del difensore di indicare il numero di fax negli atti (comma 1, lett. *f*)) e adeguando altresì al processo telematico le disposizioni sulla pubblicazione e comunicazione della sentenza (comma 1, lett. *i*)) e sulle comunicazioni di cancelleria, con l'eliminazione del "biglietto di cancelleria" e la previsione dell'uso della PEC (comma 1, lett. *n*))".

(17) Si legge nella relazione illustrativa, invero che la nuova norma La nuova norma recepisce le analoghe disposizioni contenute nel decreto-legge n. 179 del 2012.

introduce, attuando per tale via la legge delega e semplificando la interpretazione della normativa sul processo telematico.

Così, rispetto all'esaminato art. 16-*ter* d.l. 179/2012 che elencava i pubblici elenchi rilevanti ai fini della notificazione e della comunicazione non solo nella giustizia ordinaria, sia civile che penale, ma anche in quella amministrativa, contabile e nella materia stragiudiziale, la norma in esame, riferita specificamente al solo settore della giustizia civile:

1. Prevede che la notifica e la comunicazione al difensore (o alla parte presso il difensore) si eseguono ai domicili ricavati dai pubblici elenchi e spiega, poi, operando il riordino delle norme previgenti, che i pubblici elenchi rilevanti ai fini della notifica e della comunicazione telematiche nel processo civile sono quelli previsti dal CAD, che valgono in generale, ossia dagli articoli 6-*bis*, 6-*ter* e 6-*quater*.

2. A tali elenchi generali (già menzionati anche nella norma generale dell'art. 16-*ter* 179/2012), poi, aggiunge anche il REGINDE (il registro generale degli indirizzi elettronici gestito dal Ministero della Giustizia (ReGinDE art. 7, d.m. 21 febbraio 2011, n. 44) che, del resto, era a sua volta già presente nell'art. 16 ter del d.l. 179/2012, considerato pubblico elenco ai fini del processo, non solo ordinario.

3. La nuova norma in corso di approvazione, però, si preoccupa pure di regolare l'ipotesi in cui la parte stia in giudizio personalmente, per stabilire che per determinate categorie di soggetti elencati (per comodità di lettura, riportati di seguito con le lettere *a)*, *b)* e *c*)) tutte le omunicazioni e le notificazioni sono effettuate tramite posta elettronica certificata o servizio elettronico di recapito certificato qualificato, "ma" applicando quanto previsto dal neo introdotto settimo comma dell'articolo 149-*bis* del codice di procedura civile, e quindi in caso di impossibilità o mancato buon esito della notifica per causa imputabile al destinatario, con il deposito nell'area web dalla medesima norma prevista (18).

I soggetti richiamati per l'applicazione della suddetta disciplina di soggetti che stanno in giudizio personalmente, sono riferiti a:

a) chi già figuri in un pubbico elenco (e qui la norma in approvazione richiama l'art. 3-*bis* comma 1 del CAD, che si riferisce, però ai soggetti che

(18) Ed infatti, come si vedrà, lo schema di decreto interviene sulla disciplina della notificazione mediante PEC eseguita dall'ufficiale giudiziario *ex* art. 149-*bis*, al fine di semplificare gli adempimenti, omogeneizzare la disciplina con quella della notificazione effettuata con le modalità tradizionali e disciplinare il caso in cui la notifica a mezzo PEC non vada a buon fine, distinguendo le ipotesi in cui ciò avvenga per causa non imputabile al destinatario o a lui imputabile. In questo ultimo caso si prevede che l'ufficiale giudiziario la esegua mediante inserimento dell'atto da notificare nel portale dei servizi telematici gestito dal Ministero della giustizia (comma 1, lett. *o*)).

sono "obbligati" a iscriversi in elenchi, quali la pubblica amministrazione di cui all'art. 2 del medesimo CAD, che è obbligata a iscriversi all'indice PA dell'art. 6-*ter* del CAD, nonché i professionisti e gli imprenditori che, se ricadenti nell'obbligo, sono iscritti all'INIPEC);

b) chi si sia iscritto volontariamente nell'INAD (e qui la norma in approvazione richiama l'art. 3-*bis* comma 1-*bis* del CAD, che regola la facoltatività della iscrizione in tale registro per "chiunque");

c) chi abbia eletto un domicilio digitale speciale ai sensi dell'articolo 3-*bis*, comma 4-*quinquies*, del CAD (e qui la norma in apprivazione richiama il domicilio digitale "speciale" elettivo, più volte richiamato in questo volume a fini sistematici).

4. Opportunamente, poi, è "riordinata" la disciplina delle comunicazioni e notificazioni alle pubbliche amministrazioni, già evincibile dalle norme previgenti, per stabilire che le stesse, se stanno in giudizio attraverso propri dipendenti, sono effettuate agli indirizzi PEC comunicati secondo le disposizioni dell'articolo 16, comma 12, del decreto-legge n. 179 del 2012 (ossia il registro delle PA gestito dal Ministero della Giustizia); in mancanza di comunicazione di tale indirizzo, la notifica è effettuata presso il domicilio digitale indicato dell'elenco previsto dall'art. 6-*ter* del CAD, che regola l'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA).

Nel testo in corso di esame da parte del parlamento, va segnalata anche la modifica, in linea con quanto stabilito per la notifica, anche della comunicazione, poiché il nuovo art. 136 c.p.c prevede che la comunicazione sia effettuata dal cancelliere, a mezzo PEC, all'indirizzo risultante dai pubblici elenchi o al domicilio digitale speciale eletto ai sensi dell'articolo 3-*bis*, comma 4-*quinquies*, del codice dell'amministrazione digitale (19).

2.2. L'impervio cammino della notifica telematica intrecciato con le evoluzioni del domicilio digitale

La riforma introdotta dal decreto legislativo n. 149 del 2022 (cd. Riforma "Cartabia" civile) nel riscrivere e razionalizzare la disciplina delle notifiche, rendendo obbligatoria quella telematica e attribuendola definitivamente agli

(19) Anche per tale comunicazione, lo schema del correttivo prevede che quando non può essere eseguita o non ha esito positivo per causa non imputabile al destinatario, essa è trasmessa all'ufficiale giudiziario per la notifica. Se non può essere eseguita o non ha esito positivo per causa imputabile al destinatario, il cancelliere la esegue mediante inserimento dell'atto nel portale dei servizi telematici gestito dal Ministero della giustizia, con le modalità previste dall'articolo 149-*bis*.

avvocati, ha intrapreso un percorso evolutivo, tuttavia, ancora in corso nella ricerca di una modalità e di un luogo virtuale di consegna che consenta di ritenere perfezionata la notifica anche quando, come accade in molti casi, la stessa non sia andata a buon fine, poiché non risulta pervenuta la ricevuta di avvenuta consegna.

Che si tratti di un serio problema che condiziona la "digitalizzazione" dei procedimenti, è agevolmente intuibile, alla luce delle considerazioni scaturenti dalle pagine che precedono. Ed infatti non solo la notifica e la comunicazione telematica (rimesse come visto alla PEC) non sono materialmente possibili quando il destinatario non si è dotato di un domicilio digitale, ma anche quando questi non lo abbia "manutenuto", per esempio non provvedendo allo svuotamento della casella di posta elettronica che soffre di una capienza limitata per sua natura, oppure quando, pur essendo, il destinatario, un soggetto dotato per legge obbligato a dotarsi ad un certo momento di un domicilio digitale, poi in concreto, non lo abbia istituito o non lo abbia curato e "conservato".

La l. 21 gennaio 1994, n. 53 (facoltà di notificazioni di atti civili, amministrativi e stragiudiziali per gli avvocati e procuratori legali), del resto, nel disciplinare la notifica telematica degli avvocati (grazie all'innesto in tale normativa avvenuto nel 2012 dell'art. 3-*bis* ([20])) oggi resa centrale per effetto della riforma ([21]) rispetto all'intero procedimento notificatorio civile, sul punto, ha recepito in pieno la regolamentazione di cui al cit. d.p.r. 28 aprile 2005, n. 68, e al suo corpo di regole tecniche, stabilendo che, per il perfezionamento della notifica, occorre necessariamente la ricevuta di avvenuta consegna.

Tale disciplina, quindi, almeno fino ad oggi, ha precluso il "felice" completamento del procedimento notificatorio telematico, in tutti quei casi in cui la ricevuta di avvenuta consegna non sia spedita dal gestore del destinatario al mittente per fatti imputabili a quest'ultimo. Quei casi in cui,

---

([20]) L'art. 3-*bis* fu innestato nella vecchia (e inapplicata) legge sulla notifica in proprio degli avvocati, proprio da parte della legge 24 dicembre 2012, n. 228 (in SO n. 212, relativo alla G.U. 29 dicembre 2012, n. 302). Tale legge, nell'introdurre l'art. 16-*quater,* comma 1, lettera *d*) al d.l. 18 ottobre 2012, n. 179 (in S.O. n. 194 relativo alla G.U. 19 ottobre 2012, n. 245) convertito con modificazioni dalla l. 17 dicembre 2012, n. 221 (in S.O. n. 208, relativo alla G.U. 18 dicembre 2012, n. 294) ha conseguentemente disposto (con l'art. 1, comma 19, numero 2) l'introduzione dell'art. 3-*bis*.

([21]) Il decreto legislativo 10 ottobre 2022, n. 149 (in SO n. 38, relativo alla G.U. 17 ottobre 2022, n. 243) oltre a rimaneggiare l'art. 3-*bis*, ha introdotto il 3-*ter.* Altre modifiche sono poi intervenute per opera della legge 29 dicembre 2022, n. 197 (in SO n. 43, relativo alla G.U. 29 dicembre 2022, n. 303) e del decreto-legge 10 maggio 2023, n. 51 (in G.U. 10 maggio 2023, n. 108).

in buona sostanza, questa importante ricevuta che segna il momento perfezionativo, non sia prodotta, per una condotta del destinatario che, pure essendo un soggetto che avrebbe dovuto occuparsi della manutenzione del proprio domicilio PEC, si sia astenuto da tale condotta.

Proprio partendo da questa ultima considerazione si è anche sviluppato un orientamento giurisprudenziale della Corte di legittimità giunto in questi ultimi mesi al vaglio delle Sezioni Unite che dovrà esprimersi a breve (22). Oggetto di esame del Supremo collegio, infatti, proprio la interpretazione "adeguatrice" della disciplina processuale, proposta da alcune sentenze della Corte (interpretazione operante, tuttavia, una decisa forzatura del dato normativo in un terreno delicato come il contraddittorio) che hanno considerato legalmente consegnato il messaggio anche in caso di mancata consegna, addossando il mancato funzionamento del meccanismo ai destinatari purché soggetti tenuti per legge al domicilio digitale, obbligati dunque a curarlo, ma che se ne siano colpevolmente disinteressati.

Un ragionamento probabilmente non dissimile, a ben vedere, da quello che ha ispirato la norma del legislatore delegante la riforma civile, come vedremo, che all'art. 1, c. 20, lett. *b*) (legge 26 novembre 2021, n. 206) aveva richiesto la individuazione di un luogo virtuale presso il quale fosse possibile procedere alla notifica nei casi di impossibilità di perfezionamento (non essendo pervenuta la citata "fisiologica" ricevuta di avvenuta consegna) per causa imputabile al destinatario, stabilendo che solo in caso di non imputabilità si dovesse ricorrere alla notifica ordinaria (*rectius* tradizionale, analogica, attesa la ordinarietà della nuova notifica telematica obbligatoria).

Una strada, del resto, già seguita nel settore della comunicazione telematica di cancelleria, ove, per favorirne l'effettivo funzionamento e decollo, sin dal 2012 l'art. 16 del cit. d.l. n. 179 del 2012, al comma 6, aveva istituito un luogo virtuale per il medesimo ordine di casi (ossia la mancata consegna per causa imputabile al destinatario obbligato a manutenere l'indirizzo PEC), valorizzando la cd. "consegna in cancelleria".

E, perciò, da quanto accennato, che nel paragrafo seguente sarà approfondito, si evince che, ad oggi, sul piano normativo, anche se è predicata la obbligatorietà della notifica, il suo effettivo funzionamento è ancora acerbo poiché condizionato da fattori in parte fattuali in parte normativi. Sia i primi che i secondi sono in fase di evoluzione (23). Il domicilio digitale può essere obbligatorio o facoltativo, ma in ogni caso deve essere accompagnato da una "consapevolezza digitale" che possa rendere il sistema utile e affidabile.

---

(22) Sez. III, Ordinanza interlocutoria 21 novembre 2023, n. 32287.

(23) Si vedano, nel paragrafo seguente, le disposizioni dello schema di correttivo in corso di approvazione.

2.3. Il registro INAD e la notifica telematica obbligatoria della legge Cartabia

Il registro INAD assume notevole rilevanza alla luce della disciplina innovativa introdotta per la notificazione dal decreto legislativo n. 149 del 2022 (riforma Cartabia civile), poiché, nel quadro della generale digitalizzazione della giustizia civile e penale, la riforma ha sistematizzato la disciplina delle notifiche, rendendo obbligatoria quella telematica come visto, con un percorso normativo, tuttavia, ancora in corso.

Ed infatti, l'art. 1, comma 20, lett. *a*), legge-delega n. 206 del 2021 ha previsto, come sopra anticipato, che fosse resa obbligatoria la notifica telematica dell'avvocato tramite PEC nei confronti del soggetto dotato di domicilio digitale.

La medesima legge delega, poi (art. 1, c. 20, lett. *b*)) come accennato, ha richiesto la individuazione di un luogo virtuale presso il quale fosse possibile procedere alla notifica nei casi di impossibilità di perfezionamento (tramite la fisiologica ricevuta di avvenuta consegna) per causa imputabile al destinatario, stabilendo che, solo in caso di non imputabilità, si dovesse ricorrere alla notifica ordinaria (*rectius* tradizionale, analogica, attesa la guadagnata ordinarietà della nuova notifica telematica obbligatoria).

In base al testo della delega, dunque (art. 1, c. 20, lett. *c*)) la figura dell'ufficiale giudiziario diviene alquanto residuale, nella notifica, poiché ad essa deve farsi ricorso solo in caso di omesso perfezionamento per causa non imputabile al destinatario o di assenza fisiologica di domicilio digitale.

E, tuttavia, nella concreta realizzazione e riordino della disciplina della notifica non pochi problemi sono emersi, ed anche scostamenti (ammessi dallo stesso legislatore nella relazione di accompagnamento) dalla delega medesima.

Se infatti nella composita normativa della notifica, che risulta ora distribuita tra il codice di rito, tra il corpus principale (artt. 147, 147 e149-*bis*), le disposizioni di attuazione (art. 196-*octies* e ss.) oltre che nella legge 21 gennaio 1994, n. 53, spicca il nuovo articolo 3-*ter*, comma 1 di quest'ultima legge che introduce per l'avvocato l'obbligo di notifica telematica agli effetti pratici, la obbligatorietà non si accompagna sempre con l'effettività.

Certamente, e questo segna un grosso progresso, la notifica telematica risulta oggi possibile, ed anzi obbligatoria ([24]), anche nei confronti dei privati che abbiano volontariamente registrato un proprio domicilio digitale nell'I-

([24]) Dispone l'art. 3-*ter*, comma 1, che "L'avvocato esegue la notificazione degli atti giudiziali in materia civile e degli atti stragiudiziali a mezzo di posta elettronica certificata o servizio elettronico di recapito certificato qualificato quando il destinatario:

NAD divenuto effettivamente operativo dallo scorso 7 luglio 2023, quando sono state pubblicate dall'AgID le relative linee guida.

Tuttavia, nella prima formulazione della norma in commento, pur essendo predicata astrattamente la obbligatorietà della notifica telematica quanto il destinatario sia un soggetto dotato di un domicilio digitale, in concreto poi, solo se si tratta di un professionista o di un'impresa obbligati per legge (come visto) all'iscrizione nei pubblici elenchi, alla obbligatorietà consegue per legge la possibilità di completamento presso il luogo virtuale richiesto dalla legge delega.

Ed infatti, la notifica nell'area web (inizialmente individuata nell'area web riservata di cui all'art. 359 del codice della crisi di impresa e dell'insolvenza di cui al d.lgs. 12 gennaio 2019, n. 14, norma non attuata, in parte sospesa, come vedremo e attualmente in fase di modifica ad opera del cd d.lgs. "Correttivo Cartabia), e il conseguente perfezionamento a prescindere dall'effettivo completamento della trasmissione (ossia del recepimento della ricevuta di avvenuta consegna) risulta possibile solo in caso di destinatari che siano professionisti o imprese obbligati al domicilio digitale.

Se invece si tratta di un privato che si sia dotato di domicilio digitale (per aver esercitato la facoltà di iscrizione all'INAD, come evidenziato), pur permanendo la obbligatorietà della notifica telematica, ove per qualunque ragione, imputabile o non imputabile al destinatario, la notifica non vada a buon fine, risulta previsto il ricorso alla notifica "ordinaria" (*rectius* tradizionale) ([25]).

Lascia perplessi, peraltro, che analoga regola di favore sia stabilita anche nel caso di destinatario pubblica amministrazione (soggetto del pari obbligato per legge a dotarsi di domicilio digitale).

La disciplina descritta, tuttavia, come accennato, è stata in parte sospesa.

---

a) è un soggetto per il quale la legge prevede l'obbligo di munirsi di un domicilio digitale risultante dai pubblici elenchi;

b) ha eletto domicilio digitale ai sensi dell'articolo 3-*bis*, comma 1-*bis*, del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, iscritto nel pubblico elenco dei domicili digitali delle persone fisiche e degli altri enti di diritto privato non tenuti all'iscrizione in albi professionali o nel registro delle imprese ai sensi dell'articolo 6-quater del medesimo decreto".

([25]) La relazione illustrativa, al riguardo riconosce essersi trattato di "leggero discostamento dal principio di delega" ... "in considerazione della particolare delicatezza del procedimento notificatorio, che deve tendere ad assicurare quanto più possibile che il destinatario abbia effettiva conoscenza dell'atto" (in termini https://www.gnewsonline.it/riforma-del-processo-civile-la-relazione-illustrativa/).

Ed infatti, con l'art. 4-*ter*, del decreto-legge 10 maggio 2023, n. 51, convertito con modificazioni dalla l. 3 luglio 2023, n. 87 ([26]), si è stabilito che "L'efficacia delle disposizioni dei commi 2 e 3 dell'articolo 3-*ter* della l. 21 gennaio 1994, n. 53, introdotto dal decreto legislativo 10 ottobre 2022, n. 149, è sospesa fino al 31 dicembre 2023. Fino a tale data, quando la notificazione ai sensi del comma 1 dell'articolo 3-*ter* della citata l. n. 53 del 1994 non è possibile o non ha esito positivo, essa è eseguita con le modalità ordinarie e si perfeziona, per il soggetto notificante, nel momento in cui è generata la ricevuta di accettazione della notificazione dallo stesso inviata mediante posta elettronica certificata o servizio elettronico di recapito certificato qualificato".

La norma, che con ogni probabilità dovrà essere ulteriormente prorogata (atteso che il termine del 31 dicembre 2023 è decorso e, ad oggi, non risulta intervenuta ancora la previsione di una nuova area web) pur comprensibilmente dettata dall'intento di attribuire un senso all'obbligatorietà predicata dall'art. 1 del nuovo art. 3-*ter* l. n. 53 del 1995, nelle more predisposizione di un portale idoneo a consentire l'applicazione dei commi sospesi, desta alcune perplessità, poiché pare adattare la norma dell'art. 3-*bis* (dissociazione degli effetti della notifica tra notificante e destinatario), ad una situazione completamente diversa, ossia quella in cui la notifica sia iniziata telematicamente ma non si sia così perfezionata, e debba proseguire ordinariamente (ossia cartaceamente).

Fino ad ora, infatti, la scissione degli effetti della notifica (finanche nella giurisprudenza costituzionale) è stata sempre considerata all'interno del medesimo procedimento notificatorio (individuandosi momenti diversi di efficacia per mittente e destinatario, ma collegati alla stessa vicenda/notifica). In forza della disposizione in esame invece, sembra attribuito rilievo alla ricevuta di accettazione nell'ambito di un procedimento notificatorio "telematico" che, pacificamente, resterà incompleto per definizione e che dovrà essere rinnovato con modalità ordinaria (e, per ipotesi potrebbe non perfezionarsi neppure in quella modalità, per ragioni contingenti, almeno in prima battuta).

Si tratta sostanzialmente di una *fictio*, poiché, in base alla già richiamata normativa generale regolante la PEC (il cit. Decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27, della legge 16 gennaio 2003, n. 3), richiamata dalla legge n. 53 del 1994, la validità della trasmissione e ricezione del messaggio di posta elettronica certificata è

([26]) Intitolato: "Proroga in materia di disciplina delle notificazioni eseguite dagli avvocati ai sensi dell'articolo 3-*ter* della legge 21 gennaio 1994, n. 53".

attestata rispettivamente dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna, di cui all'articolo 6 (l'art. 6 del medesimo corpo normativo, che costituisce la base giuridico tecnica della PEC e che è richiamato da tutta la disciplina processuale che valorizza l'utilizzo della PEC medesima (in primis l'art. 3-*bis*, legge 21 gennaio 1994, n. 53).

In particolare tale norma prevede che "La notifica si perfeziona, per il soggetto notificante, nel momento in cui viene generata la ricevuta di accettazione prevista dall'articolo 6, comma 1, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e, per il destinatario, nel momento in cui viene generata la ricevuta di avvenuta consegna prevista dall'articolo 6, comma 2, del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, fermo quanto previsto dall'articolo 147, secondo e terzo comma, del codice di procedura civile".

Ne consegue che, sulla base della attuale disciplina, in caso di mancata consegna resta la possibilità di completare il procedimento notificatorio con la forma "ordinaria" tradizionale salvando la efficacia della mera ricevuta di accettazione.

Si verifica dunque, un caso di scissione "estrema" non tra momenti della (medesima) notifica telematica ma tra un tentativo di notifica telematica e poi una successiva notifica ordinaria.

La disposizione, tuttavia, può essere razionalizzata immaginando che il legislatore abbia voluto attribuire rilevanza giuridica al principio di affidamento in forza del quale il mittente che ritrova un indirizzo PEC in un pubblico elenco, si aspetta di realizzare efficacemente la notifica e, in caso di una condotta imputabile al destinatario (es. saturazione della capienza rappresenta, per l'inadeguata gestione dello spazio per l'archiviazione e la ricezione di nuovi messaggi), attraverso la disposizione in esame è protetto da eventuale prescrizione o decadenza in cui potrebbe incorrere.

Un ragionamento non dissimile, in realtà, da quello che ha determinato l'interpretazione della Corte di Cassazione ora al vaglio delle Sezioni Unite cit.

Concludendo, sul piano processuale, si può riepilogare che ad oggi lo scenario della notifica telematica è il seguente

La notifica telematica dell'avvocato è obbligatoria in due casi ([27]):

• A. DOMICILIO DIGITALE OBBLIGATORIO per LEGGE verso i soggetti che hanno l'obbligo di dotarsi di un domicilio digitale (ossia un indirizzo PEC);

• B. DOMICILIO DIGITALE FACOLTATIVO/ELETTIVO verso i soggetti che, pur non avendo l'obbligo, se ne siano dotati, iscrivendosi

([27]) Articolo 3-*ter* l. n. 53 del 1994.

volontariamente al registro INAD (6-*quater*), (I privati e i professionisti e le imprese non obbligati).

Tuttavia, a fronte della enunciata obbligatorietà, il concreto perfezionamento può essere frustrato nel caso della mancata ricezione della ricevuta di avvenuta consegna con il solo temperamento del rilievo la ricevuta di accettazione, se accompagnata poi da successiva notifica ordinaria (ossia analogica e tradizionale).

Occorre, tuttavia, evidenziare come la disciplina contenuta nel cd. Correttivo della riforma civile, ossia lo schema di decreto legislativo all'esame del Parlamento più volte citato, si appresta a porre rimedio ai problemi evidenziati.

Ed infatti, oltre ad aver posto in linea il processo civile con le disposizioni sul domicilio digitale, anche elettivo, con apposite norme già sopra esposte, lo schema di decreto è intervenuto sulla disciplina della notifica telematica, sia dell'avvocato che dell'ufficiale giudiziario, nonché sulla comunicazione di cancelleria.

Vanno segnalate, al riguardo, le disposizioni dell'art. 6 comma 3, che reca modifiche alla legge 21 gennaio 1994, n. 53, relativa alle notificazioni eseguite dall'avvocato (oggi divenute obbligatorie in forma telematica salvo impossibilità) e quelle dell'art. 3 comma 1 lett. *o*), che modificano l'art. 149-*bis* c.p.c che disciplina la notificazione a mezzo posta elettronica certificata eseguita dall'ufficiale giudiziario. In particolare risultano uniformate le conseguenze della impossibilità di recapito del messaggio.

Ciò che è davvero significativo è la previsione per la quale se il recapito non è possibile per causa imputabile al destinatario l'atto da notificare viene inserito in un'apposita area riservata creata sul portale dei servizi telematici del Ministero della giustizia (disciplina dettata, come visto, anche per la comunicazione); in entrambi i casi il perfezionamento per il destinatario si conseguirà nel decimo giorno successivo all'inserimento dell'atto nel portale o, se anteriore, nella data in cui il destinatario stesso accede all'area riservata. Nel caso in cui invece il mancato recapito sia stato determinato da causa non imputabile al destinatario, la notifica sarà eseguita dall'avvocato o dall'ufficiale giudiziario nelle forme "analogiche" . Come visto, analoghe disposizioni sono dettate per la comunicazione di cancelleria, con conseguenze anche sulle disposizioni dell'art. 16 del d.l. 179/2012, per il caso di comunicazione non perfezionata per ragioni imputabili al destinatario.

III.
IL DOMICILIO DIGITALE NELLE COMUNICAZIONI DI CANCELLERIA

di *Ileana Fedele*

Sommario: 3.1. Premessa. — 3.2. La disciplina delle comunicazioni e notificazioni telematiche di cancelleria. — 3.3. Applicazione giurisprudenziale. — 3.3.1. Oneri di gestione della casella PEC a cura del difensore. — 3.4. La questione dell'ammissibilità dell'elezione di domicilio digitale. — 3.5. Il rapporto con la tradizionale figura del domiciliatario. — 3.6. Considerazioni conclusive.

3.1. Premessa

La figura del domicilio digitale segna l'evoluzione del tradizionale concetto di "domicilio" — collegato ad un'ubicazione fisica — verso la sua virtualizzazione mediante l'individuazione di un recapito telematico, assistito da determinate garanzie di affidabilità. La sua adozione nel processo civile (1), dapprima in virtù di elaborazione giurisprudenziale, successivamente recepita dal legislatore nel quadro della disciplina speciale sul c.d. processo civile telematico, è stata incentrata sull'uso della posta elettronica certificata (PEC), quale strumento che offre garanzie in ordine all'identità degli autori della comunicazione, all'invio e alla ricezione dei messaggi, al riferimento temporale, assicurando anche l'integrità e l'autenticità del messaggio.

La possibilità di comunicare speditamente con i difensori grazie ad un mezzo sicuro, senza ricorrere al tramite dell'ufficiale giudiziario, ha trasformato la stessa fisionomia delle comunicazioni e notificazioni di cancelleria, in quanto, non solo ha consentito di procedere all'adempimento in maniera semplice ed immediata — in tal modo snellendo anche i tempi necessari — ma ha anche reso possibile trasmettere con la comunicazione il testo integrale del provvedimento (ormai digitalizzato) in luogo dell'estratto, sì da rendere praticamente incerti i confini tra comunicazione e notificazione a cura della

(1) Sul tema generale, così come sulla questione dell'ammissibilità dell'elezione di domicilio virtuale, sia consentito il rinvio a I. Fedele, *Il domicilio digitale nel diritto processuale civile: nozione e profili applicativi*, in *ilprocesso civile.it*, 17 luglio 2019.

cancelleria se non per le specifiche disposizioni del codice di rito ovvero di leggi speciali che, di volta in volta, continuano a prescrivere la mera comunicazione ovvero la notificazione degli atti.

Ai fini della ritualità dell'adempimento è diventato, dunque, fondamentale procedere alla corretta individuazione del domicilio digitale da utilizzare a fini processuali, anche in rapporto alla tradizionale figura del domiciliatario.

Per completezza, si accenna qui [2] che, a seguito delle modifiche apportate al d.lgs. 7 marzo 2005, n. 82 (CAD - Codice dell'Amministrazione Digitale) per allineare l'ordinamento italiano al Regolamento UE n. 910/2014 (*eIDAS - electronic IDentification Authentication and Signature*), il concetto di domicilio digitale, a livello generale, è stato adeguato (art. 1, comma 1, lett. *n-ter*) CAD) per recepire le nozioni di "servizio elettronico di recapito certificato" (art. 3, n. 36, Regolamento *eIDAS*) ovvero di "servizio elettronico di recapito certificato qualificato" qualificato (art. 3, n. 37, Regolamento *eIDAS*, che rinvia all'art. 44 del medesimo regolamento), quali standard noti a livello sovranazionale. In prosieguo, dunque, occorrerà seguire l'ulteriore sviluppo della normativa sul PCT — che prevale in virtù del principio di specialità ormai espressamente sancito dall'art. 2, comma 6, del CAD — e, comunque, interpretare le relative disposizioni in conformità alle cogenti indicazioni del Regolamento europeo, che ormai si riferiscono a soluzioni tecniche diversificate rispetto alla PEC.

3.2. La disciplina delle comunicazioni e notificazioni telematiche di cancelleria

In esito a successivi interventi normativi [3], l'attuale disciplina delle comunicazioni e notificazioni telematiche a cura della cancelleria si trova articolata nell'art. 136 c.p.c., nell'art. 45 disp. att. c.p.c., nell'art. l'art. 16, d.l. 18 ottobre 2012, n. 179, conv. con modif. dalla l. 17 dicembre 2012, n. 221, e successive modificazioni, nelle regole tecniche stabilite dall'art. 16, d.m. 21 febbraio 2011, n. 44, e nelle specifiche tecniche — previste dall'articolo 34,

---

[2] Si rinvia per l'analisi approfondita sul punto ai contributi inseriti in questo volume *Il concetto di domicilio e identità digitale nel quadro generale tra normativa interna ed europea (CAD; EIDAS, Norme speciali)*, a cura di A. Ciriello, e *Identificazione in rete: identità digitale e identità personale*, a cura di A. Mazzeo e M. Nastri, nel cui ambito è esaminato anche il nuovo quadro normativo europeo di riferimento che si profila con il c.d. Regolamento *eIDAS* 2.0, in corso di approvazione.

[3] Sull'evoluzione normativa in tema di comunicazioni e notificazioni di cancelleria, si rinvia all'analitica relazione dell'Ufficio del massimario e del ruolo n. 183 del 15 dicembre 2015, a cura di G. Fichera.

comma 1, del d.m. n. 44 del 2011 — di cui al provvedimento 16 aprile 2014 (modificato in data 28 dicembre 2015 e 30 luglio 2021) del Responsabile per i sistemi informativi automatizzati del Ministero della giustizia.

Secondo l'art. 136, comma 2, c.p.c., nell'attuale versione, il biglietto di cancelleria è consegnato dal cancelliere al destinatario, che ne rilascia ricevuta, ovvero trasmesso a mezzo posta elettronica certificata, nel rispetto della normativa anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Il terzo comma prevede che — salvo che la legge disponga diversamente — se non è possibile procedere a mezzo PEC, il biglietto è rimesso all'ufficiale giudiziario per la notifica. Pertanto, l'unica modifica apportata dal d.lgs. 10 ottobre 2022, n. 149, è stata l'eliminazione della possibilità — già prevista dal terzo comma in alternativa alla rimessione all'ufficiale giudiziario — di procedere alla comunicazione del biglietto a mezzo *telefax*, tecnologia ormai superata. Con la medesima riforma, è stato adeguato l'art. 366 c.p.c., per il giudizio in cassazione, dal quale è stato soppresso il secondo comma, eliminando la necessità di elezione di domicilio fisico in Roma (ormai superata dal domicilio digitale), ed il quarto comma, riconducendo le comunicazioni di cancelleria e le notificazioni tra avvocati alla disciplina generale di cui all'art. 136, commi 2 e 3, c.p.c.

La previsione in ordine alla integrale comunicazione del provvedimento è contenuta nel secondo comma dell'art. 45 disp. att. c.p.c. (siccome modificato dall'art. 16, comma 3, del d.l. n. 179 del 2012, cit.), secondo cui il "il biglietto contiene in ogni caso [...] il nome delle parti ed il testo integrale del provvedimento comunicato (4)", mentre, il quarto comma del medesimo articolo (nella versione modificata sempre dall'art. 16, comma 3, del del d.l. n. 179 del 2012, cit.) prevede che, nell'ipotesi di trasmissione a mezzo PEC, il "biglietto di cancelleria è costituito dal messaggio di posta elettronica certificata, formato ed inviato nel rispetto della normativa, anche regolamentare, concernente la trasmissione e ricezione dei documenti informatici".

Per la ricostruzione completa della disciplina di riferimento, occorre, tuttavia, procedere alla lettura 'integrata' delle disposizioni del codice di rito con la normativa speciale sul processo telematico, cui l'art. 136 c.p.c. e l'art. 45 disp. att. c.p.c. espressamente rinviano (5).

---

(4) L'art. 133 c.p.c. è stato opportunamente modificato, con la precisazione, al secondo comma, che la comunicazione non è idonea a far decorrere i termini per le impugnazioni di cui all'art. 325 c.p.c., salva diversa e speciale disposizione normativa, che colleghi la decorrenza del termine breve di impugnazione alla mera comunicazione del provvedimento da parte della cancelleria.

(5) L'art. 1, comma 17, lett. *h*), della legge delega 26 ottobre 2021, n. 206, aveva in effetti indicato il principio di delega inteso al riordinamento della materia ("introdurre, in

Infatti, la previsione sulla modalità ordinaria delle comunicazioni/notificazioni a cura della cancelleria si rinviene nell'art. l'art. 16, comma 4, del d.l. n. 179 del 2012 cit., ai sensi del quale "nei procedimenti civili [...] le comunicazioni e le notificazioni a cura della cancelleria sono effettuate esclusivamente per via telematica all'indirizzo di posta elettronica certificata risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni, secondo la normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici". La norma, dunque, prevede l'obbligo della modalità telematica, da eseguire all'indirizzo PEC risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni ovvero all'indirizzo PEC che la parte che sta in giudizio personalmente abbia eventualmente indicato (art. 16, comma 7, del d.l. n. 179 del 2012 cit.), mentre per le pubbliche amministrazioni rilevano unicamente gli indirizzi PEC comunicati al Ministero della giustizia ed inseriti nell'apposito registro (art. 16, comma 12, del d.l. n. 179 del 2012 cit.).

Le regole tecniche (art. 16, comma 3, del d.m. n. 44 del 2011 cit.) stabiliscono la disciplina di dettaglio, relativa alla natura e alla prova dell'esito della comunicazione (ossia la ricevuta di avvenuta consegna — c.d. RdAC — conservata nel fascicolo informatico), stabilendo che "La comunicazione per via telematica si intende perfezionata nel momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del destinatario".

Le specifiche tecniche (art. 17 del decreto dirigenziale S.I.A.) scendono ulteriormente nel dettaglio tecnico, prevedendo che "Il gestore dei servizi telematici provvede ad inviare le comunicazioni o le notificazioni per via telematica, provenienti dall'ufficio giudiziario, alla casella di posta elettronica certificata del soggetto abilitato esterno o dell'utente privato destinatario, recuperando il relativo indirizzo dai pubblici elenchi ai sensi dell'art. 16-*ter* , decreto legge 30 ottobre 2012, n. 179 oppure ai sensi dell'art. 16, comma 7, del medesimo decreto; [...] Il gestore dei servizi telematici recupera le ricevute della posta elettronica certificata e gli avvisi di mancata consegna dal gestore di PEC del Ministero e li conserva nel fascicolo informatico; la ricevuta di avvenuta consegna è di tipo breve per le comunicazioni e di tipo completo per le notificazioni".

---

funzione dell'attuazione dei principi e criteri direttivi di cui alla presente legge, misure di riordino e implementazione delle disposizioni in materia di processo civile telematico"), anche nell'intento di semplificare la 'ricomposizione' della normativa processuale; tale riordino, ad esempio, è stato operato per il deposito telematico degli atti (con inserimento delle disposizioni già contenute nell'art. 16-*bis*, d.l. n. 179 del 2012 cit. nell'art. 196-*quater,* disp. att. c.p.c.), ma non, ad esempio, per le comunicazioni di cancelleria, la cui disciplina è rimasta nell'art. 16 del d.l. n. 179 del 2012.

Per il caso in cui la notificazione o comunicazione contenga dati sensibili, la cancelleria provvede ad inviare solo l'estratto con contestuale messa a disposizione dell'atto, sul sito *internet* individuato dall'amministrazione (art. 16, comma 5, del d.l. n. 179 del 2012 cit.). Il precetto è integrato dalle regole tecniche, il cui art. 16, comma 6, prevede che "La comunicazione che contiene dati sensibili è effettuata per estratto con contestuale messa a disposizione dell'atto integrale nell'apposita area del portale dei servizi telematici, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34 e nel rispetto dei requisiti di sicurezza di cui all'articolo 26, con modalità tali da garantire l'identificazione dell'autore dell'accesso e la tracciabilità delle relative attività", precisando altresì che, in tal caso, "la comunicazione si intende perfezionata il giorno feriale successivo al momento in cui viene generata la ricevuta di avvenuta consegna da parte del gestore di posta elettronica certificata del destinatario" (art. 16, comma 7, del d.m. n. 44 del 2011). La disciplina di dettaglio è prevista dall'art. 18 delle specifiche tecniche.

Il passaggio fondamentale della disciplina dettata dall'art. 16 del d.l. n. 179 del 2012 cit. è rappresentato dal raccordo fra l'obbligatorietà della modalità telematica e la 'sanzione' della comunicazione/notificazione in cancelleria per l'ipotesi di impossibilità collegata alla mancata istituzione dell'indirizzo PEC per i soggetti che vi sono tenuti ovvero per l'esito negativo del messaggio imputabile al destinatario. Infatti, il comma 6 prevede espressamente che "Le notificazioni e comunicazioni ai soggetti [...] per i quali la legge prevede l'obbligo di munirsi di un indirizzo di posta elettronica certificata, che non hanno provveduto ad istituire o comunicare il predetto indirizzo, sono eseguite esclusivamente mediante deposito in cancelleria. Le stesse modalità si adottano nelle ipotesi di mancata consegna del messaggio di posta elettronica certificata per cause imputabili al destinatario". In caso di mancata consegna, è possibile consultare sul portale dei servizi telematici ("pst") l'avviso di avvenuta comunicazione o notificazione dell'atto nella cancelleria o segreteria dell'ufficio giudiziario (art. 16, comma 4, d.m. n. 44 del 2011 cit.). Pertanto, va qui rimarcato che, a differenza di quanto previsto dalla normativa sulla notificazione telematica ad istanza dei difensori, ai sensi della l. 21 gennaio 1994, n. 53 — almeno sino alle modifiche apportate dalla riforma di cui al d.lgs. n. 149 del 2022, cit. — l'art. 16 prevede espressamente non solo la 'sanzione' del deposito in cancelleria, ma anche la modalità attraverso cui, in caso di mancata consegna, il destinatario del messaggio può rinvenire l'avviso di avvenuta comunicazione o notificazione dell'atto stesso (per l'appunto, sul portale dei servizi telematici); ciò che, pertanto, parrebbe evidenziare che, almeno fino alla richiamata modifica, con l'introduzione dell'art. 3-*ter* della l. n. 53 del 1994, nessun meccanismo similare era previsto

per l'ipotesi di mancata notifica telematica a cura del difensore, sia pure per causa imputabile al destinatario (6).

In definitiva, alla comunicazione/notificazione in cancelleria si provvederà in tutti casi in cui il domicilio digitale è imposto dalla legge (è il caso della pubblica amministrazione, ove non abbia istituito o comunicato il proprio indirizzo ai fini del suo inserimento nel registro delle PP.AA., gestito dal Ministero della Giustizia, ai sensi del medesimo art. 16, comma 12, nonché dei professionisti — ivi compresi i difensori — e delle imprese, obbligati a munirsi di domicilio digitale) e — tuttavia — non si renda possibile effettuare la consegna, con il solo limite della non imputabilità della stessa al destinatario (commi 6-8). In tale ultima ipotesi, come pure allorché l'obbligo del domicilio digitale non sia imposto dalla legge (come accade per i privati cittadini che stiano in giudizio personalmente e che non abbiano indicato un domicilio digitale) l'atto dovrà essere trasmesso con modalità tradizionali, ai sensi degli artt. 136, comma 3, e 137 c.p.c.

Come anticipato nelle premesse, la norma ha 'rivoluzionato' le comunicazioni/notificazioni a cura della cancelleria per le immediate ricadute in termini di risparmio di tempo e di risorse, consentendo al personale amministrativo di provvedere direttamente all'adempimento attraverso le funzionalità integrate nei registri informatizzati, con l'invio del messaggio di PEC all'indirizzo rinvenuto automaticamente attraverso la valorizzazione del codice fiscale del difensore. Effettuata la consegna (ovvero certificata la mancata consegna), l'applicazione ministeriale restituisce la ricevuta, che vale come relata di notifica, e viene conservata nel fascicolo informatico.

Tutto l'impianto delle comunicazioni/notificazioni di cancelleria, pertanto, "ruota" intorno ad un indirizzo PEC particolarmente qualificato perché censito in pubblici elenchi, per tali dovendosi intendere quelli contemplati dall'art. 16-*ter* del d.l. n. 179 del 2012 cit., per la cui disamina si rinvia agli specifici contributi contenuti in questo volume (7).

In questa sede si ritiene tuttavia opportuno evidenziare che, in ordine al domicilio digitale delle PP.A. ai fini delle comunicazioni/notificazioni di

---

(6) Sul tema, si rinvia alla apposita trattazione svolta nel contributo di questo volume a cura di A. Ciriello, *Il domicilio digitale nella notifica. Applicazione delle categorie del domicilio digitale speciale e di piattaforma in seguito a norme recenti*, limitandosi qui ad evidenziare che la questione è stata di recente rimessa alle Sezioni Unite civili con ordinanza interlocutoria del 21 novembre 2023, n. 32287.

(7) In particolare, v. A. Ciriello, *Il domicilio digitale nella notifica. Applicazione delle categorie del domicilio digitale speciale e di piattaforma in seguito a norme recenti*, cit., e R. Arcella, con particolare riferimento all'INAD (Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese), di cui all'art. 6-*quater* del CAD.

cancelleria, il riferimento è univocamente contenuto nella disposizione di cui al citato comma 12 dell'art. 16, d.l. n. 179 del 2012, nella versione modificata dall'art. 28, comma 1, lettera *a*), del d.l. 16 luglio 2020, n. 76, conv, con modif. dalla l. 11 settembre 2020, n. 120, che prevede la possibilità per l'amministrazione di comunicare, accanto all'indirizzo principale, "altresì gli indirizzi di posta elettronica certificata di propri organi o articolazioni, anche territoriali, presso cui eseguire le comunicazioni o notificazioni per via telematica nel caso in cui sia stabilito presso questi l'obbligo di notifica degli atti introduttivi di giudizio in relazione a specifiche materie ovvero in caso di autonoma capacità o legittimazione processuale" (quindi, la possibilità di indicare indirizzi territoriali o secondari) nonché "Per il caso di costituzione in giudizio tramite propri dipendenti [...] ulteriori indirizzi di posta elettronica certificata, riportati in una speciale sezione dello stesso elenco di cui al presente articolo e corrispondenti a specifiche aree organizzative omogenee, presso cui eleggono domicilio ai fini del giudizio" (vale a dire la possibilità di indicare direttamente gli indirizzi PEC presso cui effettuare le comunicazioni in caso di costituzione in giudizio tramite propri funzionari), rinviandosi per le modalità tecniche con cui le comunicazioni vanno eseguite agli artt. 9-*bis* e 9-*ter* delle specifiche tecniche, nella versione modificata con il provvedimento del 30 luglio 2021.

Infatti, secondo il comma 13 del medesimo articolo 16, d.l. n. 179 del 2012, "In caso di mancata comunicazione ai sensi del comma 12, le comunicazioni e notificazioni a cura della cancelleria si effettuano ai sensi dei commi 6 e 8", vale a dire che, nel caso la P.A. abbia omesso di comunicazione l'indirizzo (o gli indirizzi, secondo la modifica intervenuta nel 2020) ai sensi del comma 12, la comunicazione/notificazione si esegue mediante deposito in cancelleria. Pertanto, a differenza di quanto previsto per la notificazione telematica ad istanza dei difensori, almeno sino alla modifica intervenuta nel 2020, in esito alla quale è stata riattivata la possibilità — in via sussidiaria — di utilizzare gli indirizzi PEC riportati nell'IPA [8] — in caso di mancata comunicazione/notificazione di cancelleria l'adempimento si ha per eseguito in cancelleria, senza necessità di rinnovarlo a mezzo dell'ufficiale giudiziario. Potrebbe, tuttavia, profilarsi il dubbio se, nell'ipotesi di pluralità di indirizzi riportati nel registro delle PP.AA. per la singola amministrazione, la cancelleria sia chiamata a discernere quale sia l'indirizzo PEC utilizzabile per il giudizio (ad esempio, quello corrispondente alla sede territoriale ovvero quello riferibile all'elezione di domicilio in caso di costituzione in giudizio tramite propri funzionari) ovvero se la comunicazione all'indirizzo PEC

[8] Per la completa ricostruzione del domicilio delle PP.AA. si rinvia all'apposito contributo a cura di M. La Greca contenuto nel volume.

'principale' ovvero ad un qualunque indirizzo riportato nel registro possa valere a considerare correttamente effettuato l'adempimento.

3.3. Applicazione giurisprudenziale (9)

In applicazione delle citate disposizioni, Cass. 22 dicembre 2016, n. 26773, ha sostenuto che "A seguito delle modifiche al processo civile apportate dall'art. 16, comma 4, d.l. n. 179 del 2012, conv., con modif., dalla l. n. 221 del 2012, le comunicazioni e notificazioni a cura della cancelleria si effettuano, per via telematica, all'indirizzo di posta elettronica certificata (PEC) del destinatario e la trasmissione del documento informatico, equivalente alla notificazione a mezzo posta, si intende perfezionata, con riferimento alla data e all'ora della sua ricezione, quando la stessa sia avvenuta in conformità alle disposizioni di cui al d.p.r. 28 aprile 2005, n. 68, il cui art. 6 stabilisce che il gestore della PEC utilizzata dal destinatario deve fornire al mittente, presso il suo indirizzo elettronico, la cd. ricevuta di avvenuta consegna (RAC), che costituisce, quindi, il documento idoneo a dimostrare, fino a prova del contrario, che il messaggio informatico è pervenuto nella casella di posta elettronica del destinatario." (in senso conforme Cass. 26 novembre 2018, n. 30532). Più di recente, Cass. 25 agosto 2020, n. 17662, ha ribadito che, quando il sistema genera la ricevuta di accettazione e consegna del messaggio nella casella del destinatario, si determina una presunzione di conoscenza da parte dello stesso, con conseguente onere a carico del destinatario di dimostrare le difficoltà di cognizione del contenuto della comunicazione correlate all'utilizzo dello strumento informatico.

In aderenza al dettato normativo, è stato quindi affermato che la mancata consegna all'avvocato della comunicazione o notificazione inviatagli a mezzo PEC produce effetti diversi a seconda che gli sia o meno imputabile: nel primo caso, le notificazioni/comunicazioni saranno eseguite esclusivamente mediante deposito in cancelleria; nel secondo, attraverso l'utilizzo delle forme ordinarie previste dal codice di rito (Cass. 18 febbraio 2020, n. 3965).

Le predette disposizioni hanno trovato applicazione anche nel giudizio di cassazione a seguito dell'emanazione dell'apposito decreto ministeriale, osservandosi che "La notificazione al difensore del decreto di fissazione dell'adunanza in camera di consiglio e della proposta del relatore, *ex* art. 380-*bis* c.p.c., ove eseguita successivamente al 15 febbraio 2016 (data di

(9) Sul punto, sia consentito il richiamo alla Rassegna tematica della giurisprudenza di legittimità sul processo civile telematico dell'Ufficio del Massimario e del Ruolo, a cura di I. Fedele, pubblicata sul sito istituzionale, con la precisazione che le citazioni sono tratte dall'archivio di *Italgiure* dedicato alla massimazione ufficiale.

entrata in vigore del d.m. 19 gennaio 2016, n. 63), va necessariamente compiuta per via telematica, *ex* art. 16, comma 4, del d.l. n. 179 del 2012, conv., con modif., dalla l. n. 221 del 2012, salva la possibilità di procedere secondo quanto previsto dai successivi commi 6 ed 8 del medesimo art. 16 — e, cioè, mediante deposito presso la cancelleria ovvero ai sensi degli artt. 136, comma 3, e 137 ss. c.p.c. — per il caso di impossibilità, imputabile o meno al destinatario, di ricorrere alla posta elettronica certificata" (Cass. 13 marzo 2017, n. 6369).

3.3.1. *Oneri di gestione della casella PEC a cura del difensore*

La disposta obbligatorietà delle comunicazioni e notificazioni telematiche, con le conseguenze previste in ordine al deposito dell'atto in cancelleria nell'ipotesi di mancata consegna del messaggio PEC per cause imputabili al destinatario, ha comportato l'approfondimento delle ipotesi in cui va riconosciuta la responsabilità del difensore in ordine alla corretta tenuta e consultazione della casella PEC.

In riferimento al giudizio di cassazione, Cass. 23 febbraio 2021, n. 4920, ha precisato che, ai fini della ritualità della comunicazione dell'avviso di fissazione dell'adunanza camerale, l'indicazione, nel ricorso, del codice fiscale del difensore, pur in mancanza di quella del relativo indirizzo PEC, comporta l'automatica domiciliazione nel proprio indirizzo figurante obbligatoriamente dal ReGIndE, sicché correttamente la cancelleria, a norma del combinato disposto degli artt. 366, ultimo comma, e 136, comma 2, c.p.c., procede all'individuazione della PEC dal ReGIndE e all'esecuzione della comunicazione presso la relativa casella; pertanto, ove la comunicazione inviata all'esito di tale individuazione non vada a buon fine per rifiuto da parte della casella di P.E.C. del destinatario, la mancata consegna dell'avviso deve ritenersi imputabile al difensore e la cancelleria non è onerata di procedere al rinnovo dell'atto attraverso una nuova comunicazione a mezzo posta, che, se effettuata tardivamente, resta irrilevante.

Più in generale, è stato osservato "Una volta ottenuta dall'ufficio giudiziario l'abilitazione all'utilizzo del sistema di posta elettronica certificata, l'avvocato, che abbia effettuato la comunicazione del proprio indirizzo di PEC al Ministero della Giustizia per il tramite del Consiglio dell'Ordine di appartenenza, diventa responsabile della gestione della propria utenza, nel senso che ha l'onere di procedere alla periodica verifica delle comunicazioni regolarmente inviategli dalla cancelleria a tale indirizzo, indicato negli atti processuali, non potendo far valere la circostanza della mancata apertura della posta per ottenere la concessione di nuovi termini per compiere attività processuali" (Cass. 2 luglio 2014, n. 15070); nel caso di specie è stata, quindi,

confermata la statuizione di improcedibilità del ricorso in appello perché il difensore non aveva proceduto ad effettuare la notifica alla controparte del decreto di fissazione dell'udienza di discussione, unitamente all'atto di appello, entro il termine di rito benché il decreto gli fosse stato ritualmente comunicato a mezzo PEC.

In senso analogo, è stata confermata la statuizione di inammissibilità per tardività dell'opposizione *ex* art. 1, comma 51, della legge 28 giugno 2012, n. 92, proposta avverso l'ordinanza che aveva rigettato l'impugnativa di licenziamento, considerato che, a seguito di comunicazione del provvedimento effettuata in via telematica con esito negativo per causa imputabile al difensore, l'atto era stato depositato in cancelleria, come previsto dalla norma, senza necessità di procedere alla notifica a mezzo *fax* (Cass. 23 gennaio 2018, n. 164720).

Il principio è stato ribadito con specifico riferimento al caso della mancata comunicazione per saturazione della casella di posta elettronica: "Il mancato buon esito della comunicazione telematica di un provvedimento giurisdizionale, dovuto alla saturazione della capienza della casella di posta elettronica del destinatario, è un evento imputabile a quest'ultimo, in ragione dell'inadeguata gestione dello spazio per l'archiviazione e la ricezione di nuovi messaggi, sicché legittima l'effettuazione della comunicazione mediante deposito dell'atto in cancelleria, ai sensi dell'art. 16, comma 6, d.l. n. 179 del 2012, conv. in l. n. 221 del 2012, come modificato dall'art. 47, d.l. 24 giugno 2014, n. 90, conv. in l. 11 agosto 2014, n. 114" (Cass. 21 marzo 2018, n. 7029; in senso conforme, sulla saturazione della casella come evento imputabile al destinatario, fra molte, Cass. 20 maggio 2019, n. 13532).

Nello stesso senso, Cass. 20 settembre 2021, n. 25426, ha ritenuto imputabile al destinatario la mancata ricezione della comunicazione a mezzo PEC di un provvedimento giurisdizionale dalla cancelleria al difensore, per l'impossibilità per il gestore della posta elettronica di completare la consegna per essere la casella inibita alla ricezione, difettando una ragione tecnica ascrivibile a terzi tale da scriminare la negligenza del titolare, con conseguente legittimità dell'effettuazione della comunicazione mediante deposito dell'atto in cancelleria.

È stato anche prospettato un particolare onere di attivazione del difensore in ordine alla configurazione delle proprie dotazioni informatiche per la lettura di documenti informatici comunicati dalla cancelleria in formato compresso: "In materia di prova testimoniale, la parte che non abbia provveduto all'intimazione dei testi ammessi non può sottrarsi alla relativa decadenza deducendo l'asserita violazione dalla normativa vigente in materia di comunicazioni telematiche, per essere stato utilizzato — ai fini della comunicazione dell'ordinanza di ammissione della prova — il formato cd.

"pdf zip", giacché il suo impiego non muta il contenuto del documento informatico, ma comprime lo stesso in modo che occupi uno spazio minore, sicché il difensore non può invocare su queste basi la scusabilità nell'errore in cui sia incorso, potendo dal medesimo esigersi l'utilizzo di idonea configurazione del computer tale da consentire l'accesso al documento nel formato compresso." (Cass. 20 luglio 2016, n. 14827).

Altro caso che evoca gli oneri di corretta gestione della casella PEC da parte del difensore è quello in cui la comunicazione telematica di un provvedimento giurisdizionale dalla cancelleria al difensore sia finita nella cartella della posta indesiderata ('*spam*') della casella P.E.C. del destinatario: infatti, tale circostanza non costituisce causa incolpevole della decadenza nella quale sia incorsa la parte, idonea a giustificare la rimessione in termini, in quanto il titolare dell'*account* di posta elettronica certificata ha il dovere di assicurarsi del corretto funzionamento della propria casella postale e di utilizzare dispositivi di vigilanza e di controllo, dotati di misure anti intrusione, oltre che di controllare prudentemente la posta in arrivo, ivi compresa quella considerata dal programma gestionale utilizzato come "posta indesiderata" (Cass. 15 marzo 2023, n. 7510).

Quanto all'ipotesi di errata attribuzione di un indirizzo PEC, la Corte è giunta anche a configurare un principio di responsabilità a carico dell'imprenditore affermando che, nel sistema normativo attuale, sia "di chiara evidenza come la PEC costituisca l'indirizzo pubblico informatico, che deve esser attivo e rinnovato nel tempo, la cui responsabilità sia nella fase di iscrizione che successivamente, grava sul legale rappresentante della società, non avendo a riguardo alcun compito di verifica l'Ufficio camerale" (Cass. 3 gennaio 2017, n. 3123). In applicazione del principio esposto, è stata cassata la sentenza con la quale la Corte d'appello aveva revocato il fallimento sul presupposto che il ricorso ed il decreto di comparizione erano stati notificati ad un indirizzo PEC che, pur risultando dal certificato camerale della società debitrice, apparteneva, in realtà, ad altra società, stabilendo un vero e proprio onere a carico dell'impresa di verificare che l'indirizzo PEC sia attivo e funzionante, facendo solo salva la possibilità di dimostrare la ricorrenza di un errore non imputabile all'imprenditore. In tal modo, si è inteso scongiurare il rischio che un comportamento scorretto (quale indicare volutamente un indirizzo PEC non idoneo), ovvero semplicemente omissivo, dell'impresa possa compromettere la funzionalità del meccanismo di notifica telematica, salvaguardando comunque la possibilità di offrire la prova dell'errore non imputabile, per il caso in cui l'iscrizione (o il mantenimento) di un indirizzo PEC errato non siano ascrivibili a colpa dell'imprenditore.

Più di recente, Cass. 21 giugno 2018, n. 16365, ha affermato che "l'indirizzo PEC che le società e gli imprenditori individuali debbono

dichiarare alla Camera di Commercio equivale ad un recapito sostanzialmente assimilabile alla sede legale di questi ultimi, sicché può affermarsi che, di regola, e salvo che venga fornita prova contraria, il mancato funzionamento, per qualunque causa, dell'indirizzo PEC dichiarato dalla società ovvero dall'imprenditore individuale alla Camera di Commercio si ascrive tra le cosiddette irreperibilità "colpevoli" del destinatario sul quale incombe l'onere di comunicare un recapito informatico che lo renda effettivamente raggiungibile".

In ordine al domicilio digitale delle PP.AA. ai fini delle comunicazioni/notificazioni di cancelleria, va segnalato che Cass. 24 maggio 2021, n. 1419543, ha escluso la possibilità di effettuare le comunicazioni al funzionario delegato invece che per via telematica agli indirizzi di posta elettronica comunicati ai sensi del comma 12 dell'art. 16, d.l. n. 179 del 2012, conv., con modif., dalla l. n. 221 del 2012, pur nel testo ora integrato dall'art. 289, comma 1, lett. *a*), d.l. 16 luglio 2020, n. 76, conv., con modif., nella l. 11 settembre 2020, n. 120, dovendosi altresì escludere l'operatività della sanatoria per raggiungimento dello scopo, in quanto la necessità di interpretare restrittivamente le norme in materia di decadenza dall'impugnazione non consente di individuare il momento di decorrenza del termine breve diverso da quello che scaturisce da una comunicazione effettuata nel rispetto delle forme telematiche specificamente individuate. In questo caso, la S.C. ha cassato la sentenza della Corte d'appello che, avendo calcolato la decorrenza del termine per l'impugnazione della sentenza di primo grado conclusiva del cd. rito Fornero dalla comunicazione del provvedimento al funzionario incaricato, presso la cancelleria, aveva dichiarato inammissibile perché tardivo il reclamo *ex* art. 1, comma 58, della l. n. 92 del 2012, proposto dall'amministrazione soccombente, sul dichiarato presupposto che fosse pacifico che un indirizzo dell'amministrazione fosse censito nel registro di cui all'art. 16, comma 12, cit., e dunque, per quanto sopra detto, era presso lo stesso che andava fatta la comunicazione utile a fini impugnatori. Nello stesso senso, Cass. 5 novembre 2021, n. 32166, ha affermato che, nel processo del lavoro, la comunicazione o notificazione, alla P.A. che si sia difesa mediante propri dipendenti, della sentenza conclusiva del giudizio di primo grado, ove effettuata successivamente all'entrata in vigore dell'art. 16, comma 7, d.l. n. 179 del 2012, conv. con modif. nella l. n. 221 del 2012, deve essere eseguita per via telematica all'indirizzo di posta elettronica comunicato ai sensi del comma 12, dell'art. 16 citato (nella formulazione in vigore fino al d.l. n. 76 del 2020, cit.), restando, pertanto, ammissibile la notificazione presso la cancelleria non già nel caso di mancata elezione di domicilio ex art. 82 del r.d. 22 gennaio 1934, n. 37, (inapplicabile ai funzionari della P.A. cui sia demandata la difesa in giudizio), bensì nella sola ipotesi di impossibilità di procedere alla notifica telematica, imputabile alla P.A. medesima.

3.4. La questione dell'ammissibilità dell'elezione di domicilio digitale

La disciplina sul domicilio digitale in ambito giudiziario, per come sopra ricostruita ed interpretata dalla giurisprudenza di legittimità in materia di comunicazioni/notificazioni a cura della cancelleria, sembra escludere l'ammissibilità di una elezione di domicilio digitale da parte del destinatario presso un proprio indirizzo PEC vincolante e diverso da quello risultante dai pubblici elenchi, essendo stata reputata irrilevante l'eventuale diversa indicazione contenuta nell'atto, tanto più dopo la modifica apportata all'art. 125 c.p.c. dall'art. 45-*bis*, comma 1, del d.l. 24 giugno 2014, n. 90, conv. con modif. dalla l. 11 agosto 2014, n. 114, che ha eliminato l'obbligo per il difensore di indicare l'indirizzo PEC comunicato al proprio ordine in quanto già risultante dai pubblici registri.

Infatti, è stata ritenuta validamente effettuata la notifica del decreto di fissazione dell'udienza, *ex* art. 380-*bis*, comma 2, c.p.c., all'indirizzo PEC del difensore risultante dal ReGIndE, ai sensi dell'art. 136, comma 2, c.p.c. e dell'art. 16, comma 4, del d.l. n. 179 del 2012, cit., senza che possa assumere rilievo l'eventuale diverso indirizzo PEC indicato negli atti difensivi (Cass. 17 ottobre 2018, n. 25948). In applicazione del medesimo principio, nel cd. rito Fornero, ai fini della decorrenza del termine breve per proporre reclamo contro la sentenza che decide il ricorso in opposizione, è stata ritenuta idonea la comunicazione telematica della sentenza all'indirizzo PEC del difensore risultante da pubblici elenchi o da registri accessibili alla pubblica amministrazione, restando irrilevante l'eventuale indicazione nell'atto di un diverso indirizzo PEC (Cass. 4 gennaio 2019, n. 83).

A diversa conclusione, invece, sembra potersi pervenire ove si intenda eleggere un domicilio virtuale riferibile ad un soggetto terzo. Soccorre, in proposito, il disposto dell'art. 141 c.p.c., da coordinare con la nozione di domicilio digitale che virtualizza il domicilio fisico. In questo caso, l'adempimento potrebbe essere validamente eseguito anche presso l'indirizzo PEC del terzo così indicato, purché risultante dai pubblici elenchi; va, però, chiarito che siffatta elezione di domicilio si aggiunge ma non esclude il domicilio digitale del difensore e prefigura l'alternativa fra eseguire la notificazione presso l'indirizzo PEC del *dominus* ovvero presso il domiciliatario. Pertanto, pur in presenza di un domicilio digitale eletto presso un terzo, il difensore potrà comunque essere legittimamente destinatario di comunicazioni e notificazioni eseguite presso l'indirizzo PEC che, per disposizione di legge, è tenuto ad istituire e comunicare al proprio ordine professionale, dovendosi escludere la configurabilità di un diritto a ricevere le notifiche esclusivamente nel domicilio eletto, sia esso fisico o virtuale (in tal senso, Cass., 24 maggio 2018, n. 12876).

Infatti, Cass. 23 febbraio 2021, n. 4920, ha precisato, in espresso riferimento alle comunicazioni di cancelleria a mezzo PEC, che il difensore esercente il patrocinio non può indicare la PEC di altro avvocato senza specificare di volersi domiciliare presso di lui, in quanto l'individuazione del difensore destinatario della comunicazione di cancelleria deve avvenire automaticamente attraverso la ricerca nel ReGIndE, a prescindere dall'indicazione espressa della PEC, cosicché non può attribuirsi rilievo all'indicazione di una PEC diversa da quella riferibile al legale in base agli appositi registri e riconducibile ad altro professionista, senza una chiara assunzione di responsabilità qual è quella sottesa alla dichiarazione di domiciliazione (in senso conforme, più di recente, Cass. 19 ottobre 2022, n. 30720).

Nella stessa linea, invero senza neppure prospettare la facoltà di una differente elezione di domicilio digitale, si pone anche Cass. 7 giugno 2021, n. 15783, secondo cui le comunicazioni al difensore, per il quale la legge prevede l'obbligo di munirsi di un indirizzo di posta elettronica certificata, devono essere eseguite, ai sensi dell'art. 16, comma 6, del d.l. n. 179 del 2012, conv. con modif. nella l. n. 221 del 2012, esclusivamente mediante deposito in cancelleria quando il difensore non abbia provveduto ad istituire o comunicare il predetto indirizzo PEC, dovendo escludersi che la cancelleria sia tenuta ad effettuare la comunicazione all'indirizzo di posta elettronica di altro difensore presso il quale quello nominato abbia dichiarato di voler ricevere le notifiche.

È stato altresì affermato che le comunicazioni di cancelleria devono essere eseguite, per i processi cui risulta applicabile la disciplina dell'art. 16, d.l. n. 179 del 2012, cit., esclusivamente presso l'indirizzo PEC del difensore della parte, senza che rilevi l'eventuale elezione di domicilio presso la cancelleria dell'ufficio giudiziario, salva la sola ipotesi in cui non sia possibile procedere, mediante PEC, ai sensi del comma 4 della citata norma, per causa non imputabile al destinatario, nel qual caso trova applicazione l'art. 136, comma 3, c.p.c. e può rilevare l'elezione di domicilio (Cass. 15 settembre 2017, n. 21519; conforme Cass. 10 maggio 2018, n. 11316 e Cass. 9 agosto 2018, n. 20698, che ha ritenuto manifestamente infondata la questione di legittimità costituzionale degli artt. 136, comma 3, c.p.c. e 16, comma 8, d.l. n. 179 del 2012, "non essendo il sistema configurato dalle disposizioni, imperniato sulla imputabilità o meno della causa al destinatario, impeditivo o gravemente limitativo del diritto di difesa del medesimo destinatario"). In senso conforme si è espressa anche Cass. 28 dicembre 2018, n. 33547.

D'altro canto, è stata ritenuta correttamente eseguita la notifica della sentenza impugnata presso l'indirizzo PEC del domiciliatario, ancorché tale indirizzo non risultasse indicato nell'atto ma fosse stato rinvenuto tramite i pubblici elenchi (Cass. 11 maggio 2017, n. 11759), in tal modo assumendo

implicitamente che l'elezione di domicilio fisico comporta di per sé anche l'elezione di domicilio virtuale (ma v. *infra* per una soluzione opposta).

Nell'ipotesi di esito negativo per causa imputabile al destinatario, la comunicazione/notificazione di cancelleria eseguita all'indirizzo PEC del *dominus* è legittimamente eseguita in cancelleria *ex* art. 16, comma 6, d.l. n. 179 del 2012 cit., senza che la cancelleria abbia l'onere di tentare l'invio anche al domiciliatario.

Sotto altro profilo, si è posta la questione della "esclusività" dell'elezione di domicilio digitale presso uno dei co-difensori, nel senso di ritenere invalida la comunicazione effettuata solo all'indirizzo PEC dell'altro difensore. In questi termini si era espressa Cass. 31 gennaio 2019, n. 2942, soffermandosi sulla circostanza che l'indirizzo PEC eletto come esclusivo per le comunicazioni era quello "ufficiale" del difensore (cioè censito in pubblici elenchi); l'assunto non pare tuttavia pienamente condivisibile, perché, da un lato, non considera l'operatività del domicilio digitale di ciascuno dei difensori, secondo le disposizioni sopra riportate, dall'altro, sembra obliare i principi più volte affermati in ordine alla ritualità della comunicazione/notifica eseguita presso uno solo degli avvocati del collegio difensivo (v., *ex multis*, Cass., S.U., 9 giugno 2014, n. 12924; Cass. 22 settembre 2016, n. 18622; Cass. 2 maggio 2017, n. 10635 e, di recente, con riferimento alla notifica a mezzo PEC ad uno solo dei procuratori costituiti, Cass. S.U., 21 novembre 2022, n. 34260). Aspetti invece tenuti ben presenti da Cass. 20 maggio 2019, n. 13532, che, con stringente motivazione, ha affermato che "Il mancato buon esito della comunicazione telematica di un provvedimento giurisdizionale dovuto alla saturazione della capienza della casella PEC del destinatario è evento imputabile a quest'ultimo; di conseguenza, è legittima l'effettuazione della comunicazione mediante deposito dell'atto in cancelleria, ai sensi dell'art. 16, comma 6, d.l. n. 179 del 2012, conv. in l. n. 221 del 2012, come modificato dall'art. 47, d.l. n. 90 del 2014, conv. in l. n. 114 del 2014, senza che, nell'ipotesi in cui il destinatario della comunicazione sia costituito nel giudizio con due procuratori, la cancelleria abbia l'onere, una volta non andato a buon fine il primo tentativo di comunicazione, di tentare l'invio del provvedimento all'altro procuratore".

Nondimeno, va evidenziato che il principio affermato da Cass. n. 2942 del 2019 in ordine alle comunicazioni, è stato esaminato e superato da successive pronunce, sia pure riferite alla notifica della sentenza effettuata nei confronti del co-difensore, indicato come domiciliatario esclusivamente in senso fisico, essendo stati indicati come domiciliatari digitali esclusivamente altri due avvocati del collegio difensivo, solo dei quali era stato espressamente riportato l'indirizzo PEC: infatti, la decisione della Corte territoriale, di accoglimento dell'appello sul presupposto della nullità della notifica telema-

tica effettuata nei confronti del difensore non indicato come domiciliatario digitale, è stata impugnata assumendo, da un lato, l'irrilevanza della indicazione dell'indirizzo PEC, a seguito delle modifiche apportate all'art. 125 c.p.c., dall'altra, il consolidato orientamento secondo cui, in presenza di più difensori, la notifica della sentenza ad uno solo di essi è idonea a far decorrere il termine breve per l'impugnazione. La questione è stata decisa da Cass. 12 novembre 2021, n. 33806, che ha ritenuto di dare continuità all'orientamento elaborato nel regime del cd. "domicilio digitale", secondo cui, in base all'art. 125 c.p.c., come modificato dall'art. 45-*bis*, comma 1, del d.l. n. 90 del 2014, conv. con mod. in l. n. 114 del 2014, non sussiste l'obbligo per il difensore di indicare nell'atto introduttivo l'indirizzo PEC "comunicato al proprio ordine" perché già risultante dal ReGIndE in virtù della trasmissione operata dall'ordine in base alla comunicazione effettuata dall'interessato (per tutte: S.U., 29 settembre 2018, n. 23620), orientamento ulteriormente consolidatosi nelle more con le pronunce rese da Cass. 3 marzo 2021, n. 246048, e da Cass. 12 febbraio 2021, n. 368549. In tal modo, la S.C. ha ritenuto superato l'isolato precedente rappresentato da Cass. n. 2942 del 2019, cit., affermando, in conclusione, che "oggi l'unico indirizzo di posta elettronica certificata rilevante ai fini processuali è quello che il difensore ha indicato, una volta per tutte, al Consiglio dell'ordine di appartenenza. In tal modo, l'art. 125 c.p.c. è stato allineato alla normativa generale in materia di domicilio digitale. Il difensore non ha più l'obbligo di indicare negli atti di parte l'indirizzo di posta elettronica certificata, né ha facoltà di indicare uno diverso da quello comunicato al Consiglio dell'ordine o di restringerne l'operatività alle sole comunicazioni di cancelleria". Di conseguenza, la Corte di legittimità, nel caso di specie, ha cassato con rinvio la decisione impugnata ritenendo rituale la notificazione della sentenza, ai fini del decorso del termine breve per l'impugnazione, effettuata all'indirizzo PEC di uno dei co-difensori, ancorché in atti fosse stato espressamente richiesto che le comunicazioni di cancelleria venissero eseguite agli indirizzi PEC degli altri due difensori nominati, in quanto validamente effettuata all'indirizzo PEC di uno dei tre difensori di fiducia, quale risultante dal ReGIndE, indipendentemente dalla sua indicazione in atti, ai sensi dell'art. 16-*sexies*, d.l. n. 179 del 2012, conv., con modif., nella l. n. 221 del 2012, non potendosi configurare un diritto a ricevere le notificazioni esclusivamente presso il domiciliatario indicato e non potendo, quindi, avere portata idonea ad escludere tale notificazione la limitazione della parte dell'indicazione del detto indirizzo per le sole comunicazioni (richiamandosi espressamente, quanto all'ultimo profilo, Cass. 12 febbraio 2021, n. 3685).

3.5. Il rapporto con la tradizionale figura del domiciliatario

A ben vedere, l'istituto del domicilio digitale e la conseguente semplificazione delle comunicazioni/notificazioni, tramite l'obbligo, posto a carico del difensore, di istituire e manutenere uno specifico indirizzo PEC con finalità di giustizia, pubblicato in appositi registri, viene di fatto a ridimensionare fortemente l'esigenza della figura del domiciliatario, tradizionalmente legato ad una ubicazione fisica, ed all'onere di domiciliazione nel luogo dove ha sede l'autorità giudiziaria adita.

Si registrano, peraltro, incertezze applicative nei casi di notificazioni eseguite nei confronti del domiciliatario, rinvenendosi, accanto a pronunce che reputano pienamente legittima la notifica eseguita all'indirizzo PEC risultante dai pubblici elenchi del domiciliatario "fisico" (v. *supra*), decisioni che giungono a ritenere "inesistente" la notifica telematica effettuata presso il procuratore domiciliatario in senso fisico, in mancanza di elezione dell'indirizzo PEC dello stesso come domicilio digitale della parte (Cass. 22 agosto 2018, n. 20946). E se tale ultimo approccio suscita perplessità, perché non sembra predicabile la sanzione dell'inesistenza nell'interpretazione residuale seguita a Cass., S.U., 20 luglio 2016, n. 14916, il primo richiede di consapevolizzare l'implicita estensione dell'elezione di domicilio fisico a quella del domicilio digitale, restando tuttora aperto il tema dell'ammissibilità e degli effetti di un'elezione di domicilio solo virtuale presso il terzo.

Viceversa, nella linea intesa ad attribuire prevalenza al domicilio digitale, si pone Cass. 1° giugno 2020, n. 10355, che ha ritenuto inidonea a determinare la decorrenza del termine breve per l'impugnazione la notifica della sentenza effettuata al domiciliatario "fisico" invece che presso l'indirizzo PEC indicato nell'atto di citazione in appello, ove la parte aveva peraltro precisato di voler ricevere "le comunicazioni e notificazioni nel corso del giudizio"; l'assunto è stato specificato nel senso che, in presenza di un indirizzo PEC ufficiale indicato dal difensore, non esplicitamente circoscritto alle sole comunicazioni, la circostanza che il difensore, come nella specie, abbia eventualmente eletto domicilio ai sensi dell'art. 82, r.d. n. 37 del 1934 "non può elidere il principio, di valenza costituzionale inerente il diritto di difesa, del rispetto della scelta legittimamente effettuata dalla parte", in tal modo configurando un obbligo del notificante di utilizzare in via esclusiva la notificazione telematica. In continuità con tale indirizzo si è espressa più di recente anche Cass. 24 marzo 2021, n. 826251.

3.6. Considerazioni conclusive

Le potenzialità offerte dall'impiego degli strumenti informatici nel processo hanno indotto il legislatore a recepire nel diritto processuale civile la

figura, di matrice giurisprudenziale, del "domicilio digitale", in chiave di semplificazione delle comunicazioni/notificazioni a cura della cancelleria.

Sono, però, emerse nuove questioni interpretative, per definire i criteri di corretta individuazione dell'indirizzo PEC rilevante ai fini del domicilio digitale ovvero per regolare i rapporti fra notifica eseguita all'indirizzo PEC del *dominus* e la notifica effettuata nei confronti del domiciliatario, fisico e/o virtuale. Proprio con riferimento alla figura del domiciliatario, tradizionalmente legata ad un'ubicazione fisica, si registrano incertezze applicative, apparendo quanto meno opportuno un intervento a livello normativo.

IV.
IL DOMICILIO DIGITALE NEL DEPOSITO TELEMATICO (CENNI)

di *Antonella Ciriello*

4.1. Il domicilio digitale nel deposito telematico (cenni)

Nel processo civile, come accennato, il deposito telematico è realizzato tramite la posta elettronica certificata, in attesa di evolvere i sistemi informatici verso soluzioni tecnologicamente più performanti (1). In particolare, si attende una evoluzione verso sistemi che consentano "*upload*" in portale o piattaforma, per superare i noti limiti della PEC (limitata capienza, difficoltà di allegare file più corposi, etc.).

Attualmente il dato normativo relativo al deposito civile è contenuto nell'art. 196-*quater*, disp.att. c.p.c, recentemente innovato per effetto dell'art. 36, d.l. 24 febbraio 2023, n. 13, e stabilisce l'obbligatorietà del deposito per tutti, difensori, soggetti nominati o delegati dall'autorità giudiziaria e per lo stesso giudice e cancelliere. L'unico limite, a tale regola, per tutti, è quello dei malfunzionamenti o (per le sole parti) di una richiesta del giudice "per ragioni specifiche".

L'art. 13 delle regole tecniche del processo telematico (il più volte citato regolamento di cui al decreto 21 febbraio 2011, n. 44), prevede, per il settore civile (con la rubrica Trasmissione dei documenti da parte dei soggetti abilitati esterni e degli utenti privati nel procedimento civile) che " Nel procedimento civile, gli atti e i documenti in forma di documento informatico di cui agli articoli 11 e 12 possono essere trasmessi da parte dei soggetti abilitati esterni mediante l'indirizzo di posta elettronica certificata risultante dal registro generale degli indirizzi elettronici, ovvero l'indirizzo di posta elettronica certificata messo a disposizione dal Ministero della giustizia secondo le specifiche tecniche stabilite dall'articolo 34".

Da quanto riportato emerge dunque che il domicilio digitale per il deposito, nel processo civile, per gli utenti esterni, è l'indirizzo di PEC

(1) Come richiesto dal comma 17 dell'art. 1 della legge 26 novembre 2021, n. 206, contenente la Delega al Governo per l'efficienza del processo civile.

risultante dal ReGinDE (di cui all'art. 7 del medesimo regolamento e all'art. 16-*ter* del più volte citato d.l. n. 179 del 2012).

La norma opera poi un riferimento agli "indirizzi di posta elettronica messi a disposizione dal Ministero", evidentemente per ricomprendere le ipotesi di cui alla normativa speciale (ci si riferisce, per esempio, a quanto previsto dal Codice della crisi di impresa, con l'art. 199 del decreto legislativo 12 gennaio 2019, n. 14, intitolato Fascicolo della procedura) che stabilisce come "Con la pubblicazione della sentenza di liquidazione giudiziale viene assegnato il domicilio digitale e viene formato il fascicolo informatico della procedura".

Le specifiche tecniche "stabilite dall'articolo 34" del regolamento 44, in corso di emanazione (sono pubblicate in bozza sul sito www.pstgiustizia.it), prevedono, all'art. 16, quanto al deposito degli utenti abilitati esterni, semplicemente che "Nel procedimento civile l'atto in forma di documento informatico e gli allegati di cui all'articolo 15, sono trasmessi dai soggetti abitati esterni mediante la posta elettronica certificata di cui al d.p.r. 11 febbraio 2005, n. 68".

Da tale normativa generale, tuttavia, fino ad oggi, era previsto un significativo scostamento (valorizzandosi il perfezionamento del deposito non, come prevederebbe la regola generale predicata dal citato d.p.r., all'atto del ricevimento da parte dell'avvocato mittente della RDAC, ma solo dopo una quarta PEC, frutto dell'esito dei cd. "controlli manuali" da parte del personale di cancelleria).

Pertanto si configurava una prima PEC (la ricevuta di accettazione) una seconda PEC, (la ricevuta di avvenuta consegna) una terza PEC (inviata dal sistema all'esito dei controlli automatici) ed infine la PEC più importante collegata all'intervento umano determinante l'ingresso dell'atto nel fascicolo informatico. Di questa disciplina, tuttavia, anche alla luce dei testi delle regole tecniche esaminate, risultaannunciata la modifica per l'allineamento con la regola generale della rilevanza della RDAC, salvo i casi di anomalie bloccanti (la modifica dovrebbe intervenire ad opera di uno degli attesi e previsti decreti legislativi correttivi della riforma introdotta con d.lgs. 10 ottobre 2022, n. 149, al momento della pubblicazione di questo testo all'esame delle camere [2].

Accanto a tale forma di domicilio digitale del deposito di utenti avvocati esterni e degli utenti interni va evidenziato come, fino ad ora, la parte che sta in giudizio personalmente ossia senza il patrocinio di un avvocato, non

---

[2] In realtà, il correttivo di rango primario rinvia alle regole e specifiche tecniche per questi aspetti. In particolare, le specifiche tecniche, frutto di un provvedimento del direttore generale SIA, non ancora pubblicate al momento della redazione di questo contributo, dovrebbero (sulla base delle notizie diffuse)disciplinare una accettazione automatica, con l'eccezione di casi di anomalie bloccanti più gravi, censite, che producono il rifiuto dell'atto o anomali meno gravi, del pari censite, che conducono all'accettazione tramite l'intervento del cancelliere.

poteva avvalersi del domicilio digitale per depositare, se non (in prospettiva) nel limitato settore della volontaria giurisdizione per il quale è stato avviato il cd. "tribunale on line" (3). Con il più volte citato d.m. 29 dicembre 2023, n. 217, è stato adeguato l'art. 7 del regolamento, prevedendosi l'allineamento del ReGIndE anche con il registro INAD, per i privati e per i professionisti non iscritti in albi (4).

Quanto ai soggetti abilitati interni, magistrati e avvocati, secondo le regole tecniche gli stessi si avvalgono di servizi e applicativi, all'interno del dominio giustizia, (definiti dal più volte citato regolamento) ai quali accedono con sistemi sicuri di identificazione (con smartcard o altre forme di autenticazione).

Come visto nel primo capitolo, paragrafo 2, le norme più recenti hanno fatto applicazione delle varie figure di domicilio (generale, speciale e di piattaforma), sia nel processo civile che nel processo penale (5).

---

(3) V. *infra* paragrafo sul domicilio digitale nella volontaria giurisdizione sez. III, cap. 2, ove si illustrano le recenti norme secondarie attuative del domicilio di piattaforma del privato ai fini del deposito telematico nel settore della volontaria giurisdizione (d.m. 22 gennaio 2024 e successive specifiche tecniche del 31 dicembre 2024).

(4) Art. 7 Registro generale degli indirizzi elettronici

1. Il registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia, contiene i dati identificativi e l'indirizzo di posta elettronica certificata dei soggetti abilitati esterni di cui al comma 3 e degli utenti privati di cui al comma 4.

2. Per i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato, il registro generale degli indirizzi elettronici è costituito mediante i dati contenuti negli elenchi riservati di cui all'articolo 16, comma 7, del decreto-legge 29 novembre 2008, n. 185, convertito nella legge del 28 gennaio 2009, n. 2, inviati al Ministero della giustizia secondo le specifiche tecniche di cui all'articolo 34.

3. Per i soggetti abilitati esterni non iscritti negli albi di cui al comma 2, il registro generale degli indirizzi elettronici è costituito mediante i dati contenuti nell'indice di cui all'articolo 6-*quater* del CAD, ove disponibili, e secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

4. Per le persone fisiche, quali utenti privati, che non operano nelle qualità di cui ai commi 2 e 3, gli indirizzi sono consultabili ai sensi dell'articolo 7 del decreto del Presidente del Consiglio dei Ministri 6 maggio 2009, secondo le specifiche tecniche stabilite ai sensi dell'articolo 34.

5. Per le imprese, gli indirizzi sono consultabili, senza oneri, ai sensi dell'articolo 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, convertito nella legge del 28 gennaio 2009, n. 2, con le modalità di cui al comma 10 del medesimo articolo e secondo le specifiche tecniche di cui all'articolo 34.

6. Il registro generale degli indirizzi elettronici è accessibile ai soggetti abilitati mediante le specifiche tecniche stabilite ai sensi dell'articolo 34.

(5) Nel paragrafo 2 del primo capitolo sono evidenziate le figure di domicilio speciale contemplate dall'art. 16, comma 7, d.l. n. 179 del 2012, per la comunicazione civile, e dall'art. 199 del decreto legislativo 12 gennaio 2019, n. 14 (intitolato Fascicolo della procedura) del Codice della crisi di impresa, nonché lo speciale domicilio di piattaforma del tribunale on-line per la volontaria giurisdizione approfondito pure in questo capitolo nella sezione terza, paragrafo 2.

V.

IL DOMICILIO DIGITALE DELLE PUBBLICHE AMMINISTRAZIONI. LE PECULIARITÀ DELL'AVVOCATURA DELLO STATO

di *Marco La Greca*

Sommario: 5.1. Il domicilio digitale delle pubbliche amministrazioni: indirizzi di posta elettronica certificata ed elenchi pubblici; una ricostruzione storica. — 5.2. Il Registro delle PA: le ragioni del mancato popolamento, sino alla novella del 2020. — 5.3. L'attuale assetto: il domicilio digitale delle Pubbliche Amministrazioni dopo la novella del 2020. — 5.4. Le peculiarità dell'Avvocatura dello Stato.

5.1. Il domicilio digitale delle pubbliche amministrazioni: indirizzi di posta elettronica certificata ed elenchi pubblici; una ricostruzione storica

Il tema relativo alla corretta individuazione del domicilio digitale, non solo per le pubbliche amministrazioni (nel prosieguo, anche PP.AA.), si è iniziato a porre a partire dall'entrata in vigore, il 1° gennaio 2012, dell'articolo 25, l. 12 novembre 2011, n. 183; si tratta della nota disposizione che, intervenendo sul testo della legge 21 gennaio 1994, n. 53, disciplinante la "*Facoltà di notificazione di atti civili, amministrativi e stragiudiziale*" a mezzo del servizio postale (nonché di una speciale notificazione "diretta", a mani), da parte degli avvocati, ha reso possibile l'effettuazione, da parte di questi, anche delle notificazioni a mezzo di posta elettronica certificata (nel prosieguo, anche "PEC").

Al momento dell'entrata in vigore della citata disposizione, in verità, non si parlava propriamente di "domicilio digitale", facendosi allora riferimento (anche se con approdo, nei fatti, sostanzialmente analogo) agli indirizzi PEC per categorie di soggetti [1]. Il concetto di domicilio digitale è poi stato

---

[1] Per quanto riguarda i cittadini, per esempio, veniva in rilievo, ai sensi dell'articolo 6 del CAD, l'indirizzo PEC comunicato nell'ambito di un determinato procedimento come il "luogo" presso il quale potevano essere effettuate le relative comunicazioni telematiche; per quanto riguardava professionisti e imprese, invece, veniva in rilievo l'indirizzo PEC comunicato, ai sensi dell'articolo 16, comma 2, del decreto-legge 29 novembre 2008, n. 158, al registro

introdotto dall'art. 1, comma 1, lett. *c*), del d.lgs. 26 agosto 2016, n. 179, che inserendo la lettera n-*ter* all'articolo 1, comma 1, decreto legislativo 7 marzo 2005, n. 82 (di seguito, CAD), l'ha definito come "*un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito <Regolamento eIDAS>, valido ai fini delle comunicazioni elettroniche aventi valore legale*".

Si tratta di un aggiornamento dettato, da una parte, da una supposta necessità di adeguamento ed armonizzazione con la normativa comunitaria, dal momento che la tecnologia della PEC era, ed è tuttora, di esclusiva pertinenza italiana (2), dall'altra, per una finalità semantica, di riproduzione, in chiave digitale, dei concetti giuridici (residenza, domicilio) propri della realtà analogica, aventi una loro rilevanza di diritto sostanziale e di diritto processuale.

Va dunque rilevato che, nel contesto digitale, avuto riguardo alla definizione contenuta nel CAD (dianzi riportata), il concerto di residenza viene assorbito in quello di domicilio digitale. Si è cioè ritenuto, muovendo dall'articolo 43 c.c., che un soggetto, pur non potendo avere la "*stabile dimora*", possa stabilire "*la sede principale dei suoi affari e interessi*" presso un determinato luogo informatico e quindi, nello specifico dell'attuale realtà tecnologica recepita dall'ordinamento interno, presso un indirizzo PEC.

Fermo restando quanto esposto, circa l'istituto del domicilio digitale e il suo avvento nella realtà giuridica, stante la successione storica e la sostanziale equivalenza tra i criteri di individuazione degli indirizzi PEC cui fare riferimento, ai fini di valide comunicazioni telematiche (intese nel senso più ampio), e l'istituto del domicilio digitale, nel prosieguo si utilizzerà tale ultima espressione, all'occorrenza, anche in relazione a fasi precedenti alla sua espressa previsione normativa.

---

delle imprese o agli ordini professionali, per la pubblicazione nell'indice nazionale degli indirizzi PEC delle imprese e dei professionisti (il cosiddetto registro "INI-PEC"), tenuto dal Ministero dello sviluppo economico, secondo quanto previsto dall'articolo 6-*bis* del CAD (introdotto dall'articolo 5, comma 2, decreto legge 18 ottobre 2012, n. 179).

(2) Va peraltro osservato che nel Regolamento (CE) 23 luglio 2014, n. 910, il cosiddetto Regolamento eIDAS ("*Regolamento in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE*"), mentre sono presenti riferimenti a modalità di recapito che, sebbene molto diversi dal punto di vista tecnlogico, risultano, circa gli effetti sostanzialmente sovrapponibili alla nostra posta elettronica certificata (i servizi di recapito di cui all'articolo 44), non sono invece presenti concetti assimilabili a quello, di diritto interno, di domicilio digitale.

Si discuteva dunque, al momento di entrata in vigore della novella della legge n. 53 del 1994, in relazione alle notificazioni a mezzo PEC, di quali fossero i "*pubblici elenchi*" da cui trarre, secondo quanto previsto dall'articolo 3, comma 3-*bis*, della stessa legge, gli indirizzi di posta elettronica certificata dei destinatari (3).

Il problema si poneva, in primo luogo, per gli avvocati, per i quali poteva essere considerato elenco pubblico, ai fini della individuazione dell'indirizzo PEC utile ai fini della notificazioni, e almeno nell'ambito del processo civile, il Registro generale degli indirizzi elettronici, previsto dall'articolo 7 del decreto ministeriale 21 febbraio 2011, n. 44 (nel prosieguo, "ReGIndE") (4) (5), consultabile, ai sensi dell'art. 7 delle Specifiche tecniche

---

(3) Sussisteva allora il dubbio circa il fatto che le notificazioni a mezzo PEC potessero essere eseguite verso soggetti diversi dagli avvocati. L'art. 4, comma 1, della l. n. 53 del 1994, nel testo risultante a seguito delle modifiche introdotte, a decorrere dal 1° febbraio 2011, dall'art. 25 della l. 12 novembre 2011, n. 183, disponeva che "*L'avvocato o il procuratore legale, munito della procura e dell'autorizzazione di cui all'articolo 1*", poteva "*eseguire notificazioni in materia civile, amministrativa e stragiudiziale, direttamente, a mezzo posta elettronica certificata*"; in tale ipotesi, secondo quanto precisato dall'art. 5, comma 1, della stessa legge, anch'esso come modificato dal più volte citato art. 25 della l. n. 183 del 2011, "*l'atto*" doveva "*essere trasmesso a mezzo posta elettronica certificata all'indirizzo di posta elettronica certificata che il destinatario*" aveva "*comunicato al proprio ordine, nel rispetto della normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici*". Il riferimento all'indirizzo PEC comunicato al Consiglio dell'ordine degli Avvocati, quale indirizzo di destinazione della notificazione telematica, portava a dubitare che la stessa potesse essere eseguita verso soggetti diversi dagli avvocati (e dunque, per esempio, verso una pubblica amministrazione); il dubbio, peraltro, sussisteva anche per l'Avvocatura dello Stato, trattandosi di un soggetto, impersonalmente inteso, che non ha alcun rapporto con i consigli dell'ordine (a differenza degli avvocati degli altri enti pubblici, iscritti nell'elenco speciale tenuto, per l'appunto, dal consiglio dell'ordine). Poiché, peraltro, l'art. 3, comma 3-*bis*, della medesima l. n. 53 del 1994, prevedeva che "*la notifica*" era "*effettuata a mezzo della posta elettronica certificata solo se l'indirizzo del destinatario*" risultava "*da pubblici elenchi*", vi erano due possibili interpretazioni del sistema approntato dalla legge, tra loro alternative:

1) interpretazione restrittiva: le notifiche via PEC erano consentite nei confronti dei soli avvocati (art. 4, comma 1), all'indirizzo comunicato al consiglio dell'ordine (art. 5, comma 1), a condizione che tale indirizzo risultasse da un pubblico elenco (art. 3, comma 3-*bis*);

2) interpretazione estensiva: le notifiche via PEC erano consentire nei confronti di chiunque, all'indirizzo di posta elettronica certificata risultante da un pubblico elenco (art. 3, comma 3-*bis*), e, se avvocato (art. 4, comma 1), all'indirizzo comunicato al consiglio dell'ordine (art. 5, comma 1).

(4) Come è noto, si tratta del regolamento ministeriale che, nella dichiarata "*attuazione dei principi previsti dal decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni*" e ai sensi dell'articolo 4, commi 1 e 2, del decreto-legge 29 dicembre 2009, n. 193, ha dettato le "*regole tecniche per l'adozione nel processo civile e nel processo penale, delle tecnologie dell'informazione e della comunicazione*".

adottate ai sensi dell'art. 34 del citato d.m., dai "soggetti abilitati esterni" (6). Vi erano poi gli elenchi, a consultazione aperta, resi disponibili dai Consigli degli Ordini Forensi, e, a livello nazionale, dal Consiglio Nazionale Forense. Si trattava di esposizione informatica e pubblica, in qualche caso aggregata (come per l'elenco offerto dal CNF), dei dati presenti sugli albi professionali tenuti dai vari Consigli degli ordini. Analogamente, potevano essere considerati elenchi pubblici quelli resi disponibili dagli albi delle varie professioni (ad esempio dei commercialisti) e, per le società e le imprese, dalle Camere di commercio (7).

Vi erano poi le PP.AA., per le quali già da tempo era stato istituito l'Indice degli indirizzi delle pubbliche amministrazioni, il cosiddetto "IPA", previsto dall'articolo 57-*bis* del CAD, e inizialmente affidato a Digit PA (poi trasformatosi in AgID). Si trattava, è forse utile ricordare, di un indice che aveva la finalità, secondo quanto espressamente stabilito dal primo comma del citato articolo 57-*bis*, di "*assicurare la pubblicità dei riferimenti telematici delle pubbliche amministrazioni e dei gestori dei pubblici servizi*", per favorire dunque le comunicazioni telematiche dei privati (cittadini, i professionisti, le imprese e le società) verso le stesse pubbliche amministrazioni e i gestori di pubblici servizi. Di qui la creazione di un elenco capillare, in cui ciascuna P.A. presentava i dati di recapito, fisico e digitale, di ogni singola area organizzativa omogena (8). Intendeva cioè, l'IPA (9), esporre la corrispondenza digitale di ogni singola articolazione di ciascuna pubblica amministrazione (o gestore di pubblici servizi).

---

(5) Taluni dubitavano che il ReGIndE potesse essere considerato elenco pubblico, in quanto ad accesso limitato e non aperto; era, peraltro, un registro accessibile a coloro i quali, cioè gli avvocati, erano gli attori esclusivi del processo notificatorio, dunque, in questa prospettiva, l'elenco ben poteva essere considerato "pubblico", in quanto accessibile a chi avrebbe dovuto poi utilizzare gli indirizzi ivi presenti, oltre al fatto che era tenuto da un soggetto pubblico, cioè il Ministero della giustizia.

(6) L'articolo 2, comma 1, n. 2 e n. 3, del d.m. n. 44 del 2011, distingueva i "*soggetti abilitati esterni*" in "*privati*" e "*pubblici*", individuando — nel testo vigente sino a prima delle modifiche introdotte dal d.m. 29 dicembre 2023, n. 217 — i primi nei difensori delle parti private, negli avvocati iscritti negli elenchi speciali, nonché negli esperti e ausiliari del giudice, e i secondi negli avvocati e procuratori dello Stato e nei dipendenti delle pubbliche amministrazioni.

(7) Nei ricordati limiti in cui, allora, i professionisti diversi dagli avvocati, oltre alle società e alle imprese, potevano essere ritenuti destinatari di notifiche.

(8) In relazione all'uso della PEC da parte delle PP.AA., l'articolo 47, comma 3, del CAD, stabiliva allora e tuttora stabilisce l'obbligo di istituire e pubblicare nell'IPA. almeno una casella di PEC per ciascun registro di protocollo. Si tratta di una disposizione che, sebbene dettata all'interno dell'articolo che disciplina lo scambio documentale tra le PP.AA., favorisce poi gli stessi soggetti amministrati, consentendo anche a loro (oltre che alle pubbliche amministrazioni), un più agevole reperimento degli indirizzi PEC dell'Amministrazione destinataria.

Una finalità, evidentemente, diversa da quella sottesa alla individuazione dell'indirizzo PEC da utilizzare per eseguire la notificazione di un atto processuale, che si esprimeva invece nella tendenziale concentrazione in uno o comunque pochi indirizzi PEC consapevolmente indicati e presidiati. A fronte di quanto evidenziato, si consideri per esempio che il Ministero dell'Interno, già allora, contava, sull'IPA, più di mille indirizzi PEC. Fermo restando che, nella maggior parte dei casi, e rimanendo all'esempio formulato, le notificazioni al Ministero dell'interno (ma è lo stesso per le altre Amministrazioni statali) dovevano e devono avere come destinataria l'Avvocatura dello Stato (10) (per la quale si pongono poi questioni differenti e che verranno specificatamente trattate nel paragrafo ad essa dedicato), vi sono taluni casi nei quali le notificazioni possono essere effettuate direttamente presso l'Amministrazione (11). Ebbene, si poteva pensare che uno qualsiasi di quei mille indirizzi PEC potesse essere destinatario di una valida notificazione a mezzo PEC verso il Ministero dell'Interno? Senza che l'Amministrazione avesse potuto scegliere o indicare quale fosse l'indirizzo PEC destinato alla notificazione di atti processuali? Una situazione che, evidentemente, avrebbe costituito una clamorosa disparità di trattamento rispetto a tutti gli altri destinatari di notifica PEC, che già allora avevano la possibilità (gli

---

L'indicazione di una PEC per ciascun registro, va precisato, è una indicazione minima, potendo ogni Amministrazione dotare di PEC, in ipotesi, anche ogni ufficio o, addirittura, ogni singolo dipendente. Nella prassi, peraltro, non vengono mai attribuiti indirizzi PEC a singoli dipendenti ma solo agli uffici.

(9) Ora l'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi, previsto dall'articolo 6-*ter* del CAD in cui è andata a confluire la struttura costituita dall'IPA, gestito da AgIG.

(10) La disciplina relativa alle notificazioni telematiche non ha mai fatto venire meno (in qualche caso, anzi, facendola espressamente salva), la disciplina prevista dal regio decreto 30 ottobre 1933, n. 1611 ("Approvazione del T.U. delle leggi e delle norme giuridiche sulla rappresentanza e difesa in giudizio dello Stato e sull'ordinamento dell'Avvocatura dello Stato", il cui articolo 11 così dispone: "*Tutte le citazioni, i ricorsi e qualsiasi altro atto di opposizione giudiziale, nonché le opposizioni ad ingiunzione e gli atti istitutivi di giudizi che si svolgono innanzi alle giurisdizioni amministrative o speciali, od innanzi agli arbitri, devono essere notificati alle Amministrazioni dello Stato presso l'ufficio dell'Avvocatura dello Stato nel cui distretto ha sede l'Autorità giudiziaria innanzi alla quale è portata la causa, nella persona del Ministro competente. Ogni altro atto giudiziale e le sentenze devono essere notificati presso l'ufficio dell'Avvocatura dello Stato nel cui distretto ha sede l'Autorità giudiziaria presso cui pende la causa o che ha pronunciato la sentenza. Le notificazioni di cui ai commi precedenti devono essere fatte presso la competente Avvocatura dello Stato a pena di nullità da pronunciarsi anche d'ufficio*".

(11) Si pensi ad esempio alla notificazione di una sentenza, non al fine di far decorrere il termine breve di impugnazione, ma come atto propedeutico all'azione esecutiva, o ai casi in cui l'Amministrazione stia in giudizio in proprio, nell'ambito dei giudizi di opposizione a sanzione amministrativa o nelle controversie individuali di lavoro *ex* art. 417-*bis*, c.p.c.

avvocati, con l'indicazione nell'atto difensivo e soprattutto con la comunicazione al consiglio dell'ordine, le società e le imprese con la comunicazione al relativo registro tenuto dalle camere di commercio), tra i molti indirizzi PEC di cui comunque potevano disporre, di scegliere quale tra quei molti fosse l'unico destinato alla notificazione di atti processuali e dunque andasse attentamente presidiato.

In parallelo con il passaggio, sin qui illustrato, relativo alla introduzione della notificazione a mezzo PEC da parte degli avvocati, ne va ricordato un altro, anch'esso decisivo nella direzione di un processo telematico che muoveva, allora, ancora i primi passi, costituito dalla modifica (disposta anch'essa dall'articolo 25 della l. 12 novembre 2011, n. 183), in particolare, degli articoli 125, 136 e 366, comma 2, c.p.c. (quest'ultimo specificatamente relativo alla notificazione dei controricorsi in cassazione) tale per cui la modalità ordinaria di invio delle comunicazioni di cancelleria divenne l'invio a mezzo PEC e, solo ove questa non fosse stata possibile, si sarebbe proceduto con le tradizionali modalità cartacee.

A partire dal 1 febbraio 2012, dunque, la modalità ordinaria di comunicazione dei biglietti di cancelleria divenne la notificazione a mezzo PEC, che per i soggetti abilitanti esterni, sia privati (difensori delle parti private, avvocati iscritti negli elenchi speciali, esperti e ausiliari del giudice), che pubblici (avvocati e procuratori dello Stato, dipendenti delle pubbliche amministrazioni), doveva essere eseguita, ai sensi dell'articolo 16 del citato d.m. n. 44 del 2011, "*all'indirizzo di posta elettronica certificata del destinatario, indicato nel registro generale degli indirizzi elettronici*" (12). Lo stesso indirizzo utilizzato, in base all'art. 13 dello stesso d.m., per potere effettuare depositi telematici (13).

---

(12) La coeva modifica dell'articolo 125 c.p.c., disposta sempre dall'articolo 25 della l. n. 183 del 2011, nel senso di aggiungere, all'obbligo di indicazione, nell'atto difensivo, dell'indirizzo PEC, le parole "*comunicato al proprio ordine*" e la soppressione delle parole "*presso cui dichiara di volere ricevere le comunicazioni*", va letto come coordinamento tra disciplina primaria e regolamentare, nella direzione della obbligatorietà delle comunicazioni telematiche, a prescindere dalla relativa manifestazione di volontà contenuta nell'atto difensivo, e della necessaria convergenza tra l'indirizzo comunicato al consiglio dell'ordine e quello comunicato al ReGIndE.

(13) Ai sensi dell'art. 13, d.m. n. 44 del 2011, l'iscrizione nel ReGIndE era presupposto necessario per potere depositare telematicamente gli atti; a quel punto, l'indirizzo PEC così registrato diveniva anche l'indirizzo al quale ricevere le comunicazioni telematiche da parte dell'ufficio giudiziario.

Per tale ragione, anche le pubbliche amministrazioni iniziarono a comunicare il proprio indirizzo PEC sul ReGIndE (14); a volte, anche una pluralità di indirizzi, ognuno riferito ad una diversa articolazione della singola Amministrazione, in qualche caso pure prescindendo dalla effettiva titolarità, in capo a quell'ufficio, di una capacità processuale autonoma rispetto all'Amministrazione di appartenenza (15).

La combinazione della incertezza legata ai registri che potevano essere considerati "pubblici" ai fini delle notificazioni a mezzo PEC e della certezza, ancorché basata su un diverso criterio, degli indirizzi da utilizzare rispetto alle comunicazioni di cancelleria, ma solo in ambito civile, rendeva evidente l'esigenza di un complessivo riassetto normativo della materia.

Tale esigenza venne parzialmente colta dal legislatore con il decreto legge 18 ottobre 2012, n. 179, con la legge di conversione 17 dicembre 2012, n. 221, e con la legge, successiva di pochi giorni a quella di conversione, 24 dicembre 2012, n. 228.

Con gli interventi normativi dianzi citati, venne dato un assetto pressocché definitivo e omogeno in relazione alle regole di individuazione degli indiritti PEC (e dunque, anche se ancora non così definiti, dei domicili digitali) rilevanti ai fini delle comunicazioni e notificazioni processuali, anche ad istanza di parte.

Venne dunque stabilito, con l'inserimento, sul tessuto della legge n. 53 del 1994, dell'articolo 3-*bis,* comma 1, che le notificazioni telematiche dovevano essere eseguite *da* e *verso* indirizzi risultanti da pubblici elenchi.

Se, poi, dal lato attivo, le notificazioni a mezzo PEC, ai sensi della legge n. 53 del 1994, potevano (e possono) essere eseguite solo dagli avvocati, dal lato passivo l'unico requisito era che il destinatario avesse un indirizzo PEC presente in un registro pubblico.

---

(14) Curarono l'iscrizione nel ReGIndE soprattutto le PP.AA. più attente o più impegnate in giudizi patrocinati con propri funzionari, in base alle funzioni svolte, ad esempio per l'applicazione di sanzioni amministrative, con i connessi giudizi di opposizione — tipicamente, e per rimanere alle articolazioni di amministrazioni statali, le Prefetture per le ordinanze ingiunzione rispetto alle violazioni al codice della strada — ovvero per la ricorrenza di casi di controversie individuali di lavoro trattate ai sensi dell'art. 417-*bis* c.p.c.

(15) Tipico fu il caso dell'allora Ministero dell'Istruzione, dell'università e della ricerca, del quale si registrarono diversi uffici scolastici regionali, ovvero Uffici che, propriamente, non hanno legittimazione autonoma rispetto all'Amministrazione centrale; di contro, non erano iscritti, o non lo erano in maniera sistematica, articolazioni di altre Amministrazioni che frequentemente hanno una legittimazione distinta da quella dell'Amministrazione di riferimento, come per esempio le Prefetture. Risultavano poi del tutto assenti uffici (dell'INPS, ogli Assessorati della Regione Sicilia) che, invece, secondo i rispettivi ordinamenti, avevano la legittimazione passiva e attiva nei relativi giudizi.

Parallelamente vennero operati altri due importanti interventi normativi. Occorre premettere che l'articolo 16, comma 12, del d.l. n. 179 del 2012, "*Al fine di favorire le comunicazioni e notificazioni per via telematica alle pubbliche amministrazioni*" aveva già previsto l'istituzione del registro che venne denominato delle Pubbliche Amministrazioni (nel prosieguo, in forma contratta "delle PA"), tenuto dal Ministero della giustizia e "*consultabile solo dagli uffici giudiziari e dagli uffici notificazioni, esecuzioni e protesti*". Il fatto che non fosse prevista una consultazione da parte degli avvocati, rendeva evidente che detto registro era originariamente pensato per una consultazione finalizzata solo alle notificazioni d'ufficio e non anche ad istanza di parte.

E qui si inserisce, rispetto al tema ora in esame, la duplice modifica apportata dalla l. 24 dicembre 2012, n. 228, al testo del d.l. n. 179 del 2012, appena convertito dalla l. n. 221 del 2012; da una parte, il registro di cui all'articolo 16, comma 12, del d.l. n. 179 del 2012, venne reso consultabile anche agli avvocati (16); dall'altra, venne inserito, sul tessuto del citato d.l. n. 179 del 2012, l'articolo 16-*ter*, che codificava quali registri dovessero essere considerati pubblici "*ai fini della notificazione e comunicazione degli atti in materia civile, penale, amministrativa e stragiudiziale*"), tra i quali, per quanto in particolare ora rileva rispetto alle PA, il registro di cui all'articolo 16, comma 12, del d.l. n. 179 del 2012 (il già menzionato Registro delle P.A.) e il registro generale degli indirizzi elettronici (previsto dal citato articolo 7, d.m. n. 44 del 2011) (17).

---

(16) Modifica apportata dall'art. 1, comma 19, n. 1), lett. *b*), l. 24 dicembre 2012, n. 228.

(17) L'articolo 16-*ter*, nella sua prima formulazione, citava anche, tra le disposizioni di riferimento per l'individuazione dei registri da considerare pubblici, l'articolo 16 del decreto-legge 29 novembre 2008, n. 185. Il richiamo a tale ultima disposizione, tuttavia, creò problemi interpretativi, perché essa menzionava due distinti registri: il registro delle imprese, al comma 6, e il registro IPA, al comma 8. Il richiamo all'IPA (in realtà indiretto, come più avanti, in questa stessa nota, si dirà) era incoerente rispetto alla istituzione del registro delle P.A. come registro di riferimento per le comunicazioni e notificazioni alle pubbliche amministrazioni, atteso che quest'ultimo (il Registro delle P.A.) intendeva ovviare, con la tendenziale previsione di un unico indirizzo PEC per ciascuna P.A. (in tal senso era poi la disciplina regolamentare dettata dal d.m. n. 44 del 2011) proprio alla proliferazione di indirizzi contenuti dell'IPA. Il legislatore intervenne a sanare tale evidente incoerenza solo con il d.l. 24 giugno 2014, n. 90, il cui articolo 45-*bis*, comma 2, lett. *a*), n. 1), inserì, all'articolo 16-*ter* del d.l. n. 179 del 2012, la specificazione che il registro da considerarsi pubblico ai fini delle comunicazioni e notificazioni telematiche era solo quello di cui al comma 6, dell'articolo 16, d.l. n. 185 del 2008, dunque quello tenuto dalla camera di commercio, per le società e le imprese, e non anche l'IPA.

Precisamente, comunque, il comma 8 stabiliva che "*le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni,*

Va a questo punto specificatamente affrontato, in materia di domicilio digitale delle pubbliche amministrazioni, il tema relativo al Registro delle P.A., il cui percorso è stato segnato da due diverse fasi, prima e dopo il decreto legge 16 luglio 2020, n. 76.

5.2. Il Registro delle PA: le ragioni del mancato popolamento, sino alla novella del 2020

L'articolo 16, comma 12, del d.l. 18 ottobre 2012, n. 179, istitutivo, come si è visto, del Registro delle P.A., aveva anche stabilito il termine di 180 giorni (dalla entrata in vigore della legge), poi prorogato al 30 novembre 2014, affinché le Pubbliche amministrazioni comunicassero "*l'indirizzo di posta elettronica certificata conforme a quanto previsto dal decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, e successive modificazioni, a cui ricevere le comunicazioni e notificazioni*".

Si trattava, secondo le intenzioni del legislatore, di stabilire quale fosse il domicilio digitale di ogni pubblica amministrazione al quale inviare le comunicazioni e le notificazioni "introduttive", perché una volta che la PA si fosse costituita in giudizio, si sarebbero seguite le relative regole di domiciliazione della parte costituita (e dunque presso il difensore).

L'uso dell'articolo determinativo ("*L'indirizzo*") rendeva palese l'intenzione del legislatore di far sì che ogni P.A. avesse uno ed un solo indirizzo di riferimento per le comunicazioni e le notificazioni a mezzo PEC (18).

---

qualora non" avessero "*provveduto ai sensi dell'articolo 47, comma 3, lettera* a)*, del Codice dell'Amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82*" e dunque qualora non avessero provveduto a comunicare i propri indirizzi PEC all'IPA, avrebbero dovuto istituire "*una casella di posta certificata o analogo indirizzo di posta elettronica di cui al comma 6 per ciascun registro di protocollo*", dandone "*comunicazione al Centro nazionale per l'informatica nella pubblica amministrazione, che provvede alla pubblicazione di tali caselle in un elenco consultabile per via telematica*". Come si vede, il comma 8, nel menzionare l'IPA, sembrava in realtà volere istituire un nuovo e distinto registro, sia pure ancora gestito dal CNIPA, nel quale le PA che non avessero provveduto a comunicare i propri indirizzi al primo registro, ne comunicassero almeno uno per ciascun registro di protocollo; il riferimento all'IPA, tuttavia, venne comunemente inteso come inclusione di tale Indice tra i registri pubblici validi ai fini delle comunicazioni e notificazioni telematiche ai sensi dell'articolo 16-*ter* del d.l. n. 179 del 2012.

(18) Come accennato, nel senso della unicità dell'indiizzo PEC per ciascuna Amministrazione, secondo lo schema che individuava un rapporto univoco tra PA, relativo codice fiscale (che si supponeva sempre esistente e unico) e corrispondente domicilio digitale erano anche le disposizioni di cui al già citato D.M. n. 44 del 2011 e le specifiche tecniche adottate ai sensi dell'articolo 34 dello stesso D.M. e, in particolare l'articolo 9-*bis*, dedicato agli "*indirizzi di posta elettronica certificata delle pubbliche amministrazioni*".

La realtà era più complessa, in primo luogo perché per le Amministrazioni soggette, ai sensi dell'articolo 1 del r.d. 30 ottobre 1933, n. 1611 ([19]), al patrocinio cosiddetto "necessario" dell'Avvocatura dello Stato, anche le comunicazioni e le notificazioni introduttive, come si è in precedenza rammentato, *ex* art. 11 dello stesso r.d. ([20]), vanno eseguite al difensore, dunque all'Avvocatura dello Stato; in secondo luogo perché nei casi di difesa in proprio della P.A., l'individuazione del domicilio di riferimento presenta profili problematici che l'istituzione del Registro delle P.A. non risolveva ed anzi complicava, perché quello comunicato a quest'ultimo diventava l'unico indirizzo PEC per le comunicazioni e le notificazioni sia prima che dopo la costituzione in giudizio. Con tutti i connessi problemi cui si farà cenno nel prosieguo.

Fatto è che, all'inizio del 2020, scaduto da oltre cinque anni il termine concesso alle Pubbliche Amministrazioni per iscriversi, il registro delle P.A. risultava ancora scarsamente popolato.

Tale, evidente e da più parti lamentato insuccesso, dipendeva, probabilmente, proprio da quanto si è appena ricordato, circa la semplicistica visione secondo cui ogni pubblica amministrazione avrebbe dovuto avere un unico domicilio digitale cui ricevere le comunicazioni e le notificazioni telematiche.

Un'ambizione stabilita (implicitamente, ma chiaramente) dalla norma primaria, che non teneva conto della complessità del fenomeno che andava a regolare: se pure è vero, infatti, che esistono Amministrazioni atomistiche, le quali ben possono avere un unico indirizzo PEC a valere per l'intera organizzazione, ve ne sono altre per le quali ciò risulta non solo disfunzionale, se si tratta di una P.A. molto estesa, ma in certi casi persino in contrasto

---

([19]) Così stabilisce l'articolo citato nel testo: "*La rappresentanza, il patrocinio e l'assistenza in giudizio delle Amministrazioni dello Stato, anche se organizzate ad ordinamento autonomo, spettano alla Avvocatura dello Stato. Gli avvocati dello Stato, esercitano le loro funzioni innanzi a tutte le giurisdizioni ed in qualunque sede e non hanno bisogno di mandato, neppure nei casi nei quali le norme ordinarie richiedono il mandato speciale, bastando che consti della loro qualità*".

([20]) Così stabilisce l'articolo citato nel testo: "*Tutte le citazioni, i ricorsi e qualsiasi altro atto di opposizione giudiziale, nonché le opposizioni ad ingiunzione e gli atti istitutivi di giudizi che si svolgono innanzi alle giurisdizioni amministrative o speciali, od innanzi agli arbitri, devono essere notificati alle Amministrazioni dello Stato presso l'ufficio dell'Avvocatura dello Stato nel cui distretto ha sede l'Autorità giudiziaria innanzi alla quale è portata la causa, nella persona del Ministro competente.*

Ogni altro atto giudiziale e le sentenze devono essere notificati presso l'ufficio dell'Avvocatura dello Stato nel cui distretto ha sede l'Autorità giudiziaria presso cui pende la causa o che ha pronunciato la sentenza.

Le notificazioni di cui ai commi precedenti devono essere fatte presso la competente Avvocatura dello Stato a pena di nullità da pronunciarsi anche d'ufficio".

con il rispettivo ordinamento, laddove, in determinate materie, loro organi o articolazioni abbiano autonoma capacità processuale (con la relativa possibilità di stare in giudizio tramite propri dipendenti), o sia comunque prevista, presso di essi, la notifica di atti giudiziari.

È quanto accade, per esempio, per le Prefetture, quali organi del Ministero dell'Interno, nei giudizi di opposizione a sanzioni amministrative, e per gli uffici territoriali dell'Agenzia delle entrate e dell'INPS, rispettivamente, nei giudizi tributari e in quelli previdenziali.

Tutte le pubbliche amministrazioni, poi, hanno la possibilità, in determinati giudizi (le controversie individuali di lavoro pubblico, *ex* art. 417-*bis* c.p.c.), di costituirsi tramite propri funzionari.

Si tratta di situazioni nelle quali l'obbligo di registrarsi con un solo indirizzo rappresentava un ostacolo al corretto dispiegarsi delle dinamiche processuali, ed è questo che, di fatto, ha comportato, da parte delle amministrazioni coinvolte, l'omissione dell'adempimento, per mantenere la tradizionale modalità cartacea di comunicazione e notificazione presso gli uffici legittimati a riceverle (21).

La risposta a questo mancato popolamento, ovviamente, non poteva essere, come da più parti veniva invocato, il recupero dell'IPA (22), un registro istituito, come ricordato, per assicurare lo scambio di corrispondenza con le pubbliche amministrazioni, ma non le qualificate transazioni costituite dalle notificazioni o comunicazioni processuali, e perciò correttamente espunto, a suo tempo, dall'articolo 16-*ter* del d.l. n. 179 del 2012 (23).

Nel caso delle PP.AA., dunque, se non poteva imporsi, a determinate condizioni, l'indicazione di un solo domicilio digitale, nemmeno poteva

---

(21) Mancava, nel testo dell'articolo 16, comma 12, del d.l. n. 179 del 2012, una disposizione che disciplinasse la modalità di effettuazione delle comunicazioni e notificazioni in caso di omissione dell'obbligo di registrazione sul registro delle P.A.; i tali casi, dunque, si ricorreva alla tradizionale modalità cartacea.

(22) Ovvero il precedente "*Indice degli indirizzi delle pubbliche amministrazioni*", già regolato dall'articolo 57-*bis* del CAD ed ora ridenominato "*Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi*" e disciplinato dall'articolo 6-*ter* dello stesso Cad, inizialmente contemplato, come si è ricordato in altra nota di questo stesso testo, dall'articolo 16-*ter* del d.l. n. 179/2012, poi espunto dall'articolo 45-*bis*, comma 2, lett. *a*), n. 1), d.l. 24 giugno 2014, n. 90, convertito, con modificazioni, dalla l. 11 agosto 2014, n. 114.

(23) In giursprudenza, si segnala, tra le altre, Cass, 25 agosto 2021, n. 23445, che, ricostruita la successione di norme rispetto agli elenchi da considerarsi pubblici ai fini delle comunicazioni e notificazioni telematiche, sino alla modifica dettata dal decreto-legge 16 luglio 2020, n. 76 (di cui si dirà diffusamente più avanti, nel testo), ha ribadito l'oramai consolidato orientamento secondo cui è nulla la notifica effettuata ad un indirizzo PEC tratto dall'IPA, fuori dai casi ora regolati dal citato d.l. n. 76 del 2020 e, in precedenza, dal breve periodo in cui l'IPA stesso era menzionato dall'articolo 16-*ter* del d.l. n. 179 del 2012.

aprirsi all'utilizzo indifferenziato di qualunque indirizzo PEC risultante dal registro IPA.

Il problema non si poneva, ovviamente, per i soggetti pubblici che si avvalgono del patrocinio *ex lege* (cosiddetto patrocinio necessario, *ex* art. 1 del r.d. n. 1611 del 1933) dell'Avvocatura dello Stato o comunque si fossero costituiti in giudizio per il tramite di quest'ultima (nell'ambito del cosiddetto patrocinio autorizzato, *ex* art. 43, r.d. n. 1611 del 1933) (24) o di Avvocati interni (nell'ambito degli uffici legali istituiti presso determinati Enti, con avvocati dipendenti iscritti nel relativo elenco speciale), dal momento che, in tali casi, la domiciliazione si radica ordinariamente presso il difensore (per l'Avvocatura dello Stato, nei casi previsti dal citato art. 1 del r.d. n. 1611 del 1933, anche prima della costituzione in giudizio) e si esula quindi dall'ambito applicativo del registro di cui all'art. 16, comma 12, d.l. n. 179 del 2012, orientato a stabilire il domicilio digitale delle pubbliche amministrazioni rispetto alle comunicazioni e notificazioni "introduttive", cioè prima della costituzione in giudizio (25).

---

(24) In base all'articolo citato nel testo, "*L'Avvocatura dello Stato può assumere la rappresentanza e la difesa nei giudizi attivi e passivi avanti le Autorità giudiziarie, i Collegi arbitrali, le giurisdizioni amministrative e speciali, di amministrazioni pubbliche non statali ed enti sovvenzionati, sottoposti a tutela od anche a sola vigilanza dello Stato, sempre che sia autorizzata da disposizione di legge, di regolamento o di altro provvedimento approvato con regio decreto. Le disposizioni e i provvedimenti anzidetti debbono essere promossi di concerto coi Ministri per la grazia e giustizia e per le finanze. Qualora sia intervenuta l'autorizzazione, di cui al primo comma, la rappresentanza e la difesa nei giudizi indicati nello stesso comma sono assunte dalla Avvocatura dello Stato in via organica ed esclusiva, eccettuati i casi di conflitto di interessi con lo Stato o con le regioni. Salve le ipotesi di conflitto, ove tali amministrazioni ed enti intendano in casi speciali non avvalersi della Avvocatura dello Stato, debbono adottare apposita motivata delibera da sottoporre agli organi di vigilanza. Le disposizioni di cui ai precedenti commi sono estese agli enti regionali, previa deliberazione degli organi competenti*".

(25) Come ulteriore fattore di complicazione, si segnala che talune amministrazioni hanno diversi codici fiscali, in alcuni casi numerosissimi codici fiscali (il Ministero dell'Interno, per esempio, ne conta ben 337), mentre altre ne hanno uno solo (e per esempio proprio l'Agenzia delle entrate e l'INPS) sicché una regola di popolamento fondata, come era stabilito dalle specifiche tecniche del Ministero della giustizia del 16 maggio 2014, sia per il Registro delle pa che per il ReGIndE, secondo lo schema "codice fiscale= persona giuridica = PEC" si rivelava inevitabilmente fallace.

Tanto più che si danno anche casi nei quali determinati organi che hanno una soggettività giuridica ed una capacità processuale distinta da quella dell'Amministrazione di cui fanno parte (ad esempio i già ricordati Assessorati della Regione Siciliana) ma sono comunque privi di un codice fiscale distinto da quello della stessa Amministrazione.

5.3. L'attuale assetto: il domicilio digitale delle Pubbliche Amministrazioni dopo la novella del 2020

Le ricordate problematiche hanno infine trovato soluzione con le modifiche che l'articolo 28, comma 1, lett. *a*) e *c*), del d.l. 16 luglio 2020, n. 76, ha apportato agli articoli 16, comma 12, e 16-*ter* del d.l. n. 179 del 2012.

Con la nuova formulazione dell'articolo 16, comma 12, del d.l. n. 179 del 2012, si è in buona sostanza preso atto della complessa realtà delle PP.AA., non riconducibili forzatamente, e, invero, un po' semplicisticamente, ad uno schema che prevedesse sempre e solo un unico indirizzo PEC (*rectius*, domicilio digitale).

Il nuovo articolo 16, comma 12, dunque, di seguito al periodo che stabilisce il perdurante obbligo di comunicare "*al Ministero della giustizia... l'indirizzo di posta elettronica certificata... a cui ricevere comunicazioni e notificazioni*", prevede ora la possibilità (si badi, non anche l'obbligo), per le PP.AA., di "*comunicare altresì gli indirizzi di posta elettronica certificata di propri organi o articolazioni, anche territoriali, presso cui eseguire le comunicazioni e notificazioni per via telematica, nel caso in cui sia stabilito presso questi l'obbligo di notifica degli atti introduttivi di giudizio in relazione a specifiche materie ovvero in caso di autonoma capacità o legittimazione processuale*". In questa prima ipotesi, la possibilità di comunicare più di un indirizzo PEC trova il suo presupposto nel fatto che vi siano articolazioni o organi presso i quali sia previsto l'obbligo di notifica degli atti introduttivi. Il legislatore ha dunque opportunamente preso atto che questa è la situazione in relazione a determinate amministrazioni o materie, rispetto alle quali, senza intervenire sul citato obbligo di notifica, ove per legge rivolto non alla sede centrale, ma all'organo o all'ufficio periferico, non poteva non essere consentita una corrispondente notificazione telematica presso quello stesso organo o ufficio. Per l'effetto, andava permessa la comunicazione anche di altri indirizzi PEC, sia pure sotto la responsabilità e per scelta dell'Amministrazione dichiarante.

Indi, con un ultimo periodo, l'articolo 16, comma 12, regola anche il caso delle Amministrazioni costituitesi in giudizio tramite propri dipendenti, in relazione all'indirizzo PEC presso cui eleggere domicilio ai fini del giudizio. Prima che il legislatore si occupasse di regolamentare la fattispecie, accadeva infatti — se ne è già fatto cenno — che le PP.AA., costituendosi in giudizio, non potessero che ricevere comunicazioni e notificazioni endo-processuali ancora verso quell'unico indirizzo previsto per le comunicazioni e notificazioni "introduttive". In relazione a tale aspetto, è ora previsto che, per l'appunto, in "*caso di costituzione in giudizio tramite propri dipendenti, le amministrazioni pubbliche possono*" — anche qui, si badi, possono ma non

devono — *"altresì comunicare ulteriori indirizzi di posta elettronica certificata, riportati in una speciale sezione dello stesso elenco di cui al presente articolo e corrispondenti a specifiche aree organizzative omogenee, presso cui eleggono domicilio ai fini del giudizio*".

Come si vede, la possibilità di inserire indirizzi PEC ulteriori, per il caso di costituzione tramite propri dipendenti, è finalizzata non alla individuazione di domicili digitali eletti con rilevanza pre-processuale, ma solo endo-processuale, essendo specificato che si tratta di elezione di domicilio "*ai fini del giudizio*" (26).

A completamento delle modifiche sin qui illustrate, è stato poi integrato anche l'articolo 16-*ter* del d.l. n. 179 del 2012. Invariato il primo comma, relativo alla individuazione degli elenchi pubblici ai fini delle comunicazioni e notificazioni degli atti in materia civile, penale, amministrativa, contabile e stragiudiziale, il comma 1-*bis* è stato aggiornato con la precisazione che anche il neo introdotto comma 1-*ter,* (come già il preesistente comma 1) trova applicazione "*alla giustizia amministrativa*" (27) .

La modifica più rilevante riguarda tuttavia proprio l'inserimento del comma 1-*ter*, volto a regolare le conseguenze derivanti dalla mancata indicazione, nel Registro delle PA, degli indirizzi di cui al precedente articolo 16, comma 12.

Il comma inizia con il precisare che restano ferme le disposizioni di cui al "*regio decreto 30 ottobre 1933, n. 1611, in materia di rappresentanza e difesa in giudizio dello Stato*". La precisazione è opportuna, volendosi così chiarire che l'istituzione del registro delle PA non fa venire meno la domiciliazione *ex lege* presso l'Avvocatura dello stato delle amministrazioni, degli enti e degli organismi di diritto pubblico soggetti al patrocinio necessario dell'Avvocatura dello Stato. Si tratta dunque di un registro che opera nei casi in cui, secondo la normativa vigente, la comunicazione o la notificazione debba o

---

(26) A seguito delle modifiche introdotte dal d.l. n. 76 del 2020, sono poi state coerentemente adeguate, con provvedimento del 26 luglio 2021, anche le specifiche tecniche adottate ai sensi dell'articolo 34 del d.m. n. 44 del 2011, alle quali è stato aggiornato l'articolo 9-*bis,* già dedicato agli "*indirizzi di posta elettronica certificata delle pubbliche amministrazioni*", e inserito l'articolo 9-*ter*, relativo proprio agli "*Indirizzi di posta elettronica certificata degli organi, delle articolazioni, anche territoriali, e delle aree organizzative omogenee delle amministrazioni pubbliche*".

(27) Come già la precisazione relativa al primo comma, anche quella relativa al comma 1-*ter*, circa l'applicabilità della disposizioe alla "giustizia amministrativa" appare per il vero uno scrupolo eccessivo del legislatore, dal momento che il riferimento alla notificazione degli atti in materia amministrativa, contenuto sia nel comma 1 che nel comma 1-*ter,* sin da quando utilizzata, per esempio, all'articolo 1, l. n. 53 del 1994, nella sua originaria formulazione, per attribuire agli avvocati la facoltà di notificazione a mezzo del servizio postale, è sempre stata intesa come riferita anche, e per l'appunto, alla giustizia amministrativa.

possa essere effettuata direttamente presso la P.A., senza volere in alcun modo intervenire, appunto, sulla normativa preesistente.

È stato quindi previso che, ove non sia stato ottemperato l'obbligo di cui all'articolo 16, comma, 12, del d.l. n. 179 del 2012, consistente nella registrazione del proprio domicilio digitale nel Registro delle PA, la notifica può essere validamente effettuata "*presso l'indirizzo di posta elettronica certificata primario indicato, secondo le previsioni delle Linee Guida di AgID, nella sezione ente dell'amministrazione pubblica destinataria*". Nel caso in cui la mancata indicazione riguardi gli organi o articolazioni, anche territoriali, presso cui è previsto l'obbligo di notifica degli atti introduttivi di giudizio, allora la notificazione può essere eseguita all'indirizzo che, per detti organi, sia pure con le diverse finalità previste da quel diverso indice, sono inserite nell'artico 6-*ter* del CAD.

La chiave ispiratrice della disposizione è stata quella di prevedere non solo un mero obbligo di comunicazione (le ulteriori comunicazioni in esame sono state anzi opportunamente costruite, si è già evidenziato, come facoltà in capo alla singola P.A.), magari anche accompagnato da un termine "canzonatorio", la cui violazione non avrebbe avuto alcun effetto, ma, semmai, e con approccio concreto, le conseguenze che sarebbero derivate da dette mancate comunicazioni, sia da quella principale, originaria e obbligatoria (l'obbligo di comunicare "*l'indirizzo di posta elettronica certificata... al quale ricevere comunicazioni e notificazioni*"), sia da queste ulteriori e facoltative. Nella individuazione delle riportate soluzioni, il legislatore ha cercato di trovare un punto di equilibro tra un profilo *lato sensu* sanzionatorio per l'inerzia della PA, l'esigenza di far evolvere il sistema, nel suo complesso, nella direzione della dematerializzazione degli scambi documentali, e l'individuazione di un rimedio che comunque permettesse di raggiungere il destinatario mettendo questi in condizione di sapere a quale indirizzo PEC sarebbe stato attinto.

5.4. Le peculiarità dell'Avvocatura dello Stato

L'Avvocatura dello Stato, come si è avuto modo di ricordare in precedenza, ha il patrocinio *ex lege* di tutte le Amministrazioni dello Stato, nonché di una molteplicità di altre pubbliche amministrazioni.

In base all'articolo 18, r.d. n. 1611 del 1933, "*L'Avvocatura dello Stato è costituita dall'Avvocatura generale e dalle avvocature distrettuali*".

L'Avvocatura generale, come è noto, ha sede in Roma, mentre le Avvocature distrettuali hanno le sedi in corrispondenza di ciascuna sede di Corte d'appello.

Il patrocinio dell'Avvocatura dello Stato trova la sua fonte normativa nel r.d. n. 1611 del 1933, ed in particolare negli articoli 1, relativo al cosiddetto

patrocinio necessario (di cui ancora si dirà più avanti, nel testo), e 43 ([28]), relativo al cosiddetto patrocinio autorizzato.

Il patrocinio autorizzato, peraltro, si differenzia rispetto al patrocinio necessario solo per quanto concerne la domiciliazione presso l'Avvocatura dello Stato e l'applicazione del foro erariale; restano invece fermi, per le Amministrazioni e gli enti ammessi al patrocinio autorizzato, l'obbligo di avvalersi dell'Avvocatura dello Stato, fatti salvi i casi di conflitto con Amministrazioni soggette al patrocinio di cui al citato articolo 1 o altre, specifiche e particolari situazioni, da motivare caso per caso.

In entrambe le ipotesi considerate dal r.d. n. 1611 del 1933, dunque, l'Avvocatura dello Stato è difensore *ex lege* dei soggetti pubblici ammessi all'una o all'altra tipologia di patrocinio.

Si tratta di un peculiare caso di patrocinio impersonale, in quanto attribuito all'Avvocatura dello Stato in quanto tale e non ai singoli Avvocati e Procuratori dello Stato.

L'art. 1, comma 1, r.d. n. 1611 del 1933, come si è già riportato in precedenza, prevede infatti che *"La rappresentanza, il patrocinio e l'assistenza in giudizio delle Amministrazioni dello Stato, anche se organizzate ad ordinamento autonomo, spettano alla Avvocatura dello Stato"*.

Sul punto, poi, è granitico l'orientamento della giurisprudenza di legittimità nel senso di ritenere "*che gli avvocati dello Stato esercitano le loro funzioni innanzi a tutte le giurisdizioni ed in qualunque sede, senza bisogno di mandato, neppur quando le norme ordinarie richiedono il mandato speciale, come nel caso di ricorso per cassazione, e che, avendo la difesa dell'Avvocatura dello Stato carattere impersonale, ed essendo quindi gli avvocati dello Stato pienamente fungibili nel compimento di atti processuali relativi ad un medesimo giudizio, l'atto introduttivo di questo è valido anche se la sottoscrizione è apposta da avvocato diverso da quello che materialmente ha redatto l'atto, unica condizione richiesta essendo la spendita della qualità professionale abilitante alla difesa*" (Cass. 28 marzo 2012, n. 4950; Cass. 7 aprile 2022, n. 11324).

È pur vero che la disciplina regolamentare del processo civile telematico, costituita dal più volte citato d.m. n. 44 del 2011 e dalle specifiche tecniche adottate ai sensi dell'articolo 34 dello stesso d.m., nel testo precedente alle modifiche da ultimo apportate dal d.m. 29 dicembre 2023, n. 217, non faceva espresso riferimento all'Avvocatura dello Stato in quanto tale ([29]), ma solo

([28]) Il testo dell'articolo è stato già riportato nella nota 23, cui si rinvia.

([29]) Se non all'articolo 23, comma 6, del d.m. n. 44 del 2011, tra i soggetti ai quali è permesso attivare un punto di accesso al PCT, in un senso dunque diverso da quello cui si fa riferimento nel testo, dunque come soggetto processuale.

agli Avvocati e Procuratori dello Stato, individuati dall'articolo 2, comma 1, lett. *m*), n. 4, come i soggetti abilitati esterni pubblici.

Si trattava, tuttavia, di una disposizione che andava letta in senso conforme alla disciplina di rango primario, e dunque come riferita, tramite gli "agenti" (gli Avvocati e i Procuratori dello Stato), al soggetto propriamente difensore, cioè a dire, si ripete, l'Avvocatura dello Stato.

Le modifiche recentemente apportate dal citato d.m. n. 217 del 2023 hanno reso esplicito questo corretto riferimento all'Avvocatura dello Stato, ora espressamente menzionata, anche nelle sue articolazioni distrettuali, all'articolo 2, comma 1, lettera *m*), n. 4, tra i soggetti abilitati esterni pubblici (30).

Rispetto al tema in esame, l'Avvocatura dello Stato si presenta sotto un duplice profilo: da una parte come PA, dall'altra, invece, come difensore. Dei registri dichiarati come "*pubblici elenchi*" dall'articolo 16-*ter* del d.l. n. 179 del 2012, vengono dunque in rilievo, rispetto al primo profilo, il registro delle P.A. di cui all'articolo 16, comma 12, dello stesso d.l. n. 179 del 2012, e, rispetto al secondo profilo, quale difensore abilitato a operare sul PCT, il ReGIndE di cui all'articolo 7, d.m. n. 44 del 2011.

In ciascuno di detti registri, è l'Avvocatura dello Stato in quanto tale, nelle sue diverse sedi distrettuali, a dover essere censita e ricercabile, non i singoli Avvocati e Procuratori dello Stato, e ciò in ragione della ricordata natura impersonale del relativo patrocinio.

È questo un aspetto che marca una differenza netta rispetto tutti gli altri Avvocati, sia del libero foro che degli Enti Pubblici (come pure, nei limitati casi in cui sia consentito, per i funzionari delle PP.AA.), venendo in questi casi il mandato difensivo sempre conferito al singolo Avvocato, in rappresentanza dell'Ente.

Rispetto alle Amministrazioni da essa patrocinate, il difensore è invece l'Avvocatura dello Stato, ed è dunque il domicilio digitale di questa a dover essere censito nei due registri di interesse, restando irrilevanti, a tali fini, i dati dei singoli Avvocati e Procuratori dello Stato.

Occorre poi, in linea teorica, distinguere se si sta notificando all'Avvocatura dello Stato come pubblica amministrazione (ad esempio nel caso del

---

(30) Il nuovo testo dell'articolo 2, comma 1, lettera *m*), d.m. n. 44 del 2011, menziona ora, al numero 3), tra i soggetti abilitati esterni privati, anche "*le persone fisiche che possono stare in giudizio personalmente e quelle che rappresentano un ente privato*", e, al numero 4), tra i soggetti abilitati esterni pubblici, dopo "*l'Avvocatura generale dello Stato, le avvocature distrettuali dello Stato*", nonché i già contemplati "*avvocati e i procuratori dello Stato, gli altri dipendenti di amministrazioni statali, regionali, metropolitane, provinciali e comunali*", anche "*il personale di polizia giudiziaria ed ogni altro soggetto tenuto per legge alla trasmissione della notizia di reato e delle comunicazioni successive*".

dipendente che notifichi un ricorso per una controversia individuale di lavoro), ipotesi nella quale viene in rilievo, per la notifica introduttiva, il Registro delle PA, o come difensore di una Pubblica Amministrazione, perché, in tale ipotesi, il registro propriamente di riferimento è quello, tra gli altri, dei difensori, e dunque il ReGIndE.

Detto del diverso profilo per cui l'Avvocatura dello Stato viene in rilievo rispetto ai due registri in esame, va anche detto che la questione, sia pure in via di fatto, perde di concreta rilevanza dal momento che l'Avvocatura stessa, nelle sue diverse sedi, è registrata con i medesimi indirizzi su entrambi i registri.

Non pare superfluo evidenziare, a completamento del presente paragrafo, che non viene invece in rilievo, per l'Avvocatura dello Stato, l'Indice nazionale dei domicili digitali delle imprese e dei professionisti (cosiddetto "INIPEC"), previsto dall'articolo 6-*bis* del CAD, anch'esso indicato dall'articolo 16-*ter* come registro pubblico. Si tratta invero di un registro le cui regole di popolamento, basate sul censimento individuale, a fronte del patrocinio impersonale dell'Avvocatura dello Stato, e sui dati provenienti, per quanto riguarda i professionisti, dai Consigli degli ordini, certamente portano ad escludere la possibile inclusione dell'Avvocatura dello Stato, dal momento che questa, dal punto di vista ordinamentale, si colloca al di fuori del perimetro di applicazione del regio decreto legge 27 novembre 1933, n. 1578, disciplinante, per l'appunto, l'ordinamento "*delle professioni di avvocato e di procuratore*".

VI.

LE PATOLOGIE DERIVANTI DALL'IMPIEGO NON CORRETTO DI IDENTITÀ O DOMICILIO DIGITALI

di *Roberto Arcella* e *Giovanni Rocchi*

Sommario: 6.1. Introduzione. — 6.2. Mancata istituzione del domicilio digitale per soggetti obbligati. — 6.2.1. Conseguenze della mancata elezione del domicilio digitale da parte delle imprese. — 6.2.2. Conseguenze della mancata elezione del domicilio digitale da parte dei professionisti. — 6.2.3. Conseguenze della mancata elezione del domicilio digitale da parte delle pubbliche amministrazioni. — 6.3. La condivisione medesimo domicilio. — 6.3.1. La sussistenza dell'obbligo di unicità del domicilio digitale. — 6.3.2. Il fenomeno nell'ambito della disciplina del PCT. — 6.4. Patologia nella pratica - Aspetti tecnico-giuridici. — 6.4.1. La trasmissione del messaggio verso il domicilio digitale. — 6.4.2. Casella inattiva o indirizzo non riconosciuto. — 6.4.3. Casella piena. — 6.5. La patologia dei domicili digitali nell'ambito delle notificazioni. — 6.5.1. La disciplina di cui all'art. 3-*ter*, legge 21 gennaio 1994, n. 53. — 6.5.2. La notificazione impossibile. — 6.5.3. La notificazione non andata a buon fine. — 6.5.4. L'area web di cui all'art. 359 del d.lgs. 12 gennaio 2019, n. 14. — 6.5.5. La sospensione dell'efficacia dei commi 2 e 3 dell'art. 3-*ter* della l. n. 53 del 1994. — 6.5.6. Riepilogo anomalie notifiche PEC.

6.1. Introduzione

La transizione dalla documentazione analogica alla digitalizzazione ha generato una significativa trasformazione di alcuni istituti giuridici tradizionali, ponendo nuove sfide e aprendo orizzonti inediti. L'inadeguatezza di alcuni concetti si è manifestata inesorabilmente e, tra essi, quello di indirizzo del destinatario richiamato nell'art. 1335 del Codice civile. Nell'ambito di comunicazioni basate sullo scambio di meri dati immateriali, l'indirizzo cui associare le presunzioni di conoscenza previste dalla norma non poteva di certo identificarsi nel domicilio fisico dei soggetti.

Il domicilio digitale rappresenta quindi un'evoluzione del concetto di domicilio tradizionalmente inteso, basato sulla fisicità e sulla localizzazione geografica.

L'esigenza che ne è derivata è stata inizialmente colmata dall'articolo 48 del Codice dell'Amministrazione Digitale, che ha regolamentato gli effetti

della trasmissione telematica mediante Posta Elettronica Certificata (PEC) con la relativa equiparazione agli effetti prodotti dalla ricezione della raccomandata di ricevuta di ritorno postale. Tanto avvenne ben prima dell'introduzione, attraverso i successivi correttivi al Codice dell'Amministrazione Digitale, della lettera *v-bis* nell'articolo 1 (nel 2010), che forniva la definizione di "posta elettronica certificata", e della lettera *n-ter* (nel 2017), che codificò l'attuale definizione di domicilio digitale.

La definizione normativa di domicilio digitale è contenuta oggi nell'articolo 3-*bis*, comma 3, del Codice dell'amministrazione digitale (CAD), secondo cui "*Il domicilio digitale è l'indirizzo elettronico eletto presso un servizio di posta elettronica certificata (PEC) o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, valido ai fini delle comunicazioni elettroniche aventi valore legale ai sensi dell'articolo 1, comma 1, della legge 23 dicembre 1997, n. 499*". Quest'ultima, in una prospettiva chiaramente evolutiva, ricomprende non solo l'indirizzo di posta elettronica certificata, ma anche gli indirizzi elettronici eletti presso un recapito elettronico certificato qualificato, con un espresso richiamo alla normativa unionale dettata dal Regolamento eIDAS. Al riguardo, conviene ricordare che, nell'ambito dell'adozione delle scelte tecniche per l'attuazione della normativa euro-unionale sui SERCQ, l'Agenzia per l'Italia Digitale (AgID) ha adottato lo standard REM (Registered Email Message, standard sviluppato dall'ETSI - *European Telecommunications Standards Institute*) con la determinazione n. 233 del 9 agosto 2022. La conformità agli standard REM comporta una serie di vantaggi per i servizi di comunicazione elettronica, vale a dire maggiore sicurezza e affidabilità delle comunicazioni elettroniche, maggiore interoperabilità tra i diversi servizi, riduzione dei costi di implementazione e gestione dei servizi SERCQ. Nello specifico, a differenza dell'attuale PEC, la cui validità ai fini delle comunicazioni e notificazioni è basata essenzialmente sull'associazione biunivoca tra soggetti ed indirizzi elettronici contenuta in elenchi pubblici, lo standard REM dovrebbe garantire la possibilità di verifica *ex se* dell'esistenza del destinatario.

Nell'attuale contesto, come accennato, la corrispondenza tra soggetti e caselle di posta elettronica certificata è assicurata dall'iscrizione di tali indirizzi in appositi elenchi, che sono quelli previsti, nell'ambito del Codice dell'Amministrazione digitale, dall'art. 6-*bis* (Indice nazionale dei domicili digitali delle imprese e dei professionisti), dall'art. 6-*ter* (Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi) e dall'art. 6-*quater* (Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese), nonché

quelli individuati dall'art. 16, comma 6, del decreto-legge 29 novembre 2008, n. 185 (Registro Imprese) e, ancora, dal Registro generale degli indirizzi elettronici, gestito dal Ministero della giustizia, previsto dall'art. 7, d.m. Giustizia 21 febbraio 2011, n. 44. V'è, inoltre, l'indirizzario dedicato alle Pubbliche Amministrazioni destinato ad interoperare con i sistemi informativi del Ministero della Giustizia, previsto dall'art. 16, d.l. 18 ottobre 2012, n. 179, che merita un discorso diverso sul quale ci si soffermerà nel prosieguo.

L'iscrizione in tali indirizzari costituisce uno specifico obbligo per particolari categorie di soggetti, come accade per le imprese, ai sensi del citato art. 16, comma 6-*bis*, d.l. n. 185 del 2008, ovvero le PP.AA., ai sensi dell'art. 16, d.l. n. 179 del 2012, od anche per i professionisti che operano quali "soggetti abilitati esterni" nell'ambito dei processi telematici (in relazione al ReGInde), i professionisti, ai sensi del citato art. 16, comma 7, d.l. n. 185 del 2008, ed infine gli indirizzi che transitano in via automatica dagli albi professionali all'INIPEC, *ex* art. 6-*bis*, CAD, e dall'INIPEC all'INAD, ai sensi dell'art. 6-*quater*, CAD.

6.2. Mancata istituzione del domicilio digitale per soggetti obbligati

La prima e più evidente tra le patologie riscontrabili nella concreta attuazione dei principi dettati dal codice dell'amministrazione digitale in materia di domicili digitali, anche nell'ambito dello stesso processo civile telematico, attiene proprio al mancato adempimento all'obbligo di iscrizione degli indirizzi PEC nei ricordati pubblici elenchi.

Come accennato, l'ultima iterazione del CAD, oltre a fornire una compiuta definizione del domicilio digitale, contiene una articolata disciplina dei domicili digitali nella quale, in primo luogo, viene ribadito l'obbligo di dotarsene per alcune categorie di soggetti.

Merita peraltro rammentare che l'equivalente obbligo di dotarsi di un indirizzo di posta elettronica certificata già sussisteva dall'entrata in vigore dell'art. 16, d.l. n. 185 del 2008, che, nel suo testo originario, l'aveva introdotto per le imprese costituite in forma societaria, per i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato e per le amministrazioni pubbliche. L'obbligo veniva successivamente esteso, con l'art. 5, co. 1, d.l. n. 179 del 2012, anche alle imprese individuali. L'art. 16, comma 6, d.l. n. 185 del 2008, prevedeva, infatti, che tutte le imprese costituite in forma societaria fossero tenute a indicare il proprio indirizzo di posta elettronica certificata nella domanda di iscrizione al registro delle imprese e che entro il 29 novembre 2011 (i.e.: "*tre anni dalla data di entrata in vigore del presente decreto...*") tutte le imprese, già costituite in forma societaria alla medesima data di entrata in vigore, erano tenute a comunicare al registro delle imprese

l'indirizzo di posta elettronica certificata. Analogo obbligo veniva sancito dal successivo comma 7 per i professionisti, obbligati a comunicare, entro il 29 novembre 2009, i propri indirizzi PEC agli Ordini o Collegi di appartenenza, e dal comma 8 della stessa norma per le pubbliche amministrazioni in relazione al registro, destinato ad evolversi nell'attuale IPA, oggi disciplinato dall'art. 6-*ter* del CAD.

A seguito di plurime modifiche, tra le quali ultima quella introdotta dal decreto semplificazioni (decreto-legge 16 luglio 2020, n. 76), l'attuale disciplina integra l'obbligo dettato dal CAD, ribadendo tale obbligo e prevedendo specifiche conseguenze per i soggetti inadempienti. Senza addentrarsi nella ricostruzione storica dei vari *maquillages* cui è stata sottoposta la normativa *in parte qua*, basterà ricordare che il citato decreto semplificazioni ha abrogato il comma 8 dell'art. 16 ed ha introdotto, dopo il comma 6 e dopo il comma 7 altrettanti commi-*bis*, che contemplano le sanzioni a carico delle imprese e dei professionisti inadempienti.

6.2.1. *Conseguenze della mancata elezione del domicilio digitale da parte delle imprese*

L'attuale art. 16, comma 7-*bis*, d.l. n. 185 del 2008 prevede che l'Ufficio del Registro delle Imprese, allorquando pervenga una richiesta di iscrizione da parte di una società costituita in forma giuridica societaria, che non abbia provveduto all'iscrizione del proprio indirizzo di domicilio digitale, anziché procedere con l'applicazione della sanzione pecuniaria stabilita dall'art. 2630 del codice civile, opta per una sospensione della suddetta domanda, in attesa che la stessa venga completata con l'inserimento del domicilio digitale. Ciò nonostante, in conformità a quanto stabilito nel primo periodo per le imprese di nuova istituzione, le imprese anzidette che non abbiano comunicato il loro domicilio digitale entro la data limite del 1° ottobre 2020, o in caso in cui il loro domicilio digitale sia stato revocato dall'Ufficio del Registro delle Imprese ai sensi del comma 6-*ter*, sono soggette alla sanzione prevista dall'art. 2630 del codice civile, in misura raddoppiata. In concomitanza con l'imposizione della sanzione, l'Ufficio del Registro delle Imprese provvede, peraltro, all'assegnazione d'ufficio di un nuovo e differente domicilio digitale per la ricezione di comunicazioni e notificazioni, il quale viene certificato presso il cassetto digitale dell'imprenditore, gestito dal sistema informativo nazionale delle Camere di Commercio. Il successivo comma 6-*ter*, poi, prevede che il Conservatore dell'Ufficio del Registro delle Imprese, al constatare, anche in seguito a una segnalazione, la presenza di un domicilio digitale non attivo, sollecita la società interessata a fornire un nuovo indirizzo di domicilio digitale entro un periodo di trenta giorni. In caso di decorrenza

di tale termine senza che la società abbia presentato opposizione, tramite un proprio atto deliberativo (reclamabile), procede alla rimozione dell'indirizzo di domicilio digitale dal registro delle imprese, e contestualmente dà avvio alla procedura prevista dal comma 6-*bis*.

Per le imprese individuali, infine, l'art. 5, commi 1 e 2, d.l. n. 179 del 2012 prevedono un procedimento e sanzioni del tutto analoghe.

6.2.2. *Conseguenze della mancata elezione del domicilio digitale da parte dei professionisti*

In coerenza con le appena esaminate disposizioni in materia di imprese, l'art. 16, comma 7-*bis*, del d.l. n. 185 del 2008 prevede che il professionista, il quale ometta di notificare il proprio indirizzo di domicilio digitale all'albo o all'elenco tenuti dal proprio Ordine o Collegio, è soggetto a una formale diffida emessa dal proprio Collegio o Ordine professionale, che lo esorta a conformarsi entro un termine di trenta giorni. Si prevede, inoltre, che qualora il professionista non adempia a tale diffida il Collegio o Ordine di appartenenza procederà con l'applicazione della sanzione consistente nella sospensione dall'albo o dall'elenco professionale, che perdurerà fino alla comunicazione del domicilio digitale.

La stessa norma prevede a carico degli Ordini e dei Collegi di professionisti l'obbligo di trasmissione di tali elenchi alle pubbliche amministrazioni, laddove la mancata pubblicazione, così come il persistente rifiuto di trasmettere alle pubbliche amministrazioni i dati richiesti dallo stesso comma, o la reiterata inosservanza dell'obbligo di comunicare all'indice di cui all'articolo 6-*bis* del decreto-legislativo 7 marzo 2005, n. 82 (INIPEC), l'elenco dei domicili digitali e i relativi aggiornamenti costituiscono cause di scioglimento e di commissariamento del Collegio o dell'Ordine inadempiente da parte del Ministero competente per la vigilanza.

6.2.3. *Conseguenze della mancata elezione del domicilio digitale da parte delle pubbliche amministrazioni*

Quanto alle pubbliche amministrazioni vige un obbligo di duplice natura. Il primo, sancito dall'art. 16, comma 8 (poi abrogato dal decreto semplificazioni del 2020) relativo alla comunicazione dell'indirizzo PEC nell'Indice P.A. La norma in parola fu poi soppressa, come appena ricordato, nell'ambito di un'opera di armonizzazione della legislazione in materia che tenne conto del fatto che, nelle more, il decreto legislativo 26 agosto 2016, n. 179, aveva, con l'art. 7, introdotto l'art. 6-*ter* del CAD che, al comma 3, obbliga le pubbliche amministrazioni e i gestori di servizi pubblici ad aggiornare prontamente gli indirizzi e i contenuti dell' "*Indice degli indirizzi*

della pubblica amministrazione e dei gestori di pubblici servizi", almeno su base semestrale, seguendo le direttive dell'AgID. La norma stabilisce altresì che la mancata trasmissione delle informazioni in parola debba essere considerata ai fini della valutazione della responsabilità direttiva e dell'assegnazione della retribuzione di risultato ai dirigenti incaricati.

Il secondo obbligo è invece sancito, nell'ambito dei processi telematici civile e penale, dall'art. 16, decreto-legge 18 ottobre 2012, n. 179. Tale norma prevede che per facilitare le comunicazioni e le notificazioni telematiche alle pubbliche amministrazioni, queste ultime hanno l'obbligo di trasmettere al Ministero della Giustizia l'indirizzo di posta elettronica certificata (PEC) destinato alla ricezione delle comunicazioni e notificazioni. Tale elenco è accessibile esclusivamente agli uffici giudiziari, agli uffici notificazioni, esecuzioni e protesti, e agli avvocati, mediante accesso in modalità autenticata al Portale Servizi Telematici del Ministero della Giustizia. Si prevede, altresì, che le amministrazioni pubbliche possono fornire gli indirizzi PEC di specifici organi o divisioni, anche a livello territoriale, per la realizzazione di comunicazioni o notificazioni telematiche, qualora sia previsto l'obbligo di notifica degli atti introduttivi di giudizio presso di essi in relazione a determinate materie, o in situazioni di autonoma capacità o legittimazione processuale. In aggiunta, nel caso di rappresentanza in giudizio tramite i propri dipendenti, le amministrazioni pubbliche possono comunicare ulteriori indirizzi PEC, da inserire in una sezione speciale dello stesso elenco, corrispondenti a specifiche aree organizzative omogenee, e designati come domicilio ai fini del procedimento giudiziario.

Va ricordato che la norma in discorso prevedeva, nella sua formulazione originaria, un termine — quello del 30 novembre 2014 — concesso alle pubbliche amministrazioni per la comunicazione del proprio domicilio digitale per le notificazioni e comunicazioni di cancelleria. Tale termine è stato, tuttavia, ampiamente disatteso, di tal che ancora oggi molte amministrazioni non hanno provveduto ad ottemperare.

Tale inadempimento ha provocato, fino al 2020, data di entrata in vigore del d.l. 16 luglio 2020, n. 76, la sostanziale impossibilità dell'esecuzione delle notificazioni in modalità telematica nei confronti delle pubbliche amministrazioni inadempienti, complice anche l'assenza di qualsivoglia sanzione a carico delle PP.AA. che avessero omesso di comunicare il proprio domicilio digitale nel Registro previsto dall'art. 16, co. 12, d.l. n. 179 del 2012. Tale impossibilità è derivata dal fatto che con la legge 11 agosto 2014, n. 114, di conversione del d.l. 24 giugno 2014, n. 90 fu espunto dall'art. 16-*ter*, d.l. n. 179 del 2012 il richiamo all'art. 16, co. 8, del d.l. n. 179 del 2012, di tal che l'Indice PA non è stato più, dall'agosto 2014 e sino all'entrata in vigore del più volte ricordato decreto semplificazioni, elenco idoneo all'estrazione dei domicili digitali utili alle notificazioni e comunicazioni di cancelleria.

Per porre rimedio a tale anomalia il legislatore, con il citato decreto-legge del 2020, si è mosso lungo due direttrici: da un lato ha modificato il comma 12 dell'art. 16 del d.l. n. 179 del 2012 prevedendo, come già detto, che le amministrazioni pubbliche possono comunicare gli indirizzi di posta elettronica certificata di propri organi o articolazioni, anche territoriali, presso cui eseguire le comunicazioni o notificazioni per via telematica nel caso in cui sia stabilito presso questi l'obbligo di notifica degli atti introduttivi di giudizio in relazione a specifiche materie ovvero in caso di autonoma capacità o legittimazione processuale. Per altro verso, è stato previsto, con la novella dell'art. 16, comma 13, d.l. n. 179 del 2012, che ove le amministrazioni non ottemperino in alcun modo a tale adempimento, la notificazione alle pubbliche amministrazioni degli atti in materia civile, penale, amministrativa, contabile e stragiudiziale possa essere validamente effettuata, a tutti gli effetti, al domicilio digitale indicato nell'elenco previsto dall'articolo 6-*ter* del decreto legislativo 7 marzo 2005, n. 82, e, ove nel predetto elenco risultino indicati, per la stessa amministrazione pubblica, più domicili digitali, la notificazione è effettuata presso l'indirizzo di posta elettronica certificata primario indicato, secondo le previsioni delle Linee guida di AgID, nella sezione ente dell'amministrazione pubblica destinataria. Nella stessa direzione, infine, si è mosso il legislatore delegato con il d.lgs. n. 149 del 2012, introducendo, nell'art. 16-*ter*, d.l. n. 179 del 2012, il comma 1-*ter*. Con tale norma si prevede in assenza di indicazione di domicilio digitale nell'elenco menzionato nell'articolo 16, comma 12, la notificazione agli enti pubblici degli atti in ambito civile, penale, amministrativo, contabile e stragiudiziale è considerata validamente eseguita, a tutti gli effetti di legge, presso il domicilio digitale riportato nell'elenco stabilito dall'articolo 6-*ter* del decreto legislativo 7 marzo 2005, n. 82 e che qualora, all'interno del predetto elenco, siano riportati più domicili digitali per la medesima amministrazione pubblica, la notificazione si effettua presso l'indirizzo di posta elettronica certificata principale, come indicato nelle Linee guida dell'Agenzia per l'Italia Digitale (AgID), nella sezione dedicata all'ente pubblico destinatario.

È stabilito, inoltre, che nel caso in cui vi sia l'obbligo di notificare gli atti introduttivi di giudizio in relazione a materie specifiche presso determinati organi o strutture, anche territoriali, delle amministrazioni pubbliche, la notificazione può avvenire all'indirizzo di posta elettronica certificata chiaramente specificato per tali organi o strutture nell'elenco di cui all'articolo 6-*ter* del decreto legislativo 7 marzo 2005, n. 82.

6.3. La condivisione medesimo domicilio

6.3.1. *La sussistenza dell'obbligo di unicità del domicilio digitale*

Si è in precedenza osservato che, nell'attuale sistema, la corrispondenza tra soggetti e rispettivi domicili digitali è assicurata attraverso l'iscrizione dei domicili nei pubblici elenchi di cui si è detto.

L'art. 16, comma 6, del decreto-legge 29 novembre 2008, n. 185, prevede, quanto alle imprese, che esse siano tenute ad indicare « *il proprio indirizzo domicilio digitale* ». Analogamente, il comma 7 del medesimo decreto-legge prevede, quanto ai professionisti, che essi debbano comunicare « *ai rispettivi ordini o collegi il proprio domicilio digitale (...)* ». L'utilizzo, in entrambi i casi dell'aggettivo possessivo "proprio" non può significare altro se non che il domicilio digitale debba essere pertanto personale ed univoco per ogni impresa e per ogni professionista.

Le su richiamate norme, quindi, impongono sul piano positivo una corrispondenza biunivoca tra l'insieme dei soggetti obbligati a dotarsi e ad eleggere un domicilio digitale e l'insieme dei domicili digitali, vale a dire che esse prescrivono che a ogni soggetto sia associato uno e un solo domicilio digitale e viceversa.

Allo stato, dunque — in attesa che l'adozione dello standard REM per i SERCQ risolva definitivamente sul piano tecnico il problema — la corrispondenza biunivoca in parola è prevista normativamente ed assicurata attraverso il "tradizionale" schema precetto-controllo-sanzione.

Si sono tuttavia registrati numerosi casi nei quali più imprese risultavano essere iscritte nel Registro Imprese con il medesimo domicilio digitale. Tale fenomeno è stato fatto oggetto di una Circolare del Ministero dello Sviluppo Economico (9 maggio 2014, n. 77684), il quale ha lapidariamente affermato che « *nel caso in cui... si rilevi, d'ufficio o su segnalazione di terzi, l'iscrizione di un indirizzo PEC, di cui sia titolare una determinata impresa, sulla posizione di un'altra (o di più altre) — ovvero, comunque, l'iscrizione sulla posizione di un'impresa di un indirizzo PEC che non sia "proprio" della stessa — dovrà avviarsi la procedura di cancellazione del dato in questione ai sensi dell'art. 2191 c.c., previa intimazione, all'impresa interessata (o alle imprese interessate), a sostituire l'indirizzo registrato con un indirizzo di PEC "proprio"* ».

6.3.2. *Il fenomeno nell'ambito della disciplina del PCT*

Nell'ambito dei professionisti e, in particolare, di coloro che, in veste di avvocati o consulenti d'ufficio, operano nel campo del processo telematico, il fenomeno della condivisione dell'indirizzo PEC è, a dire il vero, più raro. V'è però che, per limitarci all'ambito dei depositi nel processo civile telema-

tico, a partire dal maggio 2014, intervenne una modifica delle specifiche tecniche dettate dal DGSIA in virtù della quale furono soppressi i meccanismi di verifica della relazione tra l'indirizzo PEC ed il firmatario dell'atto depositato telematicamente, e ciò al dichiarato scopo di consentire a un firmatario dell'atto di utilizzare un indirizzo di PEC del ReGIndE associato anche ad altri soggetti (la c.d. "*PEC di studio*"). Si tratta, tuttavia, di casi piuttosto rari, laddove si è fatto ricorso a questo espediente per venire incontro alle necessità di eseguire tempestivamente i depositi anche in caso di temporaneo malfunzionamento della PEC, utilizzando il domicilio digitale di altro avvocato, purché iscritto al ReGInde.

Va peraltro detto, incidentalmente, che si sono accertate ipotesi — allo stato del tutto legittime ancorché non ortodosse — nelle quali l'associazione tra soggetto e rispettivo indirizzo PEC non vede rispettata la tradizionale regola della "*local part*" (la parte di un indirizzo email che si trova a sinistra dalla @ e che si distingue dalla *domain part*, sita invece a destra dell'anzidetto simbolo) corrispondente al nome+cognome del soggetto, e sono pertanto reperibili in INIPEC svariati casi di indirizzi del tipo, ad esempio, mario.rossi@pec.it che corrispondono invece al soggetto "Giuseppe Bianchi".

6.4. Patologia nella pratica - Aspetti tecnico-giuridici

L'analisi di alcune condotte patologiche nell'utilizzo dei domicili digitali non può ignorare la disciplina giuridica e, soprattutto tecnica, della posta elettronica certificata nel nostro ordinamento.

La materia, in mancanza della pubblicazione delle linee guida previste dall'art. 6 del CAD, è tuttora disciplinata dal decreto del presidente della Repubblica 11 febbraio 2005 n. 68 "Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata" e dal decreto ministeriale 2 novembre 2005 "Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della PEC".

Tale normativa non è stata aggiornata secondo la nuova impostazione impressa dal CAD che, come visto, ha introdotto il concetto di domicilio digitale, ma è fonte imprescindibile in quanto disciplina lo strumento della posta elettronica certificata che è quello in cui, allo stato, si sostanzia il domicilio digitale (1), in attesa dell'avvio dei servizi SERCQ e, in particolare, di quelli fondati sullo standard internazionale REM (2).

---

(1) CAD - art. 1, lett. *n-ter*): "domicilio digitale: un indirizzo elettronico eletto presso un *servizio di posta elettronica certificata* o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo

Le norme tecniche descrivono puntigliosamente le modalità di funzionamento del sistema, gli avvisi e le ricevute che i gestori del mittente e del destinatario devono inviare sia nell'ipotesi del buon fine della trasmissione, sia in quella di mancata consegna.

Tralasciando, per ovvi motivi, l'ipotesi fisiologica della regolare messa a disposizione del destinatario del messaggio PEC con l'invio da parte del gestore di PEC del mittente della ricevuta di accettazione (RdA) e da parte del gestore di PEC del destinatario della ricevuta di avvenuta consegna (RdAC), si analizzeranno rapidamente le ipotesi patologiche, soprattutto al fine di discernere, tra queste, quelle il cui verificarsi sia imputabile al destinatario.

6.4.1. *La trasmissione del messaggio verso il domicilio digitale*

Il sistema di recapito attraverso posta elettronica certificata è strutturato tramite l'interposizione dei gestori dei sistemi cui devono iscritti rispettivamente il mittente ed il destinatario al fine di possedere due domicili digitali validi, corrispondenti alle relative caselle PEC.

Lo schema operativo ordinario è il seguente: (1) il mittente invia il messaggio al proprio gestore PEC; (2) il gestore eseguiti positivamente alcuni controlli inserisce il messaggio in una busta di trasporto da lui sottoscritta e la invia al gestore PEC del destinatario; (3) invia inoltre la RdA al mittente; (4) il gestore del destinatario eseguiti positivamente alcuni controlli sulla busta di trasporto la mette a disposizione del destinatario; (5) invia inoltre la RdAC al gestore del mittente per l'inoltro a quest'ultimo.

Entrare nel dettaglio del funzionamento del sistema in caso di anomalie è senz'altro al di fuori dello scopo del presente scritto, ma merita di essere rimarcato come le varie ipotesi di mancato buon fine della trasmissione per anomalie tecniche relative alla formazione dei messaggio, alla presenza di virus nel medesimo o ad anomalie di funzionamento dei sistemi PEC dei due gestori che interagiscono tra loro, peraltro vincolati da stringenti livelli di servizio controllati da enti pubblici (3), non possono mai essere attribuiti alla condotta del destinatario e, quindi, non rientrano per definizione nella patologia dell'utilizzo dei domicili digitali.

Vi rientrano, però, a pieno titolo altre ipotesi che analizziamo di seguito.

---

e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, di seguito "Regolamento eIDAS", valido ai fini delle comunicazioni elettroniche aventi valore legale".

(2) Cfr. paragrafo 1.

(3) Attualmente il controllo è attribuito all'Agenzia per l'Italia Digitale (AgID).

6.4.2. *Casella inattiva o indirizzo non riconosciuto*

L'anomalia si verifica quando un indirizzo PEC (e quindi un domicilio digitale), pur regolarmente messo a disposizione del destinatario sia successivamente reso inattivo o cancellato a seguito del mancato versamento del corrispettivo contrattualmente pattuito ovvero di altri gravi inadempimenti del titolare dell'indirizzo che abbiano indotto il gestore a risolvere il rapporto contrattuale.

In tale caso il gestore PEC del destinatario genera un avviso di mancata consegna che viene restituito al gestore PEC del mittente per l'inoltro a quest'ultimo con l'indicazione della anomalia riscontrata.

Si tratta di eventualità che, salvo eccezioni difficilmente ipotizzabili, sono da ricondurre alla responsabilità del destinatario, così che il mancato recapito di un messaggio per tali ragioni può essere senz'altro imputato a costui.

6.4.3. *Casella piena*

I rapporti contrattuali con i gestori di PEC prevedono la messa a disposizione di uno spazio di archiviazione definito, usualmente non inferiore a 1 Gigabyte (4) che, peraltro, è la dimensione minima ammessa per le caselle PEC dei soggetti abilitati esterni del Processo Civile Telematico, come disposto dall'art. 21 dalle relative specifiche tecniche (5).

La finitezza dello spazio a disposizione per un verso e la circostanza che i messaggi PEC possono essere accompagnati da allegati di rilevanti dimensioni, può come naturale portare all'esaurimento dello spazio a disposizione, con conseguente saturazione della casella e impossibilità di recapitarvi nuovi messaggi.

Va precisato che usualmente i gestori di PEC inviano all'utente degli avvisi man mano che la casella si avvicina alla soglia di saturazione, invitandoli a liberare spazio o a acquistarne di ulteriore per accomodare più messaggi. Inoltre, è possibile impostare delle regole automatiche di gestione della casella che facciano sì che i messaggi di PEC vengano cancellati periodicamente, auspicabilmente dopo averli salvati su altri supporti di memoria, in modo da evitare che la casella si riempia.

Ordinariamente, quindi, un utente diligente dovrebbe disporre gli strumenti utili ad evitare di trovarsi in una tale eventualità, dovendo comunque ritenersi che l'introduzione generalizzata ed obbligatoria del domicilio digi-

---

(4) Unità di misura della quantità di informazione pari a un miliardo di byte (1 gigabyte = 10^9 byte).

(5) Provvedimento 16 aprile 2014 del responsabile per i sistemi informativi automatizzati del Ministero della giustizia.

tale dovrebbe imporre ai soggetti tenuti a dotarsene un onere di diligente organizzazione al fine di assicurarne continuo regolare il funzionamento.

Salve ipotesi eccezionali, quindi, un messaggio non recapitato in ragione della saturazione dello spazio a disposizione del destinatario rientra tra quelli che debbono essere imputati a costui.

6.5. La patologia dei domicili digitali nell'ambito delle notificazioni

La disciplina dei domicili digitali, come già descritta ai precedenti punti 1) e 2), riverbera i propri effetti nella innovativa disciplina delle notificazioni introdotta dalla riforma Cartabia, uno degli ambiti in cui la spinta innovatrice è stata più incisiva.

Il decreto legislativo 10 ottobre 2022, n. 149, infatti, ha voluto porre quale modalità di notificazione ordinaria quella a mezzo PEC (6) tutte le volte che il destinatario fosse uno dei soggetti tenuti *ex lege* a dotarsi di un domicilio digitale, nonché quando, pur non rientrando in tale novero, il destinatario che sia persona fisica, professionista o ente di diritto privato non iscritto nell'INIPEC, abbia esercitato la propria facoltà di istituire un domicilio digitale presso l'INAD (7), come previsto dall'art. 6-*quater* CAD.

Ne consegue che tali modalità di notificazione si devono necessariamente confrontare con le situazioni patologiche già sopra esaminate, a fronte delle quali il legislatore ha cercato di apprestare rimedi, non tutti rivelatisi efficaci, dei quali tratteremo nei prossimi paragrafi.

6.5.1. *La disciplina di cui all'art. 3-*ter*, legge 21 gennaio 1994, n. 53*

A mente dell'art. 35, co. 1, d.lgs. n. 150 del 2023, a far data dal 28 febbraio 2023, quando il destinatario rientri in una delle categorie di cui s'è detto, sussiste un preciso obbligo dell'avvocato di procedere alla notificazione esclusivamente a mezzo PEC ed un correlativo divieto per l'ufficiale giudiziario di procedere alla notificazione, salvo che l'avvocato: (*i*) non debba eseguirla a mezzo di posta elettronica certificata, ovvero (*ii*) dichiari che la notificazione con modalità telematiche sia impossibile o non sia andata a buon fine per cause non imputabili al destinatario (cfr. art. 137, co. 7, c.p.c.).

---

(6) La normativa in tema di notificazioni non si riferisce solo a quelle a mezzo PEC, ma richiama sempre anche quelle a mezzo servizio elettronico di recapito certificato qualificato (SERCQ). Nel testo ci si riferisce alla prima soluzione tecnica che, nel momento in cui si scrive è l'unica disponibile.

(7) L'Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese, previsto dall'art. 6-*quater* CAD.

La prima delle due eventualità si verifica quando il soggetto destinatario non rientri in alcuna delle categorie previste dalle lettere *a*) e *b*) del nuovo art. 3-*ter*, l. n. 53 del 1994 e, quindi, alternativamente non sia obbligato a dotarsi di domicilio digitale ovvero pur avendo la facoltà di dotarsene non l'abbia esercitata. In tale eventualità, stiamo parlando di notificazioni dirette a persone fisiche (8) ed enti privati non tenuti all'iscrizione al registro delle imprese, l'avvocato potrà effettuare la notificazione in proprio — necessariamente per posta (9) — ovvero richiedere all'ufficiale giudiziario di provvedervi con modalità analogiche.

Negli altri casi l'avvocato dovrà procedere alla notificazione a mente della l. n. 53 del 1994, dovendo prestare estrema attenzione alle situazioni, anche patologiche, che potrebbe trovarsi a dover gestire. Tale nuova disciplina impone, infatti, all'avvocato notificante di saper discernere tra le varie situazioni al fine di reagire adeguatamente imprimendo alla procedura notificatoria l'ulteriore corso secondo le previsioni del comma 2 del già citato art. 3-*ter*, l. n. 53 del 1994.

6.5.2. *La notificazione impossibile*

Entrambi gli artt. 137, comma 7, c.p.c. e 3-*ter*, l. n. 53 del 1994 prevedono l'eventualità che la notificazione telematica "non sia possibile", il primo per trarne la conseguenza del venir meno della limitazione del potere di notificazione dell'ufficiale giudiziario e, il secondo, per precisare quale sia la condotta che l'avvocato debba tenere in quella ipotesi.

Sennonché le ipotesi in cui tale eventualità si può verificare paiono davvero esigue e, anzi, probabilmente si limitano all'unica evenienza della mancata istituzione del domicilio digitale da parte del destinatario obbligato a dotarsene. In tutti gli altri casi, infatti, una volta che sia esistente un indirizzo PEC al quale indirizzare la notificazione, le ipotesi di mancata consegna non rientrano nel novero della notificazione "non possibile", ma in quello della notificazione "non andata a buon fine".

Tale riflessione conduce alla conseguenza che, con tutta probabilità, è inutile distinguere tra notificazioni a mezzo PEC "non possibili" per cause imputabili o meno al destinatario, posto che la mancata istituzione del domicilio digitale è sempre imputabile al soggetto inadempiente, essendo —

---

(8) Nella definizione di persona fisica ovviamente rientrano anche i professionisti diversi da quelli tenuti all'iscrizione in albi ed elenchi.

(9) Le condizioni per la notificazione a mani prevista dall'art. 4 della l. n. 53 del 1994 non possono verificarsi essendo riservata agli avvocati che abbiano la qualità di domiciliatari di una parte processuale e, quindi, a soggetti obbligati a dotarsi di domicilio digitale.

come già osservato — il caso più eclatante di patologia dell'utilizzo del domicilio digitale o, meglio, la sua stessa radicale negazione.

6.5.3. *La notificazione non andata a buon fine*

Una volta individuato un indirizzo PEC riferibile al destinatario estratto da uno degli elenchi pubblici previsti dall'art. 16-*ter,* decreto-legge 18 ottobre 2012, n. 179, tutte le eventualità che si possono verificare sono legate strettamente all'implementazione della tecnologia della posta elettronica certificata. Esse, quindi, possono essere ricondotte a quelle esemplificate al paragrafo 4.1. per essere ricondotte a cause imputabili o meno al destinatario.

Tale qualificazione è assai rilevante nell'ambito delle notificazioni del quale ci stiamo occupando, in cui le situazioni patologiche impattano con l'esigenza di certezza delle comunicazioni tra parti processuali e, di conseguenza, sulla tutela dei loro diritti in sede giurisdizionale.

La disciplina introdotta dalla Riforma Cartabia, infatti, ha esteso alle notificazioni telematiche eseguite dall'avvocato la rilevanza del concetto di mancato buon fine imputabile al destinatario già elaborato in relazione alle comunicazioni/notificazioni a cura degli uffici giudiziari (10).

6.5.4. *L'area web di cui all'art. 359 del d.lgs. 12 gennaio 2019, n. 14*

Il secondo comma del già citato art. 3-*ter*, l. n. 53 del 1994 ha esteso anche per l'ambito delle notificazioni civili a cura dell'avvocato il nuovo istituto già introdotto dal Codice della Crisi d'Impresa e dell'Insolvenza (CCII), prevedendo che se il mancato buon fine della notificazione è imputabile al destinatario la notificazione debba essere eseguita mediante inserimento nell'area web riservata prevista dall'art. 359 del CCII a spese del richiedente. In tale caso la notificazione si ha per eseguita nel decimo giorno successivo a quello in cui è compiuto l'inserimento.

Tale soluzione, però, non è stata prevista per tutti i destinatari nei confronti dei quali per l'avvocato vige l'obbligo di notificazione al domicilio digitale, ma solo nei confronti delle imprese o dei professionisti iscritti nell'indice INIPEC, rimanendo esclusi per espressa previsione normativa contenuta alla lettera *b*) della norma in commento, i soggetti iscritti ad INAD e, per esclusione tacita, le pubbliche amministrazioni, di cui la norma si è disinteressata.

---

(10) L'art. 16, comma 6, del d.l. n. 179 del 2012 in tale ambito prevede che nelle ipotesi di mancata consegna del messaggio di posta elettronica certificata per cause imputabili al destinatario le notificazioni e le comunicazioni sono eseguite esclusivamente mediante deposito in cancelleria.

Se ne ricava, quindi, che l'utilizzo patologico del domicilio digitale è soggetto a valutazioni e conseguenze diverse a seconda del soggetto che lo realizzi. Per imprese e professionisti è rilevante e merita la previsione di un sistema di perfezionamento della notificazione latamente "punitivo", che prescinde dall'effettiva consegna del messaggio PEC. Quando, invece, ad abusare del domicilio digitale sono le pubbliche amministrazioni, i privati e gli enti di diritto privato che hanno eletto domicilio digitale facoltativamente, tale condotta rimane irrilevante ed il mancato buon fine della notificazione impone al mittente di ripeterla con modalità analogiche.

Va ulteriormente sottolineato, collegandosi a quanto già scritto al punto 7.1., che la notificazione mediante inserimento nell'area web, nonostante il tenore dell'art. 3-*ter*, l. n. 53 del 1994 sembri suggerirlo, non è realizzabile nel caso di notificazione impossibile e, quindi, di mancata istituzione del domicilio digitale. Infatti, dato che tale modalità di notifica è possibile solo nei confronti di soggetti iscritti ad INIPEC ed il presupposto per tale iscrizione è l'istituzione di un domicilio digitale, nei confronti di tali soggetti la notificazione potrà al più non andare a buon fine, ma non potrà mai essere impossibile.

Tanto chiarito va però rilevato che l'area web prevista dal CCII non è mai stata attivata dal Ministero dello Sviluppo Economico che ne avrebbe la responsabilità, e, ciò, nonostante tale codice sia stato pubblicato il 14 febbraio 2019 e sia efficace dal 15 luglio 2022.

Ne consegue che stante l'impossibilità di procedere all'inserimento in tale area delle notificazioni non andate a buon fine, le stesse non possono avere altra sorte se non quella di essere ripetute con modalità analogiche, esattamente come accade per le notificazioni non andate a buon fine per cause non imputabili al destinatario in forza del comma 3 dell'art. 3-*ter*, l. n. 53 del 1994.

6.5.5. *La sospensione dell'efficacia dei commi 2 e 3 dell'art. 3-*ter *della l. n. 53 del 1994*

Preso atto della impossibile applicazione del sistema apprestato dai commi 2 e 3 dell'art. 3-*ter* della l. n. 53 del 1994 il legislatore, con l'art. 4-*ter*, decreto-legge 10 maggio 2023, n. 51, ha ritenuto di sospenderlo fino al 31 dicembre 2023, sostituendolo con una disciplina che non prevede soluzioni differenziate per le ipotesi in cui la notificazione non sia andata a buon fine per cause imputabili o meno al destinatario. Essa prevede: "*... quando la notificazione ai sensi del comma 1 dell'articolo 3-*ter *della citata legge n. 53 del 1994 non è possibile o non ha esito positivo, essa è eseguita con le modalità ordinarie e si perfeziona, per il soggetto notificante, nel momento in cui è*

generata la ricevuta di accettazione della notificazione dallo stesso inviata mediante posta elettronica certificata ...".

La soluzione adottata, che fa applicazione del principio di scissione degli effetti della notificazione tra il mittente ed il destinatario della stessa, si segnala però per la sua singolarità. Tali effetti, infatti, diversamente dagli esempi finora conosciuti che attenevano comunque ad una singola procedura notificatoria, si riferiscono a due procedure notificatorie separate. Di quella telematica, non andata a buon fine, si mantiene l'effetto a favore del mittente, ricollegandolo al momento della generazione della RdA del messaggio PEC veicolante la notificazione. Di quella analogica, cui è stato necessario ricorrere a seguito del mancato buon fine della prima, viene invece in rilievo l'effetto nei confronti del destinatario che, come ovvio, si produrrà secondo le regole ordinarie.

6.5.6. *Riepilogo anomalie notifiche PEC*

È ora possibile costruire una tavola sinottica al fine di riepilogare quali siano le conseguenze in ordine alle procedure notificatorie della gestione impropria dei domicili digitali.

<table>
<tr><th>Evento notifica</th><th>Normativa in vigore
(sospesa sino al
31 dicembre 23)</th><th>Normativa temporanea
(si applica fino al
31 dicembre 23)</th></tr>
<tr><td>Notificazione impossibile</td><td>Ripetizione con modalità analogiche</td><td>Ripetizione con modalità analogiche</td></tr>
<tr><td rowspan="2">Casella piena
Casella inattiva
Indirizzo non riconosciuto</td><td>DESTINATARIO ISCRITTO INIPEC
Inserimento area web</td><td rowspan="2">Ripetizione con modalità analogiche
PER IL MITTENTE LA NOTIFICA SI PERFEZIONA AL MOMENTO DELLA GENERAZIONE DELLA RdA</td></tr>
<tr><td>ALTRI DESTINATARI
Ripetizione con modalità analogiche</td></tr>
<tr><td>Anomalia gestore mittente</td><td>Ripetizione con modalità analogiche</td><td>Ripetizione con modalità analogiche</td></tr>
<tr><td>Anomalia gestore destinatario</td><td>Ripetizione con modalità analogiche</td><td>Ripetizione con modalità analogiche
PER IL MITTENTE LA NOTIFICA SI PERFEZIONA AL MOMENTO DELLA GENERAZIONE DELLA RdA</td></tr>
</table>

Sezione II
IL PROCESSO DI ESECUZIONE

I.
I DOMICILI DIGITALI ESECUTIVI
di *Rinaldo d'Alonzo*

Sommario: 1.1. Premessa. — 1.2. Il domicilio digitale del creditore procedente e dei creditori intervenuti. — 1.3. Il domicilio (digitale?) del debitore. — 1.4. Domicilio digitale e procedimento di vendita immobiliare. — 1.4.1. La presentazione dell'offerta di acquisto. — 1.4.2. Sottoscrizione ed invio dell'offerta: presentatore ed offerente. — 1.4.3. Le criticità della PEC identificativa per la vendita telematica: suggerimenti al legislatore. — 1.5. Domicilio digitale e vendita mobiliare telematica.

1.1. Premessa

Il macrocosmo del domicilio (o, meglio, come si vedrà, "dei domicili") digitali in sede esecutiva assume colorazioni peculiari, ed in qualche misura non sovrapponibili a quelle con le quali ci si confronta nel recinto del processo di cognizione, pur nelle sue poliedriche declinazioni, per almeno tre ragioni.

La prima alberga nella eterogeneità dei modelli disegnati dal legislatore, ciascuno dei quali retto da regole non del tutto coincidenti.

Una preliminare *summa divisio* si impone, a questo proposito, tra esecuzione individuale ed esecuzione concorsuale, entrambe ascrivibili a perimetro delle vendite coattive [1].

L'esecuzione individuale trova la sua disciplina compiuta essenzialmente nel codice di procedura civile (diciamo essenzialmente in quanto, come si vedrà, si tratta di un ambito nel quale prepotentemente irrompono, con effetti di sistema potenzialmente devastanti, fonti di rango subordinato che richiedono ad un operatore accorto di essere "addomesticate" al rispetto dei principi costituzionali del giusto processo, scanditi dall'art. 111 Cost.)

Accanto ad essa si (im)pone l'esecuzione concorsuale, che oggi pretende di conoscere una sua disciplina compiuta con il codice della crisi d'impresa

---

[1] La natura coattiva della vendita fallimentare è pacificamente ammessa sia in dottrina (cfr., *ex multis*, Panzani, *Fallimento ed altre procedure concorsuali*, diretto da Faucelia e Panzani, Torino, 2, 1225) che in giurisprudenza (Cass., 25 ottobre 2017, n. 24329).

e dell'insolvenza (approvato con il d.lgs. 12 gennaio 2019, n. 14), il quale tuttavia chiama ad operazioni di raccordo sia interno che esterno. Interno in quanto l'interprete deve cimentarsi in interventi di ortopedia interpretativa tra disposizioni di carattere generale (si pensi al discusso concetto di domicilio digitale, disciplinato dall'art. 10 c.c.i., ad alle difficoltà operative che la sua applicazione produce, anche sul piano dei costi della procedura) e previsioni specificamente dedicate a singoli istituti (il pensiero corre qui veloce all'art. 216, ed alle anfibologiche previsioni che lo contraddistinguono, frutto della volontà di procedimentalizzare anche le vendite competitive e di importare anche in esse il paradigma della vendita telematica, all'insegna della trasparenza della fase liquidatoria dell'attivo).

Ma non è tutto. La eterogeneità si coglie altresì all'interno di ciascuno dei due microcosmi (quello della esecuzione singolare e quello della esecuzione concorsuale) appena descritti, laddove si consideri che i modelli immaginati in ciascuno di essi sono più d'uno.

E così, ove si passino in rassegna le vendite esecutive, ci si imbatte in sistemi che solo apparentemente si pongono quali *species* di un unico *genus*, in quanto, ove scrutinati *funditus*, disvelano l'appartenenza a mondi diversi, distanti, neppure tangenti.

Il dato si coglie plasticamente nel d.m. giustizia 26 febbraio 2015, n. 32, recante "*Regolamento recante le regole tecniche e operative per lo svolgimento della vendita dei beni mobili e immobili con modalità telematiche nei casi previsti dal codice di procedura civile, ai sensi dell'articolo 161-*ter *delle disposizioni per l'attuazione del codice di procedura civile*". Qui, vendita immobiliare telematica e vendita mobiliare telematica (alla cui disciplina è dedicato il solo art. 25) sono regolate da norme che tracciano percorsi operativi eterogenei, retti ciascuno da regole proprie, incomunicanti, implicanti effetti probabilmente frutto di una sorta di eterogenesi dei fini.

La medesima policromia caratterizza anche la vendita concorsuale. Qui i problemi sono almeno due.

Il primo è quello di comprendere la portata del modello liquidatorio costruito dall'art. 216 c.p.c., con specifico riferimento alla possibilità che esso costituisca l'archetipo di ogni liquidazione cui si dia corso nell'ambito di uno dei procedimenti di risoluzione della crisi e dell'insolvenza (primo fra tutti il concordato che si potrebbe definire "maggiore", di cui agli artt. 84 e ss. c.c.i., per distinguerlo dal concordato semplificato, *ex* art. 25-*sexies*, c.c.i.) o di composizione della crisi da sovraindebitamento previsti dal codice della crisi.

La seconda ragione di problematicità del tema "domicilio digitale" nella materia esecutiva risiede nella difficoltà capire se, nel corpo dell'art. 216 c.c.i., sia possibile estrapolare, rispetto ai due "tipi" di vendita esecutiva immaginati, un nocciolo di regole comuni, valevoli sia per la vendita com-

petitiva che per quella che si dipana "*secondo le disposizioni del codice di procedura civile in quanto compatibili*" (così l'art. 216, comma 3, c.c.i.).

Infine, s'impone prepotentemente una esigenza di contestualizzazione delle vendite giudiziarie nel sistema Paese, precipitato della presa d'atto per cui il processo esecutivo dialoga con il mercato. Ciò significa che il tema del domicilio digitale deve essere approcciato muovendo dalla premessa per cui la procedura esecutiva annovera attori sì coprotagonisti ma non "parti" del processo, e quindi rispetto ad essi le regole del "domicilio digitale", per come normato dal codice di rito rispetto alle parti, non sono trapiantabili *in toto.*

È fin troppo noto che, per mezzo secolo circa, la materia dell'esecuzione forzata (nelle sue plurimorfi sembianze), vissuta umbratile ai margini del diritto processuale civile (2), come fase eventuale del procedimento — *lato sensu* considerato — di tutela giurisdizionale dei diritti (3), ha conosciuto, a partire dalla fine degli anni '90, un lento risveglio, man mano che sono progressivamente maturate due consapevolezze. La prima, nobilissima, è quella per cui il "giusto processo" è tale non solo in rapporto al giudizio di cognizione da cui (eventualmente) rampolla, ma anche — e forse soprattutto — in relazione al suo momento esecutivo, quello in cui il cittadino consegue, *manu militari*, il bene della vita che la sentenza, o in generale il titolo esecutivo, gli riconosce (4). Nella relazione al codice civile del 1940 si legge

---

(2) Per quanto non siano mancati approfondimenti compiuti da voci illustri del panorama dottrinario; si pensi a S. SATTA, *L'esecuzione forzata*, in *Trattato di diritto civile*, a cura di G. Vassalli, Torino, 1952, 100 ss.; C. MANDRIOLI, *L'azione esecutiva. Contributo alla teoria unitaria dell'azione e del processo*, Milano, 1955, 372 ss.; G. TARZIA, *L'oggetto del processo di espropriazione*, Milano, 1961; A. SALETTI, *Processo esecutivo e prescrizione*, Milano, 1992; R. VACCARELLA *Titolo esecutivo, precetto, opposizioni*, Torino, 1983.

(3) Sovente affidata ai magistrati di prima nomina, i quali non vedevano l'ora di cedere il testimone al collega più giovane.

(4) A questo proposito, Cass. civ., sez. I, 6 ottobre 2005, n. 19435 ha avuto modo di affermare che il diritto di ogni persona a che "*la sua causa sia esaminata... in un tempo ragionevole" — attribuito sia dall'art. 6, comma primo, della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, richiamato già dall'art. 2, comma primo, della legge 24 maggio 2001, n. 89, sia dall'art. 111 Cost. — consiste nella garanzia di ottenere, in un tempo ragionevole, concreta soddisfazione in giudizio delle proprie ragioni ovvero contezza dei motivi per cui queste non debbano essere accolte. In tale prospettiva, l'espressione "decisione... definitiva", contenuta nell'art. 4 della legge n. 89 del 2001, non coincide con quella di sentenza passata in giudicato, ma indica il momento in cui il diritto azionato ha trovato effettiva realizzazione: onde il diritto all'equa riparazione per violazione del termine ragionevole di durata del processo, ai sensi della citata legge n. 89 del 2001, è configurabile anche in relazione al procedimento di esecuzione*". Negli stessi termini, si è espressa Cass. civ., sez. VI, 26 giugno 2013, n. 16028, secondo la quale "*Il diritto all'equa riparazione, riconosciuto dall'art. 2 della legge 24 marzo 2001, n. 89, è configurabile anche in relazione al processo di esecuzione forzata ed a favore di tutte le parti del processo medesimo. Ne consegue che è legittimato a chiedere*

a questo proposito che "*Nel processo esecutivo si misura la vitalità del principio di legalità: e i periodi in cui la tutela del creditore si indebolisce e si fa incerta sono nella storia i periodi la cui anche la legge perde terreno e l'autorità dello Stato declina*". La seconda, più prosaica ma non per questo secondaria, si riassume agevolmente nel noto *pecunia non olet*: le vendite esecutive, ed in generale tutto il sistema del recupero coattivo del credito, "pesano" in termini di PIL poiché una procedura esecutiva efficiente solca il sistema macroeconomico nella misura in cui, facilitando l'erogazione del credito (dacché assicura una proficua gestione della fase patologica del rapporto) è capace di assistere il sistema finanziario (5).

Si è così giunti, grazie anche al formidabile contributo delle *best practices* adottate da alcuni pionieristici Tribunali italiani — che hanno rinverdito la preziosa esperienza del diritto "pretorile", fiore all'occhiello della giurisdizione italiana dei decenni passati — alla legge 3 settembre 1998, n. 302 con la quale è stata legislativamente prevista la possibilità di delegare la vendita immobiliare ai notai. Le riforme del 2005 e del 2006 hanno poi impresso a questo cammino una vigorosa accelerazione, ridisegnando completamente il sistema dell'esecuzione forzata.

La produzione normativa è diventata addirittura alluvionale nel secondo decennio di questo secolo. Sono infatti intervenuti nella disciplina dell'esecuzione forzata: il d.l. 24 giugno 2014, n. 90, convertito in l. 11 agosto 2014, n. 114, il d.l. 27 giugno 2015, n. 83, convertito in l. 6 agosto 2015, n. 132, il d.l. 3 maggio 2016 n. 59, convertito in l. 30 giugno 2016 n. 11, il d.l. 14 dicembre 2018, n. 135, convertito dalla legge 11 febbraio 2019, n. 12, il d.l. 30 dicembre 2019, n. 162 convertito, con modificazioni, con l. 28 febbraio 2020, n. 8. Neppure l'emergenza sanitaria in atto ha fatto segnare una battuta di arresto, tanto è vero che anche il d.l. 17 marzo 2020, n. 18 (così detto "cura Italia"), convertito, con modificazioni, con l. 24 aprile 2020, n. 27 si occupa di esecuzione forzata.

Sarebbe un evidentemente fuor d'opera scrutinare in questa la sede la portata delle richiamate iniziative normative, ma ai fini che qui rilevano è

---

l'indennizzo anche il creditore interventore, senza che possa avere rilevanza ostativa la circostanza che lo stesso creditore, a distanza di un apprezzabile periodo dal suo intervento, abbia deciso di rinunciare alla pretesa esecutiva".

(5) Osserva C. D'Arrigo *Il trattamento del credito fondiario nel nuovo codice della crisi d'impresa e dell'insolvenza d'impresa*, *www. InExecutivis.it.* 19.10.2020, a proposito della disciplina del credito fondiario, che "*ad una maggiore tutela della banca sia in sede contrattuale sia, nel caso di insolvenza, in sede esecutiva, corrispondono una maggiore facilità di accesso al credito da parte degli imprenditori capaci di offrire le garanzie richieste e un più basso costo del denaro (giacché il prestito è maggiormente garantito)*".

utile osservare come non sempre le esigenze che le hanno animate sono state sintoniche tra loro.

In questo senso è paradigmatica la disciplina della custodia, ed in particolare dell'ordine di liberazione, la quale costituisce la cartina di tornasole di come il legislatore abbia alternativamente assecondato spinte efficientistiche (ne è stato un chiaro esempio la riscrittura dei commi 3 e 4 dell'art. 560 c.p.c. ad opera del d.l. n. 59 del 2016) e controspinte garantistiche (non insensibili ad afflati populistici) ispirate ad una non meglio precisata esigenza di tutelare il debitore che abita (con la sua famiglia?) l'immobile pignorato (6), il quale non perde il possesso (*recte*, la detenzione) dell'immobile fino alla pronuncia del decreto di trasferimento, a condizione che si mostri collaborativo; il tutto, con (evidente) buona pace dell'acquirente, che versato il prezzo aspira ad una rapida consegna dell'immobile staggito (7), e con buona pace degli effetti incentivanti che produce la messa in vendita di un bene non occupato (quando non presidiato) dal debitore.

Queste modifiche testimoniano dunque, ove ancora ve ne fosse la necessità, che la disciplina delle esecuzioni forzate "*mostra in conflitto, con varie fortune secondo i tempi, due tendenze antitetiche: quella volta a favorire creditore contro la mancanza di probità del debitore, e quella volta a difendere il debitore contro la spietata avidità del creditore*" (8).

1.2. Il domicilio digitale del creditore procedente e dei creditori intervenuti

Come si diceva, il tema del domicilio digitale nell'esecuzione individuale è peculiare. Ciò in quanto le regole generali della giurisdizione qui subiscono una distorsione provocata dal fatto che il processo di esecuzione è un processo a "contraddittorio attenuato o ridotto" (9). La giurisprudenza di legittimità ha in proposito efficacemente osservato che "*anche dopo le modifiche apportate in senso più garantistico con la l. 14 maggio 2005, n. 80, modificata dalla l. 28 dicembre 2005, n. 263, e con la l. 24 febbraio 2006, n. 52, resta, comunque, imprescindibile la posizione di soggezione del debitore a fronte dell'azione esecutiva che il creditore esercita avvalendosi di un diritto consacrato in un titolo esecutivo; posizione di soggezione, fatta palese — quanto al particolare atteggiarsi del principio del contraddittorio — dalla norma*

(6) Cfr. G. Fanticini, *La liberazione dell'immobile pignorato dopo la "controriforma" del 2019*, *www. InExecutivis.it*, 14.3.2019; A. Crivelli, *L'ordine di liberazione dopo la l. 11/02/2019, n. 12*, in *Riv. Es. For.*, 2019, 4, 760 ss.

(7) Secondo i dettami dell'art. 1476 c.c.

(8) Così la relazione al Re del codice di procedura civile.

(9) Cfr. A. Soldi, *Manuale dell'esecuzione forzata*, cit., 47.

cardine dell'art. 485 c.p.c., non modificata dalle leggi citate. In tale prospettiva è stato evidenziato che nell'opposizione agli atti esecutivi, le ragioni per le quali la lesione del contraddittorio abbia comportato l'ingiustizia dell'atto dell'esecuzione contestato, causata dall'impossibilità di difendersi a tutela di un proprio diritto, devono essere poste a fondamento dell'impugnazione e vanno, pertanto, tempestivamente dedotte in sede di opposizione" (10).

Nono solo. Le regole del procedimento esecutivo conoscono momenti extraprocessuali che tuttavia sono necessariamente prodromici all'inizio dell'esecuzione forzata, che inizia, a norma dell'art. 492 c.p.c., con il pignoramento. E così, diventa apparentemente singolare il dato per cui all'interno di questa norma, dedicata appunto all'atto introduttivo del giudizio, non si rinvengano disposizioni volte a disciplinare il domicilio del soggetto che lo introduce, *id est* il creditore procedente.

L'art. 492 c.p.c. infatti, dopo aver previsto che "*il pignoramento consiste in un'ingiunzione che l'ufficiale giudiziario fa al debitore di astenersi da qualunque atto diretto a sottrarre alla garanzia del credito esattamente indicato i beni che si assoggettano all'espropriazione e i frutti di essi*" contiene tutto un faticoso elenco di contenuti obbligatori dell'atto di pignoramento, ma non prescrive che il creditore procedente debba indicare il proprio domicilio: il domicilio di cui si fa parola è solo quello del debitore, nel senso che l'atto di pignoramento deve contenere l'invito, a questi rivolto, ad effettuare presso la cancelleria del giudice dell'esecuzione la dichiarazione di residenza o l'elezione di domicilio in uno dei comuni del circondario in cui ha sede il giudice competente per l'esecuzione, con l'avvertimento che, in mancanza ovvero in caso di irreperibilità presso la residenza dichiarata o il domicilio eletto, le successive notifiche o comunicazioni a lui dirette saranno effettuate presso la cancelleria dello stesso giudice.

Il domicilio del creditore è invece menzionato nell'art. 480, comma 3, c.p.c., il quale prescrive che il precetto (atto extraprocessuale antecedente necessario all'inizio dell'esecuzione secondo quanto previsto dall'art. 479, comma 1, c.p.c.) deve contenere la dichiarazione di residenza o l'elezione di domicilio della parte istante, con l'avvertenza che in mancanza le opposizioni al precetto si propongono davanti al giudice del luogo in cui è stato notificato, e le notificazioni alla parte istante si fanno presso la cancelleria del giudice stesso. Il cerchio si chiude con la lettura dell'art. 489 c.p.c., (a mente del quale le notificazioni e le comunicazioni ai creditori pignoranti si fanno nella residenza dichiarata o nel domicilio eletto nell'atto di precetto, mentre quelle ai creditori intervenuti si eseguono nella residenza dichiarata o nel

(10) Cass., sez. III, 3 febbraio 2012, n. 1609; Cass., sez. III, 29 settembre 2014, n. 20514.

domicilio eletto nella domanda d'intervento, con l'avvertenza che in mancanza le notificazioni saranno eseguite in cancelleria) e dell'art. 557 c.p.c. il quale impone, a pena di inefficacia del pignoramento, che il creditore procedente debba depositare nella cancelleria del tribunale competente per l'esecuzione la nota di iscrizione a ruolo, unitamente alla copia (attestata conforme all'originale dall'avvocato) del titolo esecutivo, del precetto, dell'atto di pignoramento e della nota di trascrizione (11) entro quindici giorni dalla consegna dell'atto di pignoramento notificato da parte dell'ufficiale giudiziario.

Il tessuto normativo sin qui richiamato deve tuttavia essere completato con il riferimento a tre centrali previsioni.

La prima è quella di cui all'art. 16-*sexies*, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, dall' art. 1, comma 1, l. 17 dicembre 2012, n. 2221, secondo cui, quando la legge prevede che le notificazioni degli atti in materia civile al difensore siano eseguite, ad istanza di parte, presso la cancelleria, alla notificazione con queste modalità può procedersi esclusiva-

(11) Pervero, che anche l'omesso deposito della nota di trascrizione sia causa di inefficacia del pignoramento pare discutibile, visto che questo atto non è contemplato tra i documenti il cui mancato deposito causa la predetta sanzione. In un lungo *obiter dictum* Cass., 14 marzo 2016, n. 4751 ha ricondotto questa omissione ad una mera dimenticanza del legislatore, ma l'opinione è rimasta quasi del tutto isolata (In senso conforme si registra Trib Salerno, 12 dicembre 2019, in *Giur. It.*, 2020, 4, 852). Opposto avviso è stato espresso da altra giurisprudenza di legittimità (Cass., 20 aprile 2015, n. 7998.), dalla giurisprudenza di merito (Trib. Lecce, 29 novembre 2019, *www.dejure.it*; Trib. Torre Annunziata, 15 gennaio 2019, *expartecreditoris.it*; Trib. Roma, 22 gennaio 2019, in *IlCaso.it*, Trib. Verona, 17 dicembre 2021, in *www.inexecutivis.it*.)e dalla dottrina (R. Giuliano, *La digitalizzazione del processo esecutivo. Formalismo telematico e sostanza delle tutele nel processo esecutivo*, in *Riv. es. for.*, 2020, 2, 331-333; A. Soldi, *Manuale dell'esecuzione forzata*, cit., 1294 e ss.; F. De Vita, *L'onere dell'iscrizione a ruolo nell'espropriazione*, in *Giusto Proc. Civ.*, 2016, 838.). La tesi meno rigorosa si impone in primo luogo in ragione della inequivoca formulazione letterale dell'art. 557, comma terzo, c.p.c., che fa riferimento esclusivamente al mancato deposito, nel termine di 15 giorni, decorrenti dalla consegna dell'atto di pignoramento dall'ufficiale giudiziario, di copia conforme dell'atto di pignoramento, del precetto e del titolo esecutivo, senza menzionare la nota di trascrizione del pignoramento. Né questo vuoto può essere colmato in via interpretativa, atteso che le norme *lato sensu* sanzionatorie non sono suscettibili di applicazione analogica, *ex* art. 14 preleggi. Inoltre, l'esclusione della nota di trascrizione dall'elenco degli da depositarsi nel termine di quindici giorni a pena di inefficacia non costituisce un *lapsus calami*, ma una scelta consapevole del legislatore, che se da un lato richiede che il creditore provveda al tempestivo deposito del pignoramento, del precetto, del titolo esecutivo, e della nota di trascrizione, tuttavia commina la sanzione di inefficacia solo all'omesso tempestivo deposito dei primi tre atti e non della nota di trascrizione per evitare il rischio che il creditore possa trovarsi nella impossibilità di rispettare il termine perentorio di cui all'art. 557, secondo comma, c.p.c. quando la Conservatoria dei registri immobiliari gli restituisca in ritardo la nota.

mente quando non sia possibile, per causa imputabile al destinatario, la notificazione presso l'indirizzo di posta elettronica certificata, risultante dagli elenchi di cui all'articolo 6-*bis*, d.lgs. 7 marzo 2005, n. 82 nonché dal registro generale degli indirizzi elettronici, gestito dal ministero della giustizia.

La seconda è contenuta nell'art. 136, comma 2, c.p.c., che nell'attuale versione prescrive che il biglietto di cancelleria è consegnato dal cancelliere al destinatario, che ne rilascia ricevuta, ovvero trasmesso a mezzo posta elettronica certificata, nel rispetto della normativa anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Il terzo comma prevede che — salvo che la legge disponga diversamente — se non è possibile procedere a mezzo P.E.C., il biglietto è rimesso all'ufficiale giudiziario per la notifica.

La terza è rappresentata dall'art. 149-*bis* c.p.c. il quale, più in generale, prescrive che l'ufficiale giudiziario esegua le notifiche a mezzo pec ogni qualvolta il destinatario sia un soggetto per il quale la legge prevede l'obbligo di munirsi di un indirizzo di posta elettronica certificata o servizio elettronico di recapito certificato qualificato risultante dai pubblici elenchi oppure quando il destinatario abbia eletto domicilio digitale ai sensi dell'articolo 3-*bis*, comma 1-*bis*, del CAD.

Dal combitanto disposto degli artt. 136 e 149-*bis* si ricava altresì il precipitato per cui la cancelleria eseguirà le notificazioni in proprio ogni qualvolta il destinatario sia munito di una pec risultante da pubblici elenchi.

Queste disposizioni, peraltro, costituiscono il perché della eliminazione, dal corpo dell'art. 125 c.p.c., della previsione per cui negli atti di parte dovesse essere indicato anche l'indirizzo di post elettronica certificata: invero, esistendo gli elenchi pubblici di cui all'art. 6-*bis* CAD, l'indicazione del medesimo indirizzo nel corpo dell'atto risultava, all'evidenza, un inutile orpello. Non a caso, sia l'art. 16-*sexies* or ora citato che la troncatura appena indicata sono dovute al medesimo d.l. 24 giugno 2014, n. 90, convertito, con modificazioni, dalla l. 11 agosto 2014, n. 114.

1.3. Il domicilio (digitale?) del debitore

Si è detto in esergo che nel processo esecutivo va in scena un contraddittorio "attenuato", poiché l'esecuzione forzata non nasce per accertare un diritto controverso, quanto piuttosto per assicurarne, *manu militari*, l'attuazione, a fonte dell'inadempimento del debitore.

L'art. 492 c.p.c. reca chiara traccia di questa impostazione dogmatica di fondo, laddove prevede che l'atto di pignoramento debba contenere l'invito, rivolto al debitore, ad eleggere un domicilio o ad indicare la residenza in uno dei comuni del circondario in cui ha sede il giudice competente per l'esecu-

zione, con l'avvertimento che in mancanza (ovvero in caso di irreperibilità presso la residenza dichiarata o il domicilio eletto) le successive notifiche o comunicazioni a lui dirette saranno effettuate presso la cancelleria dello stesso giudice (12).

Com'è facile intuire, la norma persegue un duplice obiettivo: da un lato si preoccupa di dare certezza alle comunicazioni dirette al debitore, ponendo il creditore al riparo di un esecutato "*callido*" che tenti di rendersi irrintracciabile o di affaticare le comunicazioni e le notificazioni mutando continuamente il proprio domicilio; dall'altro, mira ad assicurare la effettiva partecipazione dell'esecutato consentendogli di indicare un domicilio per le comunicazioni.

Essa non richiede al debitore una formale costituzione in giudizio a mezzo di un difensore; è sufficiente che egli depositi in cancelleria una dichiarazione in cui indica l'indirizzo prescelto (che potrebbe essere anche una casella di posta elettronica certificata), con il solo avvertimento che deve trattarsi di un indirizzo che si trova in uno dei comuni del circondario.

A rigore, detta previsione non può essere correlata all'art. 16-*sexies* d.l. n. 179 del 2012, di cui si è detto nel paragrafo precedente. Quest'ultima, invero, si applica ai casi in cui "*la legge prevede che le notificazioni degli atti in materia civile al difensore siano eseguite, ad istanza di parte, presso la cancelleria*", e quindi non rileva per le comunicazioni da eseguirsi al debitore in ambito esecutivo, poiché questi può eleggere domicilio senza il ministero di un difensore, ed è quindi personalmente destinatario delle comunicazioni a lui dirette.

Tuttavia (salvo quanto si dirà con riferimento all'art. 149-*bis* c.p.c.) non era affatto detto che al medesimo approdo non si potesse, in taluni casi, giungere.

Il codice dell'amministrazione digitale, dopo aver definito all'art. 1, comma, 1 lett. *n-ter*) il domicilio digitale, prescrive all'art. 3-*bis,* comma 1, che le pubbliche amministrazioni, i professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese hanno l'obbligo di dotarsi di un domicilio digitale che sia iscritto nell'elenco di cui agli articoli 6-*bis* (Indice Nazionale Indirizzi PEC - INIPEC) o 6-*ter* (Indice dei domicili digitali della pubblica amministrazione e dei gestori di pubblici servizi - IPA). Aggiunge poi al comma 1-*bis* che "*Fermo restando quanto*

(12) La giurisprudenza ha escluso che l'omissione dell'invito a dichiarare la residenza o a eleggere il domicilio possa determinare nullità del pignoramento, dovendosi rinvenire mera irregolarità (Cass. civ., sez. III, 12 aprile 2011, n. 8408), ma è evidente che l'omissione dell'invito impedisce le comunicazioni e le notificazioni in cancelleria, con la conseguenza che esse dovranno compiersi nelle forme prescritte dagli artt. 136 ss. c.p.c.

previsto al comma 1, chiunque ha facoltà di eleggere o modificare il proprio domicilio digitale da iscrivere nell'elenco di cui all'articolo 6-quater", il quale a sua volta prescrive che "*È istituito il pubblico elenco dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione nell'indice di cui all'articolo 6*-bis*, nel quale sono indicati i domicili eletti ai sensi dell'articolo 3*-bis*, comma 1*-bis" (elenco che le Linee guida adottate dall'Agenzia per l'Italia digitale (AgID), definiscono con l'acronimo INAD).

Orbene, a norma dell'art. 6, comma 1, secondo capoverso, CAD, "*Le comunicazioni elettroniche trasmesse ad uno dei domicili digitali di cui all'articolo 3*-bis *producono, quanto al momento della spedizione e del ricevimento, gli stessi effetti giuridici delle comunicazioni a mezzo raccomandata con ricevuta di ritorno ed equivalgono alla notificazione per mezzo della posta salvo che la legge disponga diversamente*".

Il comma 1-*quater,* art. 3 CAD prevede invece per tutti i soggetti muniti di domicilio digitale "*l'obbligo di fare un uso diligente del proprio domicilio digitale e di comunicare ogni modifica o variazione del medesimo secondo le modalità fissate nelle Linee guida*".

Come è stato giustamente osservato in dottrina (13), la norma è particolarmente rilevante e va intesa anzitutto come obbligo di rendere possibili le comunicazioni, ovvero di tenere libero lo spazio necessario perché i messaggi giungano a destinazione (14) e pagare il servizio in modo che sia sempre

---

(13) G. Sicchiero, *Il domicilio digitale*, in. *Giur. It*., 2023, 2, 292.

(14) Secondo Cass., 11 febbraio 2020, n. 3164, "*è onere del difensore provvedere al controllo periodo dello spazio disco a disposizione sulla sua PEC, al fine di assicurare che gli effetti giuridici connessi alla notifica di atti tramite lo strumento telematico si possano produrre nel momento in cui il Gestore del servizio PEC rende disponibile il documento nella casella di posta del destinatario. Per questo, il soggetto abilitato esterno è tenuto a dotarsi di un servizio automatico di avviso dell'imminente saturazione*". A questo proposito va ricordato che la Terza sezione civile della Corte di Cassazione, con ordinanza n. 32287 del 21 novembre 2023, ha rimesso alle sezioni unite la questione relativa alla validità della notifica telematica non completata per "casella piena" (il caso di specie riguardava una sentenza di appello notificata, ai fini della decorrenza del termine breve ex art. 326 c.p.c., con messaggio PEC restituito dal sistema con la dicitura "*... è stato rilevato un errore 5.2.2 - InfoCert S.p.A. - casella piena. Il messaggio è stato rifiutato dal sistema*". L'ordinanza di rimessione ricorda che sul tema si registrano due indirizzi giurisprudenziali Il primo ritiene che "*La notificazione di un atto eseguita ad un soggetto, obbligato per legge a munirsi di un indirizzo di posta elettronica certificata, si ha per perfezionata con la ricevuta con cui l'operatore attesta di avere rinvenuto la cd. casella PEC del destinatario "piena", da considerarsi equiparata alla ricevuta di avvenuta consegna, in quanto il mancato inserimento nella casella di posta per saturazione della capienza rappresenta un evento imputabile al destinatario, per l'inadeguata gestione dello spazio per l'archiviazione e la ricezione di nuovi messaggi*" (Cass., 11 febbraio 2020, n. 3164). Il secondo (Cass., 20 dicembre 2021, n. 40758) rileva che "*In caso di notificazione a mezzo PEC del ricorso*

attivo (15). In secondo luogo, come onere di periodica consultazione, nella accezione di cui all'art. 1335 c.c., con la conseguenza che il destinatario non potrà giovarsi del disinteresse nel leggere ogni comunicazione che giunga al suo domicilio (16).

Orbene, se i domicili digitali sono quelli inseriti negli elenchi di cui si è detto, e se gli effetti delle comunicazioni ai domicili digitali sono quelle di cui all'art. 6, comma 1, CAD, è di tutta evidenza che una comunicazione da eseguirsi mediante deposito in cancelleria ben potrà essere sostituita da un inoltro al domicilio digitale, pur non potendosi confezionare un obbligo in tale senso, atteso che il richiamato art. 16-*sexies*, d.l. n. 179 del 2012 confeziona un siffatto obbligo per il solo caso di comunicazioni destinate al difensore. Anzi, questa conclusione si impone ove si ponga mente all'art. 16, comma 4, d.l. 18 ottobre 2012, n. 179, convertito, con modificazioni, con l.

---

per cassazione non andata a buon fine, ancorché per causa imputabile al destinatario (nella specie per "casella piena"), ove concorra una specifica elezione di domicilio fisico — eventualmente in associazione al domicilio digitale — il notificante ha il più composito onere di riprendere idoneamente il procedimento notificatorio presso il domiciliatario fisico eletto in un tempo adeguatamente contenuto, non potendosi, invece, ritenere la notifica perfezionata in ogni caso con il primo invio telematico".

(15) Secondo Cass., 23 giugno 2021, n. 17968, "*nell'ipotesi di notifica del decreto ingiuntivo a mezzo PEC, la circostanza che la e-mail pec di notifica sia finita nella cartella della posta indesiderata ('spam') della casella PEC del destinatario e sia stata eliminata dall'addetto alla ricezione, senza apertura e lettura della busta, per il timore di danni al sistema informatico aziendale, non può essere invocata dall'intimato come ipotesi di caso fortuito o di forza maggiore ai fini della dimostrazione della mancata tempestiva conoscenza del decreto che legittima alla proposizione dell'opposizione tardiva ai sensi dell'art. 650 c.p.c.". Nella stessa scia anche Cass. civ., 7 luglio 2016, n. 13917, in* Fallimento*, 2017, 859, "in tema di notifica telematica del ricorso di fallimento, è manifestamente infondata la questione di legittimità costituzionale dell'art. 15, comma 3 l.fall. nella parte in cui non prevede una nuova notifica dell'avviso di convocazione in caso di accertata aggressione ad opera di esterni all''account' di posta elettronica del resistente: quest'ultimo, infatti, tenuto per legge a munirsi di un indirizzo PEC, ha il dovere di assicurarsi del corretto funzionamento della propria casella postale certificata e di utilizzare dispositivi di vigilanza e di controllo, dotati di misure anti intrusione, oltre che di controllare prudentemente la posta in arrivo, ivi compresa quella considerata dal programma gestionale utilizzato come 'posta indesiderata'*".

(16) In questi termini si è espressa Cass., 2 novembre 2021, n. 31045, secondo la quale "*il Gestore della PEC utilizzata dal destinatario deve fornire al mittente, presso il suo indirizzo elettronico, la cd. ricevuta di avvenuta consegna (RAC), che costituisce, quindi, il documento idoneo a dimostrare, fino a prova del contrario, che il messaggio informatico è pervenuto nella casella di posta elettronica del destinatario; nel momento in cui il sistema genera la ricevuta di accettazione e di consegna del messaggio nella casella del destinatario, si determina, analogamente a quanto avviene per le dichiarazioni negoziali ai sensi dell'art. 1335 c.c., una presunzione di conoscenza da parte dello stesso, il quale, pertanto, ove deduca la nullità della notifica, è tenuto a dimostrare le difficoltà di cognizione del contenuto della comunicazione correlate all'utilizzo dello strumento telematico*".

17 dicembre 2012, n. 221, a mente del quale "*Nei procedimenti civili e in quelli davanti al Consiglio nazionale forense in sede giurisdizionale, le comunicazioni e le notificazioni a cura della cancelleria sono effettuate esclusivamente per via telematica all'indirizzo di posta elettronica certificata risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni*, secondo la normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici.

Chiaramente, sul tema hanno comunque gettato un fascio di luce gli artt. 136 e 149-*bis* c.p.c., richiamati nel paragrafo precedente, laddove hanno imposto che le comunicazioni e le notificazioni siano eseguite a mezzo pec ogni qualvolta il destinatario sia munito di un indirizzo digitale risultante dai pubblici elenchi.

1.4. Domicilio digitale e procedimento di vendita immobiliare

Benché la informatizzazione della giustizia non si sia certo dimostrata la soluzione di tutti i problemi, il legislatore, anche per le vendite forzate, convinto delle potenzialità dello strumento, ha deciso di fare ulteriori decisivi passi sulla via della telematizzazione, imponendone l'obbligatorietà (17).

E così, ai sensi dell'art. 569, comma 4, c.p.c., nel testo riscritto dal dall'art. 4, comma 1, lett. *e*) del d.l. n. 59 del 2016 il Giudice con l'ordinanza di vendita "*stabilisce, salvo che sia pregiudizievole per gli interessi dei creditori o per il sollecito svolgimento della procedura, che il versamento della cauzione, la presentazione delle offerte, lo svolgimento della gara tra gli offerenti e, nei casi previsti, l'incanto, nonché il pagamento del prezzo, siano effettuati con modalità telematiche, nel rispetto della normativa regolamentare di cui all'articolo 161*-ter *delle disposizioni per l'attuazione del presente codice*", il quale a suo volta dispone che "*Il Ministro della giustizia stabilisce con proprio decreto le regole tecnico-operative per lo svolgimento della vendita di beni mobili e immobili mediante gara telematica nei casi previsti dal codice, nel rispetto dei princìpi di competitività, trasparenza, semplificazione, efficacia, sicurezza, esattezza e regolarità delle procedure telematiche*".

Tale decreto, emanato solo diversi anni dopo il conio (avvenuto in forza della lettera *a*) del comma 8-*bis*, art. 4, d.l. 29 dicembre 2009, n. 193, convertito, con modificazioni, dalla l. 22 febbraio 2010, n. 24) di questa disposizione, è il n. 32 del 26 febbraio 2015; esso, a sua volta, contiene all'art. 26 un ulteriore rimando alle "*specifiche tecniche*" stabilite dal responsabile per i sistemi informativi automatizzati del Ministero, "*rese disponibili me-*

(17) A. Crivelli, *Il Portale delle vendite pubbliche e le vendite forzate telematiche nelle procedure concorsuali*, in *Il fallimento*, 2018, 401.

diante pubblicazione nell'area pubblica del Portale dei servizi telematici del Ministero".

La nascita della previsione secondo cui la vendita telematica si staglia quale paradigma del procedimento liquidatorio che si dipana in seno all'esecuzione individuale costituisce l'approdo, non ultimo, di un processo evolutivo i cui natali risalgono al decreto legge 29 dicembre 2009, n. 193 (convertito, con modificazioni, nella l. 22 febbraio 2010, n. 24) il quale per la prima volta prevedeva la possibilità (rimessa all'apprezzamento discrezionale del Giudice) che la vendita si svolgesse con modalità telematiche.

La virata rispetto alla previgente formula codicistica è netta: mentre la vecchia lettera della disposizione riconosceva al Giudice la semplice facoltà di disporre che la vendita si celebrasse con modalità telematiche (la norma infatti prevedeva che "*il Giudice può stabilire*"), il legislatore del 2016, con l'utilizzo dell'indicativo presente ha chiaramente espresso la volontà per cui la vendita telematica deve costituire il modello normale, derogabile quando "*sia pregiudizievole per gli interessi dei creditori o per il sollecito svolgimento della procedura*" (18).

1.4.1. *La presentazione dell'offerta di acquisto*

Ai sensi dell'art. 12, comma 4, d.m. 26 febbraio 2015, n. 32, l'offerta per la vendita telematica è redatta e cifrata mediante un software realizzato dal Ministero è messo a disposizione degli interessati da parte del Gestore della vendita telematica (quest'ultimo è un soggetto privato, iscritto in un apposito elenco tenuto dal Ministero, cui il Giudice affida la gestione informatica del procedimento) sul cui sito (lo stesso sul quale viene pubblicata la vendita) deve essere possibile cliccare il modulo "*offerta telematica*". Una volta inseriti i dati ed i documenti necessari, il software consentirà la generazione dell'of-

(18) Il fatto che la vendita telematica sia il modello ordinario di svolgimento del subprocedimento liquidatorio, non significa che il professionista delegato possa procedere autonomamente. Un provvedimento del Giudice si impone comunque come necessario al precipuo scopo di individuare le modalità procedurali attraverso le quali la vendita telematica deve svolgersi: scelta del Gestore, scelta della tipologia di vendita tra quelle previste dal d.m. n. 32 del 2015 (sincrona, asincrona, sincrona mista), disciplina della vendita (con particolare riguardo, come si vedrà, alle modalità di deposito delle offerte di acquisto) per il caso di mancato funzionamento del dominio giustizia (sia con riferimento alle interruzioni programmate che a quelle improvvise), disciplina dello svolgimento della gara tra gli offerenti "analogici" e "digitali" nelle ipotesi in cui si opti per la vendita sincrona mista, specificazione del fatto che nelle offerte a mezzo di procuratore speciale la procura sia rilasciata per atto pubblico o scrittura privata autenticata, visto che si tratta di precisa scelta normativa del d.m. n. 32 del 2015. Cfr., *si vis,* D'Alonzo, *Il Protale delle vendite pubbliche, la vendita telematica e le (inevitabili) lacune del neonato sistema*, in *Rass. Es. for.*, 1, 2019, 133.

ferta telematica che dovrà essere inviata all'indirizzo di posta elettronica certificata del Ministero della Giustizia.

Né il decreto né le specifiche tecniche indicano quale sia il domicilio al quale l'offerta vada inoltrata.si tratta di un indirizzo di posta elettronica (offertapvp.dgsia@giustiziacert.it) per scoprire il quale occorre leggere il "*Manuale utente*" (sic!) cui si accede, dalla sezione "FAQ" del Portale (https://pvp.giustizia.it/pvp/it/faq.page). Che il luogo di presentazione delle offerte telematiche sia di così labirintica individuazione, è per lo meno singolare, sicché è assolutamente consigliabile che questo indirizzo sia fatto proprio nella ordinanza di vendita e ben evidenziato nell'avviso di cui all'art. 571 c.p.c. Peraltro, si tratta di un indirizzo che, essendo dato, rende sostanzialmente carta straccia sia l'ultimo comma dell'art. 571 che l'art. 591-*bis,* comma 1, c.p.c., nella parte in cui dispongono che le offerte devono essere depositate presso la cancelleria del Giudice dell'esecuzione o nel luogo da questi indicato con l'ordinanza di delega delle operazioni di vendita.

In ossequio alle previsioni di cui al terzo comma dell'art. 12, d.m. n. 32 del 2015 il software è articolato in modo tale da indicare una serie di dati precostituiti, che l'offerente è dispensato dal digitare, contrariamente a quanto accade a proposito della formulazione della offerta cartacea (19). Devono essere invece caricatii tipici dati dell'offerta cartacea, e quindi: i dati del presentatore, la data, l'orario e il numero di CRO del bonifico effettuato per il versamento della cauzione, il codice IBAN del conto sul quale è stata accreditata la somma oggetto del bonifico, l'indirizzo della casella di posta elettronica certificata utilizzata per trasmettere l'offerta e per ricevere le comunicazioni previste dal regolamento, l'eventuale recapito di telefonia mobile ove l'offerente desidera ricevere le comunicazioni previste.

La presentazione dell'offerta di acquisto si snoda attraverso sei passaggi.

Il primo, di sola lettura, identifica il lotto per il quale si intende partecipare.

Segue al secondo step la indicazione delle generalità del presentatore (figura sulla quale si tornerà), individuato in colui che materialmente deposita l'offerta di acquisto (ma l'affermazione sarà meglio precisata più avanti) e della PEC utilizzata per trasmettere l'offerta e per ricevere le comunicazioni previste dal regolamento e al quale possono essere inviati i dati per il recupero offerta ed il pacchetto dell'offerta.

Nel terzo passaggio si devono inserire i dati di tutti gli offerenti, ove non coincidenti con il presentatore (nel qual caso è sufficiente spuntare un

(19) Risultano già inseriti e visibili i dati relativi a: ufficio giudiziario presso il quale pende la procedura; anno e numero di ruolo generale della procedura; numero o altro dato identificativo del lotto; descrizione del bene; indicazione del referente della procedura; data e ora fissata per l'inizio delle operazioni di vendita.

apposito campo) i dati degli offerenti sono a loro volta suddivisi in sottosezioni da compilare tutte a cura del presentatore.

Nel quarto passaggio vanno indicate le quote, espressione con cui si indica sia il tipo di diritto che si intende acquistare (proprietà, nuda proprietà, usufrutto) che la quota, intesa in termini quantitativi (1/1, ½, ecc.) del medesimo diritto.

Nel quinto passaggio si inseriscono i dati dell'offerta: prezzo offerto, termine di versamento della cauzione e relativi estremi (bonifico bancario, carta di credito, fideiussione) e gli allegati indispensabili per la validità dell'offerta (es. copia della fideiussione se per la cauzione si è utilizzato tale mezzo, es. procura rilasciata dall'offerente al presentatore). Il formato ammesso è PDF oppure p7m, con dimensione massima totale degli allegati pari a 25MB.

Il sesto passaggio ha carattere riepilogativo, e vengono riportati tutti i dati relativi all'offerta telematica compilata.

A questo punto il presentatore può procedere in due modi: A) confermare direttamente l'offerta, ed in tal caso il sistema invia una mail alla posta ordinaria o alla PEC, come scelto dal presentatore, con i dati (link e chiave) per recuperare l'offerta inserita e salvata in un'area riservata ed inoltre genera l'Hash associato all'offerta stessa necessario per effettuare il pagamento del bollo digitale; B) firmare digitalmente l'offerta, prima di confermarla. A tal fine il presentatore dovrà scaricare il documento, firmarlo digitalmente con il proprio dispositivo — o farlo firmare dall'offerente se persona diversa — e ricaricarlo nel sistema ([20]). Anche in questo caso il sistema invia una mail alla posta ordinaria o alla PEC, come scelto dal presentatore, con i dati (link e chiave) per recuperare l'offerta inserita e salvata in un'area riservata, ed inoltre genera l'Hash associato all'offerta stessa necessario per effettuare il pagamento del bollo digitale.

Dopo la conferma dell'offerta viene visualizzato l'esito dell'inserimento della stessa.

L'offerta così trasmessa sarà decifrata in maniera automatica non prima di 180 e non oltre 120 minuti antecedenti l'orario fissato per l'inizio delle operazioni di vendita, e trasmessa al Gestore della vendita telematica ([21]), il quale la renderà visibile al professionista delegato che accederà al portale del Gestore, con le proprie credenziali, per procedere all'apertura delle buste telematiche ed allo svolgimento della eventuale gara tra gli offerenti.

([20]) Le modalità di firma digitale che il presentatore può scegliere sono due: *a*) firma su client mediante Smart-Card; *b*) firma tramite Java Web Start.

([21]) A norma dell'art. 2, comma 1, lett. *b*) del citato d.m. n. 32 del 2015, il Gestore della vendita telematica è "*il soggetto costituito in forma societaria autorizzato dal giudice a gestire la vendita telematica*".

1.4.2. *Sottoscrizione ed invio dell'offerta: presentatore ed offerente*

L'invio telematico di un'offerta d'acquisto nei termini in cui esso è disciplinato dal decreto ministeriale e dalle specifiche tecniche pone il problema, sconosciuto nei tradizionali sistemi di presentazione dell'offerta cartacea, di identificazione digitale dell'offerente, di accertamento della provenienza dell'offerta e di distinzione tra presentatore dell'offerta ed offerente.

Nell'ordito normativo del codice di rito "presentatore" ed "offerente" sono figure chiaramente diverse. L'offerente è il soggetto che, a mente del primo comma dell'art. 571, formula l'offerta di acquisto dichiarando di voler acquistare personalmente o quale procuratore speciale (purché sia avvocato), anche per persona da nominare; presentatore è invece colui il quale, a norma dell'ultimo comma del citato art. 571, deposita la busta chiusa contenente l'offerta in cancelleria (o dinanzi al professionista delegato nelle ipotesi di cui all'art. 591-*bis* c.p.c.) e che viene materialmente identificato all'atto della presentazione.

Nella vendita telematica questo distinguo scolora, poiché presentatore ed offerente pur rimanendo soggetti distinti (22), in taluni casi possono coincidere, nel senso che la presentazione dell'offerta può equivalere *ipso iure* alla sottoscrizione della medesima. E tanto poiché il decreto ministeriale prevede che l'offerente sia identificato in colui che sottoscrive con firma digitale l'offerta di acquisto, oppure nel titolare della casella di posta elettronica per la vendita telematica attraverso la quale l'offerta viene presentata.

Infatti, l'art. 12, comma 4, dispone che "*L'offerta è trasmessa mediante la casella di posta elettronica certificata per la vendita telematica. La trasmissione sostituisce la firma elettronica avanzata dell'offerta*". In questo caso la posta elettronica certificata per la vendita telematica sostituisce la firma elettronica, e dunque il titolare della casella di posta elettronica equivale al sottoscrittore dell'offerta.

Al contrario, il successivo comma 5 dispone che "*L'offerta, quando è sottoscritta con firma digitale, può essere trasmessa a mezzo di casella di posta elettronica certificata anche priva dei requisiti di cui all'articolo 2, comma 1, lettera* n)". Ove ricorra questa situazione si avrà dunque che l'offerente si identificherà con colui il quale ha sottoscritto digitalmente l'offerta, la quale potrà essere inviata anche dalla casella di posta elettronica di un soggetto

(22) Secondo le specifiche tecniche il presentatore è il "*Soggetto che compila ed eventualmente firma l'Offerta telematica prima di presentarla con specificato titolo per ciascun offerente*".

diverso, non essendo richiesto che la PEC di trasmissione dell'offerta sia intestata al sottoscrittore della medesima.

Si comprende allora come sia assolutamente necessario, nel caso di presentazione di un'offerta non firmata digitalmente, verificare che la casella di posta elettronica certificata dalla quale proviene la stessa sia stata rilasciata, previa identificazione del richiedente, dal Gestore del servizio, verifica che dovrà essere compiuta accertando che il messaggio di posta elettronica, o un suo allegato, contengano la prescritta attestazione di identificazione del richiedente la PEC (23).

Il sistema così ricostruito non è privo di ricadute operative, delle quali è bene tener conto.

A mente dell'art. 16 "*Almeno trenta minuti prima dell'inizio delle operazioni di vendita il Gestore della vendita telematica invia all'indirizzo di posta elettronica certificata indicato nell'offerta*" (che è lo stesso utilizzato per l'invio dell'offerta) "*un invito a connettersi al proprio Portale*", fornendogli anche le credenziali di accesso necessarie per partecipare alla gara.

L'effetto di questa previsione è che ove l'offerta, sottoscritta digitalmente, sia stata inviata per il tramite di una PEC non intestata al titolare della firma digitale, il soggetto invitato a partecipare, destinatario delle credenziali di accesso, potrebbe non essere lo stesso che ha sottoscritto l'offerta, bensì il presentatore.

Che le credenziali siano inviate ad un soggetto potenzialmente diverso dall'offerente non è di per sé un problema. Invero, si tratta comunque dell'indirizzo PEC che l'offerente ha consapevolmente indicato quale "domicilio telematico" cui riceverle, con la conseguenza egli non potrà dolersi di questa circostanza.

Piuttosto può accadere (e qui invece gli inconvenienti ed i rischi di turbativa potrebbero essere di non poco momento) che colui il quale, nella veste di presentatore, abbia depositato più offerte di acquisto da altri firmate digitalmente ed inviate con PEC non identificativa, potrebbe materialmente partecipare alla gara per una pluralità di soggetti, (posto che riceve le credenziali di ciascuno di essi, eseguendo (o decidendo di non eseguire) rilanci che non risulterebbero formulati in nome e per conto degli offerenti, ma ad essi direttamente ascrivibili.

È chiaro dunque che di questa possibile dinamica occorre avere assoluta considerazione, e rispetto ad essa si pone in primo luogo un dubbio di

(23) Poiché l'offerta viene inviata al ministero e da questi decriptata e trasmessa al Gestore della vendita, l'art. 17 del decreto prescrive in capo a quest'ultimo lo svolgimento di questo controllo. La previsione, tuttavia, deve essere interpretata conformemente al dato codicistico (che con l'art. 591-*bis* assegna al delegato il compito di verifica di ammissibilità delle offerte di acquisto) sicché il controllo del Gestore è aggiuntivo, e non sostitutivo.

qualificazione giuridica. Infatti, pur essendo innegabile che il soggetto presentatore il quale agisca nell'interesse di una pluralità di offerenti, tutti portatori di interessi contrapposti in relazione al medesimo lotto posto in vendita, versa fatalmente in una condizione di conflitto di interessi, la sussunzione della vicenda nella cornice dell'art. 1394 c.c. non si coglie con immediatezza, poiché al suo approdo è possibile giungere solo attraverso un iter argomentativo di una certa articolazione.

Ed invero, a ben riflettere, nel momento in cui, a norma dell'art. 16, comma 1, d.m. n. 32 del 2015 le credenziali per la connessione al Portale del Gestore della vendita telematica e per la eventuale partecipazione alla gara sono trasmesse all'indirizzo di posta elettronica utilizzato per l'invio della offerta, e nella medesima offerta indicato (così l'art. 12, comma 1, lett. *n*) si ha che il regolamento, consentendo, attraverso l'utilizzo di quelle credenziali, di eseguire rilanci, li ritiene giuridicamente imputabili all'offerente come suoi propri.

Questa assimilazione deve tuttavia suscitare qualche perplessità, per le ragioni che seguono.

Ai sensi dell'art. 20, comma 1-*bis* del d.lgs. 7 marzo 2005, n. 82 (meglio noto come Codice dell'amministrazione digitale), il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia di cui all'art. 2702 c.c., quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, quando sia stato formato, previa identificazione informatica del suo autore ai sensi dell'articolo 71 dello stesso codice, con modalità tali da garantire, tra l'altro, "*in maniera manifesta e inequivoca, la sua riconducibilità all'autore*". La norma, inoltre, precisa che "*In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità*".

Ancora, va aggiunto che secondo quanto previsto dall'art. art. 61, d.p.c.m. 22 febbraio 2013, recante "*Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali*", il solo strumento che può sostituire la firma elettronica avanzata è l'invio tramite posta elettronica certificata di cui all'art. 65, comma 1, lettera *c-bis*) del Codice dell'amministrazione digitale, vale a dire posta elettronica certificata le cui credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica, secondo modalità definite dal d.p.c.m.

27 settembre 2012 (24), e ciò sia attestato dal Gestore del sistema nel messaggio o in un suo allegato (sulla PEC identificativa si tornerà a breve).

Ed allora, se così è, il rilancio eseguito previo acceso al Portale attraverso le credenziali inviate su una PEC non identificativa, vale a dire la PEC eventualmente utilizzata per l'inoltro di una offerta firmata digitalmente, non ne assicura la riferibilità all'offerente, poiché il sistema non prevede alcun controllo volto a verificare che la PEC a cui le credenziali sono trasmesse sia effettivamente intestata all'offerente, né il rilascio di una PEC non identificativa, che pure fosse intestata formalmente all'offerente, richiede la previa identificazione del richiedente, trattandosi di vaglio necessario solo per le PEC identificative.

La replica alle perplessità sin qui espresse potrebbe risiedere nella considerazione, apparentemente ineccepibile, per cui il soggetto che, a prescindere da chi redige l'offerta di acquisto (attraverso la compilazione del modulo informatico messo a disposizione del ministero), la sottoscrive digitalmente, la fa propria e quindi assume come a lui riferibile quel luogo "virtuale" rappresentato dalla pec presso cui intende ricevere le credenziali necessarie per la partecipazione, sicché le credenziali lì inviate si reputano giunte al destinatario analogamente a quanto avviene a proposito delle notificazioni eseguite presso il domicilio eletto *ex* art. 47 c.c.

Questo argomento certamente consentirebbe di salvare la tenuta del sistema sotto il profilo formale; tuttavia non può obliterarsi il dato empirico per cui è del tutto fisiologica l'ipotesi in cui il *quisque de populo*, rivolgendosi ad un presentatore "professionale" per la formulazione dell'offerta di acquisto, potrebbe non avere contezza dell'indirizzo che il presentatore indicherà quale luogo di ricezione delle credenziali di accesso, e comunque il sistema si presta certamente ad operazioni di turbativa da parte del presentatore seriale che, ad esempio, faccia mercimonio dei rilanci che può decidere di eseguire o non eseguire disponendo di più credenziali di accesso.

Andando alla ricerca di possibili soluzioni, alcuni uffici giudiziari hanno tentato di apprestare misure di cautela, indicate nell'ordinanza di vendita, prevedendo ad esempio: che firma digitale e PEC di trasmissione dell'offerta siano intestate allo stesso soggetto; limitando ogni PEC non identificativa ad una sola domanda (25); obbligando il presentatore a munirsi di procura speciale.

---

(24) Recante "*Regole tecniche per l'identificazione, anche in via telematica, del titolare della casella di posta elettronica certificata, ai sensi dell'articolo 65, comma 1, lettera* c-bis*), del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni*".

(25) Del resto, sembra essere questo il retropensiero che si ricava dalla lettura delle specifiche tecniche.

Si tratta tuttavia di previsioni la cui legittimità ed idoneità a conseguire il risultato sperato sono per lo meno incerte.

Sul primo versante, appare discutibile la previsione per cui il presentatore debba essere munito di procura speciale. Invero, il presentatore non agisce in nome e per conto dell'ente, spendendo la di lui autonomia e negoziale. Egli si limita allo svolgimento di un'attività materiale la quale corrisponde al deposito della busta cartacea o telematica.

In relazione al secondo, la pretesa che firma digitale e PEC di trasmissione dell'offerta siano intestate allo stesso soggetto è del tutto inutile, ove si osservi che il professionista delegato ed il giudice, in sede di apertura delle buste non hanno alcuna possibilità di verificare l'appartenenza sia della prima che della seconda. Allo stesso modo, limitare ogni PEC ad una sola domanda costituirebbe argine agevolmente superabile da quel presentatore il quale potrebbe munirsi di un numero indeterminato di PEC.

1.4.3. *Le criticità della PEC identificativa per la vendita telematica: suggerimenti al legislatore*

Si è visto sopra che l'art. 12, comma 4 equipara l'offerta trasmessa a mezzo PEC id alla sottoscrizione digitale. Questo pone, come ci si accinge a spiegare, alcuni interrogativi.

A pag. 7 si dice che per garantire la maggiore trasparenza possibile e la riservatezza dei dati personali degli offerenti (e del presentatore dell'offerta), il software per la compilazione e la cifratura dell'offerta elabora un documento contente l'offerta priva dei dati identificativi del presentatore e di tutti gli offerenti, in modo da permettere a tutti i partecipanti di conoscere le condizioni delle offerte.

A pag. 8 si prevede che i dati relativi all'offerta telematica sono inseriti dal presentatore, che riceve l'offerta criptata e provvede ad effettuare il pagamento del bollo.

A pag. 9 si dispone che il presentatore invia l'offerta criptata alla PEC del Ministero utilizzando la "casella di posta elettronica certificata per la vendita telematica", di posta certificata priva dei requisiti di cui sopra, laddove l'offerta sia firmata digitalmente prima rilasciata dal Gestore della PEC. In alternativa l'offerta criptata può essere trasmessa anche mediante casella di essere criptata.

A pag. 12, in armonia con l'art. 16 del decreto ministeriale, si attribuisce al Gestore delle Vendite di inviare, almeno 30 minuti prima dell'inizio delle operazioni di vendita, le credenziali per accedere al proprio Portale e per permettere al presentatore di assistere all'esperimento di vendita.

E così via a pag. 18, punto 6, pag. 19, punto 17 e nei punti successivi, dove si vede che il presentatore è colui che materialmente compila il modulo e che dialoga con il software ministeriale, indipendentemente dal fatto che sia o meno offerente.

Anche a pag. 20 si prevede che il presentatore si autentica al Portale del Gestore delle Vendite Telematiche con le credenziali ricevute e partecipa alle operazioni di vendita.

Ancora, a pag. 22 si disciplina il caso del presentatore che voglia firmare digitalmente l'offerta.

È bene subito premettere che la PEC rilasciata previa identificazione dell'offerente non è strumento nuovo nel panorama normativo (26). Come detto, ad essa faceva già riferimento l'art. 65, comma 1, lettera *c-bis*) del codice dell'amministrazione digitale, definendola come la casella di posta elettronica certificata le cui credenziali di accesso siano state rilasciate previa identificazione del titolare, anche per via telematica secondo modalità definite dal d.p.c.m. 27 settembre 2012.

Tale decreto all'art. 5 (intitolato "*Modalità di identificazione dei Titolari di caselle PEC-ID*"), prevede che all'atto del rilascio delle credenziali della casella di PEC ID, l'identificazione del richiedente può avvenire:

a) mediante la sottoscrizione del modulo di adesione al servizio ed esibizione al Gestore, da parte del Titolare, di un valido documento d'identità e del codice fiscale;

b) tramite la compilazione del modulo di adesione disponibile in rete, previa identificazione informatica tramite CIE o CNS (carta di identità elettronica o carta nazionale dei servizi);

c) mediante la sottoscrizione con firma digitale del modulo di adesione;

d) a mezzo di apparecchiature che utilizzino necessariamente una SIM/USIM dotate di codici PIN/PUK o loro evoluzioni tecnologiche rilasciate previa identificazione del titolare delle medesime nel rispetto delle disposizioni vigenti.

Il tutto è accompagnato dall'obbligo, posto in capo al Gestore della casella di posta elettronica, di verificare la corrispondenza dei dati forniti dal titolare con le generalità indicate nel documento d'identità o associate alla SIM/USIM.

Similmente, (ma con le differenze di cui tra un attimo si dirà) l'art. 2 lett. *n*) del d.m. n. 32 del 2015 definisce la PEC per la vendita telematica come: « *la casella di posta elettronica certificata richiesta dalla persona fisica o giuridica che intende formulare l'offerta, le cui credenziali di accesso sono rilasciate, previa identificazione del richiedente, a norma dell'articolo 13* ».

---

(26) La PEC identificativa, fino ad oggi rimasta nella penna del legislatore, ha fatto il suo ingresso nel mercato in forza delle regole tecniche recepite da AgID, in coerenza con il Regolamento europeo n. 910/2014 (eIDAS) e con gli standard emanati da ETSI, che consentono di trasformare la PEC in REM (Registered Electronic Mail), il che comporta:

il riconoscimento certo del mittente e del destinatario della PEC (ed infatti l'adeguamento della si sostanzia nella identificazione del titolare della casella di posta elettronica da parte del Gestore della casella medesima);

l'innalzamento del livello di sicurezza attraverso il passaggio da un sistema di autenticazione semplice (username più password) ad un sistema di autenticazione a due fattori (MFA -Multi Factor Authentication), che è il modo prescelto dallo standard europeo per garantire l'identità certa del titolare della casella di posta.

Il successivo art. 13 statuisce, a proposito della PEC ID:

a) che ciascun messaggio di posta elettronica certificata per la vendita telematica deve contenere, anche in un allegato, l'attestazione del Gestore della casella per idi di aver provveduto al rilascio delle credenziali previa identificazione del richiedente;

b) che, quando l'identificazione è eseguita per via telematica, la stessa "*può*" aver luogo mediante la trasmissione al Gestore di cui al comma 1 di una copia informatica per immagine, anche non sottoscritta con firma elettronica, di un documento analogico di identità del richiedente l'identificazione;

c) che il ministero verifica, su richiesta dei gestori di PEC ID, che il procedimento di rilascio delle credenziali di accesso sia conforme a quanto previsto dal presente articolo e li iscrive in un'apposita area pubblica del Portale dei servizi telematici del Ministero.

Come si vede, i livelli di sicurezza previsti per il rilascio di una PEC ID per la vendita telematica possono essere inferiori a quelli richiesti per la PEC ID prevista dal codice dell'amministrazione digitale. Infatti, la prescritta identificazione del richiedente può avvenire, anche per via telematica, mediante la trasmissione al Gestore di una copia informatica per immagine, anche se non sottoscritta con firma elettronica, di un documento analogico di identità.

È dunque evidente che chiunque sia in possesso della copia del documento di identità di un soggetto, può renderlo offerente a sua insaputa in una vendita telematica anche se, vale la pena di ricordarlo, questo può accadere anche nella vendita analogia, in quanto in nessuna fase è previsto che l'offerente sia identificato (salvo che si proceda alla gara), dovendolo essere solo il presentatore.

Quanto appena detto pone il serio interrogativo di individuare le sorti di una offerta non sottoscritta digitalmente, non proveniente da PEC identificativa, e tuttavia accompagnata dalla trasmissione della copia analogica del documento di identità.

Si tratta di una evenienza tutt'altro che remota, poiché il distinguo tra PEC e PEC identificativa non costituisce patrimonio conoscitivo comune, ed anzi anche un operatore mediamente esperto potrebbe incorrere nell'errore di considerare bastevole una PEC qualunque, poiché normalmente la richiesta di una PEC implica la trasmissione del documento di riconoscimento.

Dovrebbe dirsi, *prima facie*, che una offerta di tal fatta dovrebbe essere esclusa poiché difforme rispetto alle previsioni di cui all'art. 12, commi 4 e 5. Si è detto in dottrina che in questo caso vi sarebbe un vero e proprio difetto

di sottoscrizione, poiché solo la trasmissione a mezzo pec identificativa sostituisce la firma digitale (27).

Qualche riflessione ulteriore va tuttavia compiuta.

Invero, come si è visto, la PEC ID per la vendita telematica può essere rilasciata anche sulla base di una identificazione avvenuta mediante trasmissione di copia informatica per immagine (anche non sottoscritta digitalmente) di un documento analogico di identità.

Eccentrico rispetto alla struttura della PEC ID è il fatto che poi il Gestore della casella di posta elettronica ottemperi alla previsione di cui all'art. 13, comma 4, d.m. n. 32 del 2015, ossia chieda e ottenga dal ministero la verifica di conformità della identificazione dell'offerente alle prescrizioni normative. Si tratta, infatti, di un adempimento: ulteriore rispetto al rilascio della PEC; non richiesto a pena di validità della PEC medesima. Detto in altri termini: un conto è rilasciare una PEC id secondo le modalità prescritte dal decreto, altro è chiedere al ministero la verifica di conformità del procedimento eseguito. Neppure la verifica dell'assolvimento di questo onere è richiesta ad alcuno: non al delegato, non al Gestore, che a norma dell'art. 17 deve verificare solo l'esistenza dell'attestazione di previa identificazione in calce o in allegato al messaggio di PEC con cui viene trasmessa l'offerta.

Detto in altri termini: un conto è rilasciare una PEC ID secondo le modalità prescritte dal decreto, altro è chiedere al ministero la verifica di conformità del procedimento eseguito. Neppure la verifica dell'assolvimento di questo onere è richiesta ad alcuno: non al delegato, non al Gestore, che a norma dell'art. 17 deve verificare solo l'esistenza dell'attestazione di previa identificazione in calce o in allegato al messaggio di PEC con cui viene trasmessa l'offerta.

Ed allora, se la PEC ID è quella rilasciata previa identificazione eseguita con le modalità innanzi descritte, e posto che la sottoposizione al controllo del ministero del procedimento di identificazione dell'offerente da parte del Gestore non è richiesta a pena di validità dell'offerta, il medesimo risultato non si raggiunge forse se alla offerta trasmessa con PEC non id sia stata allegata la copia informatica del documento analogico? In questo modo, a ben vedere, l'offerente avrebbe adempiuto allo stesso identico onere che gli era richiesto in sede di acquisto della PEC ID, con la sola differenza che mente nel primo caso il professionista delegato ottiene da un terzo (il Gestore della casella di PEC) l'attestazione di avvenuta identificazione, nel secondo procede egli stesso alla medesima identificazione che avrebbe dovuto compiere il Gestore della casella PEC, il quale a mente dell'art. 13, comma tre, del decreto ministeriale doveva limitarsi a ricevere la copia del documento di identità.

---

(27) Così G. Fanticini, *Le opposizioni nella vendita telematica*, in *www.Inexecutivis.it.*

Si avrebbe, nella sostanza, che la copia informatica del documento analogico di identità invece che essere trasmessa al Gestore della PEC ID quale allegato alla richiesta di rilascio della pec sarebbe inviata direttamente al professionista delegato.

Certamente, l'affermazione della ammissibilità di un'offerta telematica non sottoscritta digitalmente ed inviata a mezzo PEC si espone alla obiezione per cui una soluzione tecnica di tal fatta sconterebbe l'inconveniente di impedire agli organi della procedura la identificazione dell'offerente.

Si tratta tuttavia, a parere di chi scrive, di un falso problema, o meglio di un problema che non si pone nella vendita telematica in termini diversi rispetto a quanto accade nella vendita analogica.

Ed invero, anche nella vendita tradizionale si può giungere alla pronuncia del decreto di trasferimento senza che l'aggiudicatario sia stato mai identificato. Basti osservare che la irrevocabilità dell'offerta, prescritta dall'articolo 571 c.c. e l'aggiudicazione al miglior offerente, per la quale gli articoli 572 e 573 c.p.c. non richiedono la presenza fisica di costui, determinano l'effetto concreto per cui il bene potrebbe essere aggiudicato e trasferito ad un offerente che il professionista delegato ed il giudice non hanno mai identificato, anche in considerazione del fatto che l'identificazione della aggiudicatario non è richiesta quale precondizione per la pronuncia del decreto di trasferimento. Pretendere dunque che l'offerente sottoscriva con firma digitale la propria offerta di acquisto (o che la invii per il tramite di una PEC identificativa) costituisce mero orpello procedimentale, tanto più che all'indomani delle modifiche introdotte alla disciplina dell'esecuzione forzata dal d.lgs. 10 ottobre 2022, n. 149 (c.d. *Riforma Cartabia*), l'eventuale bisogno di identificazione viene soddisfatto dal rilascio, in favore del professionista delegato, della dichiarazione antiriciclaggio, così come previsto dal novellato ultimo comma dell'art. 585 c.p.c.

1.5. Domicilio digitale e vendita mobiliare telematica

Il procedimento di identificazione, domiciliazione e presentazione delle offerte di acquisto nella vendita mobiliare telematica sconta una serie di peculiarità che la rendono ad un tempo strutturato per eccesso e per difetto ([28]). Difatti, mentre la vendita del terreno boschivo al prezzo base di *nummo uno* ([29]) soggiace al rigore procedimentale della vendita immobiliare,

([28]) Così S. Rossetti, *La pubblicità e la vendita telematica*, in *inexecutivis.it* pubblicato il 10 marzo 2018.

([29]) Ammesso che questo possa ancora accadere, stante la previsione di cui all'art. 164-*bis* disp. att. c.p.c.

l'iter che conduce alla liquidazione della lussuosa imbarcazione risulta assai scorrevole (30), di tal che è lecito domandarsi se debba semplificarsi il primo o irrigidirsi il secondo, ed è ragionevole rispondere che probabilmente occorre l'una e l'altra cosa.

La vendita mobiliare telematica si caratterizza per il fatto di attribuire enormi compiti al Gestore della vendita, il che da un lato legittima l'interrogativo che ruota intorno alla individuazione dei residui compiti del professionista delegato; dall'altro impone una riflessione sulla tenuta costituzionale del modello costruito, in relazione al principio del giusto processo regolato per legge, scolpito nell'art. 111 Cost., riflessione che suggerisce di riportare all'interno dell'ordinanza di vendita (*lex specialis* del procedimento liquidatorio), tutte quelle specifiche disposizioni rischiosamente ospitate nel decreto ministeriale n. 32 del 2015.

La semplificazione del modello di vendita telematica mobiliare rispetto alla vendita immobiliare si coglie innanzi tutto sul piano della distribuzione dei pesi all'interno del citato d.m., che dedica specificatamente alla vendita mobiliare il solo art. 25.

Colui che intenda partecipare alla vendita mobiliare deve preliminarmente registrarsi sul Portale del Gestore della vendita telematica, fornendo una serie di informazioni (dati identificativi, il codice fiscale, un indirizzo di posta elettronica anche ordinaria per le comunicazioni del Gestore, il luogo in cui intende ricevere le comunicazioni di cancelleria, il recapito di telefonia mobile).

All'esito della registrazione il sistema (e dunque il Gestore della vendita) genera le credenziali per la partecipazione dell'interessato alla vendita per la quale la registrazione è stata effettuata e gli assegna uno pseudonimo (o altri elementi distintivi in grado di assicurare l'anonimato).

Da questa previsione si comprende che:

— la domanda di partecipazione alla gara non è rivolta al Giudice (né tanto meno al professionista delegato) ma al Gestore;

— l'ammissione alla procedura di vendita non viene decisa dal Giudice o dal delegato, ma dal Gestore, che fornisce le credenziali di accesso;

— non è prevista alcuna verifica relativa alla legittimazione negoziale dell'offerente;

— non è previsto alcun controllo sui dati identificativi trasmessi, neppure l'invio della copia informatica, per immagine, del documento analogico di identità o l'indicazione di un indirizzo di posta elettronica certificata;

---

(30) L'anomalia è segnalata anche da E. FABIANI, *La vendita forzata telematica*, Padova, 2018, 70.

— la registrazione al portale del Gestore è una registrazione "per la vendita", il che impone, almeno sul piano normativo, che ci si debba registrare per ogni esperimento di vendita cui si intende partecipare;

— il sistema infine non prevede che un utente già registrato possa recuperare le credenziali e partecipare alle successive vendite del medesimo Gestore, come invece le piattaforme dell'*e-commerce* consentono di fare.

Rispetto alla vendita immobiliare, gli elementi dell'offerta per la vendita mobiliare sono solo due: prezzo offerto e cauzione versata. Non è necessario inserire nemmeno i dati dell'offerente poiché l'utente è già registrato.

Il sistema descritto si dipana dunque attraverso una scansione temporale che consta di tre fasi: registrazione dell'utente, fornitura delle credenziali di accesso, formulazione della offerta di acquisto con versamento della cauzione ([31]). Tutte le operazioni funzionali alla partecipazione vendita (registrazione, offerta e versamento del saldo) possono essere eseguite contestualmente quando il pagamento avviene con sistemi (ad esempio carta di credito) che consentono una verifica immediata da parte del Gestore.

Venendo al concreto articolarsi della vendita deve osservarsi che l'art. 25, d.m. n. 32 del 2015 prevede un modello tendenzialmente ispirato alla vendita asincrona, non contemplandone lo svolgimento secondo i meccanismi della vendita sincrona telematica o della vendita sincrona mista, rispettivamente definite alle lett. *f)* e *g)* dell'art. 2, d.m. n. 32 del 2015. Lo si evince chiaramente dal comma 1, il quale prevede che « per la presentazione dell'offerta per la vendita dei beni mobili con modalità asincrona, l'interessato si registra sul Portale del Gestore della vendita telematica ». Il medesimo art. 25 contiene, poi ai commi 6 e 7, alcuni generici riferimenti all'eventuale gara tra gli offerenti. Segnatamente, il comma 6 prevede che « il Gestore abilita a partecipare alla gara gli offerenti che hanno effettivamente versato la cauzione », mentre il comma sette aggiunge che « Nel corso della gara gli offerenti sono individuati esclusivamente mediante lo pseudonimo o gli altri elementi distintivi di cui al comma 1 », precisando ancora che « entro il secondo giorno successivo alla chiusura della gara, il Gestore trasmette al referente della procedura l'elenco delle offerte e i dati identificativi di coloro che le hanno effettuate ».

Come si vede, la struttura della vendita mobiliare telematica ha abdicato del tutto all'idea di affrontare il problema della individuazione del domicilio

([31]) Il comma sesto dell'art. 25 specifica, al secondo periodo, che queste attività devono essere completate almeno cinque giorni prima dello svolgimento delle operazioni di vendita, e che il Gestore della vendita abilita a partecipare alla gara solo gli offerenti che abbiano effettivamente versato la cauzione; si desume da ciò che il Gestore è il soggetto delegato all'accertamento dell'avvenuto corretto versamento della cauzione.

digitale dell'offerente. Invero, i dati che gli vengono richiesti per partecipare alla gara (le generalità, il codice fiscale, un indirizzo di posta elettronica anche ordinaria per le comunicazioni del Gestore, il luogo in cui intende ricevere le comunicazioni di cancelleria, il recapito di telefonia mobile), non contemplano un vero e proprio domicilio digitale, né si pone il problema di una sua effettiva identificazione.

La cosa pervero, non deve stupire, atteso che anche nel codice di rito mancano, a proposito della vendita mobiliare, disposizioni che, analogamente a quelle di cui agli artt. 582 c.p.c. e 174 disp. att. c.p.c., (disciplinanti, rispettivamente per la vendita con incanto e per quella senza incanto, l'obbligo — nel primo caso per l'aggiudicatario e nel secondo caso per l'offerente — di dichiarare la propria residenza o eleggere domicilio nel comune in cui ha sede il giudice che ha proceduto alla vendita, con l'avvertenza che in m mancanza le notificazioni e comunicazioni sarebbero state eseguite presso la cancelleria) affrontano il tema del domicilio dell'offerente.

Sezione III
LA VOLONTARIA GIURISDIZIONE

I.
NOTE SUL DOMICILIO DIGITALE DEL NOTAIO

di *Michele Nastri*

Sommario: 1.1. Il domicilio del notaio - la sede notarile. — 1.2. Riferimenti normativi sul domicilio digitale. — 1.3. Altri registri: ReGIndE; INAD. — 1.4. PEC e REM.

1.1. Il domicilio del notaio - la sede notarile

Il notaio, quale pubblico ufficiale, è incardinato per legge nel territorio di appartenenza, ed è assegnato ad un Comune di residenza nel quale deve aprire ed assistere lo studio ai sensi del primo comma dell'art. 26 della legge notarile (l. 16 febbraio 1913 n. 1989).

L'assistenza alla sede notarile è regolata dai commi successivi del citato articolo 26, che, per le modalità, rinvia anche alle delibere dei consigli notarili distrettuali. È necessario quindi che il domicilio del notaio, per la migliore disponibilità del servizio pubblico notarile, sia facilmente conoscibile. È intervenuta a migliorare tale aspetto, resosi problematico col mutare dei tempi e delle relazioni sociali rispetto al contesto della norma del 1913, la normativa del Decreto del Presidente della Repubblica 7 agosto 2012, n. 137 (Regolamento recante riforma degli ordinamenti professionali, a norma dell'art. 3, comma 5, del decreto-legge 13 agosto 2011, n. 138, convertito, con modificazioni, dalla legge 14 settembre 2011, n. 148).

L'art. 3 di tale decreto sancisce infatti che "*Gli albi territoriali relativi alle singole professioni regolamentate, tenuti dai rispettivi consigli dell'ordine o del collegio territoriale, sono pubblici e recano l'anagrafe di tutti gli iscritti, con l'annotazione dei provvedimenti disciplinari adottati nei loro confronti.*

L'insieme degli albi territoriali di ogni professione forma poi l'albo unico nazionale degli iscritti, tenuto dal consiglio nazionale competente.

Tale normativa si limita quindi a sancire l'obbligo di indicare le anagrafiche che, in un'interpretazione estensiva della legge, il Consiglio Nazionale del Notariato ha esteso agli indirizzi di posta elettronica ordinaria. L'Albo Unico dei notai è in esercizio ed è reperibile sul sito istituzionale www.notariato.it

Va detto però che tale normativa non contiene alcuna indicazione circa il domicilio digitale.

1.2. Riferimenti normativi sul domicilio digitale

La normativa relativa al domicilio digitale del notaio è quindi costituita dal complesso di norme contenute nel codice dell'amministrazione digitale (CAD, d.lgs. 7 marzo 2005, n. 82), il quale prevede, all'art. 6-*bis*, l'istituzione del pubblico elenco denominato Indice nazionale dei domicili digitali (INI-PEC) delle imprese e dei professionisti, presso il Ministero per lo sviluppo economico.

Tale registro è stato realizzato a partire dagli elenchi di indirizzi PEC costituiti presso il registro delle imprese e gli ordini o collegi professionali, in attuazione di quanto previsto dall'articolo 16 del decreto-legge 29 novembre 2008, n. 185, convertito, con modificazioni, dalla legge 28 gennaio 2009, n. 2, ed è gestito dal Ministero delle Imprese e del *Made in Italy* attraverso le strutture informatiche delle Camere di Commercio deputate alla gestione del Registro Imprese.

Gli indirizzi sono comunicati dagli ordini e collegi professionali di appartenenza in base al comma 5 del citato art. 6-*bis* del CAD, e vi è quindi un controllo pubblico sulla reperibilità del domicilio digitale del professionista.

L'iscrizione a tale registro è obbligatoria, ed il registro è liberamente accessibile al pubblico.

In tal modo, sia pure con un percorso totalmente separato, risultano reperibili al pubblico, oltre che, ovviamente, alle pubbliche amministrazioni, i domicili analogici e digitali dei notai.

1.3. Altri registri: ReGIndE; INAD

Per i soli fini dei rapporti con il sistema del processo telematico resta poi attivo il Registro Generale degli Indirizzi Elettronici, previsto dall'articolo 13 del d.m. 21 febbraio 2011, n. 44. Tale registro è utilizzato ai fini della preventiva identificazione dei soggetti esterni (e quindi anche dei notai) abilitati all'accesso al sistema, e dovrebbe essere destinato ad essere superato dai più evoluti sistemi in essere o prossimi all'utilizzo, come i servizi di REM, di cui in prosieguo.

A norma dell'art. 6-*quater* del CAD è stato poi istituito l'INAD (Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese), la cui regolamentazione di detta-

glio è contenuta nelle Linee Guida emanate ai sensi dell'art. 71 del CAD attualmente nella versione dell'8 agosto 2023.

Il domicilio digitale dei professionisti iscritti nell'INI-PEC è inserito ai sensi del comma 2 dell'art. 6-*quater* anche nell'INAD, ferma restando la possibilità di inserire in tale ultimo indice un indirizzo diverso, a norma dell'art. 3-*bis* del CAD.

Resta tuttavia sullo sfondo una delicata domanda, non rilevante ai fini di queste note, riguardanti esclusivamente il domicilio digitale professionale del notaio: se il domicilio digitale iscritto in INAD è facoltativo, è possibile per il professionista ottenere la cancellazione, e più in generale inibire l'utilizzo del proprio domicilio digitale per scopi non professionali?

1.4. PEC e REM

Attualmente il domicilio digitale è costituito da una casella di posta elettronica certificata. La posta elettronica certificata è un servizio di recapito elettronico certificato destinato, in ottemperanza agli obblighi europei ed in particolare al fine di garantire l'interoperabilità tra i servizi in tutta l'Unione e dell'adozione di un sistema basato su migliori garanzie di sicurezza e sulla identificazione preventiva del titolare, ad essere sostituito dalla REM, che è un servizio di recapito elettronico certificato qualificato.

Secondo la normativa europea, ed in particolare secondo il Regolamento eIDAS (Reg. 910/2014) il servizio di recapito elettronico certificato (art. 43) ed il servizio di recapito elettronico certificato qualificato (art. 44), offrono diverse garanzie di affidabilità e sicurezza. Per i fini che qui interessano il servizio qualificato garantisce tra l'altro l'identificazione del destinatario.

Tale migrazione, prevista a breve, sarà probabilmente in parte indolore in quanto utilizzerà gli indirizzi di posta certificata esistenti, ma porterà altre conseguenze operative volte a garantire la sicurezza, come l'autenticazione a due fattori.

In particolare, per quanto riguarda il domicilio digitale dei notai, porterà ad una gestione necessariamente allo stesso tempo più responsabile e garantita.

II.

IL DOMICILIO DIGITALE NELLA VOLONTARIA GIURISDIZIONE: APPLICAZIONE DEL DOMICILIO DI PIATTAFORMA NELLA GIUSTIZIA CIVILE

di *Antonella Ciriello*

2.1. Il domicilio digitale nella volontaria giurisdizione: applicazione del domicilio di piattaforma nella giustizia civile

Il decreto-legge 24 febbraio 2023, n. 13, all'art. 36, prevede il deposito telematico nei procedimenti di volontaria giurisdizione su un apposito portale direttamente da parte delle persone fisiche che (in tali procedimenti) possono stare in giudizio personalmente.

La norma prevede testualmente che "*Quando si avvale del portale di cui al comma 1 per il deposito in modalità telematiche di atti processuali e documenti, la parte il cui indirizzo di posta elettronica certificata non risulta da pubblici elenchi può altresì manifestare la volontà di ricevere le comunicazioni e notificazioni relative al procedimento, ai fini e per gli effetti di cui all'articolo 16, comma 7, del decreto-legge 18 ottobre 2012, n. 179, convertito, con modificazioni, dalla legge 17 dicembre 2012, n. 221, tramite il portale stesso*".

È evidente, dunque, che la norma in esame, come evidenziato nelle pagine e nei capitoli che precedono, disciplini una forma di applicazione nella giustizia civile del "domicilio digitale di piattaforma", prevista in termini generali dal CAD e dalla normativa sul domicilio di piattaforma [1], e applicata, in questo modo, al processo (pur se — per il momento — nel settore non contenzioso della volontaria giurisdizione) per superare l'assenza

---

[1] Il d.l. 16 luglio 2020, n. 76 e successive modifiche che regola all'art. 26 la "Piattaforma per la notificazione digitale degli atti della pubblica amministrazione" e il relativo domicilio di piattaforma stabilendo al comma 5 le relative disposizioni, nonché il regolamento attuativo introdotto con decreto della Presidenza del Consiglio dei Ministri - Dipartimento Per La Trasformazione Digitale 8 febbraio 2022, n. 58 (in G.U., 6 giugno 2022, n. 130).

di un domicilio digitale generale (risultante da pubblici elenchi) o speciale (eletto per il singolo procedimento) (2).

Pur trattandosi di una modalità di deposito relativa alla sole materie contemplate nel settore in esame, è innegabile il valore innovativo della normativa, che apre al privato la possibilità concreta del deposito telematico diretto nel processo sfruttando una modalità compatibile con il solo possesso di strumenti di identificazione digitale diffusi tra i cittadini (SPID, CIE, CNS), per accedere ad una piattaforma informatica, al fine non solo di depositare atti, ma di riceverne.

Per dare concreta attuazione alla normativa, il Ministro della Giustizia ha emesso il 22 gennaio 2024 il previsto decreto ministeriale, recante le "Disposizioni in materia di deposito telematico di atti processuali e documenti nei procedimenti di volontaria giurisdizione".

Sono seguite, poi, le specifiche tecniche del direttore generale SIA, rese ai sensi dell'art. 34 del d.m. 21 febbraio 2011, n. 44, per regolare concretamente questa nuovissima modalità di deposito, pubblicate sul portale dei servizi telematici con provvedimento del DGSIA del 31 gennaio 2024, nel cui testo trovano spazio concetti nuovi e rilevanti ai fini dello studio del domicilio e dell'identità digitale nel processo.

In particolare, si legge tra le definizioni (oltre alla definizione di "depositante" riferita all'utente abilitato esterno privato, pure in generale già definito dalle regole tecniche del d.m. n. 44 del 2011 all'art. 1 lettera *m*), n. 3 del decreto ministeriale, non richiamato) (3), la definizione di "PEC di servizio" (art. 1 lett. *d*), intesa come l'indirizzo di posta elettronica certificata messo a disposizione dal Ministero ai fini degli adempimenti di cui al deposito in esame, nonché di "Portale, (art. 1 lett. *e*), come "portale dedicato gestito dal Ministero attraverso cui le persone fisiche, che stanno in giudizio personalmente nei procedimenti di volontaria giurisdizione, possono depositare gli atti processuali e i documenti per via telematica", ma anche come "luogo digitale in cui le persone fisiche ricevono le comunicazioni e notificazioni relative al procedimento", infine di "*Provider* di identità" (art. 1, lett. *f*), come "soggetto che rilascia e gestisce le identità digitali".

Il decreto ministeriale citato stabilisce (Articolo 2) che, in sede di prima applicazione, il deposito telematico di atti processuali e di documenti

(2) Per la individuazione delle forme di domicilio digitale regolate in generale dalla legge, si veda *supra*, capitolo 1, par. 1.3.

(3) Il d.m. n. 44 del 2011 è stato specificamente integrato inserendo, tra i soggetti abilitati esterni privati, accanto ai difensori delle parti private, agli avvocati iscritti negli elenchi speciali, agli esperti e agli ausiliari del giudice, anche "le persone fisiche che possono stare in giudizio personalmente" evidentemente in prospettiva immaginandosi una progressiva estensione della figura del deposito telematico personale del privato, ove previsto dalla normativa.

effettuato da persone fisiche "è ammesso esclusivamente per i seguenti procedimenti di volontaria giurisdizione: *a*) amministrazione di sostegno, disciplinata dall'articolo 473-*bis.*58 del Codice di procedura civile; *b*) nomina del curatore dell'eredità giacente, disciplinata dall'articolo 782 del codice di procedura civile; *c*) autorizzazione al compimento di atti di straordinaria amministrazione in favore di minori, disciplinata dall'articolo 320 e dall'articolo 374 del Codice civile; *d*) autorizzazione al rilascio di passaporto o di documento valido per l'espatrio per figli minori, disciplinata dall'articolo 3, lettera *a*), della legge 21 novembre 1967, n. 1185" presso (Articolo 3) i tribunali di Catania, Catanzaro, L'Aquila Marsala, Napoli Nord, Trento e Verona.

L'ampliamento a ulteriori procedimenti e uffici è rimesso ad un successivo decreto del Ministro della giustizia.

Quanto all'entrata in vigore, il decreto si applica ai procedimenti di volontaria giurisdizione introdotti con ricorso depositato telematicamente dalle persone fisiche che stanno in giudizio personalmente a decorrere dal 1° marzo 2024.

Il portale concretamente realizzato, si legge nelle specifiche tecniche del 31 gennaio, "è costituito da una infrastruttura digitale che ospita la piattaforma per accedere ai servizi digitali della giustizia, comunica con i Provider di identità e interagisce con i sistemi informativi automatizzati del Ministero (in particolare attraverso Portale dei Servizi Telematici, Posta Elettronica Certificata e Processo Civile Telematico) per il corretto invio delle comunicazioni da parte del cittadino e da componenti grafici (HTML/CSS), con cui si interfaccia il cittadino per l'utilizzo della piattaforma".

Interessante il successivo articolo 2 che spiega come, ai fini dell'invio all'ufficio giudiziario competente, "il Portale crea una busta telematica crittografata, per le cui specifiche si applicano le regole tecniche indicate nell'art. 14 delle Specifiche Tecniche. La busta, contenente i documenti firmati, viene inviata tramite PEC di servizio e conservata nel sistema documentale del Portale".

È, in altre parole, una procedura che consente alla persona fisica che sta in giudizio personalmente di avvalersi della piattaforma che provvederà a operare tramite quella PEC di cui è sprovvista (la PEC di servizio, messa a disposizione dalla piattaforma), accedendo all'indirizzo web che viene fornito nelle medesime specifiche tecniche ('https://smart.giustizia.it/to') (art. 1).

Alla persona fisica è consentito di sottoscrivere apposito modulo di richiesta disponibile sul Portale, per manifestare la volontà che le notifiche ed ogni altra comunicazione inerente al procedimento gli siano effettuate tramite il Portale.

È evidente, pertanto, che in assenza di manifestazione di volontà, il portale consentirà esclusivamente il deposito (tramite accertamento dell'identità con le descritte procedure di identificazione), senza assumere la qualità di domicilio digitale e le comunicazioni seguiranno le strade tradizionali analogiche.

Dagli atti del DGSIA, già in precedenza pubblicati su PST, si può apprendere che il portale consta di due aree: una prima, pubblica meramente informativa e l'altra, riservata, dispositiva, che consente agli utenti di presentare le domande e gestire i depositi integrativi tramite procedura guidata, monitorare lo stato di avanzamento dei procedimenti e consultare lo storico del fascicolo, segnalare e ricevere supporto in relazione a problemi tecnici sul funzionamento del portale.

Va evidenziato come la nuova modalità di deposito e domicilio digitale, frutto di approfonditi studi prodotti dalla Commissione Interministeriale per la giustizia nel sud (4) costituisca un passo significativo per favorire l'accesso dei cittadini alla giustizia civile in linea con la normativa europea più recente.

(4) Commissione Covelli - Commissione Interministeriale per la giustizia nel sud per elaborare proposte di interventi in materia di giustizia nell'area del meridione e isole, https://www.giustizia.it/cmsresources/cms/documents/commissione_COVELLI_relazione_finale_15gen2022_agg19gen2022.pdf

Sezione IV

IL DOMICILIO DIGITALE NELLA CRISI D'IMPRESA

I.

CODICE DELLA CRISI E DIGITALIZZAZIONE: UN PERCORSO QUASI COMPIUTO?

di *Lorenza Calcagno*

Sommario: 1.1. Digitizzazione e digitalizzazione: significato e riflessi nella disciplina della crisi d'impesa. — 1.2. Uno sguardo tra le disposizioni del Codice della crisi e dell'insolvenza. — 1.3. Verso il futuro.

1.1. Digitizzazione e digitalizzazione: significato e riflessi nella disciplina della crisi d'impresa

Appare interessante interrogarsi sul mancato approfondimento del d.lgs. 12 gennaio 2019, n. 14 — da ora c.c.i.i. — in una prospettiva di digitalizzazione di sistema. Risulta opportuno, da qui il titolo di questo piccolo contributo, richiamare la distinzione tra digitizzazione e digitalizzazione, al fine di comprendere se, all'interno del complesso normativo che raccoglie 391 articoli, le tante disposizioni che da un lato dispongono la digitalizzazione di documenti e procedure e dall'altra prevedono il collegamento a e tra sistemi digitalizzati, non possano indicare una strada verso una disciplina della crisi d'impresa che sappia essere non solo efficiente ma anche efficace in quanto capace di utilizzare appieno la moderna tecnologia. La distinzione nasce e si sviluppa nel mondo economico. Secondo (1) il glossario Gartner (2) per "digitizzazione (*digitization*) — precisato che il tema è amplissimo, in continuo sviluppo e quindi il richiamo non ha pretese di completezza — si intende il processo di trasformazione dalla forma analogica a quella digitale", noto anche come facilitazione digitale. In altre parole, la digitizzazione parte da un processo analogico e lo modifica in una forma digitale senza intervenire in alcun modo sulla natura del processo in sé. La conversione digitale interessa ampiamento il modo giudiziario e nell'ambito della disciplina della

(1) Il Glossario IT di Gartner è un dizionario online di termini e definizioni IT.

(2) Per le definizioni dell'*innovation management* vedi in Research-Technology Management, volume 61, 2018, MatyAnne Gobble, pagine 56-59.

crisi ne troviamo un importante esempio con riguardo al domicilio digitale, introdotto, come ricordato nel capitolo successivo, con la riforma del sistema fallimentare portata dal d.lgs. 9 gennaio 2006, n. 5, il quale ha previsto la possibilità di elezione di domicilio presso un indirizzo digitale.

La digitalizzazione riguarda non i dati ma i processi. La digitizzazione di oggetti e asset rende possibile, nel campo economico nel quale si sono sviluppati gli studi, ad aziende e industrie di svolgere la digitalizzazione. Ancora secondo il glossario Gartner, la "digitalizzazione è l'uso delle tecnologie digitali per cambiare un modello di business e fornire nuove opportunità di ricavi e di produzione del valore". È il processo di passaggio a un business digitale (3).

La giurisdizione non è certamente fare impresa, ma la questione sulla quale si vuole porre l'attenzione è se la digitalizzazione e l'informatizzazione non costituiscano solo trasformazione di documenti ma possano essere esaminati in termini di collegamenti tra sistemi digitalizzati e quindi possano costituire uno strumento di lavoro per una maggiore efficacia di azione. Si tratta di verificare se il collegamento fra sistemi digitali, i quali spesso sono caratterizzati da banche dati loro proprie, possa portare anche ad una trasformazione dei processi decisionali. La domanda contenuta nel titolo vuole porre la questione se, all'interno del d.lgs. 12 gennaio 2019, n. 14, possano individuarsi alcuni indici di digitalizzazione idonei a portare non solo ad una maggiore efficienza del sistema ma a costituire anche la base per un successivo sviluppo dei procedimenti decisori.

Proponendo alcuni spunti di lettura nella prospettiva qui offerta, pare rilevante la presenza di disposizioni quali l'art. 42 c.c.i.i. già nel corpo normativo del 2019 e mai modificato nonostante i numerosi interventi che hanno interessato l'originale tessuto normativo, iniziati con il d.lgs. 26 ottobre 2020, n. 147 — il primo correttivo —, fino al d.lgs. 17 giugno 2022, n. 83 con il quale è stata recepita la direttiva (UE) 2019/1023 del Parlamento europeo e del Consiglio, del 20 giugno 2019, nota come direttiva *insolvency*, — momento finale solo per quanto attiene l'entrata in vigore del codice della crisi intervenuta nel luglio 2022, successivamente ancora corretto — ed attualmente si è in attesa di un intervento di natura generale —. Norma assente nel precedente sistema, la disposizione prevede, sia nella procedura di liquidazione giudiziale

(3) Lo sviluppo della digitalizzazione è andato di pari passo con l'accelerazione e la commercializzazione di massa ed ha visto le nuove tecnologie digitali come il *cloud computing*, il *machine learning*, l'intelligenza artificiale, la *business intelligence* e l'Internet of Things. Le tecnologie digitali emergenti svolgono un ruolo fondamentale ai fini dell'avanzamento dell'automazione nella "quarta rivoluzione industriale", espressione coniata nel 2015 da Klaus Schwab, presidente esecutivo del World Economic Forum, e tema dell'edizione 2016 della riunione annuale del Forum stesso a Davos, in Svizzera.

sia in quella di concordato preventivo, la possibilità da parte della cancelleria di acquisire "*mediante collegamento telematico diretto alle banche dati dell'Agenzia delle entrate, dell'Istituto nazionale di previdenza sociale e del Registro delle imprese*" i dati e i documenti relativi al debitore individuati dall'articolo 367 c.c.i.i. con le modalità prescritte da quella norma. La trasmissione al tribunale concorsuale dei dati rilevanti avviene, secondo la disposizione in ultimo ricordata, direttamente mediante il sistema della c.d. "cooperazione applicativa" disciplinato dall'art. 76, d.lgs. 7 marzo 2005, n. 82 (Il Codice dell'amministrazione digitale). In difetto dei sistemi informatici necessari per assicurare i programmati scambi di documenti informatici tra le pubbliche amministrazioni, il comma 5 dell'art. 367 c.c.i.i. contempla il ricorso a convenzioni a titolo gratuito, stipulate tra gli enti indicati e il Ministero della giustizia. Il comma 2 dell'articolo 42 c.c.i.i. prevede, fino alla piena operatività del sistema contemplato dall'articolo 367 c.c.i.i., la raccolta di informazioni tramite richiesta inoltrata con posta elettronica certificata. Se pure la norma non ha ancora trovato pratica applicazione nei termini dello scambio informatico, deve ritenersi che la disciplina non si limiti a rendere meno oneroso per le parti la produzione documentale richiesta dall'articolo 39 c.c.i.i. (4), ma, realizzando la possibilità di conoscenza immediata di dati di natura economica fondamentali per conoscere lo stato dell'impresa, porti un ausilio alla celerità delle decisioni da assumere nell'immediatezza dell'apertura delle procedure. È questo il senso di una digitalizzazione che diviene trasformazione dei procedimenti, rendendoli più veloci e trasparenti.

1.2. Uno sguardo tra le disposizioni del Codice della crisi e dell'insolvenza

La materia oggetto del complesso normativo si presta particolarmente ad essere investita dal processo di digitalizzazione, sia con riguardo al reperimento dei dati rilevanti ai fini delle decisioni, sia per la necessaria certezza e trasparenza delle comunicazioni interne ed esterne ai procedimenti stessi. Il Codice della crisi contiene alcune norme che sottolineano l'importanza o, meglio, la centralità della digitalizzazione sia per quanto attiene le comunicazioni — artt. 2 lett. *s*), relativo alla definizione di comunicazione digitale e 10, intitolato comunicazioni telematiche, prima di tutto — sia per quanto riguarda gli atti dei procedimenti concorsuali. Con riferimento a quest'ultimo aspetto sono molte e rilevanti le previsioni, si ricordano qui per importanza gli articoli: 39 — con la previsione del deposito anche in formato digitale delle relazioni di natura economica previste e l'indicazione del domicilio

(4) Così R. Giordano, *Codice della crisi d'impresa e dell'insolvenza*, Milano 2022, 193.

digitale dei creditori —; 40 comma 6, afferente le notificazioni e comma 7 dedicato alla previsione dell'area web; 41 u.c. e il già ricordato 42; 126 contenente la disciplina del fascicolo informatico della procedura, nel quale devono essere contenuti tutti gli atti, i provvedimenti e i ricorsi attinenti al procedimento, esclusi quelli che, per ragioni di riservatezza, debbono essere custoditi nel fascicolo riservato; 199 sull'attribuzione del domicilio digitale al curatore ad opera dell'ufficio, norma prorogata per problemi operativi con d.l. 24 febbraio 2023 n. 13, convertito con l. 21 aprile 2023, n. 41; 359 e ss. —. La direttiva (UE) 2019/1023 del Parlamento europeo e del Consiglio, del 20 giugno 2019 sulla ristrutturazione ed insolvenza già richiamata contiene alcune specifiche disposizioni sulla digitalizzazione. In particolare l'articolo 3, dedicato all'allerta precoce e all'accesso alle informazioni, dopo aver previsto la necessità di un accesso "*chiaro e trasparente*" agli strumenti di allerta, indica l'opportunità che gli Stati membri si avvalgano di tecnologie informatiche aggiornate per le notifiche e per le comunicazioni online ed al comma 4 è indicata la necessità che gli Stati provvedano a rendere disponibili le informazioni on line evidenziandone la necessaria facilità di consultazione soprattutto per le PMI; il considerando 22 è strettamente collegato alle specifiche della disposizione; il successivo articolo 28 prevede che almeno alcuni atti, oggetto di elenco specifico, interni alle procedure possano essere realizzati tramite mezzi di comunicazioni elettroniche (5).

Per quanto riguarda il sistema dell'allerta, come noto, il legislatore ha interamente sostituito il Titolo II, d.lgs. 12 gennaio 2019, n. 14 — in precedenza intitolato "*procedure di allerta e di composizione assistita della crisi*", già modificato con il d.lgs. 26 ottobre 2020, n. 147 — inserendovi l'istituto della composizione negoziata, introdotto nel nostro ordinamento con il d.l. 24 agosto 2021, n. 118 convertito con modificazioni in l. 21 ottobre 2021, n. 147 e così abrogando la procedura della composizione assistita e la disciplina dell'allerta interna ed esterna. Anche in adempimento delle indicazioni eurounitarie, la procedura di composizione negoziata è strutturata all'interno di un sistema digitalizzato. La domanda di nomina dell'esperto ed i successivi passaggi, nonché la fase precedente, sono procedimentalizzati

(5) Art. 28 Direttiva 1023/2019 "Uso di mezzi di comunicazione elettronici": Gli Stati membri provvedono affinché, nelle procedure di ristrutturazione, insolvenza ed esdebitazione, le parti coinvolte nella procedura, i professionisti e le autorità giudiziarie o amministrative possano eseguire attraverso mezzi di comunicazione elettronica, anche nelle situazioni transfrontaliere, almeno le azioni seguenti:

a) insinuazione al passivo;
b) presentazione di piani di ristrutturazione o di rimborso;
c) notifiche ai creditori;
d) presentazione di contestazioni e impugnazioni.

attraverso una piattaforma dedicata, di utilizzo ragionato di dati disponibili, con la previsione di strumenti informatici posti a disposizione di ogni imprenditore e finalizzati a rendere possibile l'emersione della presenza e dei contorni dello stato di difficoltà dell'attività economica in epoca precoce — basti pensare alla lista di controllo particolareggiata ed al test pratico per la verifica della ragionevole perseguibilità del risanamento —. L'art. 13 istituisce la piattaforma telematica nazionale attraverso la quale viene gestita la procedura e l'art. 14, dettando unitamente al successivo 15 una disposizione di assoluta novità, prevede la interoperabilità tra la piattaforma telematica nazionale per la composizione negoziata e le banche dati dell'Agenzia delle Entrate, degli istituti INPS e INAIL, dell'agente della riscossione e della Centrale dei rischi della Banca d'Italia nonché la possibilità, contenuta nell'articolo 15, per i creditori di intervenire sulla piattaforma unica nazionale. Queste disposizioni sono state modificate con il d.lgs. 17 giugno 2022, n. 83, ma erano state introdotte dal d.l. 6 novembre 2021, n. 152, convertito in l. 29 dicembre 2021, n. 233, con gli artt. 30-*ter* e 30-*quater*. Anche la segnalazione di allerta "esterna" contenuta nell'art. 30-*sexies* presente nella medesima normativa prevede la trasmissione dei dati all'imprenditore o all'organo di controllo dell'ente tramite posta elettronica certificata, pur facendo salvezza della raccomandata con avviso di ricevimento inviata all'indirizzo risultante all'anagrafe tributaria (6).

Nel quadro delineato, volto a sottolineare l'importanza di un sistema che crea collegamenti informatici tra banche dati di rilevanza centrale nella gestione economica dell'impresa, l'articolo 14 assume grande importanza in quanto permette all'esperto nominato di ottenere un quadro della situazione economico finanziaria definita nei suoi contorni più importanti, attraverso i termini debitori emergenti dalle anagrafi dei creditori pubblici qualificati e dalla centrale rischi della Banca d'Italia e, tramite l'intervento dei creditori permesso dal successivo articolo 15, anche della veridicità della situazione dichiarata dal debitore. In un sistema così strutturato ed operativo, i processi di composizione negoziata possono realizzarsi. Certamente sarà fondamentale anche la struttura organizzativa interna delle imprese, voluta dalla nuova regolamentazione introdotta con la modifica dell'art. 2086 c.c. e 3 c.c.i.i. Per quanto riguarda gli strumenti di regolazione della crisi e dell'insolvenza, l'articolo 5-*bis* c.c.i.i., in adempimento della direttiva *insolvency,* ha previsto la pubblicazione sul sito del Ministero della giustizia e del Ministero dello sviluppo economico non solo di notizie sulla disciplina legislativa dei diversi

(6) L'articolo 30-*sexies* è stato successivamente modificato, non sul punto qui in oggetto, con l'introduzione nel codice dell'articolo 25-*novies* successivamente modificato dall'art. 37-*bis*, d.l. 21 giugno 2022, n. 73, convertito in l. 4 agosto 2022, n. 122.

strumenti di regolazione della crisi, ma anche di una lista di controllo particolareggiata contente indicazioni operative per la redazione dei piani di risanamento. Inoltre, anche con riferimento agli strumenti di regolazione della crisi e dell'insolvenza, della liquidazione giudiziale e del concordato preventivo, sono state richiamate disposizioni che, tramite la generalizzazione delle comunicazioni elettroniche, dei collegamenti a sistemi organizzati di banche dati ed alla creazione di nuovi strutture informatiche — il già ricordato spazio web dell'articolo 40, comma 7 c.c.i.i. — possono permettere una maggior trasparenza ed efficienza delle procedure, attesa l'esigenza di ridurre i tempi di tutti i procedimenti rendendoli più efficaci rispetto alla preservazione del patrimonio impresa.

1.3. Verso il futuro

Può porsi a questo punto, all'esito di una analisi necessariamente superficiale, se si possa andare oltre le considerazioni fin quei svolte, limitate ad un possibile mutamento interno dei procedimenti derivante dall'esistenza di un complesso che abbiamo descritto come "*digitalizzato*" per dare atto della presenza di disposizioni che utilizzano la digitalizzazione a livelli diversi. L'analisi può spostarsi sulla centralità della natura economica dei dati posti a fondamento della procedimentalizzazione delle decisioni che caratterizzano gli strumenti disciplinati dal c.c.i.i., sul possibile utilizzo delle banche dati che quegli elementi in parte già custodiscono, in una visione in cui la conoscenza degli elementi rilevanti per la decisione sono in parte, a volte in larga parte, già estraibili da sistemi esistenti e posti a fondamento di decisioni alle quali si perviene attraverso successive analisi ed elaborazioni.

Possiamo domandarci, attese le premesse sopra svolte, se la crisi d'impresa possa costituire un ambito di elezione per lo sviluppo di strumenti di intelligenza artificiale o, meglio, di algoritmi "istruiti", anche solo in termini di ausilio all'analisi ed alla predisposizione di basi conoscitive relative all'oggetto specifico di indagine proprio dei diversi strumenti di regolazione della crisi o delle procedure di liquidazione. Su questo terreno stanno lavorando altri stati dell'UE (7). Il tema viene qui naturalmente solo suggerito in quanto la prospettiva è estremamente rilevante e comporta problematiche di grande complessità (8).

---

(7) In Spagna esistono dei progetti a livello iniziale per l'utilizzo di strumenti di intelligenza artificiale nella gestione di procedure di insolvenza dei consumatori.

(8) Questo momento storico è caratterizzato da una intensa discussione sull'utilizzo degli strumenti di A.I. nell'ambito della giurisdizione e sull'impatto sulla tutela dei diritti fondamentali. Lo scorso 9 dicembre le istituzioni europee hanno raggiunto l'accordo sull'AI Act, all'esito di un procedimento iniziato con una proposta dalla Commissione europea nell'aprile 2021.

II.
IL DOMICILIO DIGITALE NEL CODICE DELLA CRISI

di *Giuseppe Fichera*

Sommario: 2.1. Inquadramento generale. — 2.2. Il domicilio nella legge fallimentare. — 2.2.1. L'introduzione del domicilio digitale nelle procedure concorsuali. — 2.3. Il domicilio digitale nel Codice della crisi. — 2.3.1. Il domicilio digitale dei creditori. — 2.3.2. Il domicilio digitale della procedura. — 2.3.3. Il domicilio digitale del debitore.

2.1. Inquadramento generale

L'art. 1, comma 1, lett. *n-ter*), d.lgs. 7 marzo 2005, n. 82, il Codice dell'amministrazione digitale (in prosieguo *breviter* il CAD) (1), definisce "domicilio digitale" l'indirizzo elettronico eletto presso un servizio di posta elettronica certificata (PEC) attualmente ancora disciplinato dal d.p.r. 11 febbraio 2005, n. 68 (2), oppure il servizio elettronico di recapito certificato qualificato (SERCQ), come definito dal regolamento (UE) 23 luglio 2014, n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, (il c.d. Regolamento eIDAS).

Dunque, nell'ordinamento italiano il domicilio virtuale, non ancorato ad un luogo fisico bensì soltanto elettronico, può corrispondere alla tradizionale PEC, ovvero al SERCQ, ancorché quest'ultimo servizio non risulti ancora concretamente attuato nel nostro paese (3).

Il CAD, poi, si occupa di domicilio digitale in diverse sue disposizioni.

---

(1) La norma è stata inserita dall'art. 1, comma 1, lett. *c*), del d.lgs. 26 agosto 2016, n. 179, e, successivamente, così sostituita dall'art. 1, comma 1, lett. *a*), n. 2), del d.lgs. 13 dicembre 2017, n. 217.

(2) Attualmente un gruppo di lavoro coordinato da AgID, costituito a settembre 2019, ha rilasciato il documento "REM SERVICES — Criteri di adozione degli standard ETSI — Policy IT", contenente la proposta di regole tecniche per i servizi di recapito certificato qualificato eIDAS.

(3) Si tratta del Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'art. 27, legge 16 gennaio 2003, n. 3.

Ai nostri fini rilevano principalmente le norme che individuano i pubblici elenchi dove risultano iscritti i domicili digitali di imprese, professionisti, pubbliche amministrazioni e gestori di pubblici servizi.

Va ricordato, anzitutto, che ai sensi dell'art. 3-*bis*, comma 1, del CAD, le pubbliche amministrazioni e i gestori di pubblici servizi, come pure i professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese, hanno l'obbligo di dotarsi di un domicilio digitale iscritto in uno dei due pubblici elenchi previsti dall'art. 6-*bis* e dall'art. 6-*ter* del CAD.

Invero, già l'art. 16, comma 6, d.l. 29 novembre 2008, n. 185, convertito con modificazioni, dalla legge 28 gennaio 2009, n. 2, più volte modificato — da ultimo con il d.l. 16 luglio 2020, n. 76 convertito con modificazioni dalla legge 11 settembre 2020, n. 120 —, stabilisce che tutte le imprese costituite in forma societaria sono tenute a comunicare il proprio domicilio digitale al registro delle imprese.

Stesso obbligo è previsto per le imprese individuali, in forza dell'art. 5, comma 1, del d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221.

A sua volta, l'art. 16, comma 7, del d.l. n. 185 del 2008, sancisce l'obbligo di indicare il domicilio digitale per i professionisti iscritti in albi ed elenchi istituiti con legge dello Stato; in questo caso l'indirizzo PEC o il SERCQ va comunicato ai rispettivi ordini o collegi.

Tutti i domicili digitali obbligatori per imprese e professionisti, come anticipato, confluiscono oggi in un pubblico elenco denominato "Indice nazionale degli indirizzi di posta elettronica certificata delle imprese e dei professionisti" (INI-PEC), codificato dall'art. 6-*bis* del CAD.

Quanto alle pubbliche amministrazioni e ai gestori di pubblici servizi, l'obbligo di iscrizione riguarda il pubblico elenco denominato "Indice dei domicili digitali della pubblica amministrazione e dei gestori di pubblici servizi" (IPA), disciplinato dall'art. 6-*ter* del CAD.

Infine, va ricordato che l'art. 6-*quater* del CAD prevede l'istituzione di un ulteriore pubblico elenco, denominato "Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese" (INAD) (4), nel quale sono inseriti i domicili volontariamente eletti, ai sensi dell'art. 3-*bis*, comma 1-*bis* del CAD, da tutti i soggetti che non hanno alcun obbligo di legge di munirsene.

(4) L'INAD è ufficialmente accessibile, dal 6 luglio 2023, su https://domiciliodigitale.gov.it/dgit/home/public/#!/home.

2.2. Il domicilio nella legge fallimentare

La legge fallimentare del '42 in origine, com'è ovvio, non conteneva alcuna disposizione sul c.d. "domicilio digitale"; in un'epoca contrassegnata esclusivamente dalla trasmissione in forma analogica degli atti processuali, l'unico concetto rilevante per la normativa allora vigente era quello del c.d. "domicilio fisico", del fallito come pure dei creditori e di tutti i soggetti interessati alla procedura concorsuale.

Del resto, in origine l'art. 15 l. fall. prevedeva solo una mera facoltà del tribunale di ordinare la convocazione del debitore prima di dichiararlo fallito (5) e l'art. 49 l. fall. imponeva al fallito di « *non allontanarsi* » dalla sua residenza senza permesso del giudice delegato e di presentarsi al predetto, al curatore o al comitato dei creditori quando fosse stato convocato: insomma, può ben dirsi che *sub julio* non era necessario eleggere domicilio di sorta perché bisognava stare a disposizione degli organi della procedura.

Il fallito non poi era destinatario di particolari oneri informativi, essendo codificato soltanto l'obbligo di comunicargli, a cura del cancelliere, l'estratto della sentenza dichiarativa di fallimento e, su iniziativa del curatore, l'avvenuto deposito del rendiconto finale, *ex* art. 116 l. fall. Nessuna altra comunicazione era prescritta dalla legge.

Quanto ai creditori e agli altri interessati alla procedura, ricordiamo che il curatore era tenuto a trasmettere mediante lettera raccomandata gli avvisi contenenti l'indicazione dell'adunanza fissata per la formazione dello stato passivo.

Il creditore, a sua volta, ai sensi dell'art. 93, comma secondo, l. fall. doveva sempre eleggere domicilio nel comune dove aveva sede il tribunale fallimentare, altrimenti tutte le successive notificazioni sarebbero state eseguite in cancelleria, secondo il modello, già previsto per i difensori nel processo civile, dettato dall'art. 82, r.d. 22 gennaio 1934, n. 37 (6).

In sostanza, la mancata elezione di domicilio nel comune sede del tribunale fallimentare, comportava la facoltà di effettuare comunicazioni e notificazioni direttamente in cancelleria, così esonerando gli organi della procedura dalle normali incombenze di trasmissione dei provvedimenti adottati dal giudice delegato, ovvero dal tribunale fallimentare.

---

(5) Solo con Corte cost. 16 luglio 1970, n. 141, venne dichiarata l'illegittimità costituzionale dell'art. 15 l. fall., nella parte in cui non prevedeva l'obbligo di sentire il debitore da parte del tribunale fallimentare prima di dichiararne il fallimento.

(6) Ai sensi della norma citata, ancora vigente, i difensori che esercitano il proprio ufficio in un giudizio che si svolge fuori della circoscrizione del tribunale al quale appartiene il consiglio dell'ordine al quale sono iscritti, devono, all'atto della costituzione nel giudizio stesso, eleggere domicilio nel luogo dove ha sede l'autorità giudiziaria presso la quale il giudizio è in corso.

2.2.1. *L'introduzione del domicilio digitale nelle procedure concorsuali*

È con la riforma organica delle procedure concorsuali, contenuta nel d.lgs. 9 gennaio 2006, n. 5, che, per la prima volta nell'ordinamento concorsuale italiano, viene introdotta una disciplina che prevede la facoltà per le parti interessate di eleggere un domicilio presso un indirizzo virtuale diverso da quello fisico.

Così, nel procedimento c.d. prefallimentare, il secondo comma dell'art. 6 l. fall. assicurava in maniera generica al creditore istante la possibilità di avvalersi di mezzi telematici al fine di ricevere nel corso del giudizio le comunicazioni e gli avvisi previsti dalla legge, attraverso l'indicazione nel ricorso del recapito di telefax o dell'indirizzo di posta elettronica presso cui intendeva ricevere dette comunicazioni.

L'art. 92 l. fall. riformato, poi, stabiliva che la comunicazione da parte del curatore in ordine alla data fissata per l'esame dello stato passivo, potesse essere effettuata ricorrendo senz'altro all'indirizzo telefax o di posta elettronica del destinatario, senza precisare peraltro quale fosse il sistema di posta elettronica utilizzabile.

L'art. 93, comma primo, n. 5), l. fall. prevedeva seccamente che il creditore che presentava la domanda di insinuazione al passivo dovesse indicare il proprio numero di telefax o l'indirizzo di posta elettronica, oppure, in alternativa, eleggere il tradizionale domicilio fisico « *in un comune del circondario* » dove aveva sede il tribunale.

Il medesimo creditore, ancora, aveva la facoltà di chiedere che tutte le comunicazioni successive fossero effettuate tramite telefax ovvero per posta elettronica, avendo altresì l'onere di segnalare eventuali cambiamenti del numero dell'uno o dell'indirizzo dell'altra.

Come nel caso di mancata elezione del domicilio fisico, la mancata indicazione del numero di telefax o dell'indirizzo di posta elettronica, determinava l'effetto che le comunicazioni, ma solo quelle successive al deposito dello stato passivo, sarebbero state effettuate mediante deposito in cancelleria.

Inoltre, l'art. 26 l. fall. novellato prevedeva la facoltà in capo al curatore di comunicare il provvedimento reso dal giudice delegato, oltre che con lo strumento della lettera raccomandata con avviso di ricevimento, mediante telefax o posta elettronica, purché in forma tale da garantire l'avvenuta ricezione del documento trasmesso secondo la disciplina contenuta nel testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (7).

(7) Si tratta del d.p.r. 28 dicembre 2000, n. 445, il cui art. 14, concernente la trasmissione del documento informatico, risulta peraltro successivamente abrogato dal CAD.

Si trattava, come ogniuno vede, di una normativa ancora embrionale e di fatto sostanzialmente disapplicata negli uffici giudiziari, per un verso, difettando una precisa regolamentazione — anche di fonte secondaria — tesa ad assicurare la prova dell'avvenuta ricezione del telefax e, per altro verso, non avendo il legislatore neppure sentito il bisogno di chiarire se la posta elettronica utilizzabile fosse soltanto quella disciplinata dal d.p.r. 28 aprile 2005, n. 68, *id est* la posta elettronica certificata (PEC), l'unica in grado di fornire la prova della consegna del documento oggetto di trasmissione in via telematica.

La vera svolta in tema di domicilio digitale si registra nel 2012.

Con l'art. 17 del cennato d.l. 18 ottobre 2012, n. 179, convertito con modificazioni dalla legge n. 221 del 2012, novellando l'art. 15 l. fall. venne infatti stabilito che il ricorso per la dichiarazione di fallimento doveva essere notificato, a cura della cancelleria, all'indirizzo PEC del debitore risultante dal registro delle imprese, oppure dall'INI-PEC; solo in caso di impossibilità di eseguire la notifica a mezzo PEC, il ricorso poteva essere notificato personalmente, tramite ufficiale giudiziario, presso la sede dell'impresa.

La medesima norma, poi, introdusse l'art. 31-*bis* l. fall., a tenore del quale le comunicazioni ai creditori e ai titolari di diritti sui beni che la legge o il giudice delegato pone a carico del curatore potevano essere effettuate all'indirizzo PEC da loro indicato.

Quando risultava omessa l'indicazione dell'indirizzo PEC, nonché nei casi di mancata consegna del messaggio di posta elettronica certificata per cause imputabili al destinatario, tutte le comunicazioni erano eseguite esclusivamente mediante deposito in cancelleria.

Inoltre, modificando l'art. 92 l. fall., sempre il d.l. n. 179 del 2012 impose al curatore di munirsi di un indirizzo PEC da comunicare a tutti i creditori al momento dell'invio dell'avviso contenente la data fissata per l'esame dello stato passivo.

I creditori, poi, per insinuarsi allo stato passivo avrebbero dovuto trasmettere la domanda telematicamente esclusivamente all'indirizzo PEC in precedenza comunicato dal curatore.

È utile ricordare infine come, solo dopo la cennata riforma del 2012, il legislatore introdusse nel sistema processuale italiano la prima disposizione che parla espressamente di "domicilio digitale".

L'art. 90 del d.l. 24 giugno 2014, n. 90, convertito con modificazioni dalla legge 11 agosto 2014, n. 114, introdusse infatti l'art. 16-*sexies* del d.l. n. 179 del 2012, intitolato nella rubrica "domicilio digitale", che prevede la possibilità di notificare gli atti presso la cancelleria dell'ufficio giudiziario, soltanto nei casi in cui non sia possibile, per causa imputabile al destinatario, la notificazione presso l'indirizzo PEC risultante da INI-PEC, nonché dal

registro generale degli indirizzi elettronici (il ReGIndE), gestito dal Ministero della giustizia.

2.3. Il domicilio digitale nel Codice della crisi

L'art. 2, comma 1, della legge delega 19 ottobre 2017, n. 155 stabilì, tra i criteri direttivi generali imposti al legislatore delegato all'adozione della nuova disciplina sulle procedure concorsuali, alla lett. *i*), un'unica disposizione concernente il domicilio digitale.

Si tratta della previsione secondo cui la notificazione nei confronti del debitore, che sia un professionista o un imprenditore, degli atti delle procedure concorsuali e, in particolare, dell'atto che dà inizio al procedimento di accertamento dello stato di crisi, debba avere luogo obbligatoriamente tramite SERCQ, oppure all'indirizzo PEC del debitore, risultante dal registro delle imprese o da INI-PEC.

Con la volontà di utilizzare il domicilio digitale con un respiro assai più ampio rispetto alla cennata direttiva contenuta nella legge delega, il d.lgs. 12 gennaio 2019, n. 14 (il c.c.i.i.) nell'ambito del suo Titolo I dedicato alle "disposizioni generali", ha disposto con l'art. 10, intitolato "comunicazioni telematiche", una disciplina unitaria sul domicilio digitale per tutte le procedure concorsuali (8).

La regola generale, anzitutto, fissata dal comma 1 dell'art. 10, è quella a tenore della quale « *gli organi di gestione, controllo o assistenza* » delle procedure disciplinate dal Codice, devono sempre effettuare le comunicazioni previste dalla legge utilizzando modalità telematiche per la trasmissione degli atti ad un domicilio digitale.

Gli organi di gestione, controllo o assistenza di cui discute il Codice sono, in primo luogo, i curatori nella liquidazione giudiziale, i commissari giudiziali nel concordato preventivo, i liquidatori e gli organismi di composizioni della crisi (OCC) nella procedura di ristrutturazione dei debiti del consumatore, nel concordato minore e nella liquidazione controllata, i commissari liquidatori nella liquidazione coatta amministrativa; se riteniamo che la composizioni negoziata della crisi è una procedura disciplinata dal Codice, poi, vi rientra anche l'esperto nominato dalla apposita commissione istituita presso la competente camera di commercio.

Ciò significa che tutte le comunicazioni curate dai soggetti surrichiamati andranno eseguite tramite PEC, ovvero tramite SERCQ, secondo quanto stabilisce espressamente — ma ormai inutilmente considerata la cennata

(8) Sull'art. 10 c.c.i.i. vedi G. ROMANO, *sub* art. 10, in (a cura di) F. SANTANGELI, *Il codice della crisi d'impresa e dell'insolvenza*, Milano, 2023, 68 ss.

definizione di domicilio digitale contenuta nell'art. 1 del CAD — il comma 5 dell'art. 10 c.c.i.i.

Inoltre, i messaggi invitati e quelli ricevuti devono essere conservati dagli organi della procedura per tutta la sua durata e per i due anni successivi alla relativa chiusura, come prescritto dall'art. 10, comma 4, c.c.i.i. in continuità con l'abrogato art. 31-*bis* l. fall.

Ora, la norma in esame introduce rispetto alla pregressa disciplina una distinzione fondamentale, a seconda che il destinatario della comunicazione telematica sia un professionista o una impresa obbligata per legge a possedere un domicilio digitale, ovvero si tratti di un soggetto, persona fisica o giuridica, che non abbia siffatto obbligo.

Infatti, per le società, le imprese individuali e i professionisti iscritti nell'INI-PEC di cui all'art. 6-*bis* del CAD, tutte le comunicazioni andranno effettuate sempre presso il domicilio digitale che risulta dal detto elenco pubblico.

Nel caso in cui i medesimi soggetti che hanno l'obbligo di munirsi di un domicilio digitale, non abbiano provveduto ad istituirlo ovvero a comunicarlo all'INI-PEC, tutte le comunicazioni da parte degli organi della procedura concorsuale, ai sensi dell'art. 10, comma 3, c.c.i.i. saranno eseguite esclusivamente mediante deposito in cancelleria dell'atto da comunicare.

Uguale sanzione trova applicazione nel caso in cui il sistema informatico abbia restituito la ricevuta di mancata consegna del messaggio elettronico « *per cause imputabili al destinatario* ».

Ora, la descritta disciplina suscita subito qualche riserva nell'interprete.

Se invero appare certamente condivisibile la previsione della generalizzata comunicazione di tutti gli atti per via telematica ai soggetti obbligati a munirsi di un domicilio digitale, non è comprensibile la ragione che ha spinto il legislatore ad escludere siffatto obbligo nel caso di soggetti che siano iscritti comunque in altri pubblici elenchi previsti dalla legge, quali il cennato Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA), previsto dall'art. 6-*ter* del CAD, ovvero l'Indice nazionale dei domicili digitali (INAD), disciplinato dall'art. 6-*quater* del CAD.

Come per INI-PEC, invero, anche per IPA si tratta di un pubblico elenco in cui le pubbliche amministrazioni e i gestori di pubblici servizi devono iscriversi obbligatoriamente, mentre per l'INAD, una volta effettuata la scelta di iscriversi, volontariamente, non si vede perché il cittadino debba subire un trattamento diverso rispetto alle imprese e ai professionisti.

In maniera radicalmente innovativa rispetto alla pregressa disciplina, il comma 2 dell'art. 10 c.c.i.i. si occupa, poi, di tutti i soggetti che, invece, non hanno un obbligo per legge di munirsi di un domicilio digitale.

In particolare, per i creditori e ai titolari di diritti sui beni che non siano professionisti o imprese, per i soggetti che hanno sede o che risiedono

all'estero, per il debitore oppure il legale rappresentante della società o ente che siano stati sottoposti a una delle procedure concorsuale previste dal Codice, è stabilito che il curatore, il commissario, il liquidatore o l'OCC provveda ad assegnare un domicilio digitale, comunicando all'interessato il relativo indirizzo.

Le spese di attivazione del domicilio digitale sono a carico della massa, come prescrive il comma 6, dell'art. 10 c.c.i.i.

Quindi, anche i soggetti che non hanno oggi alcun obbligo di munirsi di domicilio digitale, saranno dotati di un indirizzo PEC ovvero di un indirizzo SERCQ, che sarà utilizzabile esclusivamente per le comunicazioni della procedura e che, del resto, non verrà inserito in alcun pubblico elenco previsto dal CAD.

Se poi, per cause imputabili al destinatario, nonostante l'assegnazione del domicilio digitale, viene generata la ricevuta di mancata consegna, si procederà anche in questi casi al deposito dell'atto da comunicare nella cancelleria del tribunale concorsuale.

2.3.1. *Il domicilio digitale dei creditori*

La disciplina dettata dall'art. 10 c.c.i.i. sul domicilio digitale *ex officio*, come sopra descritta, di certo assai innovativa, appare tuttavia non perfettamente allineata con le altre disposizioni del Codice dettate in tema di domicilio digitale dei creditori, che riproducono in grande misura le disposizioni dell'abrogata legge fallimentare.

Invero, l'art. 200 c.c.i.i., in tema di formazione dello stato passivo, riproducendo il regime previgente, dispone ancora oggi che il curatore, nel comunicare ai creditori la data e l'ora fissata per l'esame dello stato passivo, debba — tra le altre incombenze — pure avvertire il creditore della sussistenza dell'onere previsto dall'art. 201, comma 3, lett. *e*), c.c.i.i., cioè di indicare un indirizzo PEC, al quale ricevere tutte le comunicazioni relative alla procedura, le cui variazioni è onere comunicare al curatore medesimo, nonché delle conseguenze di cui all'art. 10, comma 3, c.c.i.i.

Stesso discorso si palesa nella liquidazione controllata, dove l'art. 273, comma 1, c.c.i.i. impone al creditore di indicare il proprio indirizzo PEC nella domanda di insinuazione al passivo, prevedendo in difetto che tutte le comunicazioni successive siano effettuate mediante deposito in cancelleria.

È singolare che, in entrambi i casi sopra, descritti il legislatore del '19 abbia dimenticato di ricordare che il creditore ha sempre diritto di comunicare, in alternativa all'indirizzo PEC, un indirizzo di SERCQ.

Quanto al concordato preventivo, l'art. 104, comma 2, c.c.i.i. dispone che il commissario giudiziale provvede a comunicare al creditore, tra l'altro,

un avviso contenente il suo indirizzo PEC, con l'invito ad indicare un indirizzo PEC, oppure un indirizzo SERCQ, le cui variazioni è onere comunicare al commissario.

Nello stesso avviso è contenuto l'avvertimento circa le conseguenze derivanti dalla mancata elezione del domicilio digitale (9); in particolare, se il creditore nel termine di quindici giorni dal ricevimento dell'avviso, non comunica al commissario giudiziale il proprio indirizzo PEC, tutte le comunicazioni successive saranno eseguite esclusivamente mediante deposito in cancelleria.

Nel concordato minore, ancora, l'art. 78, comma 4, c.c.i.i. stabilisce che il creditore nella comunicazione contenente la dichiarazione di adesione o non adesione alla proposta di concordato, deve indicare un indirizzo di PEC o un SERCQ, a cui ricevere tutte le comunicazioni. In mancanza di una siffatta comunicazione, i provvedimenti sono comunicati mediante deposito in cancelleria.

Dunque, il Codice, da un lato, in via generale in forza del ridetto art. 10 c.c.i.i., impone al curatore, al liquidatore, al commissario giudiziale e all'OCC di assegnare d'ufficio un indirizzo PEC o un SERCQ ai soggetti interessati alla procedura (compresi all'evidenza i creditori) che non ne siano obbligatoriamente muniti e, dall'altro, continua a far carico a tutti i creditori — indistintamente — di comunicare al curatore un indirizzo PEC (e nel solo concordato in alternativa un SERCQ) al quale intendono ricevere le comunicazioni inerenti alla procedura, pena la sanzione del deposito dell'atto in cancelleria.

E ciò senza neppure considerare che il comma 1 dell'art. 10 c.c.i.i. prevede che tutte le comunicazioni alle imprese e ai professionisti, cioè a coloro che risultano obbligatoriamente iscritti ad INI-PEC, siano effettuate, senza eccezione alcuna, all'indirizzo risultante dal detto elenco, mentre gli artt. 78, comma 4, 104, comma 2, 201, comma 3, lett. *e*), e 273, comma 1, c.c.i.i. lasciano parimenti libero il creditore istante, che sia impresa o professionista, nel redigere la domanda di insinuazione al passivo o la dichiarazione da trasmettere al commissario o all'OCC, di indicare una PEC o un SERCQ diversi da quella risultante da INI-PEC.

---

(9) Il testo della norma in commento parla di un « *avvertimento di cui all'articolo 200, comma 1, lettera* c) »; ma si tratta all'evidenza di un refuso, non rinvenendosi alcuna lettera *c)* nell'art. 200 c.c.i.i. Più verosimilmente il rinvio è da intendersi all'art. 201, comma 3, lett. *e*), c.c.i.i.

2.3.2. *Il domicilio digitale della procedura*

Una significativa innovazione contenuta nel Codice della crisi, riguarda l'assegnazione *ex officio* di un domicilio digitale alla procedura di liquidazione giudiziale, una volta dichiarata la sua apertura.

È noto che con l'art. 17, d.l. n. 179 del 2012, venne introdotto, per la prima volta nell'ordinamento, l'obbligo del curatore fallimentare di munirsi di un indirizzo di posta elettronica certificata relativo alla procedura fallimentare.

Prima dell'entrata in vigore del Codice, il curatore provvedeva quindi ad acquistare presso un gestore privato dei servizi di posta elettronica certificata un domicilio digitale della procedura, che comunicava poi a creditori al momento della trasmissione dell'avviso relativo alla formazione dello stato passivo.

L'art. 199, comma 1, c.c.i.i., invece, prevede oggi che il domicilio digitale della procedura sia assegnato d'ufficio dal cancelliere al momento dell'apertura della liquidazione giudiziale.

Una tale disposizione, peraltro, si è subito mostrata foriera di complicazioni, ponendo alla cancelleria l'onere di acquistare presso i gestori privati del servizio di posta elettronica certificata, per conto della procedura, un domicilio digitale che ovviamente rimarrà nella titolarità del Ministero della giustizia, cioè di colui che ha effettuato l'acquisto.

Inoltre, in maniera certo assai singolare, la disposizione sul domicilio digitale ministeriale, non si ritrova nell'ambito di altre procedure concorsuali, quali il concordato preventivo, il concordato minore e la liquidazione controllata, dove evidentemente gli organi della procedura dovranno munirsi di un indirizzo PEC dedicato, a proprie spese e salvo rimborso attingendo ai fondi della massa concorsuale.

A fronte di siffatte criticità, l'art. 38, comma 4, d.l. 24 febbraio 2023, n. 13, convertito con modificazioni dalla legge 21 aprile 2023, n. 41, ha disposto che, a partire dal 25 febbraio 2023, data di entrata in vigore del detto decreto-legge, l'assegnazione del domicilio digitale da parte della cancelleria prevista dall'art. 199, comma 1, c.c.i.i. « *è rinviata di diciotto mesi* »; ciò, ragionevolmente, nella prospettiva di sopprimere la norma in occasione dell'adozione del previsto secondo decreto correttivo al Codice della crisi (10).

(10) Non risulta che, a partire dalla data di entrata in vigore del Codice della crisi (15 luglio 2022) fino al 24 febbraio 2023 le cancellerie dei tribunali concorsuali abbiano assegnato d'ufficio il domicilio digitale alle procedure di liquidazione giudiziale apertesi.

2.3.3. *Il domicilio digitale del debitore*

In perfetta continuità con la pregressa disciplina della legge fallimentare, il Codice della crisi prevede oggi che la domanda tesa all'apertura della liquidazione giudiziale, come pure è da ritenere quella finalizzata — su richiesta del creditore — all'apertura della liquidazione controllata, sia notificata al debitore presso il suo domicilio digitale.

In particolare, l'art. 40, comma 6, c.c.i.i., stabilisce che, se la domanda finalizzata all'apertura del concorso è proposta da un creditore, da coloro che hanno funzioni di controllo e di vigilanza sull'impresa o dal pubblico ministero, il ricorso e il decreto di convocazione devono essere notificati, a cura dell'ufficio, tramite SERCQ o PEC del debitore, risultante dal registro delle imprese ovvero dall'INI-PEC.

Siffatta differenziazione, tra l'indirizzo PEC risultante nel registro delle imprese e quello risultante nell'INI-PEC, già prevista dall'abrogato art. 15 l. fall., appare ai più sostanzialmente inutile, per la decisiva considerazione che il pubblico elenco di cui all'art. 6-*bis* del CAD, è oggi formato esattamente dagli stessi indirizzi PEC delle imprese che risultano inseriti nel registro delle imprese; del resto, INI-PEC è un pubblico elenco tenuto avvalendosi delle strutture informatiche delle camere di commercio italiane deputate alla gestione del registro delle imprese.

Va peraltro segnalata una significativa novità del Codice rispetto alla disciplina previgente, nei casi in cui l'esito della notifica a mezzo PEC non è positivo.

Il Codice, infatti, distingue a seconda che l'esito infausto della notifica al domicilio telematico sia imputabile o meno al destinatario.

Quando la notificazione a mezzo PEC nei confronti del debitore non risulta possibile (perché neppure esiste un indirizzo PEC presso INI-PEC) o non ha esito positivo per causa imputabile al destinatario (è il caso di scuola della c.d. "casella piena"), secondo quanto dispone il comma 7, art. 40, c.c.i.i., il ricorso e il decreto dovrebbero essere notificati, sempre a cura della cancelleria, mediante il loro inserimento in una apposita piattaforma informatica, la c.d. "area *web* riservata", prevista dall'art. 359 c.c.i.i. La notificazione, in questo caso, si avrebbe per eseguita nel terzo giorno successivo a quello in cui è compiuto l'inserimento.

Tuttavia, attualmente l'area *web* di cui all'art. 359 c.c.i.i. non risulta ancora realizzata, né è stato emanato il decreto del Ministro del made in Italy (già dello sviluppo economico), di concerto con il Ministro della giustizia e con il Ministro per la pubblica amministrazione, sentito il Garante per la protezione dei dati — da adottare entro l'incongrua data del 1° marzo 2020 — che avrebbe dovuto disciplinare i contenuti della detta area *web*.

Dunque, in attesa di una auspicabile novella della norma in esame, in sede di correttivo, sia del Codice della crisi che del d.lgs. 10 ottobre 2022, n. 149, di attuazione della legge delega 26 novembre 2021, n. 206, per la riforma del processo civile (11), ovvero della effettiva istituzione dell'area *web*, in caso di insuccesso della notifica presso il domicilio digitale non resta che procedere alla notifica dell'atto personalmente nel domicilio fisico, secondo la regola — come si dirà *infra* — valevole per i casi di non imputabilità dell'insuccesso, come del resto avveniva prima dell'entrata in vigore del Codice stesso.

Quando la notificazione telematica non risulta possibile o non ha esito positivo, per cause non imputabili al destinatario, invece, il comma 8 dell'art. 40 c.c.i.i. stabilisce che la notifica, a cura del ricorrente, si esegue esclusivamente di persona, a norma dell'art. 107, primo comma, del d.p.r. 15 dicembre 1959, n. 1229, presso la sede risultante dal registro delle imprese o, per i soggetti che non sono iscritti nel registro delle imprese, presso la residenza.

Infine, se la notificazione personale non ha esito positivo, essa si esegue con il deposito dell'atto nella casa comunale della sede che risulta iscritta nel registro delle imprese, ovvero, per i soggetti che non sono iscritti nel registro delle imprese, nella casa comunale della residenza; siffatta notifica si perfeziona nel momento del deposito stesso.

Il codice della crisi ha poi introdotto una ulteriore disposizione di chiusura, applicabile a tutti i casi in cui il destinatario della notifica sia una persona fisica, non titolare di impresa individuale né professionista e, quindi, non obbligata a munirsi del domicilio digitale da iscrivere in INI-PEC.

In queste ipotesi, a tenore del medesimo comma 8, art. 40 c.c.i.i., se la notifica non può avvenire di persona a cura dell'ufficiale giudiziario, dell'avvenuto deposito nella casa comunale del ricorso per l'apertura della liquidazione giudiziale, è data notizia anche mediante affissione dell'avviso in busta chiusa e sigillata alla porta dell'abitazione o dell'ufficio e per raccomandata con avviso di ricevimento.

---

(11) L'art. 3-*ter*, comma 2, della legge 21 gennaio 1993, n. 54, come novellato dal d.lgs. 10 ottobre 2022, n. 149, stabilisce che nel caso di notificazione a mezzo PEC a cura degli avvocati, se la notifica non ha esito positivo per causa imputabile al destinatario, che sia un'impresa o un professionista iscritto nell'indice INI-PEC, l'avvocato deve eseguire la notificazione mediante inserimento nell'area web riservata prevista dall'art. 359 c.c.i.i. Così, in difetto della istituzione della detta area web, l'art. 4-*ter*, d.l. 10 maggio 2023, n. 51, convertito con modificazioni dalla legge 3 luglio 2023, n. 87, ha sospeso l'efficacia della detta norma fino al 31 dicembre 2023. Fino a tale data, quando la notificazione ai sensi del comma 1 dell'art. 3-*ter* della citata legge n. 53 del 1994 non è possibile o non ha esito positivo, quale che ne sia la ragione, essa è eseguita con le modalità ordinarie e si perfeziona, per il soggetto notificante, nel momento in cui è generata la ricevuta di accettazione della notificazione dallo stesso inviata mediante PEC o SERCQ.

Parte III
IDENTITÀ E DOMICILIO DIGITALI NEI GIUDIZI CIVILI DI REGNO UNITO, SPAGNA, GERMANIA E FRANCIA

I.

DIGITAL IDENTITY AND DOMICILE IN ENGLAND AND WALES (*)

di *James Henderson* e *Renato Nazzini*

1.1. Introduction

Attempts to develop national digital identity services in the UK have been seriously impacted by the controversy and baggage associated with the previous proposal for national identity cards.

In 2004 the Labour Government attempted to introduce an identity card scheme but was unable to pass the legislation before the general election in 2005. Following their victory in that election, the Labour Government again introduced identity card legislation, which was defeated in the House of Lords three times before ultimately passing in the form of the Identity Cards Act 2006. Under this legislative scheme cards would not be made mandatory, but anyone renewing their passport from 2008 would be issued a card and have their details added to a central database, the National Identity Register. The register could hold current and past addresses as well as biometric data (1). Following the general election in 2010, the new Conservative-Liberal Democrat coalition government passed the Identity Documents Act 2010 to repeal the prior act and the database was destroyed.

As will be discussed below, when addressing the issue of digital identity, the government has repeatedly sought to distance itself from the 2006 Act and avoid creating, or appearing to create, a centralised database, identity cards or mandatory digital identity scheme.

(*) La Scuola superiore della magistratura ha provveduto ad effettuare una libera traduzione, non revisionata dagli Autori, del presente saggio. La traduzione può essere consultata in appendice.

(1) Identity Cards Act 2006, Ch. 15.

Perhaps as a result, the UK's approach to digital identities has been somewhat fragmented. Government services are also almost entirely federated. Users create accounts for each specific service in isolation, each with its own standards for identity verification. Any digital identity created cannot, by default, be transferred or used for other services. In 2023 the government reported that there were more than 190 sign in routes and 44 separate accounts (2).

1.2. Verify and One Login

An attempt was made to try and address the disconnected approach to digital identities with the GOV.UK Verify ("Verify") identity assurance scheme that was in operation between May 2016 and April 2023. Rather than the centralised National Identity Register proposed under the Identity Cards Act 2006, this scheme allowed users to verify their identity via several third party "identity providers" who had been approved by the Government to carry out identity checks to a standard level of assurance. By design there was no centralised data storage and the services in question would receive the minimum amount of user information necessary.

At its peak in 2020 Verify was used for 22 services. However, Verify persistently failed to meet targets. It launched 4 years later than planned, had consistently less than expected uptake, and in 2021 had only achieved a 50% verification success rate (3).

Since 2021 the Government Digital Service ("GDS"), under the Cabinet Office, has been working to create a replacement called GOV.UK One Login ("One Login") a shared digital identity scheme for accessing online central government services (4). This is intended to be a single login to any government service, and to allow users to create a digital identity which can be verified and securely reused across government services. Verify was slated to be shut down in 2021, but this was delayed to give more time for One Login to be developed (5).

Unlike its predecessor, One Login predominately relies on in-house verification, although in August 2023 the system rolled out an in-person

(2) Cabinet Office and Government Digital Service, *Cabinet Office launches consultation on departmental data sharing* (2023) available at https://www.gov.uk/government/news/cabinet-office-launches-consultation-on-departmental-data-sharing.

(3) Government Digital Service, 'GOV.UK Dashboard' 2021) <https://webarchive.nationalarchives.gov.uk/ukgwa/20210315085419mp_/https://www.gov.uk/performance/govuk-verify> accessed 2023.

(4) Government Digital Service, *GOV.UK One Login: June 2023 update* (2023), available at https://gds.blog.gov.uk/2023/06/24/gov-uk-one-login-june-2023-update/.

(5) Hansard HC vol 693 cols 7WS-8WS (27 April 2021).

identity check at post offices, for those unwilling or unable to use the app or browser based identity verification system (6). Once again, however, there is no central data store akin to the National Identity Register; the data stored is segmented and only held for a limited period of time (7).

As of June 2023, One Login is in use for eight government services, including the Driver and Vehicle Standards Agency, HM Land Registry and HM Revenue and Customs. However, the system is currently voluntary, so government departments running services can decide when or even whether to sign up and so it is unclear what the final scope of the system will be, although GDS hopes it may be expanded to include local government services (8). The published roadmap provides little detail or insight (9).

1.3. Public Opinion

Between 4 January 2023 and 1 March 2023 the government ran a consultation on the draft Digital Government (Disclosure of Information) (Identity Verification Services) Regulations 2023 (10). The proposed regulations are designed to support the One Login rollout by enabling identity checks against a broader range of trusted data already held by public bodies and allow users to reuse their One Login identity once verified more readily.

The Public Service Delivery ('PSD') power (Chapter 1 of Part 5 of the Digital Economy Act 2017) allows specified public authorities to share personal information for objectives which are set out in regulations. To exercise the PSD power, the government must set specific objectives for which the data may be shared and designate the specific public authorities these objectives apply to. The draft regulations propose creating a new objective for the public bodies specified in Schedule 4 of the Act to enable

---

(6) Government Digital Service, *The new in-person identity check for GOV.UK One Login* (2023) available at https://gds.blog.gov.uk/2023/08/30/the-new-in-person-identity-check-for-gov-uk-one-login/.

(7) Mark Say, 'GDS promotes the prospects for GOV.UK One Login' *Uk Authority News* , available at https://www.ukauthority.com/articles/gds-promotes-the-prospects-for-govuk-one-login/.

(8) Government Digital Service, *One Login for Government: December 2021 update* (2021) available at https://gds.blog.gov.uk/2021/12/01/one-login-for-government-december-2021-update/.

(9) Government Digital Service, 'GOV.UK One Login Roadmap' 2023) <https://www.sign-in.service.gov.uk/about/roadmap> accessed 2023.

(10) Cabinet Office, *Government response to the consultation on draft legislation to support identity verification* (2023) available at https://assets.publishing.service.gov.uk/media/646cdb16382a5100139fc608/Government_response_to_the_consultation_on_draft_legislation_to_support_identity_verification.pdf.

data sharing for the purposes of digital identify verification. It also proposes adding 4 new public bodies to Schedule 4, allowing them to be authorised to undertake data sharing for identity verification and public service delivery objectives (11).

Response to the consultation was extremely negative. The majority raised concerns around data privacy and security and believed that these would outweigh any potential benefits. A substantial portion of respondents expressed concerns about far broader issues, rather than the specific questions on data sharing regulations (12).

The Government suggested that many respondents were "significantly influenced by commentaries against implementing compulsory citizen digital identity in principle and data sharing to support it", noting that 75% of emails received as part of the consultation used one of a small number of templates. In particular, there were also concerns that the scheme would lead to the introduction of national identity cards or mandatory digital identities. In response to these fears, the Government emphasised that it understood there is not public support for identity cards in the UK and stated that there are no plans to introduce a mandatory digital identity. The Government also further emphasised that public bodies are required to minimise the amount of personal data shared, ensuring that it was the minimum required for a given service (13).

There were also broader concerns expressed that identity verification services would lead to a social credit system, the phasing out of physical currency or increased governmental surveillance. Overall, up to 20% of question responses were out of scope, depending on the question (14). In response the Government released a Frequently Asked Questions page to address these misconceptions (15).

66,233 responses were received in total; however, this consultation was not a scientific poll attempting to gauge overall public opinion. There would

---

(11) Cabinet Office and Government Digital Service, *Cabinet Office launches consultation on departmental data sharing 8.*

(12) Cabinet Office, *Government response to the consultation on draft legislation to support identity verification*, pp. 12-13.

(13) Cabinet Office, Central Digital & Data Office and Government Digital Service, 'Additional information: GOV.UK One Login' 2023) <https://www.gov.uk/government/consultations/draft-legislation-to-help-more-people-prove-their-identity-online/outcome/additional-information-govuk-one-login> accessed 2023.

(14) Cabinet Office, *Government response to the consultation on draft legislation to support identity verification*, p. 13.

(15) Cabinet Office, Central Digital & Data Office and Government Digital Service, 'FAQs on government digital identity consultation response' 2023) <https://www.gov.uk/government/news/faqs-on-government-digital-identity-consultation-response> accessed 2023.

be a selection bias, with those feeling most strongly against the scheme being more likely to comment on it. Nevertheless, this consultation does appear to show that, at the very least, there is a significant minority of people who harbour extremely negative views towards digital identity schemes and their potential implications.

1.4. The Digital Identities and Attributes Trust Framework

Separately, in 2020 the Government undertook to develop a new legal framework for digital identities (16). In 2021 it then published its policy paper for a UK digital identities and attributes trust framework ("DIATF"), with the most recent version released in January 2023 (17).

Under this system the Government seeks to create a distributed and decentralised digital identity scheme. The DIATF creates a standards, guidance, and certification process for private identity service providers ("IDSPs"). To become certified an IDSPS must, among other things, follow the confidence standards set out in Good Practice Guide 45 on how to verify someone's identity and comply with standards for data security and protection. There is a voluntary data scheme that aims to make services interoperable with others. At present government licensing is not considered viable, so certification will be performed by independent certification bodies.

The framework will be overseen by a governing body. Currently this is being handled by the Department for Culture, Media and Sports ("DCMS"). This is stated to be an interim measure, but the final institutional structure is currently undecided. It is planned that future legislation will allow the governing body to issue trust marks for certified organisations, but currently the DCMS simply maintains an internal list.

The DIATF is predominantly intended for private sector use, but it is intended that public sector organisations will be able to work with the governing body to incorporate the certification framework. Live testing has already begun for the right to work, right to rent and criminal record checks.

The framework will officially go into effect with the Data Protection and Digital Information (No 2) Bill, that will both put the DIATF on a statutory

(16) Cabinet Office and Department for Digital Culture Media & Sport, 'Digital Identity: Call for Evidence Response' 2020) <https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response> accessed 2023.

(17) Department for Science Innovation and Technology, Department for Digital Culture Media & Sport and Julia Lopez, 'UK digital identity and attributes trust framework - beta version' 2023) <https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version> accessed 2023.

footing and enable certified IDSPs to obtain personal data about a user from government departments.

It is possible One Login will be integrated into the framework, either being able to act as an IDSP or by accepting externally verified digital identifies, but there has been no announcement to this effect beyond a statement from the Cabinet Office that One Login is "committed to adhering to the key tenets" of the DIATF ([18]) and that it is "collaborating with DCMS to ensure our policy and legislative proposals are complimentary" ([19]).

Currently, however, the UK Government seems to be pursuing two parallel digital identity schemes, managed by different government departments: one seeking to introduce a distributed and decentralised framework that avoids the spectre of a national identity card scheme or government issued digital identity, and the other which seeks to create a single consolidated digital identity system that can be used across public services.

1.5. Court Services

The court services are attempting their own digitisation process, the bulk of which is part of the ambitious HM Courts and Tribunal Service ("HMCTS") reform programme that has been operating since 2016 with the aim of modernising and digitising the justice system. The portfolio of programmes consists of 44 projects across five workstreams, covering crime, civil, family, tribunals, and the general court estates ([20]).

However, progress has been somewhat erratic, with delays, cost overruns and revisions. The programme was expected to be completed in 2020, and now expects completion in 2024. Further, in its haste to meet deadlines, many of the services are not working as efficiently as expected. While initially there were plans for a single common digital platform for civil, family and tribunal claims, analogous to the common platform for crime, this proposal was rejected by the Government in 2017. As such, digitisation of these services has taken the form of individual initiatives for each existing jurisdiction.

([18]) Cabinet Office, Central Digital & Data Office and Government Digital Service, 'Additional information: GOV.UK One Login' <https://www.gov.uk/government/consultations/draft-legislation-to-help-more-people-prove-their-identity-online/outcome/additional-information-govuk-one-login> accessed 2023.

([19]) Cabinet Office, Central Digital & Data Office and Government Digital Service, 'Consultation on draft legislation to support identity verification' 2023) <https://www.gov.uk/government/consultations/draft-legislation-to-help-more-people-prove-their-identity-online/consultation-on-draft-legislation-to-support-identity-verification> accessed 2023.

([20]) National Audit Office, *Progress on the courts and tribunals reform programme* (HC 1130, 2023) appendix two.

The grand aim, for most civil, family and tribunal cases, is for the entirety of the litigation process to take place online. In an important speech at King's College London, Sir Geoffrey Vos, Master of the Rolls and the Head of Civil Justice in England and Wales, has outlined a staged system where would-be litigants would be able to receive pre-action advice online, be directed to online alternate dispute resolution portals and then, if that fails, to online court processes. The ambition is that these would be integrated systems, with the same data being passed between each (21).

This process will be overseen by the Online Procedure Rule Committee, created in June 2023 and currently chaired by Sir Geoffrey, that has statutory oversight of dispute resolution processes created by the reform programme and digital pre-action portals and processes (22).

One complicating factor is that many of the portals that this framework hopes to include are not created or maintained by HMCTS: for example, the Official Injury Claim portal for whiplash claims built by the Motor Insurers Bureau, or the myriad of sites for different Ombudsmen. There may be as many as a 100 of these portals, but there is no official count. It is hoped that the Online Procedure Rules Committee will be able to set out a consistent data storage and API framework (23), but no tangible proposals have yet been made nor is it clear whether the system will be designed to be compatible with either One Login or the DIATF framework.

Many of the provisions for civil courts have been enabled via practice directions. While changes to the Civil Procedure Rules ("CPR") requires a statutory instrument (24), practice directions can be changed relatively easily. Practice directions can simply be issued by the Master of the Rolls, with the approval of the Lord Chancellor (25). Critically, CPR Part 51 allows practice directions to override the CPR for specific periods or for specific courts as part of pilot schemes (26). This has allowed for a gradual and flexible rollout. Systems may be introduced to individual courts on a voluntary basis, and then expanded to other courts, or made mandatory with relative ease.

---

(21) See Geoffrey Vos, 'Speech on the 150th Anniversary of the Technology and Construction Court' 2023) <https://www.judiciary.uk/speech-by-the-master-of-the-rolls-justice-in-the-digital-age/> accessed 2023.

(22) Judicial Review and Courts Act 2022, ss 22-24.

(23) See Geoffrey Vos, 'Speech to the Chartered Instituted of Arbitrators: Roebuck Lecture 2022' 2022) <https://www.judiciary.uk/speech-by-the-master-of-the-rolls-ciarb-roebuck-lecture/> accessed 2023.

(24) Civil Procedure Act 1997, s 4(3).

(25) Civil Procedure Act 1997, s 5. The Lord Chief Justice has nominated the Master of the Rolls to make practice directions for the civil courts under Constitutional Reform Act 2005, sch 2 pt 1.

(26) CPR 51.2.

1.6. Civil Filing

The civil courts are moving to a "digital by default" filing system for courts and tribunals. This is one of the few changes that predate the current reform programme. The 2010 Jackson report recommended, among other things, the electronic filing of statements of case and other procedural documents and the electronic storage of documents that are available to the parties, court, and judiciary.

On 16 November 2015, the implementation of e-filing was introduced at the Royal Courts of Justice at the Rolls Building, London, as the Electronic Working Pilot Scheme under Practice Direction 51O, using the CE-File system. Despite continuing to be designated as a "pilot", and having previously been labelled as an interim solution, the scheme has been expanded and extended several times, and at present there is no indication that it will be discontinued.

Today the system may be used for Part 7, Part 8, Part 20 claims and pre-action applications in the Rolls Building Jurisdictions (which incorporates the Chancery Division of the High Court, the Commercial Court, the Technology and Construction Court, the Circuit Commercial Court, and the Admiralty Court), the Business and Property Courts District Registries, the Central Office and District Registries of the King's Bench Division, and detailed assessment proceedings and Part 8 claims in the Costs Office and applications for permission to appeal and appeals in the Court of Appeal (Civil Division).

E-filing is becoming increasingly mandatory if parties are legally represented. From 30 April 2019 it became mandatory in all Business and Property courts. For the King's Bench Division, it became mandatory in London in July 2019, and for the District Registries at Birmingham, Bristol, Cardiff, Leeds, Liverpool, Manchester, and Newcastle in October 2021. It became mandatory in the Senior Courts Costs Office from October 2019 and the Court of Appeal from February 2022. E-filing is set to be introduced for the Administrative Court Office, and as of August 2023 a new case management system has been introduced as part of CE-File, although e-filing is not yet possible.

1.7. Other Civil Systems

Currently HMCTS use the "MyHMCTS account" system, launched in early 2020, as part of the 2016 reform programme. This system has not yet been integrated into One Login. At this point is not clear whether it will be, as integration with One Login is entirely voluntary.

Individuals cannot gain access to the system on their own, instead organisations must first register for a MyHMCTS account, which requires the organisation's Payment By Account ("PBA") number, DX reference number (if relevant), and the organisation's Solicitors Regulation Authority ("SRA") ID or equivalent professional registration, and the name and email of someone who will be designated the MyHMCTS "account listed administrator". This administrator is then responsible for creating accounts for individual users.

MyHMCTS is currently used for civil damages claims, civil money claims, divorce proceedings, employment tribunal responses, family public law orders, financial remedies, immigration and asylum appeals, and probate. The hope is that the administrative part of these processes can be carried out entirely online, supplemented by remote or in-person hearings. A number of these services have proven to be quite successful, with 80% of all probate applications received online and 94% positive user ratings (27) and more than 445,000 Online Civil Money Claims with 95% positive ratings (28).

Much like CE-File, the use of the system is slowly becoming mandatory for professional clients. From 22 June 2020 it became mandatory for immigration and asylum appeals (29). From 24 August 2020 the system became mandatory for financial remedy consent orders (30). From 2 November 2020 it became mandatory for all grants of probate applications (31). Finally from 4 April 2022 almost all civil damages claimed by professionally represented parties must be issued online using the damages claims portal on MyHMCTS and from 15 September this became mandatory for responses as well (32).

Beyond this, legal service in civil cases is still carried out physically by default. However, under Practice Direction 6A, parties can indicate in writing that they are willing to accept service by electronic means, such as fax or email. The inclusion of a fax number alone will be taken as sufficient written indication, but for included email addresses explicit confirmation must be given. In *Barton v Wright Hassall LLP* (33) a litigant in person attempted to serve a claim form to the respondent's solicitors via email when they had not stated they were prepared to accept service by that means. The

(27) HM Courts & Tribunal Service, *Fact sheet: Probate online* (2023).

(28) HM Courts & Tribunal Service, *Fact sheet: Online Civil Money Claims* (2023).

(29) Michael Clements, *Presidental Practice Statement No 2 or 2020: Arrangements During the COVID-19 Pandemic* (2020).

(30) T PD.

(31) The Non-Contentious Probate (Amendment) Rules 2020 SI 2020 no. 1059

(32) ZB PD.

(33) [2018] UKSC 12.

court refused to cure this mistake, finding the claimant did not take reasonable steps to serve the claim form in accordance with the rules. This case also highlighted that the specific provisions relating to service via email were designed to ensure that solicitors had the opportunity to put in place arrangements for monitoring and dealing with emails (at the time a novel mode of service). However, as the digital issuing and filing of claims gradually becomes mandatory for all civil proceedings, the court questioned whether these rules continue to serve a useful purpose (34).

If multiple email addresses are provided, the document is deemed served by sending it to any two of the e-mail addresses identified. Any email addresses provided are specific to a given proceedings, rather than having a designated email that is tied to a particular person for all legal, let alone official, correspondence.

Under Rule 6.15 courts have discretionary powers to permit service by alternate means if physical service or even standard electronic service is not practicable. This is an extremely broad provision. In *Gray v Hurley* (35) the court granted an order for the defendant to be served via WhatsApp message.

1.8. Judgments and Orders

During the COVID-19 pandemic courts handed down most reserved judgments remotely. This procedure worked so well it has now been retained in some courts. On December 2021 the Master of the Rolls gave practice guidance for the Civil Division of the Court of Appeal that, unless otherwise directed, reserved judgments will be handed down remotely via email release to BAILII and The National Archives. Likewise, from October 2022 Chancery Division judgments are sent via email as well as to The National Archives. Until April 2022 they were also released to BAILII.

Otherwise, while draft judgments are often made available to counsel electronically ahead of being entered, the judgment itself will still be handed down in court. However, if there are no applications to be made as a result of the judgment, the judgment may be handed down by a judge sitting alone (36). Service of judgments may be carried out electronically, per the rules outlined above.

Creditors seeking to enforce a money judgment currently have a potentially arduous task if the debtor does not cooperate with the process. The

(34) [2018] UKSC 12, para 29.
(35) [2019] EWHC 1636 (QB).
(36) PD 40E 5.1.

onus is entirely on the creditor for initiating the process, and there is no formal system for asking third parties, such as government departments or banks, for information. There are statutory provisions that would facilitate this under ss 95 to 102 of the Tribunals, Courts and Enforcement Act 2007 but it is not clear that these provisions will ever come into force.

1.9. The Common Platform

In contrast to the generally well received CE-File, the rollout of the Common Platform used in the criminal courts has been marred by complications and delays. Initially conceived of in 2013, the Common Platform was designed to digitise court processes and replace the existing case management systems used by HMCTS and the Crown Prosecution Service ("CPS").

Prior to this, Crown Courts utilised the Crown Court Digital Case System ("CCDCS") platform, which allowed users to view and print case documents, such as indictments, witness statements, exhibits, applications and unused materials that had been uploaded to it. As it stands, the CCDCS is still in use for case materials in the Crown Court, while the Common Platform is now used for case administration.

Registration for both services requires a secure Criminal Justice Secure eMail ("CJSM") email address. The CJSM email service is available to a wide range of organisations and individuals involved in the criminal justice system, including police, the National Health Service ("NHS"), and prisons. All applications must be sponsored by the police, central government, or NHS (37).

The Common Platform was intended to be implemented by March 2018. This proved harder than anticipated, and in 2021 it was decided that building a single system was impractical, and instead only the court system would be created that could be linked with the CPS's existing systems. As of January 2023, the interface has still not finished testing (38) Currently HMCTS expects complete delivery of the platform by March 2025 (39).

Rollout was further delayed by the COVID-19 pandemic and a pause between August 2021 and March 2022 to address major performance, stability, and speed issues. Even after the pause, problems were not entirely resolved and between March and October 2023, HMCTS recorded 231

(37) Criminal Justice Secure eMail, 'About CJSM' 2023) <https://cjsm.justice.gov.uk/why/index.html> accessed 2023.

(38) National Audit Office, *Progress on the courts and tribunals reform programme 32.*

(39) House of Commons Committee of Public Accounts, *Progress on the courts and tribunals reform programme* (HC 1002, 2023) 4.

critical incidents affecting users (40). Law Society members noted a number of serious issues, including cases disappearing from the system, difficulty in accessing case papers, directions not showing on the system, technical errors and delays due to judges, legal advisors and staff being unable to access the system (41). Courts were forced to make do, reverting back to the older system or even paper records.

The rollout was paused again in September 2022 after HMCTS found that the system had failed to notify partner agencies of required actions in approximately 3,000 (1%) cases. Further investigation found that the failure to send notifications could have affected justice outcomes in 357 cases. For example, in 35 cases an individual was not fitted with an electronic monitoring tag when they should have been (42). Since October 2022 there have been multiple instances of strike action by legal advisers and court associates at more than 60 magistrates' courts protesting the Common Platform (43).

In 2022 the Bar Council, the representative body for barristers in England and Wales, reported that the Common Platform was "widely perceived as being a failure. Court users have struggled to log on to the system, there are doubts about the design of the platform, and participants were unsure whether the roll-out was still happening as they felt there was little information or take-up" (44).

Nevertheless, the rollout is continuing, and as of August 2023 is it in use at all criminal courts (45), although many core functions are not expected to be finalised until March 2024, and the full rollout until a year later.

1.10. Conclusions

There are several plans in England and Wales for digital identities and digital reform, but at the present it is unclear if, when or even how they will ultimately bear fruit. There is no centralised, unified system, although there are several ambitions to either create one, or at the very least create a system

(40) National Audit Office, *Progress on the courts and tribunals reform programme 32.*

(41) House of Commons Committee of Public Accounts, *Progress on the courts and tribunals reform programme, CPR0003, The Law Society Submission*, 30 March 2023, para 47.

(42) National Audit Office, *Progress on the courts and tribunals reform programme*, 32-33.

(43) House of Commons Committee of Public Accounts, *Progress on the courts and tribunals reform programme, CPR0003, The Law Society Submission, 30 March 2023, para 51.*

(44) The Bar Council, *Access Denied: The state of the justice system in England and Wales in 2022* (2022) 10.

(45) HM Courts & Tribunal Service, *Every criminal court now connected to single data system for the first time* (2023).

that is designed to be interoperable. However, the protracted problems associated with the rollout of the Common Platform, which aimed to create a single unified system to cover procedural functions, and GOV.UK Verify, which aimed to create a common framework for connecting existing but disconnected systems, act as a cautionary tale. It is notable that One Login's own adoption roadmap is remarkably sparse.

It seems certain that digitisation of court services is the future, and there are some individual systems that appear to be working well. CE-File has been positively received as a digital filing system, but other systems will be needed for broader online case management. Courts have embraced efforts to enable digital justice where possible and this has been greatly aided by the flexibility of the practice directions, such as those for remote hearings and handing down judgments, but these have resulted in somewhat ad hoc solutions. A significant obstacle will be attempting to coordinate and unify these systems and concrete proposals for doing so have yet to materialise. So far, the civil courts have managed to avoid the issues plaguing the Common Platform, but integration may prove equally troublesome.

There is a fundamental tension between public opinion and government policy. On the one hand, there is a desire to avoid any kind of singular national digital identity system or any kind of centralised "big brother" data storage system, but on the other there is a desire for coordination and sharing of data, so that people do not need to log into and deal with multiple completely unconnected services. Proposals as to how to overcome this dichotomy are regrettably scarce. Until then, patchwork and informal systems will prevail.

II.

LES PRINCIPES DIRECTEURS DU PROCÈS AU SERVICE DE LA NUMÉRISATION DE LA PROCÉDURE (*)

di *Samir Merabet*

Sommaire: Table des matières: 2.1. Le numérique, remède à la crise de la justice? — 2.2. Justice 1.5. — 2.3. Les manifestations de la numerisation de la procedure en France. — 2.3.1. Les outils de numerisation de procedures. — 2.3.2. Les risques de la numerisation des procedures. — 2.4. La protection contre les dangers de la numérisation de la procédure en France. — 2.4.1. Les risques du principe de neutralité technologique. — 2.4.1.1. *De lege lata*, l'efficacité du droit au procès équitable. — 2.4.1.2. *De lege ferenda*, la consécration de principe directeur du procès numérique.

2.1. Le numérique, remède à la crise de la justice?

Intelligence artificielle, open data (1), visioconférence, systèmes d'aide à la décision, blockchain ... les innovations techniques susceptible de renouveler la pratique de la procédure sont nombreuses et peuvent susciter l'enthousiasme, alors même que l'institution judiciaire connait des difficultés, si ce n'est une « crise » (2). L'informatique a en son temps permis de considérablement faciliter l'organisation des procédures, civile comme pénale. Le Doyen Catala avait très tôt théorisé tous les bénéfices que le droit en général et la procédure en particulier pouvaient tirer de l'informatique (3).

(*) La Scuola superiore della magistratura ha provveduto ad effettuare una libera traduzione, non revisionata dall'Autore, del presente saggio. La traduzione può essere consultata in appendice.

(1) L. Cadiet (sous la dir.), *L'open data des décisions de justice*, 29 nov. 2017, disponible sur www.justice.gouv.fr.

(2) L. Cadiet et E. Jeuland, *Droit judiciaire privé*, LexisNexis, 10e éd., 2017, n. 32: « De fait, la crise de la justice n'est pas seulement d'ordre matériel: la justice est sous-équipée; son budget est insuffisant, ses moyens n'ont pas augmenté proportionnellement à la demande des justiciables. La crise de la justice est aussi morale, ou politique, ou idéologique, comme l'on veut ».

(3) P. Catala, *Le droit à l'épreuve du numérique, Juris ex Machina*, PUF, 1998.

Les nouveaux outils numériques devraient à leur tour être source de progrès. Les vertus potentielles sont nombreuses. Le numérique pourrait permettre d'automatiser certaines tâches pour un gain de temps ou encore faciliter l'accès des justiciables aux juridictions. Cette numérisation de la procédure est actuellement en cours en France.

2.2. Justice 1.5

L'institution judiciaire n'a pas de raison d'être hermétique à la numérisation croissante de la société. Certains outils numériques sont à présent relativement anciens et l'on pourrait donc penser qu'ils seraient pleinement intégrés dans l'organisation des juridictions française en général, et en matière procédurale en particulier. Pourtant, force est de constater que la révolution numérique de la justice française se fait encore attendre. La crise sanitaire et le premier confinement intervenu à compter du 17 mars 2020 a révélé toutes les limites des infrastructures numériques de l'institution judiciaire (4). D'un point de vue très pragmatique, l'essentiel des magistrats et greffiers n'était pas équipé d'ordinateurs portables professionnels. La Cour de compte s'est montrée très critique vis-à-vis de la continuité du service public de la justice au cours de cette période (5). On mesure alors le chemin qu'il reste à parcourir pour que le processus de numérisation aille à son terme. Les pouvoirs publics ont pourtant récemment pris la mesure des enjeux. Ainsi, le ministère de la justice a adopté en 2017 un plan de transformation numérique (PTN), couvrant la période 2018-2022. L'allocation d'un budget de 530 millions d'euros avait pour objectif de moderniser l'institution judiciaire et notamment permettre une meilleure dématérialisation des procédures. Si la démarche semblait ambitieuse, le résultat escompté ne semble pas avoir été atteint. La Cour des comptes a constaté que ces investissements n'avaient en réalité servi qu'à rattraper le retard accumulé au cours des années précédents. Aussi, à ce stade, la France ne fait pas figure de modèle en matière de numérisation de la justice. Néanmoins, le nombre de procédure numérisée s'étend progressivement.

---

(4) A. Coignac, *Les tribunaux judiciaires à l'épreuve de la crise sanitaire*, JCP G, 2020, n. 20-21, 624.

(5) Cour des comptes, « Le plan de continuité d'activité des juridictions judiciaires pendant la crise sanitaire liée à l'épidémie de covid 19, mai 2021 », accessible via www.coursdescomptes.fr.

2.3. Les manifestations de la numerisation de la procedure en France

2.3.1. *Les outils de numerisation de procedures*

a) *La numérisation de la procédure en droit français*

Le droit français prend progressivement le virage du numérique. Par exemple, l'article 800-1 du Code de procédure pénale envisage que tous les actes de procédures, « qu'il s'agisse d'actes d'enquête ou d'instruction ou de décisions juridictionnelles ou de toute autre pièce de la procédure, peuvent être établis ou convertis sous format numérique ». Dans cette perspective, le récent le décret du 23 juin 2020 autorise, par l'article R. 249-9 du code de procédure pénale, la création du « dossier pénal numérique », en vue de « faciliter et améliorer le traitement des dossiers pénaux par les magistrats, les greffiers et les personnes habilitées à les assister » (6). La procédure civile elle aussi est sujette à ce mouvement de numérisation.

b) *La saisie des juridictions*

Le droit français a fait le choix de numériser certains actes de saisine des juridictions. Parfois, les règles de procédures permettent à la fois la saisie numérique et la saisie traditionnelle, par voie postale ou dépôt au greffe. C'est par exemple le cas de la procédure simplifiée de recouvrement de dette. Lorsque la créance n'excède pas 5000 euros, le créancier peut initier son action entièrement en ligne, via la « plateforme des petites créances ». Lorsque la procédure va à son terme et que le débiteur refuse de s'exécuter, le créancier peut alors saisir le tribunal pour obtenir un titre exécutoire. Dans d'autres hypothèses, le numérique s'est totalement imposé et devient la seule manière de saisir une juridiction, à peine d'irrecevabilité. C'est surtout le cas pour l'ensemble des procédures d'appel qui doivent toutes être effectué par voie électronique, à peine d'irrecevabilité de l'appel, ce qui n'est pas sans causer de difficulté lorsque les outils prévus à cette fin présentent des limites techniques non anticipé par leur concepteur.

c) *La communication des pièces et des actes*

L'un des apports majeurs du numérique consiste dans la dématérialisation des échanges, permettant un gain de temps et de ressources significatifs. Aussi la communication électronique en matière judiciaire est une perspective à l'intérêt non négligeable. L'intérêt est d'autant plus important lorsque l'une des parties est établi à l'étranger voir outre-mer. L'encadrement d'une telle innovation doit néanmoins être minutieusement envisagé dans la mesure

(6) A. Chavent-Leclère, *Le dossier pénal numérique*, in *Procédures*, 2020, n. 10, alerte 15.

ou cette communication emporte d'importante conséquence sur l'opposabilité des actes et sur le principe du contradictoire. Un décret du 3 mai 2019 contribue à contribuer à la numérisation de la procédure en ce sens (7).

d) *La signature des actes*

La dématérialisation des procédures rend archaïque un certain nombre de pratique. Il en va ainsi par exemple de l'impression de l'impression d'une décision de justice, pour qu'elle soit signée par un magistrat avant d'être à nouveau numérisé. Aussi, pour éviter ces tâches fastidieuses, le droit français autorise depuis quelques années la signature électronique des actes judiciaires. En premier texte avait initié ce mouvement en matière commerciale, pour les jugements des tribunaux de commerce (8). La démarche a été étendue par la suite aux jugements rendu en matière civile par un arrêté du 20 novembre 2020 (9). Le texte envisage des modalités techniques particulières pour garantir l'intégrité des dites signatures. Ainsi, « La signature électronique contient l'identification du signataire, un jeton d'horodatage garantissant l'intégrité du document et la date de signature, un certificat de signature électronique qualifié et valide, délivré par le ministère de la justice ».

e) *Un bilan mitigé*

Cette brève présentation démontre que la numérisation de la procédure se déploie progressivement, par touche successive. Les cas envisagés semblent indiquer des innovations ponctuelles opérés par le ministère de la justice, en l'absence de véritable démarche d'ampleur visant à repenser la procédure dans son ensemble pour l'adapter aux enjeux du numérique. Plus encore, on identifie dans le même temps un certain nombre de carence non négligeables. Quelques exemples permettent de démontrer à quel point la technique n'est pas toujours à la hauteur des ambitions de l'administration judiciaire et plus généralement des professionnels du droit. Au cours des dernières années, la plateforme e-barreau a permis une accélération de la numérisation des procédures. Néanmoins subsistent malgré tous des pratiques qui paraitront bientôt désuètes. Par exemple, même si certaines

(7) Décret n. 2019-402 du 3 mai 2019 portant diverses mesures relatives à la communication électronique en matière civile et à la notification des actes à l'étranger, C. Bléry, T. Douville et J.-P. Teboul, *Nouveau décret de procédure civile: présentation générale*, Dalloz actualité, 24 mai 2019.

(8) Arrêté du 9 avril 2019 relatif à la signature électronique des décisions rendues par les tribunaux de commerce; Y. Broussole, *Les principales dispositions de l'arrêté du 9 avril 2019 relatif à la signature électronique des décisions rendues par les tribunaux de commerce*, LPA 20 sept. 2019, n. 147, p. 12.

(9) Arrêté du 20 novembre 2020 relatif à la signature électronique des décisions juridictionnelles rendues en matière civile.

procédures sont totalement dématérialisées, certaines juridictions continuent de demander que les conclusions leur soient transmises au format papier, à charge pour les parties de fournir des enveloppes affranchies pour qu'elles leur soient retournées à l'issue de la procédure. D'autres limites des outils actuels peuvent encore être relevées. Par exemple, on peut relever que la plateforme e-barreau permet l'échange de pièces via RPVA, mais avec une limite de 10 Mo maximum, obligeant à recourir à d'autres voies, comme le mail. Dans un autre registre, la procédure d'appel est elle aussi fragilisée par les limites des outils numériques. Ainsi, la déclaration d'appel en ligne est limitée à 4080 caractères. Si ce plafond peut parfois être très largement suffisant, d'autres espèces démontrent ses limites. Eu égard aux conséquences majeures qui affectent le défaut de déclaration, les conseils sont contraints de rechercher des méthodes alternatives, telles que rédiger la déclaration d'appel sur papier puis joindre la pièce à la déclaration en ligne, avec les incertitudes procédurales qui accompagnent une telle manœuvre. Loin de faciliter la procédure, les limites des outils numériques mobilisés peuvent la rendre plus difficile. Ici, la forme contraint le fond.

2.3.2. *Les risques de la numerisation des procedures*

L'on pourrait être critique vis-à-vis de la lenteur avec laquelle se déploie le numérique au sein des juridictions française. D'un autre point de vue, ce constat pourrait être interprété de manière plus positive comme la démonstration d'une certaine sagesse, de manière à ne pas précipiter des évolutions dont on peinerait à percevoir tous les dangers à présent. Il est plus vraisemblable que le retard s'explique davantage par un manque de moyens et d'anticipation mais peut être que cette situation est préférable, de manière à se préparer aux risques provoqués par la numérisation de la procédure.

a) *Des avantages aux inconvénients*

Si l'on perçoit les avantages de tels dispositifs, on peut également en deviner les éventuels inconvénients. Pour commencer, l'on peut évoquer le phénomène d'illectronisme, encore appelé illettrisme numérique. Ce terme désigne les personnes qui rencontrent des difficultés voire l'impossibilité d'utiliser les outils numériques et qui concerne près de la 15% de la population française. Pour ces personnes, l'éventuels obligation de recourir à des outils numériques pour initier une procédure judiciaire peut conduire à les priver d'accès au juge. On peut espérer qu'à terme, le renouvellement des générations conduisent à réduire ce phénomène. Le cas échéant, toutes les difficultés ne seront pas résolues. Les inquiétudes sont légitimes et ont notamment était exprimé par la CEPEJ.

b) *Formalisme numérique et accès au juge*

Aussi sophistiqué soit les dispositifs numériques utilisés, l'on n'est jamais à l'abri d'une mauvaise manipulation ou d'un beug. Chacun l'expérimente régulièrement avec les dispositifs que nous sommes amené à utiliser dans la vie quotidienne. Évidemment, il en va de même pour les dispositifs numériques utilisé à des fins de procédures. Les conséquences sont néanmoins cette fois majeures. Une éventuelle erreur ou un dysfonctionnement et c'est l'action même d'une partie qui pourrait être remise en cause. *In fine*, c'est l'accès au juge qui pourrait être compromis. Loin de faciliter les démarches procédurales des justiciable, le numérique pourrait alors constituer un nouveau piège de nature à faire échec aux prétentions des parties, seulement en raison de vice de procédure. De telles situations ne relèvent pas du cas d'écoles. Divers exemples peuvent être tirés de la jurisprudence française. Le plus significatif consiste sans doute dans la procédure d'appel.

c) *L'hypothèse de la déclaration d'appel*

Chaque fois qu'une procédure est dématérialisée, un risque d'échec d'une action à raison d'un problème informatique existe. À ce titre, les difficultés rencontrées en droit français à propos de la déclaration d'appel sont particulièrement révélatrices. En matière civile, le droit français impose que les déclarations d'appels soient remises à la cour d'appel par voie électronique, sous peine d'irrecevabilité, qui plus est relevée d'office, au sens de l'article 930-1 du Code de procédure civile. La procédure dématérialisée est donc incontournable pour que l'appel soit recevable. Cette numérisation a suscité des difficultés, en raison à la fois de règle de procédure et de contraintes techniques. D'abord, le droit français subordonne l'effet dévolutif de l'appel au respect d'un certain formalisme. Ainsi, la déclaration d'appel doit préciser quels chefs de jugement critiqués et la Cour d'appel n'est saisi que de ceux-ci. Ensuite, la plateforme utilisée pour procéder à cette déclaration d'appel connait des limitations techniques. En effet, la déclaration doit être réalisé via le Réseaux privé virtuel justice (RPVJ) plateforme permettant l'accomplissement d'acte de procédure. Or, l'espace dédié à la déclaration d'appel sur cette plateforme est limité à 4 080 caractères. Si l'espace est parfois suffisant, il ne l'est pas toujours. Aussi, les avocats ont pris l'habitude d'annexer à la déclaration d'appel un document détaillant les chefs de jugement critiqués. L'usage s'imposant, certain recourrait à cette méthode l'annexe même lorsque la limite de caractère n'était atteinte. Des contraintes techniques lié à l'outil numérique utilisé ont donc emporté de nouvelles pratiques qui, formellement, permettait tout de même que la Cour d'appel soit dument informée. Pourtant, un débat est né sur la nature de l'annexe à cette déclaration d'appel qui ne respectait pas le

formalisme électronique envisagé par les textes. Or, la Cour de cassation a adopté une approche très formelle, estimant que sauf problème technique, la Cour d'appel n'était pas saisie des chefs de jugement figurant dans l'annexe (10). Ainsi, c'est seulement si la déclaration d'appel dépasse le nombre de caractère autorisés qu'une annexe peut valablement être introduite, à condition d'y renvoyer expressément. Les conséquences de cette décision était d'autant plus dommageable que la solution était d'application immédiate, y compris aux procédures en cours, menaçant ainsi de priver les justiciable de leur voie de recours, sauf à régulariser la déclaration d'appel irrégulière. Tout cela illustre à quel point la numérisation de la procédure, loin de la faciliter, peut conduire à un formalisme excessif. En l'occurrence, le problème était surtout lié à un service arbitrairement limité à 4 080 caractères. Ainsi, la manière de concevoir l'outil numérique, indépendamment des règles de procédure applicable, est de nature à priver les justiciables de leur recours. Une réforme a été envisagée pour permettre d'en finir avec ce formalisme. Ainsi, un décret du 25 février 2022 (11) a modifié l'article 901 du Code de procédure civile, accompagné d'un arrêté du même jour modifiant l'arrêté du 20 mai 2022 (12) avec l'objectif d'admettre la validité de l'appel formé via une annexe jointe à la déclaration. La solution n'était vraisemblablement pas suffisamment claire dans la mesure où des Cour d'appel ont continuait de juger qu'une annexe n'était recevable qu'à la condition qu'il existe un empêchement technique (13). Ainsi, si les chefs de jugement critiqués représentaient moins de 4 080 caractères, ils devaient figurer directement sur le formulaire électronique de la plateforme, à peine d'irrecevabilité. Pour mettre fin aux incertitudes, la Cour de cassation a rendu un avis pour permettre la recevabilité des appels ainsi formé (14). On peut être surpris qu'une telle situation ai dû donner lieu à plusieurs arrêts de la Cour de cassation et une réforme des textes applicable. On peut surtout craindre qu'une même approche conduise bien trop souvent à ce que la

(10) Cass. Civ. 2e, 13 janv. 2022, n. 20-17.516, Dalloz actualité, 20 janv. 2022, obs. R. Laffly; D. 2022. 325, note M. Barba; ibid. 625, obs. N. Fricero; AJ FAM. 2022. 63, obs. F. Eudier et D. D'Ambra; Rev. prat. rec. 2022. 9, chron. D. Cholet, O. Cousin, M. Draillard, E. Jullien, F. Kieffer, O. Salati et C. Simon.

(11) Décret n. 2022-245 du 25 février 2022 favorisant le recours à la médiation, portant application de la loi pour la confiance dans l'institution judiciaire et modifiant diverses dispositions.

(12) Arrêté du 20 mai 2020 relatif à la communication par voie électronique en matière civile devant les cours d'appel.

(13) Cour d'appel de Rennes, 14 mars 2022.

(14) Cass. Civ. 2e, avis, 8 juill. 2022, n° 22-70.005, Dalloz actualité, 30 août 2022, obs. R. Laffly; D. 2022. 1498, note M. Barba; Gaz. Pal. 13 sept. 2022, p. 17, note M. Bencimon; ibid. 25 oct. 2022, note C. Bléry; JCP 2022. 1345, obs. L. Veyre.

numérisation de la procédure conduise à la complexifier alors que l'objectif initial était justement la simplification.

2.4. La protection contre les dangers de la numérisation de la procédure en France

2.4.1. *Les risques du principe de neutralité technologique*

De très nombreuses branches du droit sont aujourd'hui confronté au numérique emportant parfois de profonds bouleversements juridiques. Il est certain que l'évolution du droit n'est plus en mesure de suivre le rythme des innovations numériques. Aussi, il est fréquent que de nouvelles techniques trouvent à s'appliquer en l'absence de réglementation spécifiquement pensées pour s'y appliquer. Le cas échéant, il n'y a évidemment pas de vide juridique dans la mesure où de très nombreuses règles préexistantes trouveront à s'appliquer. Parfois, l'absence de réglementation spécifique n'est pas dû à un retard du législateur mais d'un véritable choix de politique législative. Créer de nouvelles règles complexifie le droit et il est parfois préférable de s'en remettre seulement à un principe de neutralité technologique selon lequel le droit s'applique indifféremment de la nature des techniques utilisée. Appliqué aux règles de procédure, cela conduit par exemple à tenir l'écrit au format papier ou électronique pour équivalent et à se contenter de dupliquer au numérique les règles de procédure préexistante. Cette méthode a le mérite de la simplicité et se justifie parfois. En revanche, il y a d'autres situation où l'absence de réglementation spécifique laisse subsister des risques qui ne trouvent pas de réponse dans le droit positif et qui appellerait davantage la consécration de principe idoine. La numérisation de la procédure ne fait pas exception. Si parfois les règles de droit positif permettent de prévenir les risques nés de la numérisation de la procédure (A), d'autres situations appellent en revanche la consécration de nouveaux principes (B).

2.4.1.1. De lege lata, *l'efficacité du droit au procès équitable*

a) *Le droit d'accès au juge*

La numérisation de la procédure peut servir un meilleur accès à la justice. En effet, la dématérialisation peut offrir un certain nombre d'outil à même de rapprocher le justiciable de l'administration judiciaire, notamment lorsqu'il est géographiquement éloigné des juridictions. Le numérique peut en revanche produire l'effet inverse. La complexité d'une procédure numérisée de même que d'éventuels bugs peuvent aboutir à empêcher une action en justice de prospérer, en raison du formalisme informatique. Le cas

échéant, ces contraintes numériques peuvent aboutir à priver le justiciable d'un recours. Dans ces circonstances, le droit d'accès au juge, démembrement du droit au procès équitable, pourrait permettre de protéger les parties contre les conséquences néfastes d'une numérisation de la procédure. C'est justement le point de vue que semble adopter la Cour européenne des droits de l'homme, à l'occasion d'un arrêt Xavier Lucas contre France, rendu le 9 juin 2022 (15). L'espèce portait sur un recours en annulation formait contre une sentence arbitrale. En principe, le recours litigieux devrait être transmis par voie électronique en application des articles 1495 et 930-1 alinéa 1er du Code de procédure civile. Néanmoins, la plateforme e-barreau prévu à cette fin ne permettrait pas de saisir un « recours en annulation d'une sentence arbitrale » sous cet intitulé. Le requérant n'avait donc pas respecté ce formalise informatique et transmis son recours de manière traditionnelle, arguant d'une « cause étrangère » dispensant des formalités électroniques. Le problème procédait sans doute d'une erreur humaine: l'hypothèse du recours en annulation d'une sentence arbitrale n'avait pas été envisagé lors de la configuration de la plateforme de sorte qu'aucune entrée correspondante n'était proposé aux requérant. Pourtant, la Cour de cassation va écarter la recevabilité du recours, faisant preuve d'une particulière rigueur (16), que vont lui reprocher les juges de la Cour de Strasbourg. En effet, la Cour européenne va sanctionner le raisonnement des juges français, jugeant qu'en « faisant prévaloir le principe de l'obligation de communiquer par voie électronique pour saisir la cour d'appel sans prendre en compte les obstacles pratiques auxquels s'était heurté le requérant pour la respecter, la Cour de cassation a fait preuve d'un formalisme que la garantie de la sécurité juridique et de la bonne administration de la justice n'imposait pas et qui doit, dès lors, être regardé comme excessif » (17). Le raisonnement ne conduit pas à remettre en cause la légitimité du formalise électronique mais seulement à en stigmatisé les excès, d'autant plus lorsque les circonstances de l'espèce démontre qu'un plaideur diligent ne pouvait pas raisonnablement satisfaire ces exigences. On peut espérer qu'un même raisonnement trouvera

(15) CEDH, 9 juin 2022, Xavier Lucas c/France, n. 15567/20, D. 2022. 2330, obs. Clay; ibid. 2023. 571, obs. Fricero; AJ FAM. 2022. 353, obs. Eudier; DALLOZ IP/IT 2022. 352, obs. Nalbant; JCP 2022. 785, obs. Milano; ibid. 1345, obs. Mayer; Gaz. Pal. 25 oct. 2022, p. 56, note Plissonnier.

(16) Cass. 26 sept. 2019, no 18-14.708 P: D. actu. 2 oct. 2019, note Bléry; ibid. 29 oct. 2019, obs. Jourdan-Marques; D. 2019. 1891; ibid. 2435, obs. Clay; JCP 2019. 1185, note Weiller; ibid. 1349, note Ortscheidt: JCP E 2019. 1554, note Casson; Gaz. Pal. 19 nov. 2019, p. 25, note Bensaude.

(17) CEDH, 9 juin 2022, Xavier Lucas c/France, préc. §57.

à s'appliquer chaque fois que la numérisation d'une procédure conduit à restreindre les droits des justiciables.

b) *Les droits de la défense*

La numérisation de la procédure peut s'accompagner d'une dématérialisation du procès. Cette dématérialisation est totale pour certaine procédure comme les injonctions de payer pour les petits litiges, elle est seulement partielle d'en d'autres procédures par exemple lorsque qu'une des parties n'est pas physiquement présente à l'audience mais seulement via un dispositif de visioconférence. Dans les deux cas, ça n'est pas tant la numérisation de la procédure mais de l'audience elle-même qu'il est question. Or, cela suscite inévitablement des difficultés sur le terrain du contradictoire. L'absence de présence physique des parties à l'audience pourrait affecter le déroulement de la procédure. Pourtant, une telle démarche a été envisagé en France, à l'occasion de la crise covid. La crise sanitaire perturbait grandement les audiences. Notamment, les parties contaminé ou susceptible de l'être ne pouvait pas se présenter ce qui emportait un risque de renvoie systématique des affaires. Pour pallier cette difficulté, l'article 2 de l'ordonnance du 18 novembre 2020 devait permettre d'imposer aux parties le recours à la visioconférence et ceux dans toutes les procédures ouvertes devant les juridictions pénales. Si l'idée de permettre d'assurer la continuité du service public de la justice à cette période était louable, la méthode retenue en revanche interpellait et avait suscité de vives réactions de la doctrine, des magistrats et des avocats. Une disposition analogue adopté pendant la première période de la pandémie avait déjà été censuré par le conseil constitutionnel dans une décision du 4 juin 2021. Il y a été jugé que l'obligation de recourir à la visioconférence sans le consentement des parties, devant les juridictions pénales, portait une atteinte aux droits fondamentaux. Plus exactement, le Conseil constitutionnel avait visé dans sa décision l'article 16 de la Déclaration des droits de l'homme et du citoyen de 1789 qui dispose que *« Toute société dans laquelle la garantie des droits n'est pas assurée, ni la séparation des pouvoirs déterminée, n'a point de Constitution » et duquel découle les droits de la défense. Appliqué au texte litigieux, le Conseil déduit qu'il* « résulte de tout ce qui précède que, eu égard à l'importance de la garantie qui peut s'attacher à la présentation physique de l'intéressé devant la juridiction pénale et en l'état des conditions dans lesquelles s'exerce le recours à ce moyen de télécommunication, ces dispositions portent une atteinte aux droits de la défense que ne pouvait justifier le contexte sanitaire particulier résultant de l'épidémie de covid-19 durant leur période d'application. Sans qu'il soit besoin d'examiner les autres griefs, elles doivent donc

être déclarées contraires à la Constitution » (18). Le Conseil d'État va se prononcer en sens équivalent en mobilisant pour sa part un autre fondement, celui du droit au procès équitable issue de l'article 6§1 de la Convention européenne des droits de l'homme. Il est ainsi jugé que les dispositions de l'article 2 de l'ordonnance du 18 novembre 2020 permettent au juge d'imposer au justiciable le recours à des moyens de télécommunication audiovisuelle devant l'ensemble des juridictions pénales. Elles ne soumettent l'exercice de cette faculté à aucune condition légale et ne l'encadrent par aucun critère. Eu égard à l'importance de la garantie qui s'attache à la présentation physique du justiciable devant la juridiction pénale, ces dispositions portent une atteinte au droit à un procès équitable garanti par l'article 6 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales que ne peut justifier le contexte de lutte contre l'épidémie de covid-19 » (19). Ces deux décisions sont instructives dans la mesure où elle n'exclut pas de manière générale et absolu le recours à des dispositifs de visioconférence. D'abord, on comprends que ce sont les garanties qui tiennent au procès pénale qui sont en cause, de sorte que rien ne semble interdire des mesures équivalente pour les procédures civiles. On peut comprendre que la singuarité du procès pénal et notamment la place qu'occupe le principe de personnalisation de la peine explique que l'absence de présence physique des parties à l'audience puisse avoir une influence déterminante sur l'issue du litige. Les mêmes enjeux ne se retrouve pas dans les procèdures civiles. En revanche, certains contentieux ont un objet également personnel qui pourrait justifier un même principe d'interdiction, notamment pourles procédures qui tiennent au droit de la famille ou à l'état des personnes. Ensuite, les interdictions ici évoqués sont en parties justifier par l'absence d'encadrement du pouvoir du juge d'imposer aux parties le recours à la visioconférence, laissant ainsi penser qu'un pouvoir non discrétionnaire et strictement encadré pourrait être compatible avec les droits de la défense. On peut sans trop de difficulté penser que la visioconférence ne présente pas systématiquement des dangers majeurs. En revanche, le cas échéant, peut-être qu'il ne serait pas suffisant de se contenter de recourir à la visioconférence, sans aucune autre adaptation des règles de procédures.

(18) Conseil Constitutionnel, 4 juin 2021, DC n. 2021-911/919 QPC, §10.
(19) CE, 4 aout 2021, n. 447916.

2.4.1.2. *De lege ferenda, la consécration de principe directeur du procès numérique*

a) *Principes directeurs du procès 2.0*

Le Code de procédure civile français s'ouvre par un chapitre consacré au « principes directeur du procès ». Au gré de vingt-quatre articles, le Code énumère des règles fondamentales qui guident l'ensemble du procès civil et les règles de procédures qui s'y appliquent. On y retrouve des principes tel que la publicité des débats (art. 22 CPC), la réparation de la charge de la preuve (art. 9) ou encore le principe du contradictoire (art. 14). Ces principes servent de boussoles pour l'applications de l'ensemble des règles de procédures. L'identification de risques propres aux procédures numériques pourrait justifier la consécration de nouveaux principes destinés à encadrer la numérisation du procès ([20]).

b) *Un principe de subsidiarité*

La numérisation des procédures judiciaires présentes plusieurs vertues. Elle peut notamment servir un objectif d'accessibilité et de célérité. En ce sens, elles doivent être accueilli avec enthousiasme. Ce constat n'est néanmoins pas absolu et ne saurait s'appliquer uniformément à tous les contentieux. Il est des domaines dans lesquels l'usage de procédés numériques pourrait au contraire nuire à la qualité de la justice. Les illustrations précédemment envisagées démontrent qu'il existe des risques non négligeables que ce processus de numérisation se fasse au détriment des justiciables. Sans doute que tous les contentieux ne se prêtent pas de la même manière à la numérisation et ils ne devraient dès lors être envisagés que lorsqu'ils servent une meilleure justice. C'est dès lors un principe de subsidiarité qui devrait gouverner le déploiement des outils numériques. Ce principe de subsidiarité permettrait d'éviter plusieurs écueils. D'abord, cela nécessiterait une politique globale et concertée sur les futures applications de ces systèmes, évitant que des ressources puissent être gaspillées dans le développement de projets qui n'iront pas à leur terme ou qui seraient inefficaces. Ensuite, cela éviterait l'éventuelle fuite en avant que produisent bien souvent les progrès techniques. Ainsi, une fois qu'un outil est déployé, notamment lorsqu'il permet un gain de temps substantielle, il y a risque non négligeable que l'on renonce à en abandonner l'usage même si des insatisfactions ou dysfonctionnement sont constatés. *In fine*, le principe de subsidiarité permettrait une réflexion plus générale sur la justice numérique et une concertation préalable, associant les diverses parties prenantes à tel ou tel

([20]) S. Merabet, *Hommage posthume à l'abandon de* DataJust*: des principes directeurs de la justice numérique*, in *Revue Pratique de la prospective et de l'innovation*, 2022-1, 4.

type de contentieux, pour penser collectivement les usages les plus vertueux de ces outils.

c) *Un principe d'accessibilité*

Le droit en général, et la procédure en particulier, sont complexes et technique. Cette technicité est inhérente à la discipline. C'est notamment pour pallier cette complexité que sont pensé les auxiliaires de justice et que la représentation par avocat est rendu obligatoire dans de nombreuses procédures. Aussi, il s'agit là d'une difficulté incompressible qui relève de la matière juridique elle-même. En revanche, il ne faudrait pas qu'à cette technicité du droit s'ajoute une technicité informatique, en raison de la numérisation des règles de procédures. C'est pourquoi il convient de s'assurer que chaque fois que des règles de procédures recourt à des outils numériques, un principe d'accessibilité commande leur conception et leur mise en œuvre. Ce principe d'accessibilité peut être assuré par divers procédés, qui tiennent à la fois aux professionnels du droit et aux justiciables.

En premier lieu, c'est la formation des professionnels de la justice qui est déterminante. La procédure numérique n'est envisageable qu'à la condition que l'ensemble des parties prenantes en maîtrise les rouages. À défaut, le risque est que l'issue d'un litige ne dépende plus de la seule règle de droit, mais de sa mise en œuvre numérique. La technique informatique pourrait alors prendre le pas sur la technique juridique. On pourrait alors s'inquiéter de l'émergence d'un ordre numérique, primant sur un ordre juridique. Ce serait par exemple le cas si une partie voit ses prétentions accueillies non pas parce qu'elle emporte la conviction d'un magistrat, mais parce qu'elle a une meilleure maîtrise de l'outil informatique.

En second lieu, l'accessibilité passe encore par un accompagnement des justiciables. La formation professionnelle aux outils numériques peut suffire à l'accessibilité de la justice lorsque la représentation par avocat est obligatoire. Il en va autrement en revanche pour les autres procédures. Dès lors qu'une part conséquente de la population est frappé d'illectronisme, l'on ne saurait déployer largement des systèmes de justice numérique sans se préoccuper de leur capacité à s'en saisir. En aucun cas l'accès à la justice ne peut être empêché ou rendu plus difficile par l'informatique. Le numérique peut rapprocher certains justiciables de la justice, mais il peut dans le même temps en écarter d'autres. En pratique, cela signifierait que chaque procédure numérisée doit être accessible autrement, par des moyens plus traditionnels. C'est d'ores et déjà le cas en France pour les procédures qui relèvent de e-barreau, mais qui peuvent être accessibles autrement pour les justiciables qui n'étant pas représentés n'ont pas accès à la plateforme. À terme, la cohabitation systématique de procédures classiques et numériques pourrait

peut-être susciter des difficultés d'organisation néanmoins. Des alternatives pourraient peut-être être envisagées, pour assurer le service public de la justice, comme des guichets de proximité dans lesquels les justiciables pourraient être accompagnés pour réaliser les formalités nécessaires. En toute hypothèse, il est certain que la numérisation de la justice devra systématiquement s'accompagner de mesures destinées à garantir l'accès effectif au juge.

d) *Un principe d'humanité*

Depuis la Révolution industrielle est évoqué la crainte de voir l'Homme remplacé par la machine. La révolution numérique renouvelle cette menace ancienne. Des outils les plus simples comme la visioconférence ou l'informatique au plus élaborés comme les systèmes d'intelligence artificielle, il y a risque que la progression du numérique s'accompagne d'un recule des personnes qui participent au système judiciaire, qu'il s'agisse des avocats, magistrats ou encore des greffiers. Le manque de moyens chronique de la justice et l'allongement des délais de procédures qui en découlent pourrait conduire à tel résultat. La CEPEJ s'en inquiète et estime que « *la digitalisation de la justice doit rendre la justice plus efficace, mais ne doit jamais chercher à remplacer le juge. Le juge doit rester au centre de la procédure* ». Les professionnels du droit eux-mêmes expriment cette inquiétude. Le 23 novembre 2021, près de 3000 magistrats français publiaient une tribune pour s'inquiéter des conséquences du manque de moyen de la justice. Ils dressaient un constat inquiétant: « *Notre justice souffre de cette logique de rationalisation qui déshumanise et tend à faire des magistrats des exécutants statistiques, là où, plus que nulle part ailleurs, il doit être question avant tout d'humanité* » (*L'appel des 3000, Le Monde, 23 nov. 2021*). Pour prévenir ces dangers, il est nécessaire de s'assurer qu'à chaque étape de la procédure, même lorsqu'elle est numérisée, les parties puissent accéder à un interlocuteur humain, pour s'assurer de son bon déroulement. L'objectif serait ainsi d'éviter par exemple qu'un recours soit irrecevable seulement parce qu'une difficulté serait intervenue avec un formulaire informatique.

III.

DIGITALE IDENTIFIZIERUNG UND ELEKTRONISCHE KOMMUNIKATION IM DEUTSCHEN ZIVILPROZESS (*)

di *Jonathan Hager* e *Wolfgang Hau*

3.1. Einleitung

Die Ziviljustiz ist eine wichtige Säule der Judikative eines jeden Rechtssystems und spielt eine entscheidende Rolle bei der Lösung von Streitigkeiten zwischen Privatpersonen, Unternehmen und staatlichen Einheiten. In diesem Zusammenhang steht Deutschland als größte Volkswirtschaft Europas im internationalen Fokus. Erfreulicherweise stellen sich die Struktur, Effizienz und Fairness des deutschen Zivilprozesses im Vergleich relativ gut dar (1). Ein anderes Bild ergibt sich leider dann, wenn man die Digitalisierung des Zivilprozesses betrachtet. Nach einer Studie aus dem Jahr 2022 befindet sich Deutschland mehrere Jahre hinter dem internationalen Durchschnitt (2). Als Hauptgründe dafür werden der Mangel an dem für die

(*) La Scuola superiore della magistratura ha provveduto ad effettuare una libera traduzione, non revisionata dagli Autori, del presente saggio. La traduzione può essere consultata in appendice.

(1) So steht Deutschland im Vergleich mit 140 Ländern nach dem *WJP Rule of Law Index* 2022 an vierter Stelle, abrufbar unter <https://worldjusticeproject.org/rule-of-law-index/global/2022/Germany/Civil%20Justice/> (alle zitierten Internetseiten wurden zuletzt am 22. August 2023 aufgerufen).

(2) Studie der Boston Consulting Group, Bucerius Law School und Legal Tech Deutschland: "The Future of Digital Justice", 2022, S. 9.

Digitalisierung notwendigen Personal sowie eine technologie-averse Haltung der Entscheidungsträger genannt (3). Dennoch wird die Fortentwicklung des Zivilprozesses durch digitale Möglichkeiten auch hierzulande von allen Seiten der Rechtswissenschaft diskutiert und betrieben. Der Gesetzgeber beabsichtigt die Digitalisierung bereits seit geraumer Zeit und hat sich die Effizienzsteigerung von Zivilverfahren durch Digitalisierung in der aktuellen Legislaturperiode auf den Plan geschrieben (4). So haben im Laufe der letzten Jahre einige Mechanismen ihren Eingang in unsere Zivilprozessordnung gefunden, wie beispielsweise eine aktive Pflicht zur elektronischen Übermittlung von Prozessunterlagen für bestimmte Beteiligte gemäß § 130d ZPO (5) oder die kommende Pflicht für Gerichte zur Führung einer elektronischen Akte gemäß § 298a Abs. 1 S. 1 ZPO. Andererseits bestehen weiterhin massive Hürden, wie beispielsweise Unstimmigkeiten innerhalb der Regierung zur Finanzierung (6).

Der vorliegende Beitrag widmet sich dem aktuellen Stand der Digitalisierung des deutschen Zivilprozesses. Die Darstellung folgt dem Gang eines Zivilprozesses, von der Einreichung der Klageschrift bis zur Vollstreckung des Urteiles. Besondere Aufmerksamkeit wird dabei der Identifizierung von Absendern sowie digitalen Zugangsmöglichkeiten geschenkt.

3.2. Beginn des Zivilprozesses

3.2.1. *Eingang der Klage bei Gericht*

Gemäß § 253 Abs. 1 ZPO wird ein Zivilprozess grundsätzlich mit Einreichung der Klage bei Gericht anhängig. Die Klageschrift kann — und muss in manchen Fällen sogar — gemäß §§ 130a, 169 Abs. 4 ZPO als elektronisches Dokument bei Gericht eingereicht werden.

3.2.1.1. *Elektronische Form*

Laut § 130a Abs. 3 S. 1 ZPO gibt es zwei Arten, ein elektronisches Dokument einzureichen: es wird entweder mit einer qualifizierten elektro-

(3) Ebenda.

(4) Koalitionsvertrag der aktuellen Regierung, abrufbar unter <https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf>, S. 84.

(5) Deutsche Zivilprozessordnung, Gesetz vom 5. Dezember 2005 (BGBl. I 3202), zuletzt geändert durch Art. 19 des Gesetzes vom 22. Februar 2023 (BGBl. 2023 I 1), im Folgenden „ZPO".

(6) Vgl. die 93. Konferenz der Justizministerinnen und —minister vom 10. November 2022 (Beschluss zu TOP I.16).

nischen Signatur der verantwortenden Person versehen (Variante 1, dazu *a*) oder einfach signiert und auf einem „sicheren Übermittlungsweg" eingereicht (Variante 2, dazu *b*). Wenn bei der elektronischen Übersendung der Klageschrift keine dieser beiden Voraussetzungen eingehalten wird, so beispielsweise bei einer Übersendung der Klageschrift als Anhang einer einfachen E-Mail, ist die prozessuale Form nicht gewahrt; die Klage ist dann nicht ordnungsgemäß eingereicht und prozessual gegenstandslos.

a) *Qualifizierte elektronische Signatur*

Die qualifizierte elektronische Signatur im Sinne von § 130a Abs. 3 S. 1 Var. 1 ZPO ist eine fortgeschrittene elektronische Signatur (vgl. Art. 3 Nr. 11 i.V.m. Art. 26 eIDAS-VO (7)), die von einer qualifizierten elektronischen Signaturerstellungseinheit erstellt wurde und auf einem qualifizierten Zertifikat für elektronische Signaturen beruht (Art. 3 Nr. 12 eIDAS-VO). In Deutschland wird dies durch besondere Software- und Hardwarekomponenten sichergestellt: Der Signaturschlüssel wird auf einer zuvor beantragten Chipkarte gespeichert, die mithilfe eines Kartenlesegerätes nach Eingabe einer PIN gelesen wird. Möglicherweise könnte dieses Verfahren zukünftig durch eine Fernsignatur vereinfacht werden, wonach der Nutzer mit einer besonderen Software den Zugriff bei einem sog. Vertrauensdiensteanbieter erhält; bei diesem Anbieter verbleibt dann die Signaturerstellungseinheit und der Nutzer muss sich lediglich via App oder Webanwendung einloggen (vgl. auch Erwägungsgrund 52 eIDAS-VO) (8).

Das Dokument kann entweder mit der Signatur als weitere Datei versehen werden („*detached*") oder die Signatur kann in das Dokument aufgenommen werden und als eine Datei versendet werden („*inline*") (9). Gemäß § 4 Abs. 2 ERVV (10) muss auch bei Absendung mehrerer Dokumente (beispielsweise einer Klage, die mit einem Antrag auf einstweiligen Rechtsschutz verbunden

(7) Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. 2014 L 257/73), im Folgenden „eIDAS-VO".

(8) *Riehm*, in: Fest/Gomille (Hrsg.), *Festschrift für Johannes Hager zum 70. Geburtstag*, 2021, S. 71, 78.

(9) *Herberger*, in: Riehm/Dörr (Hrsg.), *Digitalisierung und Zivilverfahren*, 2023, S. 293, Rn. 13.

(10) Verordnung über die technischen Rahmenbedingungen des elektronischen Rechtsverkehrs und über das besondere elektronische Behördenpostfach, in der Fassung der Bekanntmachung vom 24. November 2017 (BGBl. I 3803), zuletzt geändert durch Art. 6 des Gesetzes zum Ausbau des elektronischen Rechtsverkehrs mit den Gerichten und zur Änderung weiterer Vorschriften vom 5. Oktober 2021 (BGBl. I 4607), im Folgenden „ERVV".

ist) jedes Dokument einzeln signiert werden; eine Signatur für einen sog. Container mehrerer Dokumente ist somit nicht zulässig (11).

Der Vorteil einer qualifizierten gegenüber einer einfachen oder fortgeschrittenen Signatur ist, dass das Dokument nicht zwangsläufig auf einem sicheren Übermittlungsweg im Sinne von § 130a Abs. 4 ZPO übertragen werden muss. Gemäß § 130a Abs. 2 S. 2 ZPO in Verbindung mit § 4 Abs. 1 ERVV darf das Dokument auch an das elektronische Gerichts- und Verwaltungspostfach gesendet werden (12). Dieses bereits seit mehreren Jahren genutzte Postfach ist zwischen den Gerichten der einzelnen Bundesländer unterschiedlich ausgestaltet, da im Rahmen des föderalistischen Systems Deutschlands die Justizverwaltung in den Aufgabenbereich der Länder fällt. In den meisten Ländern loggt man sich auf einer vom Gericht zur Verfügung gestellten Plattform ein und lädt dort das entsprechende Dokument hoch. Gemeinsam haben die Postfächer aber, dass die Nachrichten Ende-zu-Ende verschlüsselt sind und durch Wahrung des sog. OSCI-Standards (13) ein Abfangen oder Manipulieren nahezu ausgeschlossen sind.

Die Übermittlungsmöglichkeiten in § 130a ZPO sind abschließend. Daraus folgt, dass elektronische Dokumente, selbst wenn sie qualifiziert signiert wurden, nicht als einfache E-Mail versendet oder dem Gericht auf einem Dateiträger übergeben werden können (14).

b) *Einfach signierte Dokumente*

Soll ein einfach signiertes Dokument im Sinne von § 130a Abs. 3 S. 1 Var. 2 ZPO an das Gericht gesendet werden, muss dies zwangsläufig auf einem sicheren Übermittlungsweg im Sinne von § 130a Abs. 4 ZPO geschehen. Die „Sicherheit" bezieht sich dabei nicht auf IT-Sicherheit, sondern auf das Erfordernis, einen sicheren Rückschluss auf die Identität des Absenders ziehen zu können (15). In der Praxis wird Anwälten trotzdem regelmäßig von der Übermittlung einfach signierter elektronischer Dokuments abgeraten, weil auf diesem Wege die Dokumente nicht gleichermaßen vor nachträglicher Manipulation geschützt sind (16).

Einfache Signaturen sind gemäß Art. 3 Nr. 10 eIDAS-VO beigefügte Daten in elektronischer Form, die der Unterzeichner zum Unterzeichen

(11) BGH, 5. Mai 2019 – VII ZB 570/18, NJW 2019, 2230.

(12) Siehe <http://www.egvp.de>.

(13) „Standard Online Services Computer Interface", hierbei werden die Nachrichteninhalte von den erforderlichen Nutzdaten bei der Übermittlung getrennt; *Müller*, E-Justice - Praxishandbuch, 6. Aufl. 2021, S. 37.

(14) BeckOK ZPO/*von Stelle*, 49. Edition 2023, § 130a, Rn. 13.

(15) *Müller*, E-Justice – Praxishandbuch, S. 28.

(16) Ebenda.

verwendet. Dafür genügt es bereits, dass der Unterzeichner seinen Namen schriftlich beifügt. Eine eigenhändige (eingescannte oder auf einem Touchpad vorgenommene) Unterschrift ist nicht erforderlich. Der praktisch wichtigste Übermittlungsweg sind besondere Postfächer, die von den Absendern verwendet werden und sich je nach Natur der Prozesspartei unterscheiden. Für die Einrichtung eines solchen Postfachs muss die Identität des Nutzers gesondert bestätigt werden. In der Praxis erhält der Nutzer danach eine Chipkarte, mit der er sich mithilfe eines Kartenlesegerätes und einer PIN vor jeder Nutzung anmelden muss. Praktisch am relevantesten ist das besondere elektronische Anwaltspostfach („beA", § 31a Abs. 6 BRAO [17]). Auch Behörden und juristische Personen des öffentlichen Rechts haben ein solches Postfach [18]. Notaren und Steuerberatern steht die Absendung über ein entsprechendes Postfaches offen [19] und auch natürliche sowie juristische Personen des Privatrechts können seit dem 1. Januar 2022 ein besonderes Postfach einrichten (§ 130 Abs. 4 Nr. 4 ZPO, §§ 10 ff. ERVV).

Die Praktikabilität dieser Vorgehensweise wird vor allem für natürliche Personen stark in Zweifel gezogen, weil das Identifizierungs- und Einrichtungsverfahren relativ aufwendig ist. Allerdings kann jeder, der die Online-Funktion seines Personalausweises aktiviert hat, eine Identifizierung ohne gesonderte Chipkarte oder Kartenlesegerät vornehmen. Erschwerend kommt aber hinzu, dass die entsprechende Software von Drittanbietern zu beziehen und kostenpflichtig ist. Die Kosten starten bei ca. 20 EUR pro Monat, sodass sich eine Einrichtung für ein Gerichtsverfahren für einzelne Betroffene kaum lohnt. Bürger können außerdem ein bestehendes Konto zur elektronischen Kommunikation mit der Verwaltung nunmehr zu Justizkommunikation verwenden. Aber auch hierfür muss zuvor eine Prüfung der Identität des Nutzers durch eine öffentliche Stelle erfolgen, sodass die Nutzbarkeit für Bürger auch auf diesem Wege noch nicht ohne logistische Hürden gewährleistet ist. Für Unternehmen kommt zusätzlich ein qualifiziertes elektronisches Siegel in Betracht, Art. 38 eIDAS-VO.

Der Vollständigkeit halber sei noch der Versand über ein besonderes E-Mail-Konto gemäß § 130a Abs. 4 S. 1 Nr. 1 ZPO genannt, für dessen Nutzung der Absender seine Identität gesondert bestätigen muss („De-Mail"). Diese Möglichkeit wird in der Praxis allerdings kaum noch genutzt; der Hauptanbieter des Dienstes, die Telekom, hat den Dienst bereits zum 31. August 2022 abgeschaltet.

---

(17) Bundesrechtsanwaltsordnung, Gesetz vom 1. August 1959 (BGBl. I 565), zuletzt geändert durch Gesetz vom 10. März 2023 (BGBl. I 64).

(18) Besonderes elektronisches Behördenpostfach („beBPo").

(19) Besonderes elektronisches Notar- bzw. Steuerberaterpostfach („beN" bzw. „BStBK").

c) *Ausgestaltung der Klageschrift*

Die Klageschrift ist gemäß § 2 Abs. 1 S. 1 ERVV grundsätzlich im PDF-Format, ausnahmsweise für die verlustfreie Darstellungen von Bildern im TIFF-Format zu übermitteln. Daraus folgt, dass die Klageschrift nur Text- und Bilddateien enthalten kann. Es ist nicht möglich, Audio- oder Videodateien in einen Schriftsatz oder Anlagen einzubetten, diese müssen separat mitgeschickt werden. Beweismittel können, soweit sie in digitaler Text- oder Bildform vorliegen, als Anlage der Klage beigefügt werden. In der Praxis wird dem Gericht häufig ein USB-Stick übergeben, der die Beweismittel in Dateiform enthält. Physische Beweismittel, wie insbesondere Originalurkunden, müssen weiterhin analog an das Gericht übermittelt werden. Einem Scan kommt dabei kaum Beweiswert zu (dazu sogleich unter C.III.3.a)).

3.2.1.2. *Aktive Nutzungspflicht*

Zusammenfassend kann ein elektronisches Dokument, auch wenn es einfach signiert ist, auf einem sicheren Übermittlungsweg, in der Praxis somit unter Nutzung besonderer Postfächer, an das Gericht übersendet werden. Ist das Dokument qualifiziert elektronisch signiert, kann es alternativ auch über eine Plattform an das elektronische Gerichtspostfach gesendet werden. Ob daneben auch herkömmliche Einreichungsmöglichkeiten (klassischerweise die Übermittlung eines unterschriebenen Schriftstückes per Post, Telefax oder Boten) genutzt werden dürfen, hängt von der Natur der beteiligten Parteien ab.

a) *Natürliche Personen*

Natürliche Personen können ohne anwaltliche Hilfe Klage vor den Amtsgerichten erheben. Diese sind — stark vereinfacht — für Streitigkeiten unter einem Gegenstandswert von 5.000 EUR und für alle Ansprüche aus Wohnraummietverhältnissen zuständig (§ 23 GVG ([20])). Möchte eine natürliche Person eine Klage erheben, kann sie dabei den elektronischen Übermittlungsweg nutzen, muss dies aber nicht; denn sie darf die Klage auch mündlich zu Protokoll der Geschäftsstelle eines Gerichts erheben. Dafür ist aber die physische Anwesenheit bei Gericht erforderlich, sodass aktuell noch nicht von einer digitalen Klageerhebung auf diesem Wege gesprochen werden kann. Eine Verbesserung soll nun ein Gesetzgebungsverfahren bringen, das eine Änderung von § 129a ZPO vorsieht: Künftig sollen Klagen

([20]) Gerichtsverfassungsgesetz, in der Fassung der Bekanntmachung vom 9. Mai 1975 (BGBl. I 1077), zuletzt geändert durch Gesetz vom 19. Dezember 2022 (BGBl. I 2606), im Folgenden „GVG".

auch mündlich per Video gegenüber der Geschäftsstelle erhoben werden können (21).

b) *Juristische Personen des Privatrechts*

Entsprechendes wie für natürliche Personen gilt für juristische Personen des Privatrechts, welche auf dem gleichen Wege durch einen Vertreter eine Klage zum Amtsgericht einreichen können.

c) *Anwälte*

Bei den nächsthöheren Zivilgerichten, den Landgerichten, muss eine Klage durch einen Anwalt eingereicht werden, damit sie wirksam ist (§ 78 Abs. 1 S. 1 ZPO). Die Gerichte sind gemäß § 71 Abs. 1 GVG grundsätzlich für alle Zivilstreitigkeiten mit einem Streitwert über 5.000 EUR zuständig.

Anwälten verbleiben seit dem 1. Januar 2022 gemäß § 130d S. 1 ZPO keine alternativen Übersendungsmöglichkeiten für Klagen, Anlagen und alle weiteren vorbereitenden Schriftsätze. Vielmehr müssen die Schriftsätze elektronisch übermittelt werden, damit sie prozessual beachtlich sind (22). Einige Ausnahmen dieser aktiven Nutzungspflicht sieht das Gesetz aber vor, namentlich gemäß § 130d S. 2 ZPO, wenn die Übermittlung aus technischen Gründen nicht möglich ist, gleich ob sie aus der Sphäre des Gerichts, des Softwareanbieters oder des Absenders stammen (23). Eine weitere Ausnahme besteht bei Dokumenten besonderer Größe gemäß § 3 ERVV in Verbindung mit § 5 Abs. 1 Nr. 3 ERVV. Höchstens 1.000 Dateien und 200 Megabyte dürfen übermittelt werden. (24) Diese Grenze wurde über die Jahre kontinuierlich nach oben verschoben und dürfte auch künftig weiter angehoben werden. Eine Schwachstelle des Postfachs ist allerdings bis heute das umständliche Interface sowie fehlende Kompatibilität mit den gängigsten Kanzleisoftwares. (25) Ein Schriftsatz kann nicht unmittelbar aus dem Datenmanagementprogramm einer Kanzlei versendet werden.

d) *Juristische Personen des öffentlichen Rechts und Behörden*

Alle Behörden und juristische Personen des öffentlichen Rechts unterliegen der gleichen Nutzungspflicht wie die Anwaltschaft, § 130d S. 1 ZPO.

---

(21) Gesetzentwurf der Bundesregierung zur Förderung des Einsatzes von Videokonferenztechnik in der Zivilgerichtsbarkeit und den Fachgerichtsbarkeiten, abrufbar unter <https://dserver.bundestag.de/brd/2023/0228-23.pdf>, im Folgenden „Gesetzentwurf".

(22) BGH, 24. November 2022 – IX ZB 11/22, NJW 2023, 525, Rn. 7.

(23) BT-Drucksache 17/12634, 27.

(24) Zweite Bekanntmachung zu § 5 der Elektronischer-Rechtsverkehr-Verordnung vom 10. Februar 2022.

(25) *Müller*, E-Justice – Praxishandbuch, S. 17 f.

Sie sind gleichermaßen verpflichtet, ein besonderes elektronisches Behördenpostfach einzurichten und zu nutzen.

e) *Notare, Steuerberater und Gerichtsvollzieher*

Diese Beteiligten müssen ein besonderes Postfach zwar einrichten und unterhalten (unterliegen also einer passiven Nutzungspflicht), können Schriftsätze an das Gericht aber weiterhin auch mit herkömmlichen Mitteln übersenden (§ 173 Abs. 2 S. 1 Nr. 1 Var. 2-4 ZPO).

3.2.2. *Weiterleitung der Klage durch das Gericht an den Beklagten*

Ist die Klage wirksam bei Gericht eingereicht worden, stellt das Gericht die Klage dem Beklagten förmlich zu. Die Art und Weise ist in den §§ 173 ff. ZPO geregelt.

3.2.2.1. *Keine Pflicht zur elektronischen Zustellung*

Gemäß § 173 Abs. 1 ZPO ist die elektronische Zustellung seit dem 1. Januar 2023 an erster Stelle der Vorschriften über Zustellungsformen geregelt. Eine Pflicht zur elektronischen Zustellung für die Gerichte ergibt sich daraus noch nicht. Andere Zustellungsformen — wie etwa die möglichen postalischen Zustellungsformen physischer Dokumente in §§ 175 ff. ZPO — können weiterhin im Rahmen des gerichtlichen Auswahlermessens genutzt werden (26). Andererseits wird der Urkundsbeamte die elektronische Zustellungsform als einfachste, sicherste und kostengünstigste Form auswählen, sofern auf Empfängerseite ein sicherer Übermittlungsweg besteht.

3.2.2.2. *Digitales Postfach der Verfahrensbeteiligten und passive Nutzungspflicht*

Voraussetzung für die Zustellung eines elektronischen Dokuments ist gemäß § 173 Abs. 1 ZPO, dass der Empfänger einen sicheren Übermittlungsweg geschaffen hat, damit seine Identität bei der Zustellung eindeutig gesichert ist. Eine Zustellung an das E-Mail-Postfach der Beteiligten ist damit nicht möglich, auch dann nicht, wenn eine qualifizierte elektronische Signatur verwendet wurde (27). Ob ein sicherer Übermittlungsweg geschaffen werden muss, hängt auch auf Empfängerseite von der Natur der Partei ab.

(26) BT-Drucksache 19/28399, 34 f.
(27) *Schultzky*, MDR 2022, 201, 204 Rn. 18.

a) *Anwälte, Behörden, Notare, Steuerberater, Gerichtsvollzieher und andere professionelle Prozessbeteiligte*

Die aktive Nutzungspflicht von Anwälten, Behörden und juristischen Personen des öffentlichen Rechts (28) spiegelt sich in einer passiven Nutzungspflicht wider (§ 173 Abs. 2 S. 1 Nr. 1 Var. 1, Nr. 2 ZPO). Aber auch Notare, Gerichtsvollzieher und Steuerberater müssen einen Übermittlungsweg für die Zustellung elektronischer Dokumente eröffnen (§ 173 Abs. 2 S. 1 Nr. 1 Var. 2-4 ZPO).

Für die in § 173 Abs. 2 ZPO genannten Personen wird durch ein elektronisches Empfangsbekenntnis nachgewiesen, dass das Dokument tatsächlich beim Empfänger zugegangen ist. Das elektronische Empfangsbekenntnis geht über eine automatisierte Empfangsbestätigung hinaus, weil es seinem Inhalt nach nicht nur den Eingang im Postfach, sondern persönlich bei der Person des Empfängers bestätigt. Dies ist bedeutsam, weil ein Nachweis über die Zustellung eines Dokuments nicht anders geführt werden kann (§ 175 Abs. 4 ZPO) (29). Das Empfangsbekenntnis ist ein Relikt des deutschen Rechts aus Zeiten physischer Dokumente, das inzwischen im Zusammenhang mit elektronischem Dokumentenaustausch unpraktikabel und systemfremd erscheint (30). In der Praxis können die Softwares der besonderen Postfächer aber die Anforderung eines Empfangsbekenntnisses automatisch erkennen und beantworten. Da dieser Weg aber zuvor besondere Einstellungen in der Software voraussetzt, schlagen zahlreiche Stimmen vor, *de lege ferenda* eine automatisierte Empfangsbestätigung ausreichen zu lassen (31).

b) *Natürliche Personen und juristische Personen des Privatrechts*

Natürliche und juristische Personen des Privatrechts betrachtet das Gesetz als regelmäßig weniger professionelle Verfahrensbeteiligte. Daher kann ihnen ein Dokument auf elektronischem Wege nur dann zugestellt werden, wenn sie der elektronischen Zustellung zugestimmt haben. Sie müssen daher selbst aktiv werden. Die Zustimmung gilt gemäß § 173 Abs. 4 S. 2 ZPO als erteilt, wenn sie zuvor ein Dokument elektronisch bei Gericht eingereicht haben, d.h. praktisch ein besonderes Postfach eingerichtet und darüber einen Schriftsatz versandt haben. Ein Zustellungsnachweis über Empfangsbekenntnis kennt das Gesetz in diesem Fall nicht. Stattdessen gilt das Dokument im Wege der Fiktion (also unabhängig von tatsächlicher

(28) Vgl. oben unter B.I.2.c), *d*).

(29) Rechtsanwälte trifft darüber hinaus eine standesrechtliche Rücksendungspflicht gemäß § 14 der Berufsordnung für Rechtsanwälte.

(30) *Herberger*, in: Riehm/Dörr (Hrsg.), *Digitalisierung und Zivilverfahren*, S. 290, Rn. 7.

(31) *Stürner*, ZZP 2022, 369, 377; *Bernhardt*, jM 2022, 90, 91.

Kenntnisnahme) am dritten Tag nach dem auf der automatisierten Eingangsbestätigung ausgewiesenen Eingangstags als zugestellt. Liegt weder eine Zustimmung noch anwaltliche Vertretung der Person vor, so verbleibt es gemäß §§ 174 ff. ZPO bei den herkömmlichen Zustellungsmethoden.

3.3. Weiterer Gang des Zivilprozesses

3.3.1. *Aktenführung*

Mit Eingang der Klage wird diese nicht nur dem Beklagten zugestellt, das Gericht legt auch eine Akte an. Aktuell kann dies gemäß § 298a Abs. 1 S. 1 ZPO elektronisch geschehen, ab dem 1. Januar 2026 ist dies sogar verpflichtend. Obwohl auch die Ausgestaltung der elektronischen Akte Ländersache ist, haben sich die Länder in zwei Gruppen zusammengeschlossen und zwei miteinander kompatible Systeme entwickelt. Der Aufbau der elektronischen Akte entspricht im Grundsatz dem einer physischen Akte: Die eingegangenen Dokumente werden chronologisch abgelegt und mit eigenen Seitenzahlen versehen. Wird ein Schriftstück physisch eingereicht, ist es einzuscannen und zur Akte zu nehmen (§ 298a Abs. 2 ZPO). Beweismittel können allerdings nur bedingt Bestandteil der e-Akte werden. Dabei kommt es auf die Form des Beweismittels an (32). Für Dokumente ist das nur dann der Fall, wenn sie bloße Text- oder Bilddateien ohne Anspruch auf Originalität sind. Etwas anderes gilt für Originalurkunden: Diese können nicht ersetzend digitalisiert werden und werden daher physisch bei Gericht aufbewahrt (33). Soweit Audio- oder Videodateien Bestandteil der Beweismittel sind, ist der aktuelle Stand der e-Akte noch nicht so weit, diese in die Akte selbst mitaufzunehmen. In der Praxis wird häufig ein PDF-Platzhalter geschaffen, der einen Link auf die anderswo gespeicherte Datei enthält (34). Physische Asservate zum Zwecke des Augenscheins werden analog bei Gericht verwahrt und die Akte mit entsprechenden Verweisen versehen.

3.3.2. *Mündliche Verhandlung*

Wendet man sich der Digitalisierung der mündlichen Verhandlung, namentlich durch Videoverhandlungen zu, so waren solche in der Theorie schon seit dem 1. Januar 2002 gemäß § 128a ZPO möglich. Aber erst seit der

(32) Dazu sogleich unter C.III.

(33) *Jansen/Schlicht*, in: Riehm/Dörr (Hrsg.), *Digitalisierung und Zivilverfahren*, S. 308, Rn. 9.

(34) Ebenda.

Covid-19 Pandemie wurde von dieser Möglichkeit nennenswerter Gebrauch gemacht. Videoverhandlungen sind in den letzten Jahren erheblich angestiegen und erreichten zeitweise Quoten von über 50 Prozent (35). Ob eine Videoverhandlung durchgeführt wird, liegt im Ermessen des Gerichts, ein Anspruch der Parteien hierauf besteht nicht. Ein aktueller Gesetzesentwurf soll dieses Ermessen deutlich in Richtung der Anordnung einer Videoverhandlung verschieben (36). Das Gericht muss sich nach heute geltendem Recht im Sitzungssaal aufhalten. Der Grundsatz der Öffentlichkeit wird dadurch gewahrt, dass im Sitzungssaal über die Bildschirme die Verhandlung verfolgt werden kann. Eine vollständig digitale mündliche Verhandlung sieht die ZPO noch nicht vor, ist aber im nunmehr vorgesehen (37). Die Übertragung der Verhandlung in das Gerichtsgebäude soll beibehalten werden.

Eine Ton- oder Videoaufzeichnung der Verhandlung ist gemäß § 128 Abs. 3 S. 1 ZPO verboten, selbst bei Einverständnis der Beteiligten. Auch einer abgesonderten Videoaufnahme einzelner Vernehmungen steht die herrschende Meinung selbst bei ausdrücklicher Zustimmung des Zeugen ablehnend gegenüber (38). Der aktuelle Gesetzesentwurf schlägt demgegenüber zumindest eine vorläufige Videoaufzeichnung der Verhandlung zum Zwecke der Protokollanfertigung vor (39). Problematisch werden weiterhin Verfahren betrachtet, bei denen sich mindestens eine Partei im Ausland befindet (40). Nach der in Deutschland herrschenden Sichtweise würde eine Videoverhandlung dem völkerrechtlichen Souveränitätsgrundsatz widersprechen, da so faktisch Staatsgewalt auf fremden Territorium ausgeübt werde (41). Dem kann entgegengehalten werden, dass solange die Teilnahme an der Verhandlung auf Freiwilligkeit beruht, von staatlichem Zwang keine Rede sein kann (42). Die Absendung von Schriftsätzen zur Vorbereitung der mündlichen Verhandlung kann gleichermaßen von fremden Territorien vorgenommen werden. Da Schriftsätze vor allem bei umfangreicheren Zivil-

(35) *Irskens*, in: Riehm/Dörr (Hrsg.), *Digitalisierung und Zivilverfahren*, S. 429, Rn. 2.

(36) Gesetzentwurf, <https://dserver.bundestag.de/brd/2023/0228-23.pdf>.

(37) Ebenda.

(38) *Mantz/Spoenle*, MDR 2020, 637, 639 Rn. 14; *Irskens*, in: Riehm/Dörr (Hrsg.), *Digitalisierung und Zivilverfahren*, S. 437, Rn. 30; *Schultzky,* NJW 2003, 313, 314. Abweichend Zöller/*Greger*, ZPO, 34. Aufl. 2022, § 128a ZPO, Rn. 9.

(39) Gesetzentwurf, <https://dserver.bundestag.de/brd/2023/0228-23.pdf>.

(40) Eingehend dazu *Voß*, in: Reuß/Windau (Hrsg.), *Göttinger Kolloquien zur Digitalisierung des Zivilverfahrensrechts*, Bd. 1, 2022, S. 43.

(41) BGH, 5. November 1999 – 1 StR 286-99, NJW 1999, 3788, 3789 (zum Strafverfahren); Musielak/Voit/*Stadler*, ZPO, 20. Aufl. 2023, § 128a, Rn. 8; Zöller/*Greger*, § 128a, Rn. 10, jeweils mit weiteren Nachweisen.

(42) *Stürner*, ZZP 2022, 369, 392.

verfahren den Großteil der Entscheidung bereits vorbereiten, stellt sich die Frage, weshalb Erklärungen in der mündlichen Verhandlung einen darüberhinausgehenden Zwangscharakter haben sollen.

3.3.3. *Beweisaufnahme*

3.3.3.1. *Vernehmung von Beweispersonen*

Die Vernehmung von Zeugen, Sachverständigen und Parteien kann grundsätzlich per Video stattfinden und in das Sitzungszimmer übertragen werden (§§ 284 S. 2, 128a Abs. 2 ZPO). Im Unterschied zur Teilnahme der Parteien und ihrer Vertreter an der mündlichen Verhandlung ist die Vernehmung zur Beweisaufnahme nur auf Antrag einer Partei möglich. Das Gericht ist nicht an den Antrag gebunden und entscheidet über ihn im freien Ermessen. Entgegen dem Trend der mündlichen Verhandlungen zu Videoterminen sind Vernehmungen Videoübertragungen immer noch die Ausnahme. So wird insbesondere die Beurteilung der Glaubhaftigkeit von Zeugenaussagen über Video als deutlich schwieriger angesehen (43), was wiederum in kritischen Fällen durch einen verantwortungsvollen Umgang der Richterschaft mit ihrem Ermessen vermieden werden kann (44). In Zukunft soll die Anordnung einer Videovernehmung auch ohne Antrag ergehen können; den betroffenen Beteiligten soll aber ein Widerspruchsrecht zustehen (45).

3.3.3.2. *Augenscheinnahme*

Die Darstellung von Beweismittel in originär digitaler Form unterfällt ohne Weiteres den Regeln über den Augenscheinbeweis, also §§ 371 ZPO ff. Hat das Beweismittel physische Gestalt, ist noch nicht gesetzlich geregelt, ob der Beweis aufgrund von §§ 284 S. 2, 128a Abs. 2 ZPO im Wege digitaler Darstellungsformen möglich sein soll. Dies wird bereits *de lege lata* von einer verbreiteten Ansicht bejaht (46), und der aktuelle Gesetzesentwurf sieht eine ausdrückliche Klarstellung vor (47). Es bleibt dann aber allemal dabei, dass sich der Beweis sinnvollerweise digital auch führen lassen muss. Da sich der Augenschein, trotz der missverständlich engen deutschen Bezeichnung, auf

(43) Zurückhaltend *Glunz*, Psychologische Effekte beim gerichtlichen Einsatz von Videotechnik, 2012.

(44) Vgl. BT-Drucksache 17/12418, S. 14.

(45) Gesetzesentwurf, https://dserver.bundestag.de/brd/2023/0228-23.pdf.

(46) Zöller/*Greger* § 128a, Rn. 7; *Schultzky,* NJW 2003, 313, 314. Abweichend Musielak/Voit/*Stadler*, § 128a, Rn. 5.

(47) Gesetzentwurf, <https://dserver.bundestag.de/brd/2023/0228-23.pdf>.

alle Sinneswahrnehmungen beziehen kann, kommt eine digitale Beweisführung nicht in Betracht, sofern es um Haptik, Gerüche oder Geschmäcker geht. Geht man davon aus, dass Bild- und Tondateien als Augenscheinbeweis zulässig sind (bzw. demnächst aufgrund der geplanten Gesetzesänderung sein werden), stehen den Parteien grundsätzlich alle Möglichkeiten offen. So können sie, wenn reine Bild- oder Tonaufzeichnungen nicht ausreichen, auch moderne Beweismittel wie VR-Darstellungen oder 3D-Simulationen anbieten. Im Wesentlichen muss die Datei dem analogen Augenschein funktional gleichwertig sein. Das Gericht entscheidet im Rahmen seines Ermessens, ob dies der Fall ist und damit, ob das Beweismittel digital oder analog beizubringen ist (48).

3.3.3.3. *Dokumente*

a) *Physische Urkunden*

Der Beweis über physische Urkunden ist grundsätzlich gemäß § 420 ZPO durch Vorlage der Originalurkunde zu führen. Parteien mit aktiver Nutzungspflicht des elektronischen Rechtsverkehrs (49) haben dem Gericht gemäß §§ 130d, 131 ZPO auch eine digitale Kopie zu übersenden. Die Vorlage einer originalen physischen Urkunde hat den Vorteil, dass sie gemäß § 416 ZPO ohne Rücksicht auf die Überzeugung des Gerichts vollen Beweis dafür begründet, dass die in ihr enthaltenen Erklärungen von den behaupteten Ausstellern stammen, sie also „echt" ist.

Der Scan einer Urkunde kann zwar vorgelegt werden, die Datei ist dann aber lediglich Augenscheinobjekt. Das bedeutet, dass sie in der Beweiswürdigung berücksichtigt werden kann, ein Beweis über ihre Echtheit aber nicht geführt ist. Aufgrund der Gefahr von Manipulationen bei eingescannten Dokumenten wird ihnen die weitreichende Beweiskraft von § 416 ZPO nicht zugebilligt (50). Dass damit nur Originalurkunden taugliches Beweismittel über ihre Echtheit sein können, wird von vielen Stimmen kritisiert: Aufgrund der elektronischen Aufbewahrung von Dokumenten in vielen Privathaushalten und Unternehmen ist die Gefahr eines Beweisverlustes relativ hoch. Der Rechtssicherheit wäre damit im Umgang mit der Aktenführung, die in der Praxis bereits häufig rein digital stattfindet, gedient, wenn die Beweiskraft gescannter Urkunden *de lege ferenda* gestärkt werden würde (51).

---

(48) *Irskens*, in: Riehm/Dörr (Hrsg.), *Digitalisierung und Zivilverfahren*, S. 440, Rn. 37.

(49) Vgl. dazu oben unter B.I.2.c), *d*).

(50) *Irskens*, in: Riehm/Dörr (Hrsg.), *Digitalisierung und Zivilverfahren*, S. 441, Rn. 39.

(51) *Irskens*, in: Riehm/Dörr (Hrsg.), *Digitalisierung und Zivilverfahren*, S. 453, Rn. 71 m.w.N.

Von deutlich höherer Beweiskraft sind öffentliche Urkunden in digitalisierter Form. Das Original begründet unabhängig von der Überzeugung des Gerichts gemäß § 415 ZPO den vollen Beweis dafür, dass die Erklärung einschließlich der darin wiedergegebenen Begleitumstände wie zum Beispiel Zeit und Ort der Vornahme, Behörde und aufnehmende Person richtig und vollständig mit dem Inhalt abgegeben wurde, der in der Urkunde niedergelegt ist ([52]). Wird eine Urkunde durch eine öffentliche Behörde eingescannt, korreliert die Beweiskraft des Scans nach § 371b ZPO mit der des Originals; auch die Echtheit des Scans wird in diesem Fall vermutet (§ 437 ZPO).

b) *Elektronische Dokumente*

Elektronische Dokumente sind nach deutschem Verständnis immer Augenscheinbeweise und entfalten nur besondere Beweiswirkungen über Sondervorschriften. Selbst besondere, in der eIDAS-VO genannte Beweismittel wie beispielsweise das qualifizierte elektronische Einschreiben sind keine Urkunden nach dem Verständnis der ZPO. Die entsprechenden Vermutungsregelungen wie etwa Art. 43 Abs. 2 eIDAS-VO gelten stattdessen unmittelbar gemäß Art. 288 AEUV.

Einfache elektronische Dokumente wie beispielsweise E-Mails, Chatverläufe oder Überwachungsdaten unterliegen als Augenscheinobjekte der freien Beweiswürdigung nach § 286 Abs. 1 ZPO. Bestreitet der Prozessgegner die Echtheit des Dokuments, muss die beweispflichtige Partei dies beweisen, beispielsweise durch Vorlage eines Sendungsprotokolls oder Übergabe des einen Chatverlauf enthaltenen Smartphones an einen Sachverständigen. Gleiches gilt für Dateien mit einer fortgeschrittenen elektronischen Signatur gemäß Art. 3 Nr. 11, Art. 26 eIDAS-VO. Ihr kann aber im Rahmen der Beweiswürdigung erhöhte Überzeugungskraft zukommen.

Liegt ein elektronisches Dokument mit einer qualifizierten elektronischen Signatur gemäß Art. 3 Nr. 12 eIDAS-VO vor, so gilt die unwiderlegbare Beweisregel des § 416 ZPO ([53]) entsprechend (§ 371a Abs. 1 ZPO), solange sich die Signatur auf die entsprechenden Erklärungen bezieht. Öffentliche elektronische Dokumente entfalten die Beweiswirkung über ihren Inhalt auch ohne qualifizierte elektronische Signatur (§ 371a Abs. 3 S. 1 in Verbindung mit § 415 ZPO). Ist eine solche Signatur darüber hinaus mit dem Dokument verbunden, begründet sie zusätzlich gemäß § 371a Abs. 3 S. 2 in Verbindung mit § 437 ZPO den vollen Beweis über ihre Echtheit. Stammt das elektronische Dokument von einer ausländischen Behörde, ist die Beweiskraft über ihren Inhalt dieselbe. Aber selbst im Falle einer

([52]) BeckOK ZPO/*Krafka*, 49. Edition 2023, § 415, Rn. 19.

([53]) Siehe oben unter C.III.3.a).

qualifizierten elektronischen Signatur wird die Echtheit nicht vermutet, weil für solche Dokumente kein entsprechender Verweis in den §§ 371 ff. ZPO auf § 416 ZPO enthalten ist (54).

3.4. Urteil und Vollstreckung

Im Rahmen der elektronischen Aktenführung kann auch das Urteil in elektronischer Form ergehen (§ 130b ZPO). Für eine erfolgreiche Vollstreckung ist aber gemäß §§ 724 Abs. 1, 725 ZPO nach wie vor eine vollstreckbare Ausfertigung des Urteils erforderlich; diese kann nur in Papierform erteilt werden (§ 317 Abs. 2 S. 1, Abs. 3 ZPO). Für den Vollstreckungsantrag gilt das gleiche wie für die Klageschrift: Auch auf Vollstreckungsebene ist für Anwälte, Behörden und juristische Personen des öffentlichen Rechts die digitale Einreichung verpflichtend (§ 753 Abs. 5 in Verbindung mit § 130d ZPO).

Ist das Gericht das zuständige Vollstreckungsorgan (so bei der Vollstreckung in Geldforderungen), kann der Antrag ohne weiteres zur e-Akte genommen werden. Vollzieht hingegen ein Gerichtsvollzieher die Vollstreckung (so bei der Pfändung beweglicher Sachen), bringt der digitale Antrag noch wenig Fortschritt: Gerichtsvollzieher müssen zwar gemäß § 173 Abs. 2 S. 1 Nr. 1 ZPO einen sicheren Übermittlungsweg für elektronische Zustellungen eröffnen, gleichzeitig aber *de lege lata* ihre Akten weiterhin in Papierform führen; denn § 298a ZPO gilt für sie nicht. Das kann dazu führen, dass ein ausgedrucktes Dokument auf Anwaltsseite eingescannt und digital übermittelt wird und der Gerichtsvollzieher dieses dann wieder ausdruckt. Um das zukünftig zu verhindern, wird die Einführung eines rein digitalen elektronischen Titelregisters gefordert, um künftig auf analoge vollstreckbare Ausfertigungen verzichten zu können (55). Schon heute erstellt der Gerichtsvollzieher immerhin die Vermögensauskunft des Schuldners nach § 802f Abs. 5 ZPO in digitaler Form und leitet sie elektronisch an das Gericht weiter, das sie digital verwaltet (§§ 802f Abs. 6, 802k Abs. 1 S. 1 ZPO). Zudem können Gerichtsvollzieher im Internet die Auskünfte einsehen, um zu entscheiden, ob eine erneute Einholung notwendig ist. Soll eine Sache versteigert werden, kann dies auf einer Internetplattform gemäß § 814 Abs. 2 Nr. 2 ZPO geschehen.

---

(54) *Kienzle*, NJW 2019, 1712, 1714.

(55) Die Arbeitsgruppe „Modernisierung des Zivilprozesses“ veröffentlichte im Jahr 2021 ein in Deutschland viel beachtetes Diskussionspapier im Auftrag der höheren Gerichte und des Bundesgerichtshofs, zugänglich unter <www.justiz.bayern.de/media/images/behoerden-und-gerichte/oberlandesgerichte/nuernberg/diskussionspapier_ag_modernisierung.pdf>, S. 106 f. (im Folgenden „Diskussionspapier“).

3.5. Fazit

Zusammenfassend lässt sich sagen, dass die Digitalisierung von Zivilverfahren in Deutschland inzwischen bedeutende Fortschritte erzielt hat. Bereits seit dem 1. Januar 2018 können fast alle Gerichte (56) rechtsverbindlich auf elektronischem Wege angerufen werden, und die digitale Weiterverarbeitung der Dokumente wird spätestens mit Geltung der e-Akten-Pflicht ab dem 1. Januar 2026 gesichert sein.

Allerdings besteht durchaus noch Reformbedarf in mehrfacher Hinsicht. Insbesondere zur Rechtsdurchsetzung natürlicher und juristischer Personen, die nicht regelmäßig mit Gerichten in Berührung kommen, wäre eine vereinfachte Kommunikation mit der Justiz wünschenswert. Hierzu wird vorgeschlagen, das elektronische Gerichtspostfach für einfach signierte elektronische Dokumente zu eröffnen (57). Denkbar erscheinen für die Durchsetzung geringerer Streitwerte auch ein vollständig digitales, beschleunigtes Verfahren (58) oder ein deutschlandweit einheitlich ausgestaltetes Justizportal der Zivilgerichte (59). Für Anwaltsprozesse wird zur Effizienzsteigerung gefordert, eine elektronische Austauschplattform für Nachrichten und Dokumente in Gerichtsverfahren zu schaffen (60). Problematisch ist im Rahmen der Verhandlung insbesondere das Verbot einer Videoverhandlung mit Verfahrensbeteiligten, die aus dem Ausland teilnehmen. Ferner wirkt sich der geringe Beweiswert gescannter Urkunden negativ auf die Praxis digitaler Aktenführung in Unternehmen und bei Privatpersonen aus.

In Anbetracht der fortschreitenden Entwicklung der letzten Jahre stellt dieser Beitrag eine bloße Momentaufnahme in einem andauernden Reformprozess dar. Auch weiterhin ist es an der Rechtswissenschaft, der Legislative und weiteren involvierten Interessengruppen, die bestehenden Probleme zu lösen und unter Ausgleich von neuen Möglichkeiten mit den Interessen der Prozessbeteiligten und den Prinzipien des Rechtsstaats den Zivilprozess an die digitale Wirklichkeit der Privatwirtschaft anzupassen.

---

(56) Eine Ausnahme besteht noch hinsichtlich des Bundes- und einiger Landesverfassungsgerichte.

(57) Diskussionspapier, S. 29 f.

(58) Diskussionspapier, S. 76 ff.

(59) Diskussionspapier, S. 10 ff.

(60) Diskussionspapier, S. 26 f.

Parte IV
IDENTITÀ E DIRITTI DEI PRIVATI

I.
IDENTITÀ DIGITALE TRA DATI PERSONALI E RELAZIONI FUNZIONALI

di *Giuseppe Corasaniti*

Sommario: 1.1. La nozione digitale di identità. — 1.2. Il Sistema Pubblico di Identità Digitale (SPID) e il Regolamento eIDAS. — 1.3. Identificazione e identificabilità: il tema della protezione dei dati personali. — 1.4. Identità e domicilio digitale. — 1.5. Metodi di autenticazione digitale ed identità: temi e problemi di quadro.

1.1. La nozione digitale di identità

L'articolo 1 del Codice dell'Amministrazione Digitale (d.lgs. 7 marzo 2005, n. 82) [1] definisce, alla lettera *u-quater*, un concetto ben preciso di "*identità digitale*" che è ogni "r*appresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale*".

Si tratta quindi di una definizione aperta, qualificabile da un lato con una "rappresentazione" di carattere informatico, cioè con una vera e propria funzione riproduttiva, che peraltro viene utilizzata dallo stesso codice per definire il documento informatico (dallo stesso articolo alla lettera *p*), definito come documento (elettronico) "*che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti*".

La norma definisce cioè quello che appare una corrispondenza univoca e coerente tra un determinato utente e i suoi specifici attributi identificativi finalizzata alle relazioni ed alle transazioni operanti in ambiente digitale. Ed è una dimensione, questa, nella quale si riconoscono da un lato una opzione operativa propria e libera del soggetto interessato, e dall'altro quello che è

---

[1] Sulla dimensione funzionale del CAD cfr. E. De Giovanni, *Il codice dell'Amministrazione digitale: genesi, evoluzione, principi costituzionali e linee generali*, in *Rassegna Avvocatura dello Stato*, 3/2018, 155; B. Carotti, *Il correttivo al Codice dell'amministrazione digitale: una meta-riforma*, in *Giornale di diritto amministrativo*, 2/2018, 131 e *L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice*, in *Giornale di diritto amministrativo*, 1/2017, 7.

l'aspetto (tecnico) legato alle credenziali che assume in determinati ambienti digitali, ovvero il suo modo di essere riconosciuto dal punto di vista soggettivo attraverso l'associazione sistematica ad un "insieme" di dati (a lui) esclusivamente riferibili e raccolti e registrati in quella che è la forma digitale.

Si tratta, in altre parole, di quei dati mediante i quali ogni sistema informatico "riconosce" l'utente, lo abilita allo svolgimento di determinate funzioni applicative, lo inserisce ad un livello specifico di abilitazione all'accesso alle informazioni che raccoglie e che l'utente stesso immette o che è abilitato sistematicamente a consultare o a modificare.

Si tratta perciò di una definizione molto ampia che ricomprende soprattutto una associazione logica, espressa in chiave alfanumerica di una descrizione formale ad un riconoscimento che si lega da un lato all'esercizio di una opzione operativa da parte del soggetto interessato e dall'altro dalle modalità con le quali egli accede al sistema informatico ed è riconosciuto come tale dal sistema stesso.

Tali modalità, che poi sono determinate tecnicamente dall'art. 64 e, sul piano tecnico, dal decreto attuativo di competenza dell'AgIG, corrispondono nella loro interazione e nel loro effetto abilitativo ad un nucleo centrale di diritti definito dall'art. 3 nella sua dimensione essenziale di "*cittadinanza digitale",* funzionale all'uso generalizzato (cioè pubblico innanzitutto e privato) e soprattutto "effettivo" delle tecnologie informatiche (2) che peraltro ben si coordina con la garanzia di partecipazione al procedimento amministrativo informatico (art. 4), con le comunicazioni in modalità digitale tra imprese e amministrazioni pubbliche (art. 5-*bis*), con il "diritto" alla domiciliazione digitale (art. 6) a "conoscere i domicili digitali delle amministrazioni" che sono inseriti in un apposito elenco pubblico (art. 6-*ter*) e al diritto di fruire di servizi on line semplici e integrati (art. 7).

Si tratta quindi di un vero e proprio diritto soggettivo (così art. 3, n. 1-*quinquies* del Codice) riconosciuto a cittadini e ad imprese in termini di assegnazione (o di libera opzione) per un'identità digitale (3) attraverso la quale utilizzare i servizi erogati in rete dai soggetti pubblici in un quadro di

(2) P. Lopriore, *L'effettività del diritto all'uso delle tecnologie nel Codice, dell'Amministrazione Digitale. La sentenza del T.A.R. Basilicata n. 478/2011*, in *Ciberspazio e Diritto*, 1/2012, 121; D. Passigli, *L'uso delle tecnologie dell'informazione e della comunicazione quale fattore di progresso nel rapporto tra i cittadini e la pubblica amministrazione. Potenzialità, rischi e problematiche anche alla luce delle recenti integrazioni al codice dell'amministrazione digitale*, in *Informator*, 3/2006, 9.

(3) Cfr. M. Nastri, *Identità personale, identità digitale e identificazione elettronica alla luce del decreto semplificazioni*, in *Notariato*, 6/2020, 608.

sostanziale legalità (4) che corrisponde a precisi obiettivi di ordine costituzionale (art. 97 Cost.) (5), e che nel contempo si delinea quale condizione comune per lo sviluppo in senso digitale e soprattutto interattivo di soggetti privati e pubblici, nell'ottica integrata europea della transizione digitale.

Privati e imprese, al pari dei professionisti, quei soggetti, cioè, che necessitano di un quadro relazionale costante tra di loro e operano congiuntamente per lo svolgimento di rapporti tanto di carattere interlocutorio che di carattere fiduciario e procedimentale o processuale hanno perciò, nella dimensione funzionale del Codice,un proprio ruolo specifico, come sembra confermato dall'art. 2 (*Finalità e ambito di applicazione*) che appunto al comma 2-*bis* (nel testo risultante dalle integrazioni del 2017) richiama il concetto comune di "*servizi fiduciari*" ed indica proprio l'*identità digitale* quale strumento intermedio tra la identificazione (da parte del soggetto pubblico con Carta di identità elettronica (art. 66 insieme alla Carta Nazionale dei servizi) e lo strumento informatico della identità digitale che vede la cooperazione pubblico-privato quale obiettivo qualificante per la costruzione di un sistema comune di identità digitali reciprocamente riconosciuto ed utilizzabile nelle varie relazioni e nelle differenti dimensioni della accessibilità digitale (6).

1.2. Il Sistema Pubblico di Identità Digitale (SPID) e il Regolamento eIDAS

Il quadro è sostanzialmente molto ampio e in esso confluiscono sistemi identificativi diversi: quello tipico di identificazione amministrativa (disciplinato dalle disposizioni del *Testo Unico sulla documentazione amministrativa*, d.p.r. 28 dicembre 2000, n. 445) e quello, molto più vasto, delle effettive e costanti relazioni economiche e istituzionali chiamate a operare ed a orga-

(4) Cfr. particolarmente le fondamentali osservazioni a riguardo di F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Il Diritto dell'informazione e dell'informatica*, 2/2015, 227.

(5) F. Luciani, *Brevi note sull'innovazione tecnologica come strumento di buona amministrazione*, in *La Cittadinanza europea*, 2/2022, p. 199.

(6) Un processo poi non privo di aspetti controversi e di controverso è stato definito di "commodificazione", v. M. Mursia M., C.A. Trovato, *The commodification of our digital identity: limits on monetizing personal data in the European context*, in *MediaLaws*, 2/2021, 165. Ma tale prospettiva inquadra insieme soggetti privati (volti a identificare ed a fidelizzare con il rilascio di identificazioni "integrate") e soggetti pubblici, che invece hanno esigenza di identificare con certezza gli interlocutori per una comunicazione efficace sui servizi. Proprio la prospettiva europea sembra muoversi nel senso della massima libertà di scelta degli utilizzatori accompagnata da idonee e forti garanzie e di privacy e di sicurezza dei dati personali.

nizzarsi sempre di più attraverso sistemi interattivi di carattere digitale, cioè connotati da una costante operatività interattiva che implica immediatezza e rapidità delle informazioni raccolte e diffuse e controlli tanto rapidi quanto automatici sulle comunicazioni e sulle transazioni di carattere digitale.

Il *Sistema Pubblico di Identità Digitale* (7) (in acronimo *SPID*) previsto dall'art. 64 del Codice è infatti il sistema "unico" o se si vuole "congiunto" di accesso che sfrutta appunto l'identità digitale per l'accesso ai servizi online della pubblica amministrazione italiana, e dei privati aderenti.

Cittadini e imprese possono quindi, con molta semplicità, avvalendosi di un provider privato che è appositamente autorizzato e controllato, accedere a tali servizi giovandosi di un (unico) sistema identificativo che ne permette l'accesso semplificato e la fruizione da qualsiasi dispositivo (anziché utilizzare un apposito lettore). Tale sistema sostanzialmente soddisfa quindi pienamente la esigenza di poter disporre di un uno *set* di credenziali in grado di garantire comunque l'accesso a qualsiasi servizio *web.* La normativa sostanziale, definita in linea generale dall'art. 64 del CAD è poi integrata da un notevole *corpus* di regolamentazioni tecniche di dettaglio spettanti all'AgID, nelle quali si sono definiti progressivamente requisiti specifici di conformità attraverso l'indicazione di *standards* relativi a sistemi informatici e dati e documenti trattati, sulla base di criteri comuni e di specifiche caratteristiche volte per lo più ad assicurare una immediata comprensione applicativa di requisiti richiesti dalla norma (8).

---

(7) Cfr. A. Contaldo, *La Carta Nazionale dei Servizi e l'identità digitale dopo l'introduzione di SPID,* in *Rivista Amministrativa della Repubblica Italiana*, 11-12/2019, 2, 643; M. Ferretti, *Servizi on-line e accesso SPID: il caso della Regione Toscana*, in *RU Risorse umane nella pubblica amministrazione*, 6/2018, 46; A. Contaldo, *La disciplina dello SPID e la definizione giuridica dei suoi gestori,* in *giustiziacivile.com*, 4/2017, 6; F. Trojani, *La Riforma del Codice dell'amministrazione digitale: una prima lettura a caldo: cittadinanza digitale, SPID e nuove forme di relazione tra cittadini/imprese e p.a.*, in *Comuni d'Italia*, 2/2016, 13; R. Titomanlio, *Considerazioni introduttive sul Sistema Pubblico per la Gestione dell'Identità Digitale (SPID)*, in *GiustAmm.it*, 3/2015, 9; L. Abba, V. Amenta, A. Lazzaroni, *L'identità digitale: dalle nuove frontiere del Sistema Pubblico di Identificazione (SPID) alle problematiche legate al "web"*, in *Ciberspazio e Diritto*, 1/2015, 11.

(8) L'art. 64 del CAD ha poi affidato all'agenzia per l'Italia digitale (AgID) il compito di attivare e sostanzialmente regolamentare il sistema SPID, mentre un successivo Decreto del Presidente del Consiglio dei Ministri del 24 ottobre 2014. Tale normativa attuativa ha definito caratteristiche generali di Spid, indicando tempi e modalità di adozione da parte di imprese e P.A.. L'AgID quindi ha provveduto a definire progressivamente la regolamentazione con propri atti delegati. Cfr. in particolare Determinazione 17 maggio 2018, n. 160. Per le linee guida dell'indice dei domicili digitali delle P.A. e dei gestori di pubblici servizi. Determinazione 4 aprile 2019, n. 97/2019. Per le linee guida su acquisizione e riuso di *software* per le pubbliche amministrazioni la Determinazione 9 maggio 2019, n. 115/2019. Per le linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati

È un sistema, quello dello SPID, che si presenta anche molto semplice nella utilizzazione per l'utente finale, e che presenta caratteristiche uniformi a livello nazionale, non esclusivo ma sostanzialmente inclusivo, e perciò pienamente integrabile al sistema europeo.

Attraverso una scelta di un modello (eventualmente integrato in piattaforme di gestione di servizi come posta elettronica certificata e firma digitale) cittadini e imprese possono così essere in grado di accedere ai servizi online della pubblica amministrazione e di altri soggetti aderenti, utilizzando un'unica identità digitale. Il che rappresenta un volano fondamentale per tutto il processo di digitalizzazione del Paese perché semplifica e rende sostanzialmente anche molto più sicuro l'accesso ai servizi online, garantendo nel contempo la protezione dei dati personali e la riservatezza delle informazioni. Il sistema consente di usufruire di alcuni fondamentali vantaggi, collegabili alla piena risoluzione del problema identificativo in ogni genere di rapporto digitale, almeno ad un livello di base, offrendo la possibilità di richiedere e ottenere documenti e certificati in formato digitale, di pagare le tasse e le bollette online, di accedere ai servizi sanitari e scolastici, e molte altre prestazioni. Le caratteristiche generali e gli ambiti di utilizzazione sono stati peraltro determinati con apposita regolamentazione amministrativa (9).

L'autenticazione con SPID prevede ben tre livelli di sicurezza delle credenziali, a seconda della tipologia di servizio richiesto. E ciò poi corrisponde in buona sostanza, nei suoi requisiti essenziali e funzionali, anche ai requisiti definiti dal regolamento UE eIDAS. (Regolamento UE 910/2014 (*electronic IDentification, Authentication and trust Services*) (10) che disciplina l'identificazione elettronica e i servizi fiduciari per le transazioni elettroniche

---

elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate, Determinazione 17 maggio 2019, n. 121. Per le linee guida per il rilascio dell'identità digitale per uso professionale, Determinazione 5 novembre 2019, n. 318/2019. Per le linee guida per la realizzazione di un modello R.A.O. pubblico Determinazione 21 novembre 2019, n. 344/2019. Per le Linee guida per la sottoscrizione elettronica di documenti vedi la Determinazione 23 marzo 2020, n. 157/2020. Per le Linee guida « La sicurezza nel procurement ICT » Determinazione 17 maggio 2020, n. 220/2020. Per le Linee guida tecnologie, e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici Linee guida sull'interoperabilità tecnica delle pubbliche amministrazioni, Determinazione 1 ottobre 2021, n. 547. Linee guida su OpenID Connect in SPID, Determinazione 2 dicembre 2021 n. 616/2021. Per un aggiornamento costante cfr. https://www.agid.gov.it/it/linee-guida

(9) D.p.c.m. 24 ottobre 2014 recante "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.

(10) G. Finocchiaro, *Una prima lettura del Reg. UE n. 910/2014 (c.d. "eIDAS"): identificazione "on line", firme elettroniche e servizi fiduciari (reg. UE n. 910/2014)*, in *Le Nuove leggi civili commentate*, 3/2015, 419.

nel mercato unico europeo. Il regolamento eIDAS, infatti, fissa norme generali e procedure comuni agli Stati membri, per garantire interazioni elettroniche effettivamente sicure fra cittadini, imprese e autorità pubbliche. In tale prospettiva generale viene incrementata la sicurezza e l'efficacia dei servizi elettronici e delle transazioni di e-business e commercio elettronico nell'Ue. Inoltre proprio tale regolamento costituisce ornai un riferimento costante e un quadro giuridico puntuale ed uniforme in materia di firme elettroniche, sigilli elettronici, validazioni temporali elettroniche, documenti elettronici, servizi elettronici di recapito certificato e servizi relativi ai certificati di autenticazione di siti *web*. Proprio tale normativa fissa le condizioni minime a cui gli Stati membri debbono fare riferimento per riconoscere i mezzi di identificazione elettronica delle persone fisiche e giuridiche che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro.

Il Regolamento eIDAS (attualmente in fase di revisione nell'ottica della costruzione di un unico "*Wallet*" di identità digitali europee integrato) pone le basi giuridiche per creare un mercato unico europeo dei servizi digitali. La prospettiva di riforma imminente secondo la Commissione europea ha l'obiettivo di pervenire ad una unica identità elettronica europea sicura con la conseguenza che ogni cittadino europeo possa avere modo di usare ovunque in Europa., una tecnologia unica per identificarsi in cui sia possibile anche il controllo di "quali dati e come vengono utilizzati". In sostanza la Commissione europea si pone ancora di più l'obiettivo di definire ben distinte aree regolamentari per offrire la più ampia copertura possibile dei sistemi di identificazione elettronica, l'accettazione reciproca di questi sistemi da parte degli Stati membri e infine l'uso costante dell'autenticazione transfrontaliera attraverso un unico sistema di servizi comuni di identificazione nello spazio europeo.

1.3. Identificazione e identificabilità: il tema della protezione dei dati personali

Quanto al rapporto problematico tra identità digitale (in trasformazione) e *privacy* (11) è da sottolineare che non può dubitarsi della natura di dato personale e dell'identificativo digitale così come delle sequenze univoche utilizzate per i processi di autenticazione che vi risultino in concreto abbi-

(11) A. Ortalda, S. Leucci, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD* in *Rivista italiana di informatica e diritto*, 1/2022, 2, 145, S. Calzolaio, "*Digital (and privacy) by default". L'identità costituzionale della amministrazione digitale,* in *Giornale di storia costituzionale*, 31/2016, 185.

nabili. Il riferimento al principio di "dato personale" utilizzato dal GDPR Regolamento (UE) n. 2016/679 (12), che stabilisce chiaramente all'art. 4 (n. 1) come dato personale sia da intendersi proprio *"qualsiasi informazione che riguarda una persona fisica identificata o identificabile*" e di conseguenza prevede una particolare protezione in ambito europeo appare sostanzialmente un assunto oggettivo.

Identificazione e *identificabilità* nell'ottica della protezione dei dati personali significano appunto una ben precisa caratterizzazione del dato, che è consistente nella abbinabilità univoca e sicura tra dato trattato e soggetto che ne è "titolare" in un rapporto di mediazione che si basa su un elemento centrale che è rappresentato dal consenso del soggetto interessato, ovvero dalla sua adesione consapevole ed informata ad ogni fase del processo di trattamento e di diffusione dei dati che lo riguardano (13).

Ne consegue che ogni trattamento di tali dati identificativi deve sempre avvenire nel rispetto dei fondamentali principi definiti all'art. 5 del GDPR di presidio funzionale di ogni trattamento da parte di soggetti pubblici o provati quali liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione, esattezza, limitazione della conservazione, integrità e riservatezza. Peraltro l'art. 9 del GDPR collega la possibilità di trattamento di dati personali da parte dei soggetti pubblici alle ipotesi in cui tale trattamento sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve comunque essere "proporzionato" alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere anche misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. E con particolare riguardo alla gestione di un sistema identificativo digitale si prospettano ampie garanzie che attengono al consenso ed alla utilizzabilità dei dati al di fuori di quello che appare l'obiettivo funzionale principale, liberamente prescelto

---

(12) L. Stilo, *La pubblica amministrazione tra diritto di accesso e trattamento dei dati personali*, in *Il Nuovo Diritto*, 11-12/2006, 1135.

(13) T. Pertot, *Personal data supplying: the issue of bundled consent*, in *Jus civile*, 3/2023, 673; M. Giuliano, *Dati personali, consenso e privacy nell'era digitale: sfide legali e implicazioni negoziali*, in *giustiziacivile.com*, 5/2023, 4; Gallo P., *Il consenso al trattamento dei dati personali come prestazione*, in *Rivista di diritto civile*, 6/2022, 1054; G. Versaci, *Consenso al trattamento dei dati personali e "dark patterns" tra opzionalità e condizionalità*, in *Le Nuove leggi civili commentate*, 5/2022, 1130; A. Purpura, *Il consenso nel mercato dei dati personali. Considerazioni al tempo dei "big data"*, in *Jus civile*, 4/2022, 891; V. D'Antonio, P. D'Elia, *The remuneration dynamics in consent to the processing of personal data,* in *Comparazione e diritto civile*, 3/2022, 773; R. Rolli, M. D'Ambrosio, *Consenso e "accountability": i poli del commercio dei dati personali "online*", in *P.A. Persona e Amministrazione,* 1/2022, 783; F. Castagna, *Trasparenza algoritmica e validità del consenso al trattamento dei dati personali, in Responsabilità civile e previdenza*, 1-2/2022, 501.

dagli interlocutori in un rapporto comunicativo essenziale limitato nella connotazione e nella diffusione ai soli aspetti intrinseci e dichiarati in quanto il dato identificativo è destinato a inserirsi nell'ambito di una interlocuzione limitata funzionalmente dal consenso prestato dal titolare dei dati personali in termini di utilizzazione e diffusione e conservazione non eccedente lo scopo presentato o prevedibile (14).

È di fondamentale importanza anche per la tematica del rapporto tra identità digitali e privacy anche il concetto di "base giuridica" che deve accompagnare ogni trattamento in base all'art. 6 del GDPR. Esso si riferisce essenzialmente alle finalità del trattamento e ne definisce la necessarietà per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

Tale base giuridica potrebbe contenere sempre disposizioni adeguate a garantire l''applicazione delle norme del regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto, quali quelle per specifiche situazioni di trattamento in base ai principi espressi dal diritto dell'Unione o degli Stati membri in rapporto ad un obiettivo di interesse pubblico che dovrebbe essere proporzionato all'obiettivo legittimo perseguito.

Quanto alla dimensione di tale prescrizione è agevole richiamare il considerando (41) che afferma che "*Qualora il presente regolamento faccia riferimento a una base giuridica o a una misura legislativa, ciò non richiede necessariamente l'adozione di un atto legislativo da parte di un Parlamento, fatte salve le prescrizioni dell'ordinamento costituzionale dello Stato membro interessato. Tuttavia, tale base giuridica o misura legislativa dovrebbe essere chiara e precisa, e la sua applicazione prevedibile, per le persone che vi sono sottoposte, in conformità della giurisprudenza della Corte di giustizia dell'Unione europea (la « Corte di giustizia ») e della Corte europea dei diritti dell'uomo.*" Peraltro anche altri considerando si riferiscono al medesimo principio chiarendo come da un lato ogni trattamento debba essere "manifestamente" fondato su di essa (46) e dall'altro che spetta al legislatore

(14) Cfr. diffusamente A. Ortalda, S. Leucci, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Rivista italiana di informatica e diritto*, 1/2022, 2, 145; E. Tosi, *Tutela della persona e circolazione dei dati: riservatezza, protezione dei dati personali, identità digitale (Prima parte)*, in *Studium iuris*, 11/2022, 1296.

(interno) prevedere per legge la base giuridica che autorizza le autorità pubbliche a trattare i dati personali (47) e che comunque *la base giuridica per un legittimo interesse del titolare del trattamento non dovrebbe valere per il trattamento effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti* (già regolati per legge).

Inoltre in tema di identità digitali si prospetta di particolare rilevanza l'art. 32 del GDPR, che attiene alla sicurezza del trattamento considera i margini "effettivi" di conoscenza tecnologica, dei costi di attuazione sopportabili, come pure la natura, l'oggetto, il contesto e le finalità del trattamento, o anche fattori di rischio comunque di varia probabilità e gravità per i diritti e le libertà delle persone fisiche (15). In tali termini quindi il titolare del trattamento e il responsabile del trattamento debbono sempre perciò mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza "adeguato" al rischio.

Tali misure comprendono, tra le altre, se del caso: *a*) la *pseudonimizzazione* e la cifratura dei dati personali; *b*) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la *resilienza* dei sistemi e dei servizi di trattamento; *c*) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; *d*) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

La norma prevede che nel valutare l'adeguato livello di sicurezza, si debba tener conto in special modo dei rischi presentati dal trattamento che

---

(15) In tali termini il titolare del trattamento e il responsabile del trattamento debbono perciò mettere in atto *misure tecniche e organizzative adeguate* per garantire un *livello di sicurezza adeguato al rischio*. Tali misure comprendono, tra le altre, se del caso: *a*) la pseudonimizzazione e la cifratura dei dati personali; *b*) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; *c*) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; *d*) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento. La norma prevede che nel valutare l'adeguato livello di sicurezza, si debba tener conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'adesione a un codice di condotta approvato o a un meccanismo di certificazione approvato (artt. 41 e 42) può sempre essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. Il titolare del trattamento e il responsabile del trattamento — in tale prospettiva — fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'adesione a un adeguato codice di condotta approvato o a un meccanismo di certificazione approvato (artt. 41 e 42) può ben essere utilizzata come elemento per dimostrare la conformità ai requisiti richiesti in via generale. Il titolare del trattamento e il responsabile del trattamento — in tale prospettiva — fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o dei singoli Stati membri.

È infatti lo stesso Codice dell'amministrazione digitale a specificare e sottolineare come "*Le disposizioni del presente Codice si applicano nel rispetto della disciplina in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice in materia di protezione dei dati personali approvato con decreto legislativo 30 giugno 2003, n. 196*" (art. 2 c. 5). Ora, al di là del richiamo normativo espresso, pur se evidentemente concepito anteriormente alla entrata in vigore del GDPR appare manifesto il ripetuto riferimento alla disciplina dei dati personali nei procedimenti generali di regolamentazione integrativa in tema di amministrazione digitale che hanno visto coinvolto il Garante per la protezione dei dati personali.

Di certo il testo dell'art. 50 del Codice in tema di disponibilità dei dati delle pubbliche amministrazioni (in vigore dal 2021) ne tiene conto ancora di più, prevedendo anche che i dati delle pubbliche amministrazioni siano sempre formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati in condizioni che rispettino quei *limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti,* che sono appunto fissati dalla normativa *in materia di protezione dei dati personali* ed il rispetto della normativa europea in materia di riutilizzo delle informazioni generali (dataset) del settore pubblico (16).

Ed ancora qualunque dato trattato da una pubblica amministrazione, con le esclusioni delle disposizioni in materia di accesso nei procedimenti amministrativi deve essere trattato nel rispetto della normativa in materia di protezione dei dati personali, è reso accessibile e fruibile alle altre amministrazioni, quando l'utilizzazione del dato sia necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, senza oneri a carico di

(16) G. Carullo, *"Open Data" e partecipazione democratica*, in *Istituzioni del Federalismo*, 3/2019, 685; A.F. Spagnuolo, Sorrentino E., *"Open data" per l'"e-democracy"*, in *Rivista italiana di informatica e diritto*, 1/2022, 2, 273.

quest'ultima, salvo per la prestazione di elaborazioni aggiuntive. Ed inoltre (comma 2-*bis*) sono proprio le pubbliche amministrazioni, nell'ambito delle proprie funzioni istituzionali, a procedere all'analisi sistematica dei propri dati anche in combinazione con quelli detenuti da altri soggetti privati abilitati fermi restando "*i limiti di cui al comma 1*", cioè appunto quelle limitazioni previste in via generale concernenti l'uso e la diffusione di dati personali acquisiti e trattati. La gestione delle identità digitali si svolge secondo appropriate modalità tecniche individuate dall'AgID con apposite Linee guida (17).

In tal senso le pubbliche amministrazioni certificanti detentrici dei dati ne assicurano la fruizione da parte dei soggetti che hanno diritto ad accedervi e assicurano, su richiesta dei soggetti privati coinvolti nel processo di certificazione digitale collegato al rilascio delle identità digitali, conferma scritta della corrispondenza di quanto dichiarato in sede di rilascio con le risultanze dei dati da essa custoditi, definendo (c.3-*bis*3 come ogni trasferimento di un dato da un sistema informativo a un altro non modifica la titolarità del dato e del trattamento, ferme restando le responsabilità delle amministrazioni che ricevono e trattano il dato in qualità di "titolari autonomi del trattamento", anche cioè al fine di individuare le specifiche responsabilità collegate agli adempimenti in tema di protezione di dati personali.

Come è noto l'art. 2 del CAD definisce anche ambiti normativi sottratti non certo in via generale alla sua applicazione, ma alla ristretta forma dell'esercizio delle attività e funzioni di ordine e sicurezza pubblica, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e consultazioni elettorali, nonché alle comunicazioni di emergenza e di allerta in ambito di protezione civile. E tale enunciazione appunto si prospetta articolata e forse problematica sotto il profilo della generale vigenza e validità di strumentazioni digitali previste dal Regolamento europeo eIDAS, fermo restando che tale deroga sembrerebbe comunque avere senso e appunto limitarsi ad aspetti di stretta aderenza all'esercizio di funzioni autonome tutte caratterizzate da uno stretto e specifico parametro di sicurezza identificativa che coincide con controlli specifici, con determinazioni particolarmente riservate o urgentissime correlabili tutte in termini di strettissima connotazione con forme rigidamente definite e qualificate per legge, anche sotto il

(17) P. Falletta, *Le linee guida dell'Agenzia per l'Italia digitale*, in *Giornale di diritto amministrativo*, 2/2021, 163; F. Notari, *Il percorso della digitalizzazione delle amministrazioni pubbliche: ambiti normativi mobili e nuovi modelli di "governance"*, in *Giornale di diritto amministrativo*, 1/2020, 21; D. Manetti, *Brevi note intorno alle "Linee guida contenenti le regole tecniche e raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate" rilasciate dall'AGID [Agenzia per l'Italia Digitale]*, in *Lo Stato Civile Italiano*, 12/2019, 21.

profilo della identificazione di specifici soggetti esercenti funzioni pubbliche o per la abilitazione formale di comunicazioni digitali in determinati procedimenti aventi regolamentazione autonoma, sorretta da un più elevato livello di sicurezza nelle transazioni identificative.

Pur tuttavia la stessa norma stabilisce che le disposizioni del Codice "*si applicano al processo civile, penale, amministrativo, contabile e tributario, in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico*". Il che in tutta evidenza ha suscitato nei commentatori qualche perplessità (18) tenuto conto dell'orientamento normativo omogeneo che è direttamente qualificabile in base al chiaro disposto di "apertura" e di non emarginazione degli strumenti fiduciari digitali "sicuri" che è alla base proprio del Regolamento europeo eIDAS, che si presta ad essere poi a divenire l'unico vero parametro di riferimento, in quanto normativa di portata generale congegnata proprio per una applicazione omogenea su tutto lo spazio giuridico e sul mercato comune europeo.

1.4. Identità e domicilio digitale

L'identità digitale è oggi qualificata perciò come vero e proprio diritto (art. 3, comma 1-*sexies*) declinato con riferimento all'uso effettivo delle tecnologie poiché tutti gli iscritti all'Anagrafe nazionale della popolazione residente (ANPR) hanno comunque il diritto di *essere identificati* dalle pubbliche amministrazioni mediante l'identità digitale nonché di potere inviare comunicazioni e documenti alle pubbliche amministrazioni e di riceverne dalle stesse tramite un apposito domicilio digitale (19).

Soggetti pubblici e privati incontrano la medesima disciplina per quanto attiene anche agli obblighi di riproduzione e conservazione dei documenti informatici e l'identità digitale (art. 43) ma ai soggetti pubblici — in base a quanto espressamente richiamato dal Capo V del CAD che si riferisce a "*dati delle pubbliche amministrazioni, identità digitali, istanze e servizi on-line*" — sono ricollegabili specifiche condotte di protezione e di trattamento dei dati raccolti (art. 50), ricomprese nella definizione del principio della "disponibilità" dei dati delle pubbliche amministrazioni per cui essi debbono essere

(18) N. Vella, *Le attività ispettive e di controllo fiscale restano escluse dall'ambito di applicazione delle norme del Codice dell'Amministrazione Digitale*, in *GT - Rivista di giurisprudenza tributaria*, 7/2018, 632; D. Marongiu, *Le fonti del diritto e l'amministrazione digitale: l'armonizzazione tra livelli di normazione nell'attuale sistema*, in *Diritto dell'Internet*, 6/2006, 600.

(19) G. Sicchiero, *Il domicilio digitale*, in *Contratto e impresa*, 4/2022, 1006; D. Giorio, *Il domicilio digitale diventa legge*, in *Lo Stato Civile Italiano*, 12/2021, 64.

formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati; restano salvi i limiti alla conoscibilità dei dati previsti dalle leggi e dai regolamenti, e appunto ancora una volta proprio le norme in materia di protezione dei dati personali ed il rispetto della normativa comunitaria in materia di riutilizzo delle informazioni del settore pubblico (c.d. "*open data*") (20).

Perciò qualunque dato trattato da una pubblica amministrazione, nel rispetto della normativa in materia di protezione dei dati personali, deve intendersi reso potenzialmente accessibile e fruibile dalle altre amministrazioni quando l'utilizzazione stessa sia assolutamente necessaria per lo svolgimento dei compiti istituzionali dell'amministrazione richiedente, e nell'ambito delle condizioni poste dal Regolamento europeo sui dati personali senza alcun onere salvo per la possibile prestazione di elaborazioni aggiuntive.

In tale prospettiva le amministrazioni pubbliche, nell'ambito delle proprie funzioni istituzionali, procedono all'analisi dei propri dati anche in combinazione con quelli detenuti da altri soggetti pubblici (fermi restando i limiti previsti dalla protezione dei dati personali) e tale attività si svolge secondo le modalità individuate dall'AgID con apposite Linee guida tecniche nell'ambito di una governance che si presenta composta e suddivisa tra elaborazione di strategie politiche generali e definizione di specifiche indicazioni tecniche di conformità (21). Inoltre le pubbliche amministrazioni certificanti detentrici dei dati ne assicurano comunque la fruizione da parte dei soggetti che hanno diritto ad accedervi. Esse assicurano, su richiesta dei soggetti privati nel caso in cui occorra confermare l'identità anagrafica e documentale di un soggetto privato conferma scritta della corrispondenza di quanto dichiarato con le risultanze dei dati da essa custoditi, in particolare ciò si rende indispensabile ogni qual volta vi sia giustificata esigenza di

(20) G. Fasano, *La sfida della digitalizzazione della pubblica amministrazione nel quadro dei valori costituzionali: tra "open data", riuso delle informazioni Pubbliche e diritto al buon andamento,* in *dirittifondamentali.it*, 2/2023, 166; G. Strazza, *I dati aperti in Italia: un focus sull'"openness" digitale dei Comuni*, in *federalismi.it*, 34/2022, 152; R. Caso, *Open Data, ricerca scientifica e privatizzazione della conoscenza*, in *Il Diritto dell'informazione e dell'informatica*, 4-5/2022, 815; P.S. Maglione, *L'"apertura" dei dati come servizio pubblico: spunti ricostruttivi alla luce della nuova disciplina sul riutilizzo dell'informazione del settore pubblico,* in *Il diritto dell'economia*, 2/2022, 327.

(21) P. Clarizia, *La digitalizzazione*, in *Giornale di diritto amministrativo*, 3/2023, 302; L. Golisano, *Il governo del digitale: strutture di governo e innovazione digitale*, in *Giornale di diritto amministrativo*, 6/2022, 824; F. Pubusa, *Le scelte digitali dell'amministrazione: le implicazioni sul regime dell'organizzazione e dell'attività*, in *Diritto e processo amministrativo*, 4/2022, 1085.

conferma della effettiva identità di un soggetto accedente o al fine di rendere possibile l'utilizzo in via telematica dei dati di una pubblica amministrazione da parte dei sistemi informatici di altre amministrazioni. In particolare proprio (comma 3-*bis*) il trasferimento di un dato da un sistema informativo a un altro "non modifica la titolarità del dato e del trattamento", ferme restando le responsabilità delle amministrazioni che ricevono e trattano il dato in qualità di titolari autonomi del trattamento.

Ciò ha una evidente ricaduta in termini di responsabilità relative alla protezione dei dati personali, definendo cioè una particolare dimensione "interattiva" circa i dati raccolti dai soggetti pubblici e immessi in circolazione nel sistema interattivo pubblico. In primo luogo il perimetro di utilizzabilità dei dati personali sembra doversi perciò saldamente ancorare al consenso espresso e consapevole dell'individuo interessato nel rapporto con i soggetti titolari del trattamento, il che implica una adeguata informazione circa le funzionalità alla base della raccolta di dati, circa la prevedibile diffusione e le modalità di conservazione e di utilizzazione in rapporto alle procedure digitali di volta in volta definibili (22). Si tratta di responsabilità che vanno declinate in costante rapporto con l'organizzazione interna del soggetto interessato e ben modulate in relazione a quelli che sono gli effettivi strumenti di controllo e di interlocuzione nello spirito di "*accountability*" della disciplina generale sulla utilizzazione dei dati personali (23).

È appena il caso anche di richiamare il costante indirizzo giurisprudenziale della Corte di Cassazione che in sede civile, occupandosi per lo più di fissare alcuni punti centrali e qualificanti della disciplina dei dati personali ha avuto modo di ribadire come (Cass., Sez. I, Ord. 26 aprile 2021, n. 11020) la tutela della riservatezza, il trattamento dei dati personali deve essere sempre effettuato nel rispetto del "criterio di minimizzazione" dell'uso degli stessi, dovendo cioè essere utilizzati *solo se indispensabili, pertinenti e limitati a quanto necessario per il perseguimento delle finalità per cui sono raccolti e trattati, essendo irrilevante, al fine di derogare a tale principio, la circostanza che la divulgazione avvenga nell'ambito di una procedura di rilevanza pubblica*. Inoltre (Sez. II, Ord. 3 settembre 2020, n. 18288) proprio le ipotesi di omessa

(22) Cfr. A. Tortora, *Il nuovo regolamento europeo per la protezione dei dati (GDPR) e la figura del "Data Protection Officer" (DPO): incidenza sulla attività della pubblica amministrazione*, in *Amministrativ@mente*, 5-6/2018, 3; G. Garofalo, *Identità digitale e diritto all'oblio: questioni aperte all'indomani dell'approvazione del GDPR*, in *Il Diritto di famiglia e delle persone*, 3/2021, 2, 1505.

(23) Cfr. A. Punzi, *Algoritmi di indicizzazione, identità digitale e diritto all'oblio*, in *Le Corti fiorentine*, 1-3/2020, 23; M. F. Cocuccio, *Il diritto all'identità personale e l'identità "digitale"*, in *Il Diritto di famiglia e delle persone*, 3/2016, 2, 949; M. Zanichelli, *Il diritto all'oblio tra privacy e identità digitale*, in *Informatica e diritto*, 1/2016, 9.

informativa o di omessa acquisizione del consenso possono configurarsi anche per i dati disponibili pubblicamente (si trattava delle liste elettorali). Inoltre (Sez. I, Sentenza 2 luglio 2018, n. 17278) il consenso è validamente prestato solo se espresso *liberamente e specificamente in riferimento ad un trattamento chiaramente individuato,* o ancora valutando (Sez. I, Sentenza 29 maggio 2015, n. 11223) l'illecito trattamento di dati sensibili l'avvenuta comunicazione, anche se effettuata in maniera riservata, da un soggetto pubblico ad un altro di dati (sanitari) dettagliati relativi ad accertamenti clinici e strumentali svolti, nonché ad informazioni anamnestiche, che possano considerarsi irrilevanti ai fini del buon esito del procedimento e, pertanto, ragionevolmente da omettere. Anche la diffusione massiva non espressamente autorizzata di dati comunque pubblici (Sez. II, Sentenza 24 giugno 2014, n. 14326) è stata valutata in contrasto con i principi generali di protezione dei dati.

Inoltre il principio di (libero) accesso telematico e di (generale) riutilizzo dei dati (art. 52) che si applica a dati, documenti e procedimenti utilizzati in un ciclo di riutilizzo appare disciplinato dai soggetti pubblici secondo modalità conformi alle disposizioni del CAD, ma soprattutto "nel rispetto della normativa vigente", quindi anche quella in tema di dati personali.

Le pubbliche amministrazioni pubblicano nel proprio l'elenco di tutti i domicili digitali interni — ed il principio è ulteriormente richiamato col riferimento al comma 1, lettere *l-bis*) e *l-ter*), del Codice — definendo una eccezione (alla regola della trasparenza digitale) proprio nei casi in cui la pubblicazione riguardi dati personali. Tale disposizione va letta proprio in relazione all'art. 3-*bis* del Codice dell'amministrazione digitale che stabilisce anche il diritto di chiunque di accedere ai servizi *on-line* offerti dai soggetti pubblici "tramite la propria identità digitale" e anche attraverso un apposito "punto di accesso telematico" specificando anche l'obbligo di dotarsi di un domicilio digitale per tutti i soggetti pubblici (e quindi anche per tutte le possibili articolazioni soggettive e centri di imputazione di responsabilità pubbliche in via generale) così come per professionisti tenuti all'iscrizione in albi ed elenchi e i soggetti tenuti all'iscrizione nel registro delle imprese che viene iscritto in un apposito elenco pubblico (art. 6 *bis* o 6-*ter*). Pertanto per gli esercenti un servizio pubblico o aperto al pubblico (tendenzialmente svolto con modalità digitali) l'adozione di un domicilio digitale è appunto un obbligo, qualificabile in termini generali di trasparenza circa l'attività esercitata e con finalità di semplificazione nella individuazione di un recapito certo e collegabile alla attività pubblica o di rilievo pubblico svolta che impone un riferimento costante e interattivo, mentre per i cittadini risulta una libera opzione, ricollegabile e valutabile nella sua concreta organizzazione e potenziale disponibilità a seconda del rapporto comunicativo e delle sue specifiche esigenze.

La definizione di domicilio digitale è generale e si concreta, in base all'art. 1 (lettera *n-ter*) del CAD nel richiamo ad "*un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato così come definito dal regolamento (UE) 23 luglio 2014 n. 910 eIDAS*" (24). Tale indirizzo dovrà essere considerato a tutti gli effetti valido ai fini delle comunicazioni elettroniche aventi valore legale (25).

Si tratta di una opzione comunicativa che spetta comunque a chiunque in termini di facoltà e che comprende tanto la facoltà di eleggere quanto quella di modificare il proprio domicilio digitale da iscrivere nell'elenco apposito (art. 6-*quater*) in funzione di una interattività comunicativa costante dal momento che ogni qual volta il domicilio eletto risulti non più attivo si procede alla sua cancellazione d'ufficio dall'indice secondo modalità fissate nelle Linee guida.

La scelta del domicilio digitale (comma 1-*ter*) riguarda le persone fisiche che possono avvalersi anche di un apposito servizio on line reso disponibile *on-line* dall'Anagrafe nazionale della popolazione residente (ANPR) di cui all'articolo 62, ovvero recandosi presso l'ufficio anagrafe del proprio comune di residenza. Con l'elezione di tale domicilio i cittadini possono perciò indicare uno specifico indirizzo di Posta elettronica certificata dove ricevere tutte le comunicazioni ufficiali e le notifiche della Pubblica Amministrazione mediante un *'Indice Nazionale dei Domicili Digitali* (INAD) (26).

I soggetti titolari di domicilio digitale hanno comunque l'obbligo di farne un uso "diligente" e di comunicare ogni modifica o variazione. Tale diligenza, che la norma prescrive sembra richiamare implicitamente una attenzione interlocutoria costante, ovvero una opportuna precauzione comportamentale diretta a osservare cautele di massima onde evitarne preventivamente una utilizzazione indiscriminata che possa concretare il rischio di

---

(24) G. Sicchiero, *Il domicilio digitale*, in *Contratto e impresa*, 4/2022, 1006; D. Giorio, *Il domicilio digitale diventa legge*, in *Lo Stato Civile Italiano*, 12/2021, 64.

(25) E. Manoni, *La casella PEC impone obblighi comunicativi e di gestione: i riflessi processuali*, in *Diritto e pratica tributaria*, 6/2020, 2790; M. Bruzzone, *Notifiche di atti tributari a destinatari irreperibili nel "domicilio digitale"*, in *Corriere tributario*, 12/2019, 1083. Sul punto va segnalata la posizione delle S.U. civili della Corte di cassazione che, con Sentenza 18 maggio 2022, n. 15979, hanno ritenuto pienamente valida la notificazione a mezzo PEC eseguita proprio utilizzando l'Indice di cui all'art. 6-*ter* del d.lgs. n. 82 del 2005 poiché una maggiore rigidità formale in tema di notifiche digitali è richiesta per l'individuazione dell'indirizzo del destinatario, cioè del soggetto passivo a cui è associato un onere di tenuta diligente del proprio casellario, ma non anche del mittente.

(26) L'opzione avviene al sito internet: https://domiciliodigitale.gov.it accedendo direttamente mediante SPID, CIE o CNS, e inserendo il proprio recapito certificato eventualmente disponibile.

acquisizione massiva o di compromissione identificativa, per esempio utilizzando il domicilio in un ambiente on line privo dei requisiti richiesti dalla regolamentazione eIDAS.

Anche qui si tratta di un preciso diritto delineato per tutti i cittadini dall'art. 1 (comma 1-*sexies*) che così esercitano un "diritto di essere identificati dalle pubbliche amministrazioni *tramite l'identità digitale di cui al comma 1*-quinquies, nonché di inviare comunicazioni e documenti alle pubbliche amministrazioni e di riceverne dalle stesse *tramite un domicilio digitale*, alle condizioni di cui all'articolo 3-*bis*.

1.5. Metodi di autenticazione digitale ed identità: temi e problemi di quadro

Identità e domicilio digitale sono quindi le due componenti essenziali del processo di transizione digitale, ma non possono certo essere considerati come sinonimi: l'una attiene cioè ad un requisito "formale" ed "univoco" quale l'identità cioè il processo di riconoscimento entro un (qualsiasi) sistema digitale mediante dati collegabili (e liberamente valutabili a seconda del metodo informatico), mentre il domicilio assicura un ulteriore elemento di certezza alle transazioni quanto a modalità e forme comunicative, correlando uno specifico punto in un percorso di comunicazione sicuro e certificato, che peraltro direttamente si richiama ad una regolamentazione in ambito europeo.

Sono definite specifiche regole circa le modalità di gestione e di aggiornamento dell'elenco anche nei casi di decesso del titolare del domicilio digitale già eletto, con conseguente potenziale problematica circa la valenza in sede successoria dei dati di accesso al patrimonio informativo da parte degli aventi diritto (27) o di impossibilità sopravvenuta di avvalersi del domicilio.

Restano sullo sfondo anche tematiche tipiche della elaborazione dei dati personali, quali la deindicizzazione una volta esaurito lo scopo della rac-

(27) V. Putortì. *Patrimonio digitale e successione "mortis causa"*, in *Giustizia civile*, 1/2021, 163; S. Nardi, *"Successione digitale" e successione nel patrimonio digitale*, in *Diritto delle successioni e della famiglia*, 3/2020, 955; L. DI Lorenzo, *Il legato di password* in *Notariato*, 2/2014, 144. L. Di Lorenzo, *L'eredità digitale*, in *Notariato*, 2/2021, 138. V. Iorio, *Identità digitale e trasmissione a causa di morte*, in *Diritto delle successioni e della famiglia*, 1/2022, 91; M. Ziccardi, *Identità digitale e fenomeno successorio. Considerazioni sulla trasmissione "mortis causa" delle criptovalute*, in *Annali Società italiana degli studiosi del diritto civile*, 7/2021, 199.

colta (28) o la stessa funzione della identità nel contesto dei servizi digitali che sempre di più va ad inquadrarsi in ambito europeo (29).

L'opzione comporta l'inserimento del dato identificativo nell'Anagrafe nazionale della popolazione residente - ANPR (30) e reso disponibile a tutte le pubbliche amministrazioni e ai gestori o esercenti di pubblici servizi ed inerisce "esclusivamente" alle comunicazioni e alle notifiche e costituisce "mezzo esclusivo di comunicazione e notifica da parte dei soggetti pubblici", proprio tale sottolineatura finisce per delineare una particolare cautela circa la diffusione e la stessa utilizzazione dei dati esterni dei domicili e dei metadati che vi si collegano univocamente al di fuori di quello che è il circuito relazione tipico di una pubblica funzione o per obiettivi funzionali che non appaiono a questa direttamente collegabili e asseverati dal consenso diretto degli interessati in quanto pienamente informati e consapevoli della possibile utilizzazione esterna di propri dati di riferimento rilasciati solo per una funzione comunicativa da e fra soggetti pubblici in termini di semplificazione procedimentale e di accesso semplificato ai servizi da essi resi.

Ma le identità digitali (art. 63) si manifestano componenti essenziali — e perciò strettamente funzionali per la fruizione generalizzata e la conseguente identificazione (sicura) nell'ambito di istanze e servizi pubblici *on-line* — per la modalità di erogazione in base a criteri di valutazione di *efficacia, economicità ed utilità e* nel rispetto dei principi di eguaglianza e non discriminazione, tenendo comunque presenti le dimensioni dell'utenza, la frequenza dell'uso e l'eventuale destinazione all'utilizzazione da parte di categorie in situazioni di disagio.

Il che poi apre un capitolo nuovo e fondamentale che è quello del rapporto tra semplicità di uso delle procedure di identificazione digitale e strumenti concreti di accessibilità degli strumenti e delle soluzioni digitali (31). La norma interviene appunto per assicurare insieme progettazione sicura e realizzazione di servizi in rete sempre affidabili anche in termini di

---

(28) T. Bonamini, *Identità digitale e diritto all'oblio*, in *Jus civile*, 1/2022, 23; G. Garofalo, *Identità digitale e diritto all'oblio: questioni aperte all'indomani dell'approvazione del GDPR*, in *Il Diritto di famiglia e delle persone*, 3/2021, 2, 1505.

(29) V. Tevere, *Verso un quadro comune europeo sull'identità digitale: modifica della Commissione del regolamento (UE) n. 910/2014*, in *Lo Stato Civile Italiano*, 1/2022, 77.

(30) Cfr. A. De Luca, *ANPR: la nuova anagrafe*, in *Lo Stato Civile Italiano*, 10/2019, 37; E. Nannizzi, *Chiarimenti sull'accesso alla banca dati anagrafe*, in *Lo Stato Civile Italiano*, 10/2020, 61.

(31) Cfr. A. G. Orofino, F. Cimbali, *L'uso delle tecniche informatiche nella prestazione di servizi pubblici*, in *Giurisprudenza italiana*, 6/2022, 1523. A. Contaldo, *Accessibilità dei siti Web pubblici: dalla direttiva 2016/2102/UE alle Linee guida AgID,* in *Rivista Amministrativa della Repubblica Italiana*, 9-12/2020, 2, 563; M. Caporale, *L'accessibilità ai siti web e alle*

qualità, per la migliore soddisfazione delle esigenze degli utenti, in particolare garantendo loro la completezza del procedimento, la certificazione dell'esito e assicurando anche l'accertamento del grado di soddisfazione manifestato. Ed in tal senso i soggetti pubblici sono comunque tenuti anche ad adottare strumenti idonei alla rilevazione immediata, continua e sicura del giudizio degli utenti. In tale prospettiva le pubbliche amministrazioni collaborano costantemente fra loro per integrare i procedimenti di rispettiva competenza, proprio al fine di agevolare gli adempimenti di cittadini ed imprese e rendere più efficienti i procedimenti che interessano più amministrazioni, attraverso idonei ed efficaci sistemi di cooperazione.

La dimensione interpretativa deve però limitarsi a tutti gli ambiti di comunicazione informale, come ad esempio la prenotazione di prestazioni o il rilascio di informazioni generali sui servizi o sulle modalità di accesso, ponendosi come modello sussidiario di tutte le comunicazioni che non richiedano un adempimento formale o una particolare forma di accertamento certificato da parte dei soggetti richiedenti, lasciando ampio spazio alle amministrazioni circa la organizzazione e la prestazione di servizi in forma digitale, a seconda delle funzioni e delle richieste da gestire e ripartire in base alla propria organizzazione concreta, con una ampia scelta di strategie o di soluzioni volte a garantire la migliore soddisfazione in concreto dell'utente (32).

Proprio la definizione di un "*Sistema*" pubblico (integrato) per la gestione delle identità digitali (33) in rapporto alle modalità di accesso ai servizi erogati in rete dalle pubbliche amministrazioni posta nettamente dall'art. 64 del CAD comprende allora in via generale un insieme variegato e liberamente opzionabile di strumenti di identificazione utilizzabili che comprendono tanto la carta d'identità elettronica (CIE) quanto la carta nazionale dei servizi (CNS), considerati strumenti fondamentali per l'accesso ai servizi erogati in rete dalle pubbliche amministrazioni in quanto documenti personali destinati a operare anche come strumenti digitali per i quali sia necessaria l'identificazione informatica.

Tali strumenti tuttavia implicano quasi sempre l'uso di un apparato

---

applicazioni mobili delle pubbliche amministrazioni, in *Giornale di diritto amministrativo*, 3/2019, 357.

(32) Cfr. M. Martoni, *Identità personale anagrafica (autorizzata) vs identità personale autorappresentativa (manifestata)*, in *Rivista trimestrale di diritto e procedura civile*, 1/2020, 179.

(33) A. Contaldo, *La Carta Nazionale dei Servizi e l'identità digitale dopo l'introduzione di SPID*, in *Rivista Amministrativa della Repubblica Italiana*, 11-12/2019, 2, 643; A. Contaldo, *La disciplina dello SPID e la definizione giuridica dei suoi gestori,* in *giustiziacivile.com*, 4/2017, 6.

esterno di lettura dei dati incorporati, e cioè di un codice alfanumerico che attraverso una apposita interfaccia sia collegato e disponibile, basandosi l'identificazione sul codice associato univocamente al documento stesso, ed in genere non dispongono di associazioni tecnologiche più vaste (come quella ad una utenza telefonica o ad un domicilio digitale) conformi a quelli che sono gli standards europei, basati su procedure di autenticazione "forti" attraverso sistemi di conferma articolati e interattivi della propria identità (34).

L'attuale stato delle tecnologie informatiche comprende molti efficaci metodi di autenticazione che vanno sempre di più a sostituire le classiche "*password*" che possono risultare insufficienti a garantire adeguatamente la sicurezza in quanto facilmente acquisibili anche indipendentemente dalla condotta colposa del soggetto interessato. Gli attuali metodi più sicuri di autenticazione digitale sono divisi in tre classi, in base a: qualcosa che so (es. password, parola chiave o numero di identificazione personale (PIN)) e si può riferire alla password o ad un'autenticazione *pattern-based*, cioè in pratica integrata nei sistemi operativi o un'autenticazione basata sul codice PIN (che integra il sistema operativo di provenienza e lo riconosce sistematicamente) 1come per i bancomat. Ad un secondo livello il riconoscimento comprende qualcosa *che si ha* (un come tesserino identificativo o un dispositivo esterno) ed è molto spesso un token (35) installato su un dispositivo mobile che si possiede. Ma il sistema può comprendere, per generare ancora un miglior livello di sicurezza anche qualcosa che "si è" (identificatori biometrici), ed è manifesto che una soluzione di autenticazione adeguatamente sicura avviene solo con la combinazione intelligente di più metodi come attraverso procedure di conferma variabili su canali in grado di assicurare il diretto coinvolgimento confermativo del titolare. La scelta dei diversi metodi di autenticazione è poi molto spesso condizionata dai diversi

(34) Il sistema di Strong authentication viene già utilizzato in attuazione di specifiche normative europee in ambiente bancario, sul punto M. V. Zammitti, *Operazioni di pagamento tramite "wallet" e responsabilità da omessa applicazione della "Strong Customer Authentication" (SCA)*, in *Banca borsa e titoli di credito*, 6/2022, 2, 868; S. Balsamo Tagnani, *Il mercato europeo dei servizi di pagamento si rinnova con la PSD2 (Payment Legislative Package Directive 2)*, in *Contratto e impresa. Europa*, 2018, 609. Cfr. la Direttiva (UE) 2015/2366 del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno.) Cfr. anche F. Marasà, *Il trattamento dei dati personali dell'utente dei servizi di pagamento tra PSD2 e GDPR*, in *Orizzonti del diritto commerciale*, 2/2020, 629.

(35) Esistono infatti almeno due tipologie principali di token mobile: Token che si usano online (challenge/response based) Token che si usano offline (*time*, *sequence* o *OTP based*), in entrambi i casi il dispositivo genera una sequenza casuale che viene utilizzata per abilitare indivisualmente l'accesso al sistema.

fattori tra cui in concreto l'usabilità, l'importanza delle informazioni da proteggere ed il costo complessivo del sistema e della sua manutenzione.

L'uso di un sistema integrato e integrabile come SPID appare uno strumento semplice e diffuso, con differenti modalità di uso e modulabile in base alle effettive esigenze della utilizzazione in più livelli di sicurezza. Ed in tal senso i soggetti pubblici possono consentire l'accesso ai servizi in rete da esse erogati che richiedono l'identificazione informatica anche con strumenti diversi dalla carta d'identità elettronica e dalla carta nazionale dei servizi, *purché tali strumenti consentano l'individuazione del soggetto che richiede il servizio.* Con l'istituzione del sistema Spid i soggetti pubblici dispongono di un insieme allargato ed integrato ai servizi interoperabili che richiedano una attestazione di identità qualificandosi un principio di libertà di opzione di acceso digitale ai servizi indipendentemente dalle modalità di accesso predisposte dalle singole amministrazioni.

La funzione essenziale dello SPID in tale contesto è infatti quella (comma 2-*bis*) di favorire la massima diffusione di servizi in rete e nel contempo di agevolare l'accesso (rapido e semplificato) agli stessi da parte di cittadini e imprese *anche in mobilità,* ovvero avvalendosi di strumenti quali *smarphones* o *tablets* che non richiedono appositi lettori (36). È un insieme comunque "aperto" di soggetti pubblici e privati che, previo accreditamento da parte dell'AgID, seguendo modalità tecniche da essa definite e condivise, identificano sistematicamente gli utenti proprio per consentire loro il compimento di attività e l'accesso a (tutti i) servizi pubblici in rete. E tale prospettiva di insieme interattivo coinvolge anche i soggetti privati (comma 2-*quinquies*). Ai fini dell'erogazione dei propri servizi in rete, è altresì riconosciuta ai soggetti privati, che hanno facoltà di avvalersi del sistema Spid per la gestione dell'identità digitale dei propri utenti, oltre che di avvalersi della carta di identità elettronica. L'adesione al sistema ovvero l'utilizzo della carta di identità elettronica per la verifica dell'accesso ai propri servizi erogati in rete per i quali è richiesto il riconoscimento dell'utente esonera infatti i predetti soggetti da un obbligo generale di sorveglianza delle attività sui propri siti (ad esempio nelle procedure come l'attivazione o la disattivazione di una utenza o di un servizio digitale). È significativo che la norma anche qui prevede, in ogni passaggio regolamentare, l'acquisizione del parere del Garante per la protezione dei dati personali.

Infine la nozione di *"identità digitale*" a seguito della introduzione dell'art. 640-*ter*, comma 3, Codice penale ha un supporto fondamentale volto

(36) Cfr. L. Abba, V. Amenta, A. Lazzaroni, *L'identità digitale: dalle nuove frontiere del Sistema Pubblico di Identificazione (SPID) alle problematiche legate al "web"*, in *Ciberspazio e Diritto*, 1/2015, 11; R. Titomanlio, *Considerazioni introduttive sul Sistema Pubblico per la Gestione dell'Identità Digitale (SPID)*, in *Giust. Amm.it*, 3/2015, 9.

a garantirne ogni utilizzazione illecita funzionale al conseguimento di un illecito profitto patrimoniale (37).

L'apparato normativo penale sembra infatti presidiare adeguatamente l'identità digitale sotto il profilo di possibili utilizzazioni fraudolente e ingannevoli (38) presidiando quelle che sono condotte di utilizzazione impropria dell'identità digitale o la costruzione di false identità digitali.

Sotto il profilo problematico infatti il rapporto tra uso legittimo e potenziale abuso delle identità digitali e la *privacy* viene ad essere uno dei temi cruciali nell'era digitale. In particolare tale rapporto comprende ogni forma di raccolta sistematica e utilizzo dei dati e dei metadati spesso senza il pieno consenso degli utenti individuabili che appaiono particolarmente esposti, in assenza di un adeguato sistema di sicurezza al furto di identità.

In ambito civile si è più volte sottolineata l'importanza ed il ruolo centrale del consenso quale strumento adesivo e di costante informazione completa circa l'utilizzazione dei dati personali nel rapporto comunicativo digitale, tanto più in presenza di un sistema di utilizzazione globale e derivato che, di fatto, rende molto difficile qualsiasi controllo e qualsiasi piena conoscibilità circa la effettiva diffusione in ambito digitale (39).

---

(37) V. in proposito Cass., Sez. II penale, Sentenza 20 settembre 2022, n. 40862, che afferma come in tema di frode informatica, la nozione di "identità digitale", che integra l'aggravante di cui all'art. 640-*ter*, comma terzo, c.p., non presuppone una procedura di validazione adottata dalla Pubblica Amministrazione, ma trova applicazione anche nel caso di utilizzo di credenziali di accesso a sistemi informatici gestiti da privati. (Fattispecie in cui è stata ritenuta l'aggravante in un caso di accesso abusivo a un servizio di "home banking"). Cass., Sez. V pen., Sentenza 6 luglio 2020, n. 22049, Ud. "Integra il delitto di sostituzione di persona la condotta di colui che crea ed utilizza un "profilo" su "social network", servendosi abusivamente dell'immagine di un diverso soggetto, inconsapevole, in quanto idonea alla rappresentazione di un'identità digitale non corrispondente al soggetto che ne fa uso. (Fattispecie relativa alla creazione di falsi profili "facebook").

(38) Cfr. sul punto M. Martoni, *Note sulla vulnerabilità dell'identità personale digitale autorappresentativa,* in *Notizie di Politeia*, 136/2019, 23 e V. Gangemi, *Usurpazione dell'identità digitale: la sorte del contratto telematico concluso illegittimamente da terzi*, in *Il Foro padano*, 3/2022, 1, 233; M. D'Agostino Panebianco, *Digital Identity: Between Human Rights And Cybercrimes*, in *ambientediritto.it*, 1/2021, 1002; M. Tarsetti, *Il reato di sostituzione di persona nella identità digitale. Interpretazione estensiva o norma creativa?*, in *La Giustizia Penal,* 4/2020, 2, 230; C. Crescioli, *La tutela penale dell'identità digitale*, in *Diritto penale contemporaneo*, 5/2018, 265.

(39) Cfr. A. Spatuzzi, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali*, in *Notariato*, 4/2021, 371; F. Stassi, *Consenso dell'interessato e dati personali al tempo dei "big data"*, in *Rivista di Diritto dell'Economia, dei Trasporti e dell'Ambiente*, 2021, 105; E. Guarnieri, *Il consenso al trattamento dei dati personali ed il contratto di conto corrente*, in *giustiziacivile.com*, 3/2020, 17; C. Basunti, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali,* in

Il diaframma normativo tra necessaria acquisizione di dati in qualche modo "sistemici" cioè essenziali allo svolgimento di compiti pubblici ed inquadrati in attività funzionalmente già regolate cui corrispondono specifiche responsabilità si pone quindi come una condizione generale,che richiede un intervento normativo anche di carattere integrativo mirato alla più agevole definizione di quei profili di "*accountability*" posti generalmente dal GDPR, profili che poi si risolvono in assetti ed in responsabilità ben definiti come anche nella conduzione trasparente e funzionalmente e temporalmente limitata del trattamento stesso (40).

L'impatto del principio di *accountability* si traduce in una più estesa responsabilizzazione, in una azione costante di ricerca e di integrazione rispetto ad altre discipline (come in particolare quella informatica), che compone insieme tanto gli aspetti del danno potenziale a terzi quanto il profilo della efficiente gestione dei sistemi di trattamento secondo metodi e moduli innovativi che siano in grado insieme di assicurare trasparenza e sicurezza operativa, comprensione dei margini di rischio possibile e interventi tecnologici di prevenzione modulati sulla base di esperienze comuni (41).

Contratto e impresa, 2/2020, 860; A. Vivarelli, "*Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche",* in *Rassegna di diritto civile*, 1/2020, 357; F. Caggia, *Il consenso al trattamento dei dati personali nel diritto europeo*, in *Rivista del diritto commerciale e del diritto generale delle obbligazioni*, 3/2019, 1, 405; F. Bravo, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto,* in *Contratto e impresa*, 1/2019, 34, F. Naddeo, *Il consenso al trattamento dei dati personali del minore*, in *Il Diritto dell'informazione e dell'informatica*, 1/2018, 27; I. A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Osservatorio del diritto civile e commerciale*, 1/2018, 67.

(40) Essenzialmente cfr. G. Finocchiaro, *Il principio di "accountability"*, in *Giurisprudenza italiana*, 12/2019, 2778; A. Valeriani, *L'"accountability" delle autorità amministrative indipendenti. Possibili linee evolutive*, in *Rivista del Diritto della Sicurezza Sociale*, 4/2019, 761; D. Amram, *Responsabilità, danno e "accountability" nella società dell'informazione*, in *Danno e responsabilità*, 2/2019, 243.

(41) A. Tomo, *La "forza centripeta" del diritto alla protezione dei dati personali: la Corte di giustizia sulla rilevanza in ambito tributario dei principi di proporzionalità, "accountability" e minimizzazione*, in *Diritto e pratica tributaria internazionale*, 2/2022, 908; M. G. Stanzione, *La protezione dei dati personali tra « consumerizzazione » della "privacy" e principio di "accountability",* in *Comparazione e diritto civile*, 1/2022, 1; R. Rolli, M. D'Ambrosio, *Consenso e "accountability": i poli del commercio dei dati personali "online"*, in *P.A. Persona e Amministrazione*, 1/2022, 783; G. Bazzoni, *L'evoluzione normativa dell'intermediazione digitale: nuovi profili di responsabilizzazione*, in *Rivista italiana di informatica e diritt*o, 1/2022, 2, 201.

E ciò comporta gravi e significativi problemi collegabili all'uso costante di algoritmi di profilazione (42), tanto più in mancanza di un insieme puntuale di *standards* globali di riferimento e in un quadro normativo ben assestato in Italia ed in Europa, ma ancora non ben definito proprio nell'ambiente *cloud* e dei grandi servizi *social,* qualificandosi sempre di più l'esigenza di regolamentazioni efficaci, mirate a garantire trasparenza da parte delle aziende, educazione dell'utente e lo sviluppo di tecnologie sicure per ogni forma di transazione digitale (43).

Per mitigare i rischi di vulnerabilità — che emergono continuamente e che sono oggetto di specifiche regolamentazioni in tema di sicurezza di reti e infrastrutture digitale — le pubbliche amministrazioni dovranno adottare sempre di più misure di sicurezza "resilienti" e cioè nel contempo implementare politiche interne di *privacy* anche molto rigorose basate sul controllo

---

(42) G. Comandé, *Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali* in *Danno e responsabilità*, 2/2022, 141; G. Comandè, *Leggibilità algoritmica e consenso al trattamento dei dati personali*, in *Danno e responsabilità*, 1/2022, 33; A. P. Seminara, *"Cookie" e libertà del consenso al trattamento dei dati personali*, in *Persona e Mercato*, 4/2021, 857; A. Vigorito, *La declinazione "algoritmica" del consenso dell'interessato al trattamento dei dati personali. Il caso Mevaluate e il "rating" reputazionale "privato",* in *Rivista critica del diritto privato*, 3/2021, 441; C. Angiolini, *A proposito del Caso "Orange Romania" deciso dalla Corte di Giustizia dell'UE: il rapporto fra contratto e consenso al trattamento dei dati personali,* in *Le Nuove leggi civili commentate*, 1/2021, 247; I. A. Caggiano, L. Gatt, R. Montanari, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2/2017, 363.

(43) Cfr. S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità,* in Europa e diritto privato 2/2016, p. 513; E. Volkova, *Stati Uniti d'America, Federazione Russa e Italia: consenso e informativa nella disciplina del trattamento dei dati personali (e confronto tra i diversi approcci normativi)*, in *Ciberspazio e Diritto*, 1-2/2016, 185; R. De Meo, *Autodeterminazione e consenso nella profilazione dei dati personali*, in *Il Diritto dell'informazione e dell'informatica*, 3/2013, 587; R. Frau, *Profili del consenso al trattamento dei dati personali per fini economici nell'esperienza italiana. Raffronti con la normativa spagnola*, in *Responsabilità civile e previdenza*, 12/2010, 2598, S. Niger, *Il "mito" del consenso alla luce del codice in materia di protezione dei dati personali,* in *Ciberspazio e Diritto*, 4/2005, 499; S. Sica, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Rivista di diritto civile*, 6/2001, 2, 621; S. Cagli, *La rilevanza del consenso nella disciplina del trattamento dei dati personali* in *L'Indice penale*, 2/2001, 855; G. Resta, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali* in *Rivista critica del diritto privato*, 2/2000, 299; S. Patti, *Il consenso dell'interessato al trattamento dei dati personali*, in *Rivista di diritto civile*, 4/1999, 2, 455; R. Pardolesi, *Informative personali e richieste di consenso al cliente da parte di banca per il trattamento di dati personali* in *Il Foro italiano*, 6/1997, 3, 317; G. Comandè, *La funzione "giurisprudenziale" del Garante per la protezione dei dati personali: a proposito di una recente decisione su informativa e consenso al trattamento*, in *Il Diritto dell'informazione e dell'informatica*, 6/1997, 975.

dei soggetti titolari dei dati personali, che siano in grado di impedire anche che i dati raccolti siano utilizzati per finalità non dichiarate o non rese trasparenti o ancora che possano comunque entrare in possesso di soggetti esterni intenzionati ad utilizzarli (o a riutilizzarli) per finalità illecite o non espressamente consentite dagli interessati (44).

Tutto ciò implica un'azione di adeguamento e di aggiornamento costante dei codici di condotta interni ed una formazione sempre adeguata del personale e dei soggetti coinvolti in tema di protezione e sicurezza dei dati, che poi è il presupposto di ogni identificazione personale "sicura" e della garanzia della *privacy* in un vicendevole rapporto proattivo e positivo fondamentale per instaurare e mantenere la fiducia dei cittadini nell'accesso ai servizi *on line* così come nel contempo per proteggerne adeguatamente i loro dati personali e sensibili in una efficace sinergia tra misure giuridiche di ordine generale come specifiche,ed aggiornate, misure tecnologiche di protezione.

(44) F. Lorè, P. Musacchio, *"Cybersecurity" e protezione dei dati personali ai tempi dell'"accountability": verso un cambio di prospettiva?*, in *Amministrativ@mente*, 1/2021, 65.

II.

L'IDENTITÀ PERSONALE DEL MINORE DI ETÀ NEL *CYBERSPAZIO* TRA AUTODETERMINAZIONE E *PARENTAL CONTROL SYSTEM*

di *Roberto Senigaglia*

Sommario: 2.1. Il fenomeno e il contesto. — 2.2. Gli orizzonti funzionali dell'identità personale nella dimensione esperienziale digitale. — 2.3. La funzione educativa del minorenne in formazione identitaria. — 2.4. Il principio della necessaria esclusività "incarnata" del ruolo educativo dei genitori. — 2.5. Il dovere di vigilanza dei genitori *vs*. il libero accesso del minore ai contenuti della rete. — 2.6. La protezione del minore da contenuti illegali. I sistemi di controllo parentale. — 2.7. *Segue*. Proporzionalità e ragionevolezza delle misure di controllo parentale. Il *Children's Act* inglese. — 2.8. Identità personale, misure di protezione e differenziazione della minore età.

2.1. Il fenomeno e il contesto

La complessità della fenomenologia dell'attività e della vita sociale del minore in *Internet* è nota e ampiamente trattata specie dalle scienze sociali, attente a evidenziare, sul piano individuale, le ricadute psicologiche e razionali incidenti sullo sviluppo della personalità e, sul piano sociologico, i differenti impatti relazionali e antropologici, anche rispetto alle generazioni future.

La realtà *educativa* di riferimento, nel contesto della transizione tecnologica, è ben illustrata nella Comunicazione della Commissione europea su « Un decennio digitale per bambini e giovani: la nuova strategia europea per un internet migliore per i ragazzi (BIK+) ». Nell'introduzione si constata che « i minori iniziano a creare, giocare e interagire *online* a un'età sempre più precoce, avvalendosi delle tecnologie dell'informazione e della comunicazione a fini di istruzione, intrattenimento, contatti sociali e partecipazione alla società. In tal modo, si imbattono spesso in contenuti e servizi digitali che non sono stati concepiti tenendo conto di loro » (1).

(1) Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato della regione, *Un decennio digitale per bambini*

È dinanzi a questi accessi che le fragilità dell'identità personale reclamano protezione.

Ma lo specifico profilo di interesse del giurista che osserva il fenomeno consta, anzitutto, nell'individuare il tipo normativo di problema sollevato da quelle istanze di protezione promananti dai "consumatori" della rete (2) — nella specie i minorenni e le persone istituzionalmente preposte alla loro cura — nonché le misure rimediali apprestabili. E ciò nella piena coscienza che nel *cyberspazio* gli interessi meritevoli di tutela assumono contorni senz'altro originali o per la novità della loro sostanza o per la forma del rimedio, esigendo costantemente un riadattamento del metodo valutativo e decisionale al contesto della rete: senza tempo e senza luogo, avulso dai caratteri tipici della fisicità e, dunque, non pienamente comprensibile se si continua a ritenerlo « come una sorta di prolungamento e di estensione della vita sociale ». Tanto è vero che lo *spazio* del *web* è visto come uno stravolgimento della vita sociale *offline* « perché sono implicate delle libertà de-situate, smaterializzate ed enfatizzate psicologicamente » (3).

2.2. Gli orizzonti funzionali dell'identità personale nella dimensione esperienziale digitale

Dalla specola del civilista, il tipo di problema riguarda l'impatto dell'esperienza (4) digitale sull'identità del minore, riguardante, in particolar modo, la sua biografia (e non tanto l'anagrafe e il profilo genetico, i quali, dunque, esulano da questa indagine) (5), e sulle capacità di risposta norma-

---

e giovani: la nuova strategia europea per un'internet migliore per i ragazzi (BIK+), 11 maggio 2022, COM (2022) 212 final, in https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52022DC0212.

(2) Ad essi si riferiscono le Linee guida dell'Autorità per le Garanzie nelle Comunicazioni finalizzate all'attuazione dell'art. 7-*bis* del Decreto Legge 30 aprile 2020, n. 28 in materia di "sistemi di protezione dei minori dai rischi del cyberspazio", in https://www.agcom.it/documents/10179/29648921/Allegato+21-2-2023/b6b81dba-b5c0-4372-82e7-25a78e300f96?version=1.0

(3) A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, Milano-Udine, 2023, 114.

(4) Riferita non soltanto a ciò che ci capita, ma anche a ciò che facciamo di quello che ci capita; in proposito, v. A. Pessina, *op. cit.*, 41, il quale riprende, in questi termini, l'espressione di Huxley.

(5) Sulle diverse dimensioni dell'identità si rinvia a P. Zatti, *Dimensioni e aspetti dell'identità nel diritto privato attuale*, in *L'identità nell'orizzonte del diritto privato*, in *Nuova giur. civ. comm.*, Supplemento al fascicolo 4/2007, 1 ss.; S. Rodotà, *Quattro paradigmi per l'identità*, ivi, 21 ss.; V. Scalisi, *L'ermeneutica della dignità*, Milano, 2018, *passim*; A. La Spina, *Complessità e identità personale*, Napoli, 2022, *passim*.

tiva. L'originalità della sua articolazione discende dall'implicazione della cifra ermeneutica dell'*altrove*, così come recentemente pensata, del fatto che « il server è *altrove*, rispetto all'artefatto tecnologico che stiamo usando, così come sono *altrove* le possibili persone con cui possiamo interagire ed è sempre *altrove* la fonte dei contenuti di cui fruiamo » (6).

Un *altrove* che, diversamente da come possa essere affrontato con riferimento alla persona adulta, conosce profili di maggiore complessità quando entra in contatto con una persona minorenne. Difatti, mentre per l'adulto lo specifico problema si traduce, principalmente, nell'apprestare gli strumenti più idonei a tutelare il diritto a non vedere pregiudicata (finanche sottratta), in vario modo, la propria identità personale; per il minorenne può indirizzarsi, anche in via esclusiva, alla salvaguardia dell'interesse a *formarsi* una propria identità, essendo compito dello Stato assicurare « in tutta la misura del possibile, la sopravvivenza e lo sviluppo del fanciullo » (art. 6, par. 2, Convenzione di New York sui diritti del fanciullo).

Segnatamente, con riguardo alla "stagione" della minore età, l'identità personale, intesa come diritto ad « essere uguale solo a sé stesso e diverso da tutti gli altri » (7), si pone in una duplice direzione funzionale: *costruttiva* e *conservativa* della personalità. La minore età passa, infatti, « da una fase nella quale l'interesse della persona concorre a costruirne l'identità a una fase in cui l'acquisita identità determina — o dovrebbe determinare — il contenuto dell'interesse » (8). Specialmente nei primi anni di vita e comunque fino all'età del discernimento, il diritto all'identità personale si sostanzia, principalmente, nell'interesse della persona alla costruzione *libera* e *naturale* del proprio essere; si traduce, invece, (anche) nell'interesse a preservare *ciò che si è* nel momento in cui la personalità (o frammenti di essa) si è edificata, preservando pur sempre la logica del suo continuo divenire (9). Due orizzonti funzionali, questi, che ben si colgono nella Convenzione di New York sui diritti del fanciullo del 1989, rispettivamente negli art. 5 e 8, ove gli Stati si

(6) A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., 47.

(7) F. Giardina, *Interesse del minore: gli aspetti identitari*, in *Nuova giur. civ. comm.*, 2016, II, 159.

(8) *Ibidem*.

(9) S. Rodotà, *Quattro paradigmi per l'identità*, cit., 21 ss. L'a. si riferisce a una « identità nomade, perennemente incompiuta, costruzione incessante e interminata, dunque faticosamente riconducibile a schemi giuridici che vogliono eguaglianza, regolarità, uniformità. E qui si coglie il riflesso d'una situazione più generale, della dialettica tra eguaglianza e diversità registrata anche dall'art. 22 della Carta dei diritti fondamentali dell'Unione europea, dove il riconoscimento della diversità viene significativamente collocato appunto nel capo dedicato all'eguaglianza ».

vincolano a rispettare il diritto e dovere delle persone legalmente responsabili del fanciullo, da un lato « di dare a quest'ultimo, in maniera corrispondente allo sviluppo delle sue capacità, l'orientamento e i consigli adeguati all'esercizio dei diritti che gli sono riconosciuti » dalla Convenzione (fase *costruttiva* dell'identità); dall'altro, a « rispettare il diritto del fanciullo a preservare la propria identità » e di assisterlo e proteggerlo nel caso in cui sia « illegalmente privato degli elementi costitutivi della sua identità o di alcuni di essi » (fase *conservativa* dell'identità) (10).

Orbene, la frequentazione disincarnata dell'ambiente digitale, per come strutturato, espone a rischi elevati entrambi i profili dell'identità personale più propriamente biografica (11).

È nell'ordine di questa consapevolezza che l'art. 28 del Reg. (UE) 2022/2065 (*Digital Services Act*) sancisce che « i fornitori di piattaforme *online* accessibili ai minori adottano misure adeguate e proporzionate per garantire un elevato livello di tutela della vita privata, di sicurezza e di protezione dei minori sul loro servizio ».

Sono noti i differenti contorni esperienziali che caratterizzano la vita sociale *online* rispetto a quella *offline*, sollecitati dall'assenza di limiti territoriali, temporali e di ostacoli all'accesso, le cui traiettorie sono accompagnate dalla diffusa percezione di "navigare" verso orizzonti isolati (12), connotati dall'anonimia dei corpi e delle parole, la quale porta ad assumere comportamenti che normalmente non si terrebbero (13). Lo attesta, con chiarezza, la differente latitudine che assume il cyberbullismo (l. n. 71/2017) (14) rispetto alle tradizionali condotte di bullismo, di solito circoscritte al proprio ambito di frequentazione (ad es. scolastica) e tenute da persone dal

---

(10) E. Meligrana, G. Scorza, *La privacy degli ultimi*, prefazione di A. Spadaro S.I., Soveria Mannelli, 2022, 46 segnalano che la *Barclays Bank* « stima in oltre sette milioni i furti di identità che si consumeranno da qui al 2030 a causa dello *sharenting* — una contrazione di *share* (condividere) e *parenting* (genitorialità) —, espressione con la quale si definisce la sistematica esibizione dei figli a mezzo social e in oltre 800 milioni di dollari il bottino delle frodi informatiche rese possibili da questo fenomeno ».

(11) E. Andreola, *Minori e incapaci in* Internet, Napoli, 2019, 122. L'a. osserva che « in rete l'identità diventa "identità digitale" che attiene all'interesse della persona alla non manipolabilità di quello che essa rappresenta virtualmente, vedendosi riconoscere nel *web* la propria peculiarità intellettuale, politica, sociale e religiosa ».

(12) A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., 48, il quale segnala che « l'isolamento è questione di corpi, la solitudine, invece, è questione di *pensieri* ».

(13) Cfr. E. Andreola, *Misure cautelari a tutela dei minori nei* social network, in *Fam. dir.*, 2021, 853.

(14) Si veda, in proposito, C. Perlingieri, *Profili civilistici dei social networks*, Napoli, 2014, 33 ss.; C. Panicali, *Il* cyberbullismo: *i nuovi strumenti (extrapenali) predisposti dalla legge n. 71/2017 e la tutela penale*, in *Resp. civ. prev.*, 2017, 2081 ss.; R. Bocchini, M.

carattere forte e dominante (15). Nel *cyberspazio* il "bullo" è mosso da altre forze interiori, per la cui comprensione, in termini di esplicazione della libertà, si presta, con straordinaria efficacia euristica, proprio la categoria ermeneutica dell'*altrove*; tant'è che « gli oltraggi, le minacce, le aggressioni verbali, sono rese possibili proprio e soprattutto perché sia chi le attua sia chi le subisce è *altrove*. Non si possono guardare le reazioni emotive di chi è oggetto di violenza, non ci si sente guardati da coloro che vedono o possono vedere ciò che si sta mostrando: questa assenza di sguardi fa scivolare tutto sulla superficie dei *display* » (16). Ma la stessa dinamica si osserva nelle pratiche di *hating*, *phishing*, ecc.

Pertanto, dinanzi alle insidie identitarie del *web*, disincarnate e desituate, le esigenze di protezione si diversificano, nella sostanza, da quelle che si profilano nei medesimi contesti conflittuali *offline*, traducendosi nell'interesse alla tutela della propria personalità fisica e morale (17), non soltanto nei confronti *dell'altro* (una persona o un gruppo identificato), ma *dell'altrove*, che comprende l'ignoto. Deve, di conseguenza, essere rimeditato il tipo di rimedio, orientandolo a contrastare, effettivamente, l'incontrollabilità dei percorsi comunicativi della rete, le "maschere" con cui si interagisce e i congegni tecnici e tecnologici, sempre più sofisticati e intelligenti, di moltiplicazione delle fonti di "danno". È proprio la spazialità dell'eco generata da ogni parola immessa nel *web* che, già da tempo, ha condotto la giurispru-

---

MONTANARI, *Le nuove disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del Cyberbullismo (l. 29 maggio 2017, n. 71)*, in *Nuova giur. civ. comm.*, II, 2018, 340 ss.; S. STANCO, *Il Cyberbullismo: le condotte tipiche e i soggetti coinvolti*, in *Ciberspazio e diritto*, 2018, 279 ss.; E. ANDREOLA, *Minori e incapaci in* Internet, cit., 243 ss.; M. BIANCA, *Il minore e i nuovi* media, in R. SENIGAGLIA (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, Pisa, 2019, 148 ss.; P. VIRGADAMO, *Minori e nuovi* media, in A. CORDIANO e R. SENIGAGLIA (a cura di), *Diritto civile minorile*, Napoli, 2022, 367 ss.

(15) A. CORDIANO, *Cyberbullismo e maleducazione digitale: la legge n. 71 del 2017 tra nuove politiche educative e strumenti tradizionali*, in *Foro nap.*, 2021, 41 ss.; E. BATTELLI, *Minori e* social network: *cyberbullismo e limiti della* parental responsibility, in *Corr. giur.*, 2021, 1269 ss.; C. MURGO, *Frammenti sul bullismo, tra doveri educativi e compensazioni risarcitorie*, in *Resp. civ. prev.*, 2020, 505 ss.

(16) A. PESSINA, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., 114.

(17) G. RESTA, *Dignità, persone e mercati*, Torino, 2014, 102 ss. spiega che con l'espressione "personalità fisica" « si designano generalmente i diritti sugli elementi corporei della personalità: dunque il corpo umano, le sue parti (come organi e tessuti) e i suoi prodotti »; con l'espressione "personalità morale" si designano, invece, « i diritti sugli attributi immateriali e in particolare sugli elementi connotativi dell'identità (nome, immagine voce, ecc.) ». Parla rispettivamente di « beni presupposto » e di « beni fine », costituenti l'identità individuale, A. NICOLUSSI, voce *Autonomia privata e diritti della personalità*, in *Enc. dir.*, Annali, IV, Milano, 2011, 134 ss.

denza a ritenere che « la diffusione di un messaggio diffamatorio attraverso l'uso di una bacheca "facebook" integra un'ipotesi di diffamazione aggravata ai sensi dell'art. 595, comma 3, c.p. sotto il profilo dell'offesa arrecata "con qualsiasi altro mezzo di pubblicità" diverso dalla stampa » (18).

2.3. La funzione educativa del minorenne in formazione identitaria

Nell'esperienza digitale del minore, delle due direzioni funzionali dell'identità personale, poc'anzi segnalate, assume maggiore interesse (se non altro perché meno indagata) quella *costruttiva*, concernente cioè il momento formativo della personalità morale (19). L'ingresso del digitale nella vita della persona *in formazione*, veicolata dalla pratica dell'addomesticamento tecnologico (20), reclama all'ordinamento, con indubbio carattere d'urgenza, la tutela degli interessi identitari coinvolti. Il riferimento è, infatti, a quella fase della vita in cui prende forma la biografia della persona, in cui l'essere si afferma nell'apparire (21), in una dinamica in cui si edifica, per mezzo dell'attività educativa, la capacità di discernimento, di saper distinguere ciò che è conforme da ciò che è contrario al proprio interesse (22). È il momento in cui si celebra l'interazione tra educazione e identità, nel senso che « se

(18) Cass. pen., 20 luglio 2023, n. 31709, in banca dati *De jure*. E questo in quanto « la condotta in tal modo realizzata è potenzialmente capace di raggiungere un numero indeterminato, o comunque quantitativamente apprezzabile, di persone, tenendo altresì conto che la contestualità delle offese in presenza (virtuale) della persona offesa non può certo ricavarsi dalla circostanza che la persona offesa ha dichiarato di avere letto personalmente le offese. Riferire di avere letto un post non può certamente significare di avere avuto immediata contezza delle frasi pubblicate ». V. anche Cass. pen., 25 gennaio 2021, n. 13979, in *Resp. civ. prev.*, 2021, 1943 ss., con nota di G. Manca, *Il bilanciamento fra tutela dell'onore e diritto di critica nella diffamazione sui social network: la « porta stretta » della « insostituibilità lessicale »*. Cfr. inoltre V. Zeno-Zencovich, *La pretesa estensione alla telematica del regime della stampa*, in *Dir. inf.*, 1998, 12 ss.; E. Andreola, *Illecito diffamatorio a mezzo giornale telematico, danno e onere della prova*, in *Danno resp.*, 2023, 201 ss.

(19) A. Nicolussi, voce *Autonomia privata e diritti della personalità*, cit., 138; G. Resta, *Dignità, persone e mercati*, cit., 103.

(20) V. Andreoli, *La famiglia digitale. Come la tecnologia ci sta cambiando*, Milano, 2021, 49 ss.

(21) F. Giardina, *Interesse del minore: gli aspetti identitari*, cit., 160; A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., 39, il quale aggiunge che « apparire significa, sempre, anche essere ».

(22) Su questi profili problematici, si vedano, in particolare i lavori monografici di P. Stanzione, *Capacità e minore età nella problematica della persona umana*, con la prefazione di R. Pane, rist. dell'edizione del 1975, Napoli, 2018; F. Giardina, *La condizione giuridica del minore*, Napoli, 1984; G. Palmieri, *Diritti senza poteri. La condizione giuridica dei minori*, Napoli, 1994; L. Tafaro, *L'età per l'attività*, Napoli, 2003; M. Cinque, *Il minore contraente. Contesti e limiti della capacità*, Padova, 2007; R. Senigaglia, *Minore età e contratto. Contributo*

l'educazione è destinata a creare un'identità, l'identità orienta e dirige l'educazione » (23). Ma è anche il momento in cui l'essere è facilmente plasmabile dal bisogno di apparire, dai desiderata altrui, da come si vorrebbe essere percepiti (24).

Ebbene, l'irrompere del digitale nella vita del minore, sin dalla prima infanzia, assume, da subito, carattere pervasivo della persona (25): non soltanto a seguito dell'utilizzo diretto degli artefatti tecnologici per giocare, comunicare, informarsi, ecc., ma pure per effetto della circolazione (e, dunque, del trattamento *ex* art. 4, par. 1, n. 2), Reg. (UE) 2016/679) dei suoi dati personali nella rete, innescata, in special modo, dai genitori o da altri familiari nel momento in cui postano sui *social network*, sovente in modo compulsivo, immagini o comunque informazioni, anche intime, riguardanti la persona del minore (26). Ma pure per iniziativa di altri soggetti (27), ivi inclusi gli operatori del *web*, i quali attingono quelle informazioni dallo

---

alla teoria della capacità, Torino, 2020. Rileva segnalare in proposito anche Cass., 28 agosto 2009, n. 18804, in *Dir. fam.*, 2010, 654, nel passaggio in cui specifica che il dovere di educazione e di formazione consiste nell'aver fatto conseguire al figlio « l'equilibrato sviluppo psicoemotivo, la capacità di dominare gli istinti, il rispetto degli altri e tutto ciò in cui si estrinseca la maturità personale ».

(23) F. Giardina, *Interesse del minore: gli aspetti identitari*, cit., 164.

(24) L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, 68.

(25) Sul tema V. Corriero, Privacy *del minore e potestà dei genitori*, in *Rass. dir. civ.*, 2004; A. Thiene, *L'inconsistente tutela dei minori nel mondo digitale*, in *Studium iuris*, 2012, 528 ss.; C. Camardi, *Minori e* privacy *nel contesto delle relazioni familiari*, in R. Senigaglia (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, cit., 122; V. Andreoli, *La famiglia digitale. Come la tecnologia ci sta cambiando*, cit., *passim*; R. Senigaglia, *Il dovere di educare i figli nell'era digitale*, in *Pers. merc.*, 2021, 518 ss.; E. Battelli, *Il trattamento dei dati nel prisma della tutela della persona minore di età*, in *Dir. inf.*, 2022, 267.

(26) Su questo fenomeno v. E. Meligrana, G. Scorza, *La privacy degli ultimi*, prefazione di A. Spadaro S.I., cit., 42-45, in cui si segnala che « i bambini, una delle categorie più vulnerabili rispetto alle cose della privacy — e non solo della privacy—, si ritrovano, così, inconsapevolmente, a pagare con miliardi di frammenti della loro identità personale qualche ora di gioco o di sorrisi. (...) È già storia che le fotografie di tre miliardi di utenti di social network e siti internet diversi siano finiti — grazie a un'imponente operazione di pesca a strascico alla quale non c'è ragione di ritenere che siano state sottratte le foto dei più piccoli presenti *online* — negli archivi di una società, la Clearview AI, che fornisce alle forze dell'ordine e alle agenzie di intelligence di mezzo mondo servizi di riconoscimento intelligente ». V. anche F. Scia, *Diritti dei minori e responsabilità dei genitori nell'era digitale*, Napoli, 2020, 17 ss.; I. Garaci, *Il « superiore interesse del minore » nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, in *Nuove leggi civ. comm.*, 2021, 801 ss. L'inserimento di fotografie di minorenni nei *social network* è ritenuto di per sé potenzialmente dannoso, « in quanto ciò determina la diffusione delle immagini fra un numero indeterminato di persone, conosciute e non, le quali possono essere malintenzionate e avvicinarsi ai bambini dopo averli visti più volte in foto *online*, non potendo inoltre andare sottaciuto l'ulteriore pericolo

spazio digitale dei dati personali e dai colossi dell'economia di *internet*, i quali "catturano" i dati dall'utilizzo che il minore fa dei contenuti, dei servizi e delle relative tecnologie, anche applicate al corpo (si pensi alla sempre più diffusa pratica dei *wearables* e, in generale, dell'*Internet of Things*), le quali comunicano frammenti dell'identità anagrafica o biologica, ma anche biografica del minore (28). E ciò con il rischio che i dati personali, spesso acquisiti nel mancato rispetto delle coordinate fissate dal GDPR tra protezione e circolazione (29), finiscano in qualche trama della rete che "restituisca" al minore pezzi mancanti della sua identità, *eteroimposti* dalla tirannia degli al-

---

costituito dalla condotta di soggetti che taggano le foto on-line dei minori e, con procedimenti di fotomontaggio, ne traggono materiale pedopornografico da far circolare fra gli interessati. Dunque, il pregiudizio per il minore è insito nella diffusione della sua immagine sui *social network* sicché l'ordine di inibitoria e di rimozione va impartito immediatamente », così Trib. Trani, 7 settembre 2021, in banca dati *OneLegale*. Si veda inoltre Trib. Livorno, 30 gennaio 2013, n. 94, in banca dati *De jure*; Trib. Mantova, 19 settembre 2017, in *www.Ilfamiliarista.it*, 18 gennaio 2018, con nota di Molfino, *Vietato pubblicare le foto dei figli sui social network senza il consenso dell'altro genitore*.

(27) Relativamente alla pubblicazione di immagini del minore da parte dell'ex compagna del padre v. Trib. Bari, 7 novembre 2019, in *Dir. internet*, 2020, 87 ss., con commento di Maggi, *Consenso e tutela del diritto all'immagine del minorenne: tra diritto della personalità e protezione dei dati dei minori*.

(28) Sul tema v. S. Stefanelli, *Privacy e immagine dei minori in Internet*, in *Cyberspazio e diritto*, 2, 2012, 233 ss.; E. Andreola, *Minori e incapaci in* Internet, cit., 148 ss.; V. Andreoli, *La famiglia digitale. Come la tecnologia ci sta cambiando*, cit., 44 s. La comunicazione della Commissione su *Un decennio digitale per bambini e giovani: la nuova strategia europea per un internet migliore per i ragazzi (BIK+)*, COM (2022) 212 final, segnala che « oggigiorno i servizi digitali raccolgono e condividono dati sui minori senza soluzione di continuità; la "datificazione" ha inizio persino prima della nascita. Se l'aggregazione di megadati può consentire di ottenere informazioni innovative, ad esempio per quanto concerne la salute e l'istruzione dei minori, la datificazione dell'infanzia può anche provocare ripercussioni potenzialmente negative per tutta la vita sul benessere e lo sviluppo dei minori ». Sull'*Internet of Things*, v. R. Schulze, D. Staudenmayer (a cura di), *Digital Revolution: challenges for contract law in practice*, Baden-Baden, 2016, 135 ss.; S. Wachter, *Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR*, in *Computer Law & Security Review*, 2018, 436 ss.; Id., *The GDPR and the Internet of Things: a three-step transparency model*, in *Law, Innovation and Technology*, 2018, 266 ss.

(29) Su questi aspetti si rinvia ad Aa.Vv., *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, opera diretta da G. Finocchiaro, Bologna 2017; V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; A. De Franceschi, R. Schulze, *Digital revolution-new challenges for law. Data protection, artificial intelligence, smart products, blockchain technology and virtual currencies*, Baden-Baden, 2019, 75 ss.; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019; C.J. Hoofnagle, B. van der Sloot, F. Zuiderveen Borgesius, *The European Union general data protection regulation: what it is and what it means*, in *Information & Communications Technology Law*, 2019, 65 ss.; L. Bozzi, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in *Eur. dir. priv.*, 2020, 253; R. Senigaglia, *Minore*

goritmi (30) e, quindi, sottratti alla formazione *naturale* della sua personalità morale, rispondente alle sue capacità, aspirazioni e inclinazioni naturali.

Ebbene, il fattore eversivo dello statuto educativo del minore *in formazione* sta esattamente nella *eteroimposizione* anziché nella *eterodeterminazione* della sua identità personale (31).

Difatti, il "piccolo minore", sprovvisto della capacità di discernimento, dal momento della nascita e nei primi anni di vita edifica la propria identità personale in gran parte in modo eterodeterminato. Questo accade senz'altro con riguardo alla sua identità genetica (definita dalla c.d. « lotteria dei geni ») ed anagrafica, ma pure relativamente alla sua identità biografica, agli aspetti costitutivi la sua personalità morale (32).

Ora, tralasciando le ordinarie influenze promananti dall'ambiente sociale di riferimento, le quali rinviano al « sé concepito come un sistema informazionale complesso » (33), l'opera principale di edificazione della personalità del minore compete ai genitori nell'esercizio della responsabilità genitoriale (art. 316 c.c.). E si tratta di un'attività *complessa* fatta di educazione, istruzione e assistenza morale, oggi consegnata a un metodo comunionale, avulso da ogni forma di autarchia, richiedente ai genitori un atteggiamento empatico nella cura del figlio (34).

---

età e contratto. Contributo alla teoria della capacità, cit., 75 ss.; V. Ricciuto, *L'equivoco della privacy. Persona vs. dato personale*, Napoli, 2022, *passim*; B. Parenzo, *Sull'importanza del dire le cose come stanno: ovvero, sul perché della necessità di riconoscere la natura patrimoniale dei dati personali e l'esistenza di uno scambio sotteso ai c.d. servizi digitali gratuiti*, in *Dir. fam.*, 2021, 1457 ss.; A. Bernes, *Enhancing Transparency of Data Processing and Data Subject's Rights Through Technical Tools: The PIMS and PDS Solution*, in R. Senigaglia, C. Irti, A. Bernes, *Privacy and Data Protection in Software Services*, Singapore, 2022, 197 ss.

(30) Si rinvia a T.Z. Zarsky, *"Mine your own business!": making the case for the implications of the data mining of personal information in the forum of public opinion*, in *Yale Journal of Law and Technology*, 2003, 1 ss.; F. Pasquale, *The Black Box Society. The secret algorithms that control money and information*, Cambridge, Massachusetts, London, 2015; S. Rodotà, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014, 38 ss.; L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., 72 ss.; S. Zuboff, *Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri,* Roma*,* 2019, *passim*.

(31) Su questi diversi profili si rinvia a P. Zatti, *Dimensioni e aspetti dell'identità nel diritto privato attuale*, cit., 4 ss.

(32) L. Lenti, *L'identità del minorenne*, in *L'identità nell'orizzonte del diritto privato*, cit., 67 s.

(33) L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., 78, il quale aggiunge che « in questa prospettiva, noi siamo le nostre informazioni. Dal momento che condizionano profondamente questi schemi informazionali, le ICT sono invero potenti tecnologie del sé ».

(34) Cfr. P. Donati, *La famiglia come relazione sociale*, II ed., Milano, 1992, *passim;* N. Luhmann, *Il sistema sociale famiglia*, in *La ricerca sociale*, n. 39, 1989, 233 ss.

Abbattuti gli ultimi stigmi normativi della rappresentazione gerarchica dei rapporti familiari, ivi inclusi quelli discendenti dalla impostazione adultocentrica e autoritaria del rapporto di filiazione propria della situazione soggettiva della potestà (patria prima, genitoriale poi), dopo la riforma del 2012-2013 i genitori sono chiamati a istruire, educare e assistere moralmente il figlio non più « *tenendo conto* » ma « *nel rispetto* » delle sue capacità, inclinazioni naturali e aspirazioni (artt. 147 e 315-*bis* c.c.) (35).

In sostanza, l'opera edificante identitaria, di cui i genitori detengono la *responsabilità*, deve essere amministrata nel rispetto della personalità del figlio a mano a mano che emerge; detto altrimenti, ogni frammento della stessa offre ai genitori spunti di metodo per tracciare i percorsi educativi (36). I genitori, in pratica, sono chiamati a porsi in perenne ascolto del migliore interesse del minore, assumendo, progressivamente, il punto di vista del figlio fino a far maturare in lui la capacità di discernimento e, dunque, la libertà di autodeterminarsi. È così che, nei primi anni di vita del figlio, la "lettura" del suo *best interest* compete alla *responsabilità* genitoriale ed è condotta prevalentemente all'insegna della cultura della famiglia dei genitori e del fine di affermarne una continuità nella persona del figlio (37). Una cultura, che per incontrare il *best interest* deve essere conforme ai valori del vivere sociale e deve adattarsi ai profili identitari del figlio via via che emergono (38). In questo ordine di senso, il concetto di responsabilità genitoriale si declina, in

---

(35) Su questo profilo funzionale v. F. Ruscello, *La funzione educativa: dottrina e giurisprudenza a* confronto, in *Rass. dir. civ.*, 1986, 430 ss.; A. Trabucchi, *Il "vero interesse" del minore e i diritti di chi ha l'obbligo di educare*, in *Riv. dir. civ.*, 1988, 737 ss.; G.F. Basini, *I diritti-doveri dei genitori e dei figli*, in *Tratt. dir. fam.*, diretto da G. Bonilini, vol. IV, *La filiazione e l'adozione*, Torino, 2016, 4045 ss.; A. Gorgoni, *Filiazione e responsabilità genitoriale*, Padova, 2017, 104 ss.; M. Tamponi, *Del convivere. La società postfamiliare*, Milano, 2019, 259; P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, IV ed. riscritta e ampliata, III, *Situazioni giuridiche soggettive*, Napoli, 2020, 373 ss.; R. Senigaglia, *Il dovere di rispettare i genitori nella coercibilità dell'ordinamento giuridico*, in *Dir. fam. pers.*, 2023, 840 ss.

(36) P. Zatti, *Dimensioni e aspetti dell'identità nel diritto privato attuale*, cit., 7. L'a. sottolinea che il legislatore del '75 ha voluto imprimere questa cifra alla funzione educativa dei genitori; « ciò significa sostituire ad un obiettivo di omologazione a valori prefissati un obiettivo che in linguaggio psicologico si potrebbe chiamare *individuazione*: consentire e promuovere l'emersione di ciò che la persona del minore, nella sua integrità e profondità, può essere; ancora una volta, del « destino personale » e non di una legge di vita imposta ».

(37) In questo senso S. Patti, *Le nuove frontiere della responsabilità genitoriale*, in *Familia*, 2022, 145. Si veda, inoltre, A. Trabucchi, *Il "vero interesse" del minore e i diritti di chi ha l'obbligo di educare*, cit., 745 s.; L. Rossi Carleo, *La famiglia dei figli*, in *Giur. it.*, 2014, V, 1262 ss.; R. Senigaglia, *Il dovere di educare i figli nell'era digitale*, cit., 519.

(38) Cfr. P. Zatti, *Rapporto educativo ed intervento del giudice*, in A. Belvedere e M. De Cristofaro (a cura di), *L'autonomia dei minori tra famiglia e società*, Milano, 1980, 234 ss.; P.

sintesi, nel rispondere all'interesse del figlio, nel senso di cogliere in ogni momento della crescita, con l'empatia tipica della genitorialità, ciò che maggiormente edifica il suo benessere personale, forgiando, in tal modo, la sua identità (39).

In definitiva, è essenzialmente l'assolvimento del dovere di educazione che porta a compimento l'opera di edificazione della personalità del figlio (40). Una funzione che già la Costituzione assegna anzitutto ai genitori e, soltanto in caso di incapacità di questi, demanda alla legge il compito di individuare delle figure vicarie (art. 30, commi 1 e 2); comunque, essa deve essere assolta in modo *naturale*, ovvero non secondo schemi astratti, definiti una volta per tutte, ma cogliendo dalla narrazione dell'*essere* del figlio gli spunti di metodo della pedagogia dell'*apparire* (41).

Il valore fondamentale di questo ordinamento della funzione genitoriale è espresso dal regime rimediale apprestato dal legislatore per far fronte all'incapacità dei genitori di "leggere" e di realizzare il migliore interesse del figlio nel « rispetto » della sua personalità, tanto da rendere *precaria* la responsabilità genitoriale: la violazione o la trascuratezza dei doveri o l'abuso dei poteri genitoriali, può comportare limitazioni o finanche la decadenza dalla responsabilità genitoriale (artt. 330 e 333 c.c.), specie quando il figlio è "piccolo" e la disfunzione denunciata incide, inevitabilmente, sulla sua identità personale *in formazione*.

2.4. Il principio della necessaria esclusività "incarnata" del ruolo educativo dei genitori

Nell'era predigitale, la funzione *costruttiva* dell'identità personale del figlio era pacificamente prerogativa *esclusiva* dei genitori o della persona preposta dalla legge ad esercitare tutte o alcune delle funzioni genitoriali

---

Perlingieri, *La libertà di educazione*, in *Rass. dir. civ.*, 1987, 681 ss.; M. Paradiso, *I rapporti personali tra coniugi, Artt. 143-148*, in *Comm. Schlesinger*, Milano, 2012, 289 ss.

(39) Sulla formazione dell'identità nei primi anni di vita si rinvia a L. Lenti, *L'identità del minorenne*, cit., 65.

(40) Cfr. A. Thiene, *Gioventù bruciata online: quale responsabilità per i genitori?*, in A. Annoni e A. Thiene (a cura di), *Minori e privacy. La tutela dei dati personali dei bambini e degli adolescenti alla luce del Regolamento (UE) 2016/679*, Napoli, 2019, 41 ss.

(41) Nel preambolo della Convenzione di New York sui diritti del fanciullo del 20 novembre 1989 si esprime la convinzione « che la famiglia, unità fondamentale della società e ambiente naturale per la crescita e il benessere di tutti i suoi membri e in particolare dei fanciulli, deve ricevere la protezione e l'assistenza di cui necessita per poter svolgere integralmente il suo ruolo nella collettività, riconoscendo che il fanciullo, ai fini dello sviluppo armonioso e completo della sua personalità deve crescere in un ambiente familiare in un clima di felicità, di amore e di comprensione ».

(tutore, affidatario, ecc.). Questa esclusività, *ab origine* discendente dal diritto naturale (42) e che ancora connota la vita sociale del minore *offline*, è garantita anche nel caso in cui intervengano elementi di alterità; altri soggetti, cioè, partecipino all'educazione del figlio, come nel caso di *baby sitter*, della scuola, della parrocchia, ecc. (43), cooperando alla formazione della sua biografia. In queste situazioni, invero, i genitori versano nella condizione materiale di poter affermare la loro "esclusiva", giacché l'esposizione antropologica del figlio riguarda comunque *altri* (identificati o identificabili), permanendo, quindi, nella loro sfera di controllo; specialmente quando il figlio è "piccolo", i genitori autorizzano le relazioni anzidette ed esercitano costantemente il controllo e la sorveglianza sia sugli educatori sia sul figlio. Ma anche nelle relazioni sociali non istituzionalizzate, i genitori possono informarsi e osservare l'ambiente e le persone frequentate dal figlio e, sulla scorta dell'empatia che deve caratterizzare la genitorialità, ricondurre ad esse eventuali segnali di disagio.

Questa *esclusività*, almeno in termini pratici, rischia, invece, di essere scardinata nel momento in cui il figlio accede alla rete (44). E normalmente ciò avviene sin dai primi anni di vita, in cui l'ambiente digitale si apre al minore come spazio insaziabile di gioco, di apprendimento, di osservazione e di interazione. È così che il *web*, per mezzo del meccanismo, talvolta spasmodico e inconsapevole, (45) di *input* (composti per lo più da dati personali del minore) e *output* (composti da dati scelti e comunicati dalla rete) partecipa all'educazione del figlio impattando, inevitabilmente, sulla sua identità (46). Per questo i minori sono considerati meritevoli di una « specifica protezione relativamente ai loro dati personali » la quale « dovrebbe, in

---

(42) È esplicita, in questi termini, la Costituzione tedesca, la quale all'art. 6 si esprime in termini di diritto naturale, prevedendo che « *Pflege und Erziehung der Kinder sind das natürliche Recht der Eltern und die zuvörderst ihnen obliegende Pflicht. Über ihre Betätigung wacht die staatliche Gemeinschaft* ». Sull'idea e sul ruolo del diritto naturale si rinvia a F. Viola, *1900-2020. Una storia del diritto naturale*, Torino, 2021, *passim*.

(43) Si veda, in proposito, G. Abbamonte, *Il diritto all'educazione*, in *Iustitia*, 1982, 201 ss.

(44) Cfr. E. Andreola, *Misure cautelari a tutela dei minori nei* social network, cit., 850, la quale osserva che la tutela del minore in questo ambiente « attiene alla garanzia delle prerogative costituzionali della persona (diritto all'immagine, alla riservatezza, all'integrità morale) ». V. pure V. Andreoli, *La famiglia digitale. Come la tecnologia ci sta cambiando*, cit., 73 ss.

(45) A. Mantelero, *Children online and the future EU data protection framework. Empirical evidences and legal analysis*, in *International Journal of Technology Policy & Law*, 2016, 1 ss.

(46) Si veda, in proposito, F. Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, 384 ss.; A. Thiene,

particolare, riguardare l'utilizzo dei dati personali dei minori ai fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore » (Considerando 38, GDPR); inoltre, le informazioni privacy a loro rivolte dovrebbero « utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente » (Considerando 58 e art. 12, par. 1, GDPR) (47).

Ma il carattere inedito rispetto a quanto accade nelle relazioni *offline*, peraltro oggi "mescolate" a quelle *online* nella dimensione dell'*onlife* (48), è che l'esperienza digitale del minore può facilmente avvenire al di fuori delle concrete possibilità di controllo e di sorveglianza dei genitori. Il *libero* accesso al *cyberspazio*, in pratica, produce inevitabilmente un effetto eversivo del principio dell'esclusività educativa dei genitori, nei termini anzidetti, e istituisce un altro centro di esclusività educativa in capo ai titolari delle piattaforme del *web*, questa volta "oscurato", disincarnato e avvinto dall'analfabetismo emotivo (49). La stessa velocità di interazione e di consultazione, in uno con l'abilità tecnologica che il *cybernauta* minorenne presto acquisisce, anche nel non lasciare tracce evidenti delle proprie visite e dei propri *input*, sottrae al controllo del genitore le imposizioni, gli stimoli e gli abusi identitari promananti dalla rete (50).

E questo specialmente in ragione della sovraesposizione antropologica che contraddistingue l'ambiente digitale, essendo esso strutturato all'insegna di una componente di alterità non decifrabile, perché governata da « altri, da una miriade di altri, di cui solo alcuni appaiono » (51).

L'unica via per difendere le prerogative genitoriali sarebbe escludere il figlio dall'accesso alla rete; decisione, questa, non legittima perché lesiva dello sviluppo della personalità del minore, atteso che l'accesso al *web* è un diritto fondamentale e, specialmente per gli adolescenti, una forma di

---

Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo, in *Nuove leggi civ. comm.*, 2017, 424.

(47) Su questi profili problematici v. S. Stefanelli, *Privacy e immagine dei minori in internet*, cit., 233 ss.

(48) Su questo concetto v. L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., 47 ss.

(49) Su internet come spazio delle emozioni e non dei sentimenti v. U. Galimberti, *L'ospite inquietante. Il nichilismo e i giovani*, Milano, 2007; D. Goleman, *Intelligenza emotiva. Che cos'è e perché può renderci felici*, Milano, 2011.

(50) Cfr. E. Andreola, *Misure cautelari a tutela dei minori nei* social network, cit., 859.

(51) A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., 39.

sopravvivenza sociale (52), estrinsecazione, a sua volta, della libertà di espressione e di informazione (art. 11 CDFUE; artt. 14 e 17 CNY). È in nome di questo interesse che si spiegano i tre pilastri indicati dalla Commissione europea nell'ambito della strategia BIK+ (un internet migliore per i ragazzi) (53), all'insegna dei quali devono attuarsi le azioni dell'Unione europea: 1) esperienze digitali sicure per proteggere i minori e per migliorare il loro benessere *online*; 2) conferimento di maggiore autonomia e responsabilità digitali; 3) partecipazione attiva, nel rispetto dei minori, ai quali sarà data voce nell'ambiente digitale (54).

Ebbene, al cospetto del sistema ordinamentale, l'accesso *libero* alla rete del "piccolo minore" sia come attore sia come spettatore (55), con le conseguenze che ne discendono in termini *costitutivi* della sua identità personale, pone principalmente due problemi di tenuta valoriale: da un lato, come si è poc'anzi osservato, dà luogo a "contatti" de-situati e disincarnati, i quali contrastano col principio di esclusività educativa che ordina il rapporto genitori-figli, di fonte costituzionale e convenzionale (art. 30 Cost.; artt. 5 e 18 CNY); dall'altro, confligge pure con il diritto fondamentale del figlio alla formazione *libera* e *naturale* della sua identità personale. Formazione, che, per essere tale nel concorso di educazione, istruzione e assistenza morale, come ben chiarisce l'art. 315-*bis* c.c., deve essere *rispettosa* delle capacità, inclinazioni naturali e aspirazioni dei figli; deve essere, in sostanza, aderente alla (o ai frammenti della) singolare personalità del figlio. In altre parole, l'assiologia dell'educazione del minore è tutta ordinata dalla cifra ermeneutica dell'*incarnazione*, consegnata, normalmente, alla figura dei genitori, i quali la praticano all'insegna dell'interazione empatica, comunionale e de-

---

(52) Si veda J. Bakan, *Assalto all'infanzia. Come le* corporation *stanno trasformando i nostri figli in consumatori sfrenati*, prefazione di C. Saraceno, Milano, 2012, 55 ss.; F. Scia, *Diritti dei minori e responsabilità dei genitori nell'era digitale*, cit., 36.

(53) Vedi *supra* nota n. 1.

(54) Segnatamente, i "tre pilastri" sono descritti dalla Commissione in questi termini: « 1. Esperienze digitali sicure per proteggere i minori online da contenuti, condotte, contatti e rischi per i consumatori dannosi e illegali e per migliorare il loro benessere online attraverso un ambiente digitale adeguato all'età e sicuro; 2. Conferimento di maggiore autonomia e responsabilità digitali in modo che i minori acquisiscano le competenze e le abilità necessarie per compiere scelte consapevoli ed esprimersi nell'ambiente online in modo sicuro e responsabile; 3. Partecipazione attiva, nel rispetto dei minori, ai quali sarà data voce nell'ambiente digitale, con più attività guidate dai minori per promuovere esperienze digitali sicure, innovative e creative ».

(55) A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., 111; l'a. segnala che « i *social* sono il regno dell'individuale, costruiti secondo la logica dello *spettatore* e questo comporta l'esigenza della spettacolarizzazione di tutto quanto viene comunicato ».

mocratica con la persona del figlio. Chiara, in questo senso, è la Convenzione di New York sui diritti del fanciullo, la quale riconosce al minore il diritto alla libertà di pensiero, di coscienza e di religione e, nel contempo, vincola gli Stati parti a rispettare il dovere dei genitori (ecco l'emersione del principio di esclusività) di « guidare il fanciullo nell'esercizio del summenzionato diritto in modo che corrisponda allo sviluppo delle sue capacità » (art. 14 CNY).

È evidente che le tecniche e le tecnologie della rete sono strutturalmente incapaci e, quindi, oggettivamente inidonee ad assolvere alla funzione educativa e, quindi, a contribuire alla formazione *libera* e *naturale* dell'identità del minore, specie della sua personalità morale, selezionando i percorsi che meglio si addicono al suo *best interest*.

La rete conosce il minore soltanto, e non sempre, nella sua identità anagrafica, in qualche isolato frammento della sua biografia (56), e spesso sulla base di *input* (dati) che intendono farle pervenire un'identità "isolata", "episodica" e comunque ipocrita; non lo può, invece, conoscere nella sua "carne", nella concretezza del suo interesse (57).

E si tratta, ribadiamo, di un fattore di indubbia rilevanza giuridica atteso che l'interesse del minore di essere formato in consonanza con il (nel pieno rispetto del) suo concreto *best interest* è oggetto di un diritto fondamentale del figlio, come chiaramente sancito anche dal nostro codice civile all'art. 315-*bis* (58).

La rete, pertanto, interagisce non con la persona, ma con il profilo *deciso* (anche in modo autonomo) dall'algoritmo (59), nutrito dai dati comunicati dall'utente minorenne, che consentono finanche di collocarlo in dei *cluster* e di qui nutrirlo di informazioni per *imporgli*, anche attraverso il meccanismo

---

(56) Cfr. A. La Spina, *Complessità e identità personale*, cit., 288. L'a. sottolinea che sotto il profilo identificativo « l'identità nella realtà *online* (aggettivabile come digitale, elettronica o informatica) costituisce per il soggetto la porta di accesso al sistema digitale globale ».

(57) Cfr. G. Garofalo, *Identità digitale e diritto all'oblio: questioni aperte dopo l'approvazione del GDPR*, in *Dir. fam. pers.*, 2021, 1506 ss.

(58) Si veda E. Al Mureden e M. Sesta, Sub *art. 315*-bis, in M. Sesta (a cura di), *Codice della famiglia*, III ed., Milano, 2015, 1166.

(59) Su questi meccanismi v. M. Hildebrandt, *The Dawn of a Critical Transparency Right for the Profiling Era*, in *Digital Enlightement Yearbook*, 2012, 41 ss.; B. Van der Sloot, D. Broeders, E. Schrijvers (a cura di)*, Exploring the boundaries of big data,* Amsterdam, 2016; M. Bianca, *La filter bubble e il problema dell'identità digitale*, in *Media Laws*, 2019, 46 ss.; E. Cirone, *Big data e tutela dei diritti fondamentali: la ricerca di un (difficile) equilibrio nell'ambito delle iniziative europee*, in Dorigo (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Firenze, 2020, 145 ss.; G. Di Rosa, *Quali regole per i sistemi automatizzati "intelligenti"?*, in *Riv. dir. civ.*, 2021, 832; I. Garaci, *Il « superiore interesse del minore » nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, in *Nuove leggi civ. comm.*, 2021, 817 ss.

della *filter bubble* (60), i tratti identitari, omologati, del *cluster*, facendogli assumere un sé sociale pre-determinato (61); tutto ciò per fini non di solidarietà familiare o comunque sociale, bensì sempre e soltanto per perseguire interessi di carattere patrimoniale, posto che la logica personalistica non apparterebbe all'ecosistema di Internet (62). È esattamente nella coscienza della logica individualistica del capitalismo delle piattaforme (63) che il legislatore europeo, nell'articolare i requisiti di sicurezza e le misure di controllo dell'ambiente digitale, nel *Digital Services Act* ha considerato che « i fornitori di piattaforme online non dovrebbero presentare inserzioni pubblicitarie basate sulla profilazione utilizzando i dati personali del destinatario del servizio se sono consapevoli con ragionevole certezza che il destinatario del servizio è minore » (Considerando 71, Reg. (UE) 2022/2065) (64).

Alla stregua dei meccanismi sin qui esposti si forma e si afferma l'« *identità in Rete* » (65), la quale partecipa all'*altrove* disincarnato e artificiale, e può essere altro dall'identità personale, la quale è l'unica a costituire il fondamentale giuridico, fatti salvi i casi in cui la prima assuma carattere unicamente identificativo della persona (come in talune ipotesi di *nickname*), integrando i presupposti della tutela dello pseudonimo (66).

---

(60) Si rinvia a E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, New York, 2011; M. Bianca, *La filter bubble e il problema dell'identità digitale*, cit., 44 ss.

(61) L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, 69, il quale segnala che « il sé sociale è il principale canale attraverso cui le ICT, e in particolar modo i social media interattivi, esercitano il loro profondo impatto sulle nostre identità personali ».

(62) Cfr. A. La Spina, *Complessità e identità personale*, cit., la quale, ritiene che « la finalità perseguita mediante l'attività di profilazione, specificamente la classificazione in classi dei soggetti, e, quindi, la funzione che il profilo è chiamato ad assolvere, nonché le modalità con le quali vengono raccolti i dati da utilizzare a tal fine, evidenziano le ragioni per le quali il profilo non può coincidere con l'identità personale né delinearla, in quanto ne dà inevitabilmente una rappresentazione parziale e in qualche misura falsa e, pertanto, attualizza inevitabilmente già in sé il rischio della lesione del diritto all'identità ».

(63) In proposito, D. Di Sabato, *Diritto e* new economy, Napoli, 2020, 152 s.

(64) Ha pure considerato che « conformemente al regolamento (UE) 2016/679, in particolare al principio della minimizzazione dei dati di cui al suo articolo 5, paragrafo 1, lettera *c*), tale divieto non dovrebbe indurre il fornitore della piattaforma online a mantenere, acquisire o trattare un numero di dati personali superiore a quello di cui dispone già per valutare se il destinatario del servizio è un minore. Pertanto, tale obbligo non dovrebbe incentivare i fornitori di piattaforme *online* a rilevare l'età del destinatario del servizio prima del loro utilizzo ».

(65) S. Rodotà, *Vivere la democrazia*, Bari-Roma, 2018, 10.

(66) In proposito, si veda G. Piazza, voce *Pseudonimo*, in *Enc. dir.*, XXXVII, Milano, 1988, 893; P. Zatti, *Dimensioni e aspetti dell'identità nel diritto privato attuale*, cit., 4; A. La

Si comprende allora che, nell'esperienza digitale del minore (specialmente se "piccolo") governata da una « "sovraesposizione antropologica" della realtà » (67), l'interesse meritevole di protezione consiste nell'evitare di cadere vittima di percorsi e tecniche tendenti, talvolta in modo subdolo, a *imporgli* un'identità, con metodo del tutto avulso dalla cultura, dalla sensibilità e dalla responsabilità umana, ma pure dalla personalità morale, via via che emerge, del minore. Elementi, questi, che, come dicevamo, non possono non accompagnare la formazione del figlio e che, proprio in ragione di ciò, il sistema ordinamentale demanda ai genitori e alle altre persone che la legge designa alla cura del minore. L'interesse si traduce, pertanto, nell'apprestare le garanzie, ragionevoli e proporzionate, all'*esclusività dell'educazione*, della responsabilità dei genitori « di allevare il fanciullo e di provvedere al suo sviluppo » (art. 18, par. 1, CNY), anche in termini di possibilità di sorvegliare l'attività del figlio nell'ambiente digitale.

2.5. Il dovere di vigilanza dei genitori *vs.* il libero accesso del minore ai contenuti della rete

Il dovere di sorveglianza — o meglio, stando agli attuali assetti assiologici del rapporto di filiazione, di vigilanza (68) — costituisce uno dei contenuti della responsabilità genitoriale: la sua inosservanza può comportare non soltanto un provvedimento *de potestate,* in caso di pregiudizio dell'interesse del figlio, ma pure l'esposizione del genitore alla responsabilità per danni cagionati a terzi dal figlio *ex* artt. 2047 e 2048 c.c.

Pur differenziandosi nella fattispecie, a seconda che il figlio versi o meno in uno stato di incapacità di intendere o di volere al momento della commissione del fatto dannoso, il presupposto comune per l'operatività di entrambe le previsioni di responsabilità è proprio la *culpa in vigilando* ovvero l'omissione dei doveri di sorveglianza (69), in termini di

---

Spina, *Complessità e identità personale*, cit., 287 ss. In giurisprudenza v., in particolare, Cass. pen., 28 novembre 2012, n. 18826, in *Guida al dir.*, 2013, 63.

(67) Espressione utilizzata da A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., 39 con lo scopo di segnalare « come l'esperienza individuale, con l'avvento delle nuove tecnologie, sia continuamente *sovraesposta* dall'intervento di altri "punti di vista" antropologici, che restano sullo sfondo, mentre ci presentano frammenti di mondo ».

(68) R. Senigaglia, *Responsabilità genitoriale e responsabilità dei genitori nella complessità generata (anche) dalla vita sociale digitale*, in *Dir. succ. fam.*, 2022, 1031 ss. V. inoltre M. Sesta, *Genitori e figli tra potestà e responsabilità*, in *Riv. dir. priv.*, 2000, 238 ss.

(69) M. Comporti, *Fatti illeciti: le responsabilità presunte. Artt. 2044-2048*, in *Il cod. civ. comm.*, fondato da P. Schlesinger, diretto da F.D. Busnelli, Milano, 2002, 241; l'a. sintetizza la questione in questi termini: « Se si riflette sui diversi e maggiori doveri che, sotto il profilo

controllo dell'esercizio della libertà del figlio, che incombono in capo ai genitori (70).

Ebbene, in caso di pregiudizio subito dal minore nella rete o da lui cagionato a terzi nella rete, è difficile immaginare che il genitore possa liberarsi dalla responsabilità invocando l'impossibilità tecnologica, specie, come meglio si andrà a chiarire, se la vittima o l'autore del fatto è un minore "piccolo", normalmente ritenuto incapace di intendere e di volere (71).

Ne discende che l'unico modo per consentire ai genitori di sottrarsi da codeste forme di responsabilità sarebbe vietare al figlio l'accesso alla rete ed eventualmente addurre, in caso di pregiudizi comunque subiti o cagionati dal minore nell'ambiente digitale, che l'accesso è avvenuto contro la loro volontà e fuori dal loro possibile controllo.

Epperò, come dicevamo, quello digitale è un ambiente (*recte* una formazione) sociale anche per il minore; sì che escluderlo significa incidere sullo sviluppo della sua personalità (72). Vale, quindi, come principio generale quello che il *Children's Code* inglese (73) pone a premessa di senso del suo articolato, ovvero che «*This code achieves this not by seeking to protect*

---

delle funzioni educative, gravano sui genitori, rispetto a quelli di mera sorveglianza gravanti sul sorvegliante dell'incapace, si comprenderà bene come, nonostante la stessa formula della prova liberatoria « di non aver potuto impedire il fatto », la giurisprudenza richieda nell'art. 2047 la prova dell'assenza di *culpa in vigilando*, e richieda invece nell'art. 2048 la prova dell'assenza sia di *culpa in vigilando* che di *culpa in educando* ».

(70) E. Meligrana, G. Scorza, *La privacy degli ultimi*, prefazione di A. Spadaro S.I., cit., 45, riferiscono che « gli atti delle indagini condotte e dei processi celebrati in ogni parte del mondo negli ultimi vent'anni raccontano che il web — assieme a milioni di altre cose straordinariamente positive — è anche il più grande book fotografico dal quale i pedofili scelgono le loro vittime ». Sulla questione v. anche E. Andreola, *Minori e incapaci in* Internet, cit., 113; V. Corriero, Privacy *del minore e potestà dei genitori*, cit., 1001 ss. In giurisprudenza, si segnala Cass., 10 settembre 2019, n. 22541, in *Nuova giur. civ. comm.*, 2020, I, 342, con nota di V. Caredda, *Provocazione e reazione nel giudizio di responsabilità*.

(71) Si veda, in proposito, Cass., 19 novembre 2010, n. 23464, in *Foro it.*, 2011, I, 1448 ss., in cui si afferma che « non è necessario che il giudice svolga indagini tecniche di carattere psicologico per affermare o escludere l'incapacità di intendere o di volere di un minore per gli effetti di cui all'art. 2047 c.c. quando le modalità del fatto e l'età del minore siano tali da autorizzare una conclusione in un senso o nell'altro ».

(72) M. Prensky, *Digital natives, Digital Immigrants*, in *On the Horizon*, 9, 5, I, Bladford, 2001; D. Tapscott, Net generation. *Come la generazione digitale sta cambiando il mondo*, Roma, 2011; C. Perlingieri, *La tutela dei minori nei social networks*, in *Rass. dir. civ.*, 2016, 1331 ss.; C. Irti, *Persona minore di età e libertà di autodeterminazione*, in *Giust. civ.*, 2019, 623 ss.; I. Garaci, *La "capacità digitale" del minore nella società dell'informazione. Riflessioni sul corretto esercizio della responsabilità genitoriale fra esigenze di autonomia e di protezione*, in *Nuovo dir. civ.*, 2019, 63 ss.

(73) Il riferimento è al *Children's Code* (*Age appropriate design: a code of practice for online* services) del 2 settembre 2020, in https://ico.org.uk/media/for-organisations/guide-to-

children from the digital world, but by protecting them whithin it ». E se a ciò si aggiunge quanto afferma con chiarezza la Dichiarazione dei diritti in Internet (74), vale a dire che « l'accesso a Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale », sicuramente il problema si concentra sulla tutela della persona *nel* e non *dal* digitale (75).

Ma come garantire la vigilanza dei genitori e quindi far salva l'esclusività del loro ruolo educativo, costituzionalmente garantita, e nel contempo tutelare il principio dell'*Internet free speech* esplicitato, con particolare riguardo al minore, dal sistema dei suoi diritti alla libertà di espressione (art. 13 CNY), alla libertà di pensiero, di coscienza e di religione (art. 14 CNY), alla libertà di associazione e di riunione (art. 15 CNY) alla vita privata (art. 16 CNY), all'accesso a informazioni e materiali provenienti da fonti nazionali e internazionali (art. 17 CNY)? Insomma, all'insegna di quali coordinate va bilanciato l'interesse dei genitori di operare, in via esclusiva, le scelte educative del figlio con l'interesse del minore all'esercizio delle sue libertà individuali e sociali? La risposta, oltretutto, va ricercata nella piena osservanza del principio di ingerenza minima dello Stato negli affari familiari, sancito dal sistema degli artt. 29-30-31 Cost (76).

Come abbiamo evidenziato in precedenza, le insidie identitarie del *cyberspazio* si discostano da quelle comuni principalmente per l'assenza di confini fisici e temporali, la quale, tra l'altro, produce un « disallineamento cronologico tra il nostro sé e il nostro *habitat online* » (77), con evidenti ricadute sulla dimensione identitaria. Lo spazio sconfinato in cui si naviga, contraddistinto dalla sovraesposizione antropologica e informativa (78), facilmente può condurre a orizzonti in cui i valori del vivere sociale, recepiti dalla Costituzione e a cui si riferisce l'art. 29 della Convenzione di New York, sono contrastati da contenuti di vario genere. Oltre a ciò, gli stessi meccanismi di *identificazione* algoritmica (*recte* profilazione), sempre più diffusi e sofisticati,

---

data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services-2-1.pdf.

(74) Reperibile in https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf

(75) In proposito, E. Andreola, *Minori e incapaci in* Internet, cit., 107; R. Senigaglia, *Minore età e contratto. Contributo alla teoria della capacità*, cit., 80 ss.

(76) P. Zatti, *Rapporto educativo ed intervento del giudice*, cit., 225; N. Biligotti, *La tutela dei minori nel cyberspazio.* Parental Control *di Stato e libera circolazione dei contenuti: un delicato equilibrio*, in *MediaLaws*, 1/2023, 360.

(77) L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, cit., 81.

(78) A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., 50.

sono capaci di attrarre l'utente in *cluster* lesivi della sua identità (79), veicolati da ciò che risulta essere più attraente per il suo profilo (disincarnato); congegni, quindi, idonei a imporgli, in modo *leggero* (nascosto), un'identità che si trasforma in una risorsa dell'economia della rete (80).

Una dinamica, questa, scandita da accessi che impattano sullo sviluppo della personalità del minore, istruendolo ed educandolo non all'insegna dei valori della società giuridica, nel rispetto delle sue capacità, inclinazioni naturali e aspirazioni, ma di interessi patrimoniali, viziando, con tutte le tecniche possibili, il suo percorso *naturale* di formazione dell'identità personale. Si pensi, in proposito, al fenomeno dei *baby influencer*: immagini e video che i minori postano nei *social* cumulando numeri significativi (che creano valori per il mercato) di *followers*, finendo col fungere da veicoli pubblicitari alimentati da fini lucrativi; a ciò si aggiunge la condotta di molti genitori che "sfruttano" l'immagine dei loro figli trasformandoli in degli *influencer* per fare soldi, incidendo sulla loro identità, anche con significative ricadute nella vita adulta del figlio (81).

---

(79) Si veda S. Gutwirth, Y. Poullet, P. De Hert (a cura di), *Data protection in a profiled world*, Dordrecht, 2010; B. Custers, T. Calders, B. Schermer, T. Zarsky (a cura di), *Discrimination and Privacy in the Information Society. Data Mining and Profiling in Large Databases*, Berlin, 2013, *passim*; E. Giorgini, *Algorythms and Law*, in *The Italian Law Journal*, 2019, 131 ss.; S. Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioral advertising*, in *Berkeley Technology Law Journal*, 2020, 367 ss.; B. Parenzo, *Profilazione e discriminazione. Dal GDPR alla proposta di Regolamento sull'intelligenza artificiale*, in C. Camardi (a cura di), *La via europea per l'intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021*, Milano, 2022, 335 ss.

(80) Cfr. J. Turow, *The daily you. How the new advertising industry is defining your identity and your worth*, New Haven, London, 2011, *passim*; C. Perlingieri, *La tutela dei minori di età nei* social networks, cit., 1328 s.; G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 2017, 723 ss.; M. Bianca, *La* filter bubble *e il problema dell'identità digitale*, cit., 11 ss.; M. Foglia, *Identità digitale, trattamento dei dati e tutela della persona*, in *Rass. dir. civ.*, 2021, 92 ss.

(81) E. Meligrana, G. Scorza, *La privacy degli ultimi*, prefazione di A. Spadaro S.I., cit., 50, osservano, in proposito, che « per una manciata di famiglie che diventano ricche svendendo sul web la privacy dei più piccoli ce ne sono, purtroppo, centinaia di migliaia che immolano l'immagine, i dati, una vita normale dei loro bambini sull'altare di un successo che non arriverà mai ». V. anche E. Andreola, *Misure cautelari a tutela dei minori nei* social network, cit., 857. Senz'altro rilevante, in proposito, è lo spunto normativo, in senso rimediale, che proviene dal legislatore francese con la *loi* n. 2020-1266 del 19 ottobre 2020 volta a regolare lo sfruttamento commerciale dell'immagine dei minori infrasedicenni sulle piattaforme *online*. L'art. 3, in presenza di determinati presupposti di durata e numero dei contenuti nonché di misura del corrispettivo, subordina la diffusione dell'immagine di un minore infrasedicenne su un servizio di piattaforma di condivisione video, quando il minore è il soggetto principale, a una dichiarazione che gli esercenti la responsabilità genitoriale devono

Ora, se si tratta di tutelare il minore *nella* rete e non *dalla* rete, il primo intervento normativo senz'altro necessario dovrebbe essere volto a non consentire al minore il libero accesso ai contenuti digitali "pericolosi" per lo sviluppo della sua personalità, a quegli spazi, cioè, i cui contenuti confliggono con i valori fondamentali della pacifica convivenza sociale (*fake news*, *hate speech*, *challenges* che incitano all'autolesionismo, pornografia, ecc. (82)).

Trattandosi di una questione che può assumere contorni diversi in ragione delle tradizioni dei singoli ordinamenti, la definizione del livello di sicurezza e dei contenuti da sottrarre al libero accesso del minore può competere anche ai singoli Stati membri; evidenti esigenze di effettività esigono che non sia demandata, in via esclusiva, ai gestori dei servizi dell'informazione, in particolare agli *Internet Service Provider* (d'ora in poi, ISP) (83). Tant'è che l'art. 3, par. 1, lett. *h*), del Reg. (UE) 2022/2065, nel definire il significato di « contenuto illegale » si riferisce a « qualsiasi informazione che, di per sé o in relazione a un'attività, tra cui la vendita di prodotti o la prestazione di servizi, non è conforme al diritto dell'Unione o di qualunque Stato membro conforme con il diritto dell'Unione, indipendentemente dalla natura o dall'oggetto specifico di tale diritto » (84).

---

rendere all'autorità competente. Prevede inoltre che questa stessa autorità debba formulare delle raccomandazioni, di impatto identitario, agli esercenti la responsabilità genitoriale. È anche previsto che, se i redditi derivanti dalla distribuzione di questi contenuti superano una certa soglia, siano versati presso la Cassa depositi e prestiti e gestiti dalla stessa fino al raggiungimento della maggiore età del figlio o, se del caso, fino alla data della sua emancipazione. Nell'ambito lavoristico, l'intervento normativo ha esteso la previsione dell'art. L. 7124-1 del *Code du Travail* — la quale sancisce che un minore infrasedicenne non può, senza una preventiva autorizzazione concessa dall'autorità amministrativa, essere, a qualsiasi titolo assunto — anche all'ipotesi in cui l'assunzione avvenga da parte di « un datore di lavoro la cui attività consista nella realizzazione di registrazioni audiovisive in cui soggetto principale è un minore con meno di 16 anni, per la distribuzione su un servizio di piattaforma di video-sharing a scopo di lucro». In questo caso, se si ottiene la prescritta autorizzazione, è previsto che l'autorità amministrativa fornisca « ai rappresentanti legali delle informazioni relative alla protezione dei diritti del minore nell'ambito della realizzazione di questi video, che riguardano in particolare le conseguenze sulla vita privata del minore della diffusione della sua immagine su una piattaforma di condivisione video. Queste informazioni riguardano anche i loro obblighi finanziari ai sensi dell'articolo L. 7124-25 ».

(82) Si veda, in proposito, O. Pollicino, *Fake news, Internet and Metaphors. (To be handled carefully)*, in *MediaLaws*, 2017, 23 ss.

(83) Questo emerge con chiarezza nella dir. (UE) 2018/1808 ma anche nel Reg. (UE) 2022/2065.

(84) Sempre a tenore del *Digital Services Act,* « il concetto di « contenuto illegale » dovrebbe essere definito in senso lato per coprire anche le informazioni riguardanti i contenuti, i prodotti, i servizi e le attività illegali. Tale concetto dovrebbe, in particolare, intendersi riferito alle informazioni, indipendentemente dalla loro forma, che ai sensi del

Peraltro, sempre il *Digital Services Act* traccia le coordinate dei livelli di sicurezza della rete nella consapevolezza che la protezione dei minori è un importante obiettivo politico dell'Unione; di qui la cifra rimediale tracciata dal considerando, secondo cui « i fornitori di piattaforme *online* utilizzate dai minori dovrebbero adottare misure adeguate e proporzionate per proteggere i minori, ad esempio progettando le loro interfacce *online* o parti di esse con il massimo livello di privacy, sicurezza e protezione dei minori per impostazione predefinita, a seconda dei casi, o adottando norme per la protezione dei minori, o aderendo a codici di condotta per la protezione dei minori » (Considerando 71).

2.6. La protezione del minore da contenuti illegali. I sistemi di controllo parentale

Degli interessi di protezione sin qui segnalati e della definizione delle loro coordinate tende a farsi carico, nel nostro ordinamento, il d.l. 30 aprile 2020, n. 28 (convertito, con modificazioni, dalla l. 25 giugno 2020, n. 70), il quale impone ai fornitori di servizi di comunicazione elettronica la prestazione di servizi preattivati di sistemi di controllo parentale (d'ora in poi SCP). Segnatamente l'art. 7-*bis*, rubricato "Sistemi di protezione dei minori dai rischi del *cyberspazio*", sancisce che « i contratti di fornitura nei servizi di comunicazione elettronica, disciplinati dal Codice di cui al d.lgs. 1 agosto 2003, n. 259 (n.d.a. Codice delle comunicazioni elettroniche), devono prevedere tra i servizi preattivati sistemi di controllo parentale ovvero di filtro di contenuti inappropriati per i minori e di blocco di contenuti riservati ad un pubblico di età superiore ai diciotto anni ». Dispone, inoltre, la necessaria gratuità della prestazione di questi servizi e la possibilità di disattivarli

---

diritto applicabile sono di per sé illegali, quali l'illecito incitamento all'odio o i contenuti terroristici illegali e i contenuti discriminatori illegali, o che le norme applicabili rendono illegali in considerazione del fatto che riguardano attività illegali. Tra queste figurano, a titolo illustrativo, la condivisione di immagini che ritraggono abusi sessuali su minori, la condivisione non consensuale illegale di immagini private, il cyberstalking (pedinamento informatico), la vendita di prodotti non conformi o contraffatti, la vendita di prodotti o la prestazione di servizi in violazione della normativa sulla tutela dei consumatori, l'utilizzo non autorizzato di materiale protetto dal diritto d'autore, l'offerta illegale di servizi ricettivi o la vendita illegale di animali vivi. Per contro, un video di un testimone oculare di un potenziale reato non dovrebbe essere considerato un contenuto illegale per il solo motivo di mostrare un atto illecito quando la registrazione o la diffusione di tale video al pubblico non è illegale ai sensi del diritto nazionale o dell'Unione. A tale riguardo è irrilevante che l'illegalità delle informazioni o delle attività sia sancita dal diritto dell'Unione o dal diritto nazionale conforme al diritto dell'Unione e quale sia la natura esatta o l'oggetto preciso della legge in questione »; così il considerando 12.

soltanto in capo al consumatore, titolare del contratto. Ai fini, poi, di diffondere la consapevolezza di queste misure di protezione, è demandato agli operatori di telefonia, di reti televisive e di comunicazioni elettroniche il compito di assicurare adeguate forme di pubblicità in modo da consentire ai consumatori di compiere scelte informate.

In più, l'art. 13, comma 2, del d.l. 15 settembre 2023, n. 123 (convertito, con modificazioni, dalla l. 13 novembre 2023, n. 159) — contenente « misure urgenti di contrasto al disagio giovanile, alla povertà educativa e alla criminalità minorile, nonché per la sicurezza dei minori in ambito digitale » (85) — esige che i produttori dei dispositivi di comunicazione elettronica assicurino che i sistemi operativi ivi installati consentano l'utilizzo e includano la disponibilità di applicazioni di controllo parentale (86).

Tutto ciò in linea con quanto ora sancisce il Reg. (UE) 2022/2065, il quale vincola i fornitori di piattaforme *online* o di motori di ricerca di dimensioni molto grandi ad adottare misure di attenuazione dei rischi ragionevoli, proporzionate ed efficaci, « prestando particolare attenzione agli effetti di tali misure sui diritti fondamentali » (art. 35, par. 1); tra le possibili misure di protezione dei diritti dei minori vengono annoverati gli « strumenti di verifica dell'età e di controllo parentale, o strumenti volti ad aiutare i minori a segnalare abusi o ottenere sostegno, a seconda dei casi » (art. 35, par. 1, lett. *j*) (87).

---

(85) Ai sensi di quest'ultimo decreto per *controllo parentale* s'intende « la possibilità di limitare e controllare, da parte dei genitori o di coloro che esercitano la responsabilità genitoriale, l'accesso ai contenuti e/o alla rete da parte dei minori, mediante la scelta degli spazi digitali e dei tempi di utilizzo » (art. 13, comma 1, lett. *a*).

(86) La stessa disposizione normativa sancisce che i produttori devono ottemperare l'obbligo prescritto entro un anno dall'entrata in vigore del decreto legge (art. 13, comma 2). Inoltre, il comma 3 pone a carico dei produttori, anche per il tramite dei distributori operanti in Italia, l'obbligo di informare « l'utente sulla possibilità e sull'importanza di utilizzare applicazioni di controllo parentale. Tale adempimento può essere assicurato anche tramite l'inserimento nelle confezioni di vendita di uno specifico foglio illustrativo o tramite l'apposizione sulla confezione dello specifico supporto adesivo che, con apposita evidenziazione grafica, segnali, con chiarezza e semplicità, l'esistenza delle applicazioni di controllo parentale suddette, potenzialmente attivabili, rinviando per maggiori informazioni ai siti internet della Presidenza del Consiglio dei Ministri - Dipartimento per le politiche per la famiglia e dell'Autorità per le garanzie nelle comunicazioni ». Anche per tali servizi è prescritta la gratuità.

(87) Con specifico riferimento agli strumenti di verifica dell'età, la Comunicazione della Commissione su *Un decennio digitale per i bambini e giovani: la nuova strategia europea per un internet migliore per i ragazzi (BIK+)*, COM(2022) 212 final, segnala che « a dispetto di quanto stabilito dal diritto vigente dell'UE (direttiva AVMS e GDPR), i meccanismi di verifica dell'età e gli strumenti che consentono ai genitori di esprimere il loro consenso sono ancora in molti casi inefficaci e agli utenti è spesso richiesto soltanto di inserire la data di nascita al momento

Con specifico riferimento ai contenuti ad accesso non libero, a tutela essenzialmente dell'identità personale del minore, in mancanza di apposite previsioni di fonte eurounionale, la selezione compete agli Stati membri (88). E il referente normativo per l'attuazione dell'art. 7-*bis*, d.l. 30 aprile 2020, n. 28, è l'art. 37 d. lgs. 8 novembre 2021, n. 208, (89), contenente « Disposizioni a tutela dei minori nella programmazione audiovisiva ». Già scorrendo gli ambiti contenutistici, si intuisce che l'oggetto di tutela è proprio la costituzione *libera* e *naturale* dell'identità del minore, negli aspetti riguardanti la sua personalità morale. Il divieto, infatti, concerne tutti quei programmi, siti e contenuti che diffondono una cultura contraria ai valori fondamentali della società giuridica (scene di violenza gratuita o insistita o efferata, scene di pornografia e in generale contenuti nocivi allo sviluppo fisico, psichico e morale dei minori). È comunque demandato all'Autorità per le Garanzie nelle Comunicazioni (AGCOM) il compito di fissare, con apposite procedure di co-regolamentazione (90), i criteri a cui devono attenersi i fornitori dei relativi servizi.

Stando quindi a queste indicazioni e procedure, pure l'effettività dell'obbligo di prestazione gratuita di servizi preattivati di sistemi di controllo parentale da parte degli ISP, sancito dall'art. 7-*bis*, d.l. n. 28 del 2020, attende

---

della registrazione »; la Commissione si impegna poi a promuovere « strumenti di verifica dell'età sicuri e rispettosi della vita privata, che siano riconosciuti in tutta l'UE » e a collaborare con gli Stati membri, i portatori di interessi pertinenti e gli enti di normazione europei « per rafforzare gli strumenti di verifica dell'età efficaci in via prioritaria ».

(88) È chiaro, in questo senso, il considerando 270 della Dir. (UE) 2018/1972, che istituisce il "Codice europeo delle comunicazioni elettroniche", ove precisa che « in mancanza di norme applicabili di diritto dell'Unione, i contenuti, le applicazioni e i servizi sono considerati legali o dannosi ai sensi del diritto nazionale sostanziale e procedurale. Spetta agli Stati membri, e non ai fornitori di reti o servizi di comunicazione elettronica, decidere, seguendo le normali procedure, se i contenuti, le applicazioni e i servizi siano legali o dannosi ».

(89) Si tratta del decreto attuativo della Dir. (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato. Con particolare riferimento alle misure di protezione dei minori di età v. F. Donati, *La tutela dei minori nella direttiva 2018/1808*, in *MediaLaws*, 2019, 1, 60 ss.

(90) Il comma 5 dell'art. 37, d.lgs. n. 208 del 2020, delinea la procedura di co-regolamentazione: « L'Autorità, d'intesa con il Ministero, sentiti l'Autorità garante per l'infanzia e l'adolescenza e il Comitato di applicazione del Codice di autoregolamentazione media e minori, al fine di garantire un adeguato livello di tutela della dignità umana e dello sviluppo fisico, mentale e morale dei minori, adotta con procedure di co-regolamentazione, la disciplina di dettaglio contenente l'indicazione degli accorgimenti tecnici idonei a escludere che i minori vedano o ascoltino normalmente i programmi di cui al comma 3, fra cui l'uso di numeri di identificazione personale e sistemi di filtraggio, di verifica dell'età o di identificazione, nel rispetto dei seguenti criteri generali (...) ».

la definizione dei criteri da parte dell'AGCOM di selezione dei contenuti da ritenere nocivi allo sviluppo della personalità dei minori. Criteri ai quali la stessa norma assegna, inequivocabilmente, carattere di precettività, attribuendo all'AGCOM poteri sanzionatori in caso di violazione (91).

Soltanto il 21 gennaio 2023, l'Autorità Garante ha emanato le linee guida finalizzate all'attuazione dell'art. 7-*bis*, d.l. n. 28 del 2020 (92). Più precisamente, in attesa di definire dei criteri dettagliati per la comunicazione digitale, l'AGCOM si è limitata a classificare i contenuti "a visione non libera", attingendo dal sistema dei decreti legislativi nn. 207 e 208 dell'8 novembre 2021 (93), a partire dalle categorie elencate dall'art. 37 d.lgs. n. 208/2021. Un quadro normativo, questo, completato, con riferimento all'ambito *dell'Information and Communication Technologies*, dal Reg. (UE) 2022/2065 (94), tendente a fare del *web 2.0* (95) un ambiente non più inteso come spazio di libertà di idee e di contenuti (come nel *web 1.0*, presidiato dalla *E-Commerce Directive*), ma come spazio in cui deve essere garantito, per mezzo anche del diretto coinvolgimento regolativo dei gestori della rete, un determinato livello di sicurezza e qualità dei contenuti (96).

---

(91) L'ultimo comma dell'art. 7-*bis*, d.l. n. 28 del 2020 sancisce che « in caso di violazione di obblighi di cui al presente articolo, l'Autorità per le garanzie nelle comunicazioni ordina all'operatore la cessazione della condotta e la restituzione delle eventuali somme ingiustificatamente addebitate agli utenti, indicando in ogni caso un termine non inferiore a sessanta giorni entro cui adempiere ».

(92) Nei tre anni di "vuoto normativo" l'implementazione del sistema del *parental control* è stata soltanto parziale e peraltro non sempre conforme ai parametri fissati dalla legge: gli ISP si sono diversamente atteggiati rispetto all'obbligo sancito dalla legge, alcuni preattivando sistemi di controllo parentale, non sempre però all'insegna della gratuità, altri continuando a consentire il libero accesso in attesa della emanazione delle linee guida dell'AGCOM.

(93) Questi decreti hanno trasposto nell'ordinamento italiano rispettivamente la Dir. UE 2018/1972, istitutiva del Codice europeo delle comunicazioni elettroniche e, come già precisato, la Dir. UE 2018/1808 modificativa della dir. 2010/13/UE (Direttiva sui servizi di media audiovisi)

(94) Il *Digital Services Act* (Reg. (UE) 2022/2065) individua quattro distinte classi di rischio, in base all'incidenza dell'attività sui diritti fondamentali delle persone. Alle classi di rischio più elevate si riferiscono obblighi informativi più ampi. V. i considerando 80 e ss.

(95) Si veda, in proposito, il Libro Bianco *Media e minori 2.0* dell'AGCOM del 16 gennaio 2018, in https://www.agcom.it/documentazione/documento?p_p_auth=fLw7zRht&p_p_id=101_INSTANCE_FnOw5lVOIXoE&p_p_lifecycle=0&p_p_col_id=column1&p_p_col_count=1&_101_INSTANCE_FnOw5lVOIXoE_struts_action=%2Fasset_publisher%2Fview_content&_101_INSTANCE_FnOw5lVOIXoE_assetEntryId=9340369&_101_INSTANCE_FnOw5lVOIXoE_type=document.

(96) Cfr. F. D'Ambrogio, "*Parental control": accorgimenti tecnici per escludere la fruizione da parte dei minori di contenuti classificati a visione non libera*, in *Familia*, 2018, 237 ss.;

Ebbene, quanto all'individuazione dei contenuti da filtrare o bloccare, in attesa della definizione di criteri specifici, l'AGCOM ordina agli ISP di fare riferimento alle liste di « domini/sottodomini e contenuti determinati secondo le proprie specifiche di servizio e/o fornite da soggetti terzi esperti », segnalando, comunque, a titolo di indicazione generale, un elenco di categorie di contenuti selezionati da quanto riferito dai soggetti interpellati in sede di consultazione pubblica.

In sintesi, le linee guida obbligano gli ISP a mettere a disposizione del consumatore, a titolo gratuito e senza alcun costo aggiuntivo, dei sistemi di *parental control*, includendoli e attivandoli nelle offerte dedicate ai minori, rendendoli disponibili per essere attivati dal titolare del contratto nelle altre offerte. L'obbligo di pre-attivazione del sistema di *parental control* si riferisce, dunque, alle sole offerte dirette ai minori; per le altre offerte, invece, deve essere soltanto reso disponibile per l'attivazione a discrezione del titolare del contratto (97). Un differente livello di imposizione, che pare ragionevole in nome della diversità della cifra di bilanciamento degli interessi in gioco, a seconda che sia implicato o meno, in termini inequivocabili, l'interesse del minore.

Per i servizi rivolti ai minori, le funzioni di attivazione, disattivazione e configurazione del SCP spettano *sempre* all'esercente la responsabilità genitoriale attraverso delle chiavi di accesso fornite direttamente dall'operatore (98).

Il passo successivo sarà, quindi, la definizione dell'elenco dei contenuti da oscurare o filtrare da parte della stessa AGCOM, all'esito di procedure di co-regolamentazione svolte in sinergia con gli ISP. Nel frattempo, fatte salve le suddette indicazioni di ordine generale, è demandato agli stessi ISP il compito di individuare i contenuti "a visione non libera", avvalendosi di professionisti qualificati. In ogni caso, tanto l'attività regolativa degli operatori quanto (e soprattutto) quella dell'AGCOM dovranno tendere a superare la classificazione generica di categorie e contenuti (con la conseguente

---

I.A. Caggiano, *Protecting minors as technologically vulnerable persons through data protection: an analysis on the effectiveness of law*, in *European Journal of Privacy Law & Technologies*, 2022, 27 ss.; N. Biligotti, *La tutela dei minori nel cyberspazio.* Parental Control *di Stato e libera circolazione dei contenuti: un delicato equilibrio*, cit., 362-363.

(97) N. Biligotti, *La tutela dei minori nel cyberspazio.* Parental Control *di Stato e libera circolazione dei contenuti: un delicato equilibrio*, cit., 365.

(98) Gli ISP hanno l'obbligo di fornire tutte le informazioni e l'assistenza gratuita per consentire l'attivazione di queste funzioni che comunque deve essere agevole e intuitiva. Deve essere garantita inoltre ampia pubblicità all'obbligo di prestazione di servizi di controllo parentale, non soltanto da parte degli ISP, ma anche degli operatori di telefonia, di reti televisive e di comunicazioni elettroniche.

riconduzione allo stesso statuto normativo di contenuti tra loro ontologicamente e funzionalmente dissimili), approdando, invece, a indicazioni specifiche, idonee a garantire la ragionevolezza del bilanciamento tra la tutela dell'interesse identitario del minore e la tutela dell'interesse alla libertà di espressione e di informazione (99).

2.7. *Segue.* Proporzionalità e ragionevolezza delle misure di controllo parentale. Il *Children's Act* inglese

Sulla scorta dei principi espressi dal sistema ordinamentale minorile contemporaneo, le misure di blocco e di filtro dei contenuti attraverso il SCP, così come pensate dal d.l. n. 28 del 2020 e dalle linee guida dell'AGCOM, sono da ritenersi senz'altro una valida forma di protezione del *best interest* quando si tratta di un "piccolo minore", sprovvisto della capacità di discernimento. Con esse si è inteso articolare una soluzione bilanciata tra *i*) l'interesse dei genitori all'esclusività del ruolo educativo/formativo dell'identità personale del figlio, potendo decidere, nella loro responsabilità, anche di disattivare il sistema di controllo o di attuare una configurazione personale modificando quelle predefinite; *ii*) l'interesse del minore alla costituzione *libera* e *naturale* della sua identità biografica; *iii*) l'interesse del minore all'accesso alla rete, alla sua libertà di espressione, allo sviluppo della propria personalità.

Epperò, occorre testare il presidio del principio di proporzionalità nella specifica misura di protezione, anzitutto con riguardo alla libertà di espressione e informazione, considerata l'architrave assiologica della democrazia, e che l'art. 11 della Carta dei diritti UE garantisce a ogni uomo, puntualizzando che « tale diritto include la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiere ». Le limitazioni a questa libertà sono consentite soltanto ad opera della legge nel rispetto del principio di proporzionalità e «solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui » (art. 52, par. 1, Carta diritti UE).

La tutela del migliore interesse (identitario) del minore può senz'altro giustificare il sacrificio della libertà di espressione e informazione, anche per mezzo di idonei strumenti di garanzia, nel *cyberspazio*, dell'esclusività del ruolo educativo genitoriale; s'impone, però, il monitoraggio del *tipo* di soluzione sotto il profilo dell'effettività e della proporzionalità.

---

(99) N. Biligotti, *La tutela dei minori nel cyberspazio.* Parental Control *di Stato e libera circolazione dei contenuti: un delicato equilibrio*, cit., 367.

Il primo profilo, come si osservava, respinge soluzioni generiche nel consegnare al controllo dei genitori l'accesso alla rete del figlio. Tanto è vero che la discrezionalità educativa *incarnata*, che compete al genitore, impone di accordare a quest'ultimo la possibilità di disattivare, nella propria "responsabilità", il servizio di controllo parentale, ma pure di configurare (personalizzare) i contenuti da oscurare, selezionarli da un elenco *specifico*, nel rispetto della personalità del figlio (100). Peraltro, questa possibilità dovrebbe essere sempre consentita dagli ISP ai genitori; viceversa, le linee guida la prevedono soltanto come facoltativa, obbligando gli ISP a fornire solo le funzioni di attivazione e disattivazione (101).

D'altro canto, in termini di proporzionalità e ragionevolezza (102), l'imposizione di servizi preattivati di controllo parentale in *tutti* i casi in cui l'utente sia un minorenne suscita non poche perplessità con riferimento al caso in cui si tratti di un "grande minore", munito della capacità di discernimento e la cui dinamica identitaria ha pressoché abbandonato la funzione *costruttiva* per assestarsi in quella *conservativa*.

Detto altrimenti, non differenziare la minore età nel sacrificare la libertà di espressione e informazione, accusa non poche distonie sistematiche.

Difatti, la condizione giuridica del minore con discernimento conosce, come regola generale, la libertà di autodeterminazione. Oltre alle non poche previsioni normative che gli accordano il diritto di scegliere direttamente (consenso all'adozione, interruzione volontaria della gravidanza, riconoscimento come figlio dal proprio genitore, richiesta di nomina di un curatore speciale, ecc.) e alle soluzioni già da tempo affermate in via ermeneutica, giungendo senz'altro ad attrarre nella sfera della sua libertà di autodeterminazione l'esercizio dei diritti personali (103), al "grande minore" è comunque

---

(100) A titolo esemplificativo un divieto genericamente riferito a immagini di nudità porterebbe a porre sullo stesso piano contenuti pornografici e contenuti di film, la cui visione può essere ritenuta dai genitori funzionale all'istruzione del figlio, nel rispetto della sua identità.

(101) N. Biligotti, *La tutela dei minori nel cyberspazio.* Parental Control *di Stato e libera circolazione dei contenuti: un delicato equilibrio*, cit., 367-368.

(102) Su questi parametri si rinvia a G. Perlingieri, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, *passim*. N. Biligotti, *op. cit.*, 361, segnala che « se è indubbio, sul piano generale, che la salute psico-fisica dei soggetti minorenni sia un diritto fondamentale titolato ad operare in bilanciamento con altri valori fondamentali (quale, nel caso di specie, la libertà di espressione), è tuttavia necessario prestare particolare attenzione al versante della proporzionalità per quanto attiene alla massima estensione della compressione della libertà fondamentale ritenuta tollerabile, al fine, dall'ordinamento giuridico. Oltrepassato tale stringente confine, ciò che si prospetta è, invero, il conflitto della norma con i principi fondanti dell'ordinamento e, dunque, la sua invalidità costituzionale ».

(103) Si veda, in particolare, Trib. min. Milano, 15 febbraio 2010, in *Fam. dir.*, 2011, 401 ss., con nota di F. Ruscello, *Minore età e capacità di discernimento: quando i concetti assurgono*

accordato dal sistema ordinamentale il diritto di "leggere" il proprio migliore interesse e di affermarlo nelle decisioni che lo riguardano (104). Conclusione, questa, a cui si approda muovendo dal dato normativo alla stregua del quale la capacità di discernimento, quale « strumento indispensabile per la ricostruzione dell'identità in divenire del figlio » (105), nel momento in cui matura istituisce in capo alla persona minore di età il diritto di essere ascoltata in tutte le questioni e procedure che la riguardano (art. 12, par. 2, CNY, art. 315-*bis* c.c.; art. 473-*bis* 4 c.p.c.). Si tratta di un diritto che si traduce,

---

a "supernorme"; Trib. min. Milano, 30 marzo 2010, in banca dati *OneLegale*. Per quanto concerne la capacità del minore ad esercitare i diritti patrimoniali si rinvia a P. Stanzione, *Capacità e minore età nella problematica della persona umana*, con la prefazione di R. Pane, cit.; F. Giardina, *La condizione giuridica del minore*, cit.; M. Cinque, *Il minore contraente. Contesti e limiti della capacità*, cit.; R. Senigaglia, *Minore età e contratto. Contributo alla teoria della capacità*, cit.; G. Carapezza Figlia, *Teoria della capacità e tutela della persona umana. Per una nuova dogmatica minorile*, in *Rass. dir. civ.*, 2023, 328 s.

(104) Su questi principi si rinvia, in particolare, a M.L. Quadrato, *Il minore tra interessi e diritti. Una lettura comparata*, Bari, 1995; G. Ferrando, *Diritti e interesse del minore tra principi e clausole generali*, in *Pol. dir.*, 1998, 167 ss.; E. Quadri, *L'interesse del minore nel sistema della legge civile*, in *Fam. dir.*, 1999, 80 ss.; E. La Rosa, *Tutela dei minori e contesti familiari. Contributo allo studio per uno statuto dei diritti dei minori*, Milano, 2005, 5 ss.; M. Bianca, *L'uguaglianza dello stato giuridico dei figli nella recente legge n. 219 del 2012*, in *Giust. civ.*, 2013, II, 205 ss.; E. Moscati, *Il minore nel diritto privato, da soggetto da proteggere a persona da valorizzare (contributo allo studio dell'interesse del minore)*, in *Dir. fam.*, 2014, 1141 ss.; G. Sicchiero, *La nozione di interesse del minore*, in *Fam. dir.*, 2015, 72 ss.; L. Lenti, *Note critiche in tema di interesse del minore*, in *Riv. dir. civ.*, 2016, 86 ss.; F. Giardina, *L'interesse del minore: gli aspetti identitari*, cit., 159 ss.; E. Lamarque, *Prima i bambini. Il principio dei* best interests of the child *nella prospettiva costituzionale*, prefazione di L. Pomodoro, Milano, 2016, 64 ss.; G. Recinto, *Il superiore interesse del minore tra prospettive interne "adultocentriche" e scelte apparentemente "minorecentriche" della Corte europea dei diritti dell'uomo*, in *Foro it.*, 2017, I, c. 3669 ss.; G. Corapi, *La tutela dell'interesse superiore del minore*, in *Dir. succ. fam.*, 2017, 777 ss.; V. Scalisi, *Il superiore interesse del minore ovvero il fatto come diritto*, in *Riv. dir. civ.*, 2018, 405 ss.; M.R. Marella, *Fra* status *e identità. L'interesse del minore e la costruzione della genitorialità*, in Aa.Vv., Liber Amicorum *Pietro Rescigno in occasione del novantesimo compleanno*, Napoli, 2018, 1213 ss.; F. Viola, *Nell'interesse del minore: la tutela giuridica tra sfide vecchie e nuove*, Relazione al convegno internazionale "Prendiamoci cura di me. Servizi, scuole, famiglie per la tutela dei minori", Rimini, 9-10 novembre 2018; S. Sonelli, *L'interesse superiore del minore. Ulteriori « tessere » per la ricostruzione di una nozione poliedrica*, in *Riv. trim. dir. proc. civ.*, 2018, 1373 ss.; G. Ballarani, *La responsabilità genitoriale e l'interesse del minore (tra norme e principi)*, in P. Perlingieri, S. Giova (a cura di), *Comunioni di vita e familiari tra libertà, sussidiarietà e inderogabilità*, Napoli, 2019, 318 ss.; E. Bilotti, *Diritti e interesse del minore*, in R. Senigaglia (a cura di), *Autodeterminazione e minore età. Itinerari di diritto minorile*, cit., 34 ss.; A.C. Di Landro, Best interest of the Child *e tutela dei minori nel dialogo tra legislazione e giurisprudenza*, in *Nuove leggi civ. comm.*, 2020, II, 451 ss.; M. Di Masi, *L'interesse del minore. Il principio e la clausola generale*, Napoli, 2020, *passim*; R. Senigaglia, *Minore età e contratto. Contributo alla teoria della capacità*, cit., 48 ss.

(105) F. Giardina, *Interesse del minore: gli aspetti identitari*, cit., 164.

appunto, nell'interesse della persona di affermare il proprio *best interest* e di realizzarlo nell'ordine della complementarità che presidia il rapporto tra l'interesse del minore e la sua identità (106).

In pratica, mentre con riferimento al "piccolo minore" sprovvisto della capacità di discernimento la lettura del suo migliore interesse è operata anzitutto dai genitori nel rispetto delle sue capacità, inclinazioni naturali e aspirazioni; relativamente al "grande minore" con capacità di discernimento — che il nostro ordinamento presume al compimento del dodicesimo anno di età (art. 315-*bis* c.c.) — i genitori, dovendo ascoltarlo, sono chiamati a recepire la lettura, *libera* e *informata* che egli conduce del proprio migliore interesse. Il ruolo dei genitori, in questa fase, si traduce, quindi, nel vigilare affinché la libertà del figlio, nel suo esplicarsi, sia effettiva e nell'intervenire, in funzione *sostitutiva*, soltanto quando, sulla base della loro sensibilità genitoriale, risulti evidente che il minore si sta orientando a scelte contrastanti con il suo *best interest*, perché turbate, nei percorsi valutativi, da condizionamenti esterni (107); i quali possono essere integrati anche dalla stessa tecnologia, che « è velocità e come tale non aiuta a prendere tempo per valutare » (108), portando finanche a percepire la *privacy* soltanto come un peso burocratico facendola soccombere al fascino della condivisone (109).

È in questo quadro assiologico che si fonda la ragione del dubbio sulla ragionevolezza di una misura rigida di controllo parentale estesa, in termini indifferenziati, alla minore età.

---

(106) In questi termini L. Lenti, *L'identità del minorenne*, cit., 66.

(107) Sul tema v. G. De Cristofaro, *Dalla potestà alla responsabilità genitoriale: profili problematici di una innovazione discutibile*, in *Nuove leggi civ. comm.*, 2014, 796 ss.; E. Al Mureden, Sub *art. 316 c.c.*, in M. Sesta (a cura di), *Codice della famiglia*, cit., 1166; C. Camardi, *Relazione di filiazione e* privacy. *Brevi note sull'autodeterminazione del minore*, in *Jus civile*, 2018, 843 ss.; I.A. Caggiano, *Il consenso al trattamento dei dati personali tra nuovo Regolamento europeo e analisi comportamentale*, in *Oss. dir. civ. comm.*, 2018, 7 ss.; E. Andreola, *Minori e incapaci in* Internet, cit., 143 ss.; L. Bozzi, *I dati del minore tra protezione e circolazione: per una lettura non retorica del fenomeno*, in *Eur. dir. priv.*, 2020, 258; I. Garaci, *Il « superiore interesse del minore » nel quadro di uno sviluppo sostenibile dell'ambiente digitale*, cit., 812 ss.; R. Senigaglia, *I principi e le categorie del diritto civile minorile*, in A. Cordiano, R. Senigaglia (a cura di), *Diritto civile minorile*, cit., 25 ss.

(108) A. Pessina, *L'essere altrove. L'esperienza umana nell'epoca dell'intelligenza artificiale*, cit., 31.

(109) A.M. McDonald, L. Cranor, *The cost of reading privacy policies*, in *Journal of Law and Policy for the Information Society*, 2008, 543 ss.; D.J. Solove, *Introduction: privacy self-management and the consent dilemma*, in *Harvard Law Review*, 2013, 1880 ss.; A. Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo,* cit., 410; Id., *L'inconsistente tutela dei minori nel mondo digitale*, cit., 528 ss.

Un diverso metodo accompagna, invece, il *Children's Code* (*Age appropriate design: a code of practice for online services*) del 2 settembre 2020: una sorta di Codice di condotta promanante dall'Autorità garante inglese per la protezione dei dati personali (ICO, *Information Commissioner's Office*), applicabile ai servizi della società dell'informazione a cui possono accedere i minori. Il codice si rivolge ai responsabili della progettazione, dello sviluppo e della fornitura dei servizi *online* (*app*, programmi, giocattoli e dispositivi connessi, motori di ricerca, piattaforme di *social media*, servizi di *streaming*, giochi *online*, notizie o siti *web* educativi e siti *web* che offrono altri beni o servizi agli utenti su Internet) indicando loro degli *standards* di comportamento, specialmente impostazioni predefinite a privacy elevata, la cui osservanza rende agevole la prova di conformità del proprio operato alla disciplina di *Data Protection*, altrimenti resa assai difficoltosa.

Con specifico riguardo allo *standard* del *parental control*, il Codice inglese, dopo aver evidenziato l'importanza dello strumento per sostenere i genitori nella protezione e nella promozione del migliore interesse identitario del figlio, esprime una duplice consapevolezza: da un lato, il forte impatto che la misura di controllo esercita sul diritto del bambino alla vita privata, all'associazione, al gioco, all'accesso all'informazione e alla libertà di espressione; dall'altro, che i minori « *have different needs at different ages* », tanto che a mano a mano che matura la percezione della propria *privacy*, un monitoraggio ostinato dell'attività può essere vissuto dal minore (evidentemente grande) come una restrizione opprimente dello spazio della propria vita privata con inevitabili conseguenze sullo sviluppo e sulla comprensione della propria identità.

Il *Children's Code*, dunque, valorizza la *persona* del minore, differenziando gli obblighi di informazione in ragione dell'età (110) e prevedendo la predisposizione di un segnale evidente (ad es. un'icona luminosa) idoneo a rendere il minore edotto del fatto che la sua attività *online* è monitorata dal genitore. Nello stesso ordine di senso si inserisce lo *standard* sulla geolocalizzazione, il quale prevede che per impostazione predefinita venga disattivata l'opzione e, anche in questo caso, l'attivazione di un segnale evidente quando il tracciamento della sua posizione è attivo.

---

(110) Ebbene, proprio al fine di rendere effettive le esigenze di trasparenza e consapevolezza, il *Children's Code* articola delle linee guida sulle informazioni da comunicare e sulle modalità di comunicazione differenziando la disciplina in ragione di cinque fasce in cui suddivide la "stagione" della minore età. Esso individua le seguenti fasce di età al fine di consentire agli operatori dei servizi digitali di valutare ciò che è appropriato per i bambini e le misure di protezione da adottare: 0-5 anni: pre-alfabetizzazione e prima alfabetizzazione; 6-9 anni: età della scuola primaria di base; 10-12 anni: età della transizione; 13-15 anni: prima adolescenza; 16-17 anni: avvicinamento all'età adulta.

2.8. Identità personale, misure di protezione e differenziazione della minore età

Una soluzione rigida, che disponga il sistema di controllo parentale nella stessa "misura" per tutta la durata della minore età, solleva, dunque, non pochi dubbi in termini di proporzionalità e ragionevolezza; pare, infatti, imposta dal sistema ordinamentale la necessità di operare una differenziazione in ragione della diversa considerazione della condizione giuridica del minore a seconda che sia sprovvisto o meno della capacità di discernimento.

In termini pratici, si pone la seguente domanda: un minore di quindici anni può opporsi all'attivazione o può chiedere la disattivazione di un SCP facendo valere il proprio interesse alla vita privata, alla libertà di espressione e informazione, e quindi al libero sviluppo della propria personalità?

Alla semplicità della formulazione della domanda si accompagna la complessità del *tipo* di risposta. Complessità dettata al fatto che nel diritto minorile mal si adatta la soluzione concepita sotto forma di fattispecie, valida una volta per tutte; è sempre la cifra dell'*incarnazione* che, così come orienta l'educazione, deve pure ordinare il *tipo* di risposta, la quale esige la conoscenza della singolare condizione contestuale del minore.

Il nostro ordinamento, come si diceva, presume che la capacità di discernimento maturi al compimento del dodicesimo anno d'età (art. 315-*bis* c.c., art. 473-*bis*.4 c.p.c.), pur potendo in concreto ravvisarsi prima. Da questo momento si radica in capo al minore il diritto fondamentale di essere ascoltato in tutte le decisioni e i procedimenti che lo riguardano. Diritto all'ascolto che, inteso nei termini poc'anzi precisati, conferisce al minore il potere di autodeterminarsi nelle scelte, di affermare e realizzare il proprio migliore interesse (111).

Ciò significa che se il minore decide con *effettivo* discernimento, è questa la scelta che deve ritenersi conforme al suo migliore interesse. Nel nostro caso, quindi, se il minore con discernimento ritiene di saper tutelare la propria identità, anche dinanzi alle pressioni esercitate dalla sovraesposizione antropologica e informativa del *cyberspazio*, e che il controllo parentale si traduce in una invadenza ingiustificata nella sua vita privata, la scelta di opporsi alla sua attivazione ha ragione di essere assecondata, anzitutto dai

(111) Su questo profilo tematico v., in particolare, F. GIARDINA, *La condizione giuridica del minore*, cit., 87 ss.; R. SENIGAGLIA, *Minore età e contratto. Contributo alla teoria della capacità*, cit., 43 ss.; G. CARAPEZZA FIGLIA, *Teoria della capacità e tutela della persona umana. Per una nuova dogmatica minorile*, cit., 330 ss.

genitori che nel loro rapporto comunionale con il figlio hanno evidenza del fatto che si sta autodeterminando con discernimento (112).

Ma se quei genitori, pur al cospetto di questa evidenza, si ostinano a mantenere il *controllo parentale* e a non disattivarlo, operando quindi una scelta antagonista all'interesse del figlio e orientata soltanto dal proprio interesse, allora si assiste a una disfunzione della responsabilità genitoriale con la possibilità di approdare a un provvedimento *de potestate*.

Il rispetto dell'ambito di autodeterminazione del minore con discernimento deve essere, in ogni caso, presidiato dall'obbligo di informazione trasparente dei rischi che possono derivare alla sua identità personale dalla disattivazione degli strumenti di controllo, e quindi dalla sottrazione alla vigilanza dei propri genitori, al loro aiuto ancora prezioso in un momento della vita in cui residua pur sempre un margine di vulnerabilità (113).

Viceversa, nel caso in cui la scelta del minore *in età* di discernimento si riveli non libera e comunque non conforme al suo migliore interesse — valutazione questa che dovrà essere operata, nella loro "responsabilità", anzitutto dai genitori — allora il SCP avrà ragione di essere attivato o di continuare ad essere mantenuto così come era stato impostato o, tutt'al più, con una diversa configurazione, in ragione dei margini di maturità conquistati dal figlio.

Insomma, se nell'età in cui manca il discernimento si giustifica la massima estensione della vigilanza parentale, nell'età del discernimento il suo perimetro va diversamente definito in base alla maturità del figlio che può a sua volta differenziarsi in ragione del contesto, potendo, ad esempio, rivelarsi idonea all'autodeterminazione negli spazi della rete preposti unicamente ad attingere informazioni e non nei *social* network, rispetto ai quali la libertà di quel minore dimostra di accusare il peso del giudizio altrui o di un pensiero polarizzato (114).

---

(112) Sul punto v. M. Ferrari, *È lecito che il genitore controlli il cellulare del figlio minorenne?*, in *www.personaedanno.it*, 2016; V. Corriero, *Privacy del minore e potestà dei genitori*, cit., 998 ss.; F. Scia, *Diritti dei minori e responsabilità dei genitori nell'era digitale*, cit., 139 ss. V. anche Cass. pen., 17 luglio 2014, n. 41192, in banca dati *De jure*.

(113) Un obbligo di informazione sulle restrizioni attuate deve ritenersi sussistere anche nei confronti degli stessi minori, alla stregua di quanto dispone l'art. 14, par. 3, Reg. UE 2022/2065, ove si sancisce che « se un servizio intermediario è principalmente destinato a minori o è utilizzato in prevalenza da questi, il prestatore di tale servizio intermediario spiega in modo comprensibile per i minori le condizioni e le restrizioni che si applicano all'utilizzo del servizio ». Sul tema dell'informazione al minore v. C. Perlingieri, *La tutela dei minori di età nei* social networks, cit., 1324 ss.; C. Camardi, *Relazione di filiazione e privacy. Brevi note sull'autodeterminazione del minore*, cit., 831 ss.; C. Irti, *Persona minore di età e libertà di autodeterminazione*, cit., 617 ss.; M. Bianca, *Il minore e i nuovi* media, cit., 151 ss.

(114) Si rinvia, in proposito, a C. Perlingieri, *Social Networks and Private Law*, Napoli, 2017, *passim*.

L'istituzione rigida e indifferenziata di forme di controllo sull'attività del minore nella rete contrasta, oltretutto, con la capacità riconosciuta al minore di sedici anni (in Italia di quattordici anni) di esprimere il consenso al trattamento dei propri dati personali nei servizi della società dell'informazione (art. 8 Reg. (UE) 2016/679 e art. 2-*quinquies*, d.lgs. 30 giugno 2003, n. 196). Capacità che, come si è avuto modo di argomentare in altra sede (115), si estende inevitabilmente anche al contratto di fornitura di contenuti o servizi digitali contro la fornitura di dati personali, regolato dalla Dir. (UE) 2019/770 e dagli artt. 135-*octies* ss. cod. cons.

È evidente che, trattandosi di un riconoscimento di capacità formulato in termini generali, peraltro ad opera di una fonte eurounitaria (116), senza alcuna distinzione di contenuti o categorie di servizi della società dell'informazione, non può ammettersi ad opera degli Stati membri l'istituzione di uno strumento di controllo, che abbia come effetto la negazione di codesta libertà. E comunque la limitazione potrà essere giustificata soltanto in nome dell'interesse superiore del minore, da valutarsi con riferimento al singolo caso, alla condizione contestuale in cui versa quel determinato minorenne. In altre parole, posto che nelle situazioni di equilibrio dell'assetto di interessi in gioco la cifra del bilanciamento sancita dall'art. 8 del GDPR tutela l'interesse del minore ad autodeterminarsi nei servizi della società dell'informazione, facendolo prevalere su ogni altro interesse, è soltanto in nome dello stesso *best interest*, valutato in concreto, che può essere corretta quella cifra.

In definitiva, le ragioni dell'identità personale del minore nel *web*, in cui l'altrove disincarnato sa soltanto profilare e sfruttare ma non "curare" i profili identitari, esigono, senz'altro, l'attivazione di efficaci misure di protezione, conformi, però, alla condizione giuridica del minore, la quale non può prescindere dal suo contesto singolare (117).

---

(115) Il riferimento è a *Minore età e contratto. Contributo alla teoria della capacità*, cit., 23 ss.

(116) Cfr. E. Andreola, *Minori e incapaci in* Internet, cit., 126 ss.; A. Astone, *I dati personali dei minori in rete. Dall'internet delle persone all'internet delle cose*, Milano, 2019, *passim*; R. Senigaglia, *Minore età e contratto. Contributo alla teoria della capacità*, cit., 75 ss.; M. Foglia, *Identità digitale, trattamento dei dati e tutela della persona*, 95 ss.; C. Irti, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, 87 ss.; V. Ricciuto, *L'equivoco della privacy. Persona vs. dato personale*, cit., 43 ss.

(117) Su questi profili teorici, si rinvia a G. Zaccaria, *Postdiritto. Nuove fonti, nuove categorie*, Bologna, 2022, 263 ss.

III.
IDENTITÀ DIGITALE E SUCCESSIONI PER CAUSA DI MORTE

di *Francesca Bartolini*

Sommario: 3.1. Identità personale e identità digitale. — 3.2. Le questioni dell'identità digitale successoria. — 3.3. (*Segue*): la successibilità dell'account. — 3.4. Il mandatario del *de cuius*. — 3.5. Autonomia privata "negativa" sull'account. — 3.6. I diritti dei terzi. — 3.7. Prospettive.

3.1. Identità personale e identità digitale

La questione dell'identità digitale della persona implica, fra le varie sue 'ramificazioni', quella del rapporto con la dimensione del *post mortem*.

Se l'identità digitale della persona possa qualificarsi come complesso di diritti idoneo a circolare anche dopo la morte della persona, secondo quali regole e in relazione a quali altri plessi normativi che, pure, aspirano a disciplinarne aspetti centrali, sono interrogativi di grande interesse non solo per lo studioso, ma anche per l'operatore del diritto, che da qualche anno si misura con un conflitto crescente e con le prime epifanie normative di specifico conio (1).

Il discorso sull'identità digitale nella successione *mortis causa* non è possibile senza un preliminare chiarimento su natura e struttura dell'identità digitale, prodromico a scrutinarne la successibilità; natura, anzitutto, che non può che ricondursi all'identità personale come poliforme dimensione della persona, la quale, come nella teoria delle anime confederate di *Sostiene Pereira* (2), ne aggiunge, oggi, una ulteriore (3).

---

(1) Supportato dalle ricostruzioni di alcuni pregevoli studi monografici: V. Confortini, *Persona e patrimonio nella successione digitale*, Torino, 2023, A.A. Mollo, *Eredità digitale e piattaforme online. Tutela e profili di pianificazione*, Napoli, 2021, A. Vesto, *Successione digitale e circolazione dei beni online. Note in tema di eredità digitale*, Napoli, 2020.

(2) A. Tabucchi, *Sostiene Pereira*, Feltrinelli (I Narratori), 1994.

(3) Più che una « moltiplicazione » o uno « sdoppiamento », mi pare si tratti di cogliere una ulteriore manifestazione dell'identità della persona. Ma cfr. su questo A. Vesto, *Successione digitale e circolazione dei beni online*, cit., 46 ss.

Se la nozione di identità personale emerse con forza negli anni '60-'70, al tempo dell'espansione dei media, come risposta giuridica a un fenomeno sociale allora dilagante e incontrollabile, anche l'identità digitale è fenomeno la cui crescita di importanza sul piano giuridico risponde all'esigenza di colmare un vuoto: perché oggi l'identità personale non è più limitata a ciò che la persona fa nel mondo reale (nella vita personale o in quella professionale), ma comprende anche, da una parte, ciò che la persona fa nel mondo virtuale, dall'altra e secondo 'altra' prospettiva, il modo in cui la persona è percepita dai componenti della comunità virtuale.

Del resto, la Costituzione protegge, fra i diritti della personalità di cui all'art. 2, il diritto della persona a esprimersi, a « svolgere » la sua personalità, quale diritto inviolabile della persona (4); in questo senso l'identità personale può identificarsi come proiezione sociale della complessiva personalità dell'individuo, il cui interesse a essere rappresentato con la sua reale identità — e, cioè, a non veder modificato, offuscato o, comunque, alterato all'esterno il proprio patrimonio intellettuale, ideologico, politico, etico, religioso, professionale (5) — integra un valore costituzionalmente rilevante (6).

In ambito sovranazionale, l'art. 8 della Carta dei diritti fondamentali dell'Unione europea cristallizza il diritto della persona alla protezione dei dati di carattere personale che la riguardino; le esigenze di protezione nascono originariamente flessibili, capaci cioè di plasmarsi e di adattarsi all'evolversi degli strumenti di comunicazione, che cambiano così rapidamente da sfuggire a descrizioni normative troppo dettagliate. L'evoluzione non ha tardato a manifestarsi e oggi l'identità personale è anche — e sarà sempre più — digitale.

L'identità digitale esibisce una specificità particolarmente rilevante: si

---

(4) In che senso possa parlarsi di protezione costituzionale del diritto all'identità personale, e attraverso quale percorso si sia arrivati alla riferibilità costituzionale di un diritto che manca nel quadro della disciplina codicistica è ben chiarito da G. Resta, *Il modello codicistico dei diritti della personalità e la costituzionalizzazione del diritto privato*, in G. Alpa, G. Resta, *Le persone e la famiglia*, 1, *Le persone fisiche e i diritti della personalità*, nel *Trattato di Diritto Civile*, diretto da R. Sacco, II ed., Milano, 2019, 316 ss., ove emerge chiara la centralità del ruolo della giurisprudenza.

(5) La locuzione « identità personale » è qui intesa nella accezione « moderna » proposta da G. Resta, *Identità personale e identità digitale*, in *Diritto dell'informazione e dell'informatica*, 2007, 511 ss., e spec. 513, come « sintesi ideale della biografia » della persona. La definizione menzionata nel testo corrisponde a quella, di fonte giurisprudenziale, individuata dall'Autore, al cui ricco apparato critico si rinvia.

(6) Il diritto all'identità personale ha assunto una dignità normativa specifica, osserva ancora G. Resta, *ibidem*, nelle discipline sulla protezione dei dati personali (il riferimento è alla l. 31 dicembre 1996, n. 675, all'art. 2, d.lgs. n. 30 giugno 2003, n. 196, e all'art. 126, comma 2, d.lgs. 22 gennaio 2004, n. 42) che « contemplano, ma non definiscono » l'identità personale.

cristallizza nei dati digitali. Post, battute di dialoghi, immagini, etc., non possono considerarsi soltanto elementi dell'universo empirico, ma, lo si riconosce ormai pacificamente, possono essere oggetto di diritti, proprio nel senso per cui possono generare un conflitto fra soggetti; si tratta di una considerazione più intuitiva quando i dati relativi all'identità digitale hanno un contenuto di tipo patrimoniale — e quindi un valore economico immediatamente percepibile — oppure quando l'identità personale e quella digitale si fondono nelle nuove professioni digitali — influencer, blogger e così via —; casi nei quali il binomio dati relativi all'identità digitale/bene idoneo alla circolazione — *inter vivos* o anche *mortis causa* è più chiaro; un accostamento meno lineare, invece, con riferimento a dati digitali di contenuto strettamente personale (e di valore non economico ma, eventualmente, affettivo). Nell'economia digitale, peraltro, questa distinzione, che può ancora mostrare una qualche rilevanza sul piano successorio, nel contesto del mercato dei beni e dei servizi si stempera, perché i dati sono sempre "merce di scambio" fra operatori professionisti e utenti, anche quando il provider/il social network offra i propri servizi gratuitamente (7).

3.2. Le questioni dell'identità digitale successoria

Se, dunque, non è dubbio che sussista un interesse alla circolazione dei dati, si pone il problema di individuare il destino dei dati che più essenzialmente caratterizzano l'identità della persona dopo la sua morte. Si tratta di beni/diritti successibili? Qual è il ruolo dell'autonomia privata nella gestione *post mortem* di questi dati? Esiste una disciplina applicabile, e se no, come potrebbe costruirsene una su questi temi, che intersecano l'area del diritto alla riservatezza, oltre che delle regole successorie e di quelle contrattuali? (8)

Questi temi sono stati trattati frontalmente in un caso sottoposto alla Corte federale tedesca — *Bundesgerichtshof* (*BGH*) — nel 2018 (9), divenuto

(7) Così G. Resta, *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, in *Contr. impr.*, 2018, 85 ss., ma spec. 88. In merito al modello « servizi contro dati », v. Id, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la direttiva (UE) 2019/770 e il regolamento (UE) 2016/679*, in *Annuario del contratto 2018*, Torino, 2019, 125 ss., spec. 128 ss. Sul mercato dei dati personali basta vedere C. Angiolini, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020, V. Bachelet, *Il consenso oltre il consenso. Dati personali, contratto, mercato*, Pisa, 2023 e G. Versaci, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020.

(8) Pone bene in luce queste intersezioni V. Confortini, *Persona e patrimonio*, cit., 17 ss.

(9) BGH, 12 luglio 2018, III ZR 183/17, in *Neue Juristische Wochenschrift*, 2018, 3178 ss.; (in lingua italiana) in *Nuova giur. civ. comm.*, 2019, I, 691, con nota di R. Mattera, *La successione nell'*account *digitale*; con commento di F.P. Patti, F. Bartolini, *Digital Inheritance*

assai noto per aver innescato un dibattito di grande interesse, destinato senz'altro ad arricchirsi ulteriormente nel prossimo futuro. In quella vicenda, una quindicenne morì travolta da un treno, a Berlino, in circostanze poco chiare; i genitori chiesero di poter accedere ai dati dell'account Facebook della figlia defunta, con lo scopo dichiarato di meglio ricostruire le circostanze della morte da un lato, e di carpire da quei dati qualcosa in più sulle relazioni interpersonali della figlia con possibili eventuali responsabili del tragico evento; Facebook negò l'accesso, invocando il diritto alla privacy dei soggetti coinvolti e il principio di segretezza della corrispondenza.

Come è noto, il GDPR (10) non si applica ai dati delle persone decedute (11), restando in capo ai singoli Stati membri la scelta sul se e sul come predisporre una specifica disciplina. D'altra parte, lo stesso legislatore europeo invita i legislatori nazionali a intervenire (12), e il parlamento italiano ha provveduto, cogliendo l'occasione del necessario adattamento delle regole sulla privacy — d.lgs. 30 giugno 2003, n. 196 — al Regolamento europeo con il d.lgs. 10 agosto 2018, n. 101 (13).

Le soluzioni scelte dal legislatore italiano possono considerarsi frutto di un dibattito piuttosto consapevole, sui temi della « successione digitale » o

---

and Post Mortem Data Protection: The Italian Reform, in *European Review of Private Law*, 2019, 1181; con commento di G. Resta, *Personal data and digital assets after death: a comparative law perspective on the BGH* Facebook *ruling*, in *EuCML (Journal of European Consumer and Market Law)*, 2018, 201; con commento di M.-O. Mackenrodt, *Digital Inheritance in Germany*, in *EuCML*, 2018, 41, L. Wüsthof, *Germany's Supreme Court Rules in Favour of "Digital Inheritance"*, in *EuCML* 2018, 205; con commento di T. Traschler, *Der Wettlauf um den digitalen Nachlass aus rechtsvergleichender Perspektive*, in *Zeitschrift für Europäisches Privatrecht*, 2020, 168 ss.

(10) Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, in G.U.U.E. L 119.

(11) V. il *Considerando* n. 27 GDPR.

(12) Cfr. il considerando n. 27 del Regolamento (UE) 2016/679, secondo cui « Il presente regolamento non si applica ai dati personali delle persone decedute. Gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute ». Sul punto, v. G. Resta, *Personal data and digital assets after death*, cit., 202, il quale osserva che molti Stati europei hanno adottato norme specifiche concernenti la protezione dei dati dei defunti; T. Traschler, cit., 172; nonché, per una posizione scettica sull'uso di questa discrezionalità, E. Harbinja, *Post-mortem privacy 2.0: theory, law and technology*, in *International Review of Law, Computers & Technology*, 2017, 26 spec. 34.

(13) D.lgs. 10 agosto 2018, n. 101: *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679*, in G.U., n. 205 del 4 settembre 2018.

della « eredità digitale » (14), maturato in letteratura, in assenza di una specifica casistica giurisprudenziale; un contesto, piuttosto, orientato alla comparazione con le opzioni accolte da sistemi diversi dal nostro (15).

Nel prosieguo si isolano tre problemi: in che modo si provveda a proteggere i dati della persona deceduta; come vadano qualificati i beni digitali; che spazio abbia l'autonomia privata nella disposizione *post mortem* di beni digitali (16).

Le disposizioni rilevanti ai fini dell'indagine sono contenute nell'art. 2 del d.lgs. n. 101 del 2018, che, modificando il d.lgs. n. 196 del 2003, vi inserisce l'art. 2-*terdecies*, rubricato *Diritti riguardanti le persone decedute*.

La regola base, contenuta nel comma 1, prescrive che « i diritti di cui agli articoli da 15 a 22 del Regolamento [ovvero l'accesso, la rettifica, la cancellazione e la portabilità dei dati, n.d.r.] riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione ».

Tuttavia, l'esercizio di questi diritti incontra alcuni limiti: non è ammesso negli specifici casi indicati dalla legge, ovvero quando, « limitatamente all'offerta diretta di servizi della società dell'informazione », sia stato l'interessato a esprimere il divieto con « dichiarazione scritta presentata al titolare del trattamento o a quest'ultimo comunicata » (17). Per assicurarsi che questa volontà "negativa" sull'esercizio dei diritti sia certa e consapevole, si pretende, da un lato, che la scelta risulti « in modo non equivoco » e sia

---

(14) V. in particolare V. Zeno-Zencovich, *La successione nei dati personali e nei beni digitali*, in *Riv. giur. sarda,* 2013, 448; G. Resta, *La "morte" digitale*, in *Diritto dell'informazione e dell'informatica*, 2014, 891; M. Cinque, *La successione nel "patrimonio digitale": prime considerazioni*, in *Nuova giur. civ. comm*., 2012, II, 645; A. Magnani, *L'eredità digitale*, in *Riv. not.,* 2014, 147; S. Deplano, *La successione a causa di morte nel patrimonio digitale*, in C. Perlingieri, L. Ruggieri (a cura di), *Internet e diritto civile*, Napoli, 2015, 427; U. Bechini, *Identità ed eredità digitale*, in O. Pollicino, V. Lubello, M. Bassini (a cura di)*, Identità ed eredità digitali. Stato dell'arte e possibili soluzioni al servizio del cittadino*, Roma, 2016, 43; M. Mattioni, *Profili civilistici dell'identità digitale tra tutela e accertamento*, *ivi*, 62-65; L. Liguori, *Eredità digitale. L'esercizio dei diritti dell'interessato deceduto*, *ivi*, 75; C. Marchisotti, *Digital identity and posthumous protection*, *ivi*, 85; V. Barba, *Contenuto del testamento e atti di ultima volontà*, Napoli, 2018, spec. 282-297; G. Marino, *La "successione digitale*", in *ODCC*, 2018, 167.

(15) G. Resta, *La "morte" digitale*, cit., 895-899 con riferimento ai sistemi inglese, brasiliano e americano.

(16) Nella prospettiva sociologica, si occupa di questi temi G. Ziccardi, *Il libro digitale dei morti*, Milano, 2017; ma v. anche i riferimenti offerti da G. Resta, *Identità personale e identità digitale*, cit., 511, nt. 1.

(17) Art. 2-*terdecies*, comma 2, d.lgs. 10 agosto 2018, n. 101.

« specifica, libera e informata », dall'altro che il divieto possa in ogni momento essere revocato o modificato dall'interessato (18).

Il legislatore considera peraltro la posizione dei terzi potenzialmente coinvolti, stabilendo, al comma 4, che « il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi ».

3.3. *Segue*: la successibilità dell'account

Nell'ordinamento tedesco, posto il problema della successibilità dell'account social nel caso segnalato in apertura, la soluzione si è trovata attraverso una piana applicazione del principio di successione universale di cui al § 1922 del BGB (19). Trasmesso agli eredi il rapporto contrattuale fra l'utente deceduto e il social network, si trasmettono di questo rapporto i contenuti, e quindi i diritti e gli obblighi ivi previsti (20), di talché gli eredi devono poter vantare il diritto ad accedere all'account e ai suoi contenuti, di natura personale e patrimoniale.

Nel nostro ordinamento è invece intervenuto il legislatore, preferendo agire diversamente: invece di intervenire nell'ambito della disciplina successoria, ha scelto di farlo sulla (21) protezione dei dati personali.

Si è già menzionata la regola secondo cui i diritti di accesso, rettifica, cancellazione, portabilità dell'account dell'utente defunto possono essere esercitati da soggetti che agiscono nell'interesse proprio o al fine di proteggere gli interessi del defunto. Non è chiaro se questi diritti possano essere esercitati *iure*

---

(18) Art. 2-*terdecies*, comma 4, d.lgs. 10 agosto 2018, n. 101.

(19) § 1922 BGB: *Gesamtrechtsnachfolge - (1) Mit dem Tode einer Person (Erbfall) geht deren Vermögen (Erbschaft) als Ganzes auf eine oder mehrere andere Personen (Erben) über*. [...].

(20) BGH, 12 luglio 2018, III ZR 183/17, par. 21. V. per i primi commenti, *supra*, n. 8. Per una lettura critica, V. Confortini, *Persona e patrimonio*, cit., 72 ss. e A. Vesto, *Successione digitale e circolazione dei beni online*, cit., 117 ss.

(21) Fin dal 2003 il legislatore italiano si è occupato dei diritti sui dati personali dei defunti, offrendo alcune indicazioni utili a determinare la sorte di questi dati. Secondo l'art. 9, c. 3 d.lgs. 30 giugno 2003, n. 196 — Codice della privacy —, ora sostituito dall'art. 2 *terdecies* d.lgs. 10 agosto, n. 101), « [i] diritti relativi a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione »; la disposizione non affrontava le questioni poste alla Corte federale tedesca limitandosi a nominare una serie di soggetti legittimati all'esercizio di diritti relativi ai dati della persona defunta (cfr. C. Marchisotti, *Digital identity and posthumous protection*, cit., 102). Peraltro, il legislatore italiano, così come quello francese, ha colto l'occasione dell'attuazione del GDPR per intervenire sul problema dei dati delle persone decedute.

proprio o *mortis causa*, ma i più attenti commentatori identificano una sorta di proiezione dei diritti sui dati oltre la fine della persona fisica, fenomeno particolarmente rilevante con riferimento ai rimedi offerti dal GDPR (22).

Nel catalogo dei diritti c'è quello ad accedere all'account social (23), a ottenere la rettifica dei dati (24), o la cancellazione (25), il diritto alla portabilità dei dati (26). Si è segnalato come questa disposizione sia volta a ridurre il rischio di incorrere in una situazione di stallo con riferimento al complesso dei dati della persona defunta, in cui non sia possibile assumere una decisione sulla circolazione, sulla cancellazione o su un uso diverso; si è inteso, dunque, consentire il controllo sul destino del complesso di dati riferibili alla persona (27). La menzionata disposizione, del resto, avrebbe il pregio di poter generare un incremento di concorrenza fra i diversi provider: il concorrente dovrebbe poter assicurare al potenziale utente di essere in grado di integrare tutti suoi dati (o almeno parte di essi), se sceglierà di "trasferirgli" la sua posizione (28).

---

(22) Così F.P. Patti, in F. Bartolini, F.P. Patti, *Identità digitale e circolazione dei dati* post mortem, in D. Mantucci, G. Perlingieri, M. D'Ambrosio (a cura di), *Dibattito sulle ricerche della dottrina civilistica nel biennio 2017-2018*, Napoli, 2021, 467 ss., ove si segnalano C. Camardi, *L'eredità digitale. Tra reale e virtuale*, in *Diritto dell'informazione e dell'informatica*, 2018, 81 e G. Resta, *La successione nei rapporti digitali,* cit., 85.

(23) Art. 15, GDPR (Reg. U.E. 2016/679).

(24) Art. 16 GDPR.

(25) Art. 17 GDPR. In tema di cancellazione dei dati come diritto della persona v. F. Di Ciommo, *Privacy in Europe After Regulation (EU) No 2016/679: What Will Remain of the Right to Be Forgotten?*, in *Italian Law Journal* 2017, 623. In giurisprudenza, v. Cass., sez. un., 22 luglio 2019, n. 19681, in *Corriere giur*., 2019, 1189, con commento di V. Cuffaro, *Una decisione assennata sul diritto all'oblio*; in *Danno resp*., 2019, 604, con commento di D. Muscillo, *Oblio e divieto di lettera scarlatta*; con commento di R. Pardolesi, *Oblio e anonimato storiografico: «* usque tandem *... »?*, in *Foro it*., 2019, I, 3071; con commento di R. Citarella, *Diritto all'oblio: un passo avanti, tre di lato*, in *Resp. civ. prev*., 2019, 1556. Cfr. su questo in dottrina M. Bianca, *Memoria ed oblio: due reali antagonisti?*, in *MediaLaws*, 3/2019, 23.

(26) Art. 20 GDPR: « [l]'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti [...] ». V. sul punto R. Janal, *Data Portability - A Tale of Two Concepts*, in *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 2017, 59, secondo cui « [u]pon request, data controllers are required to provide personal data to the data subject in a structured, commonly used and machine-readable format, which enables the data subject to transfer their personal data between controllers ».

(27) G. Resta, *La successione nei rapporti digitali*, cit., 101, secondo il quale il diritto alla portabilità dovrebbe potersi accordare solo in capo agli eredi o fiduciari, ma non a chiunque « invochi un mero "interesse proprio" ».

(28) V. F.P. Patti, *Identità digitale e circolazione dei dati* post mortem, cit., 469.

Anche nel nostro ordinamento, peraltro, la disciplina delle successioni *mortis causa* ha un ruolo significativo; del resto il principio della successione universale è trasversale ai diversi ordinamenti (29): anche in Italia, dunque, il rapporto contrattuale fra l'utente deceduto e il social network fa parte del complessivo patrimonio che, nella sua universalità, si trasmette agli eredi (30).

Si riconosce all'autonomia privata di escludere la trasmissione del rapporto agli eredi, ma la regola ha natura dispositiva (31); in mancanza di un divieto espresso, anche nel nostro ordinamento gli eredi avrebbero ottenuto accesso all'account *iure successionis*.

Emerge chiaro il possibile problema, irrisolto sul piano normativodel-l'eventuale conflitto fra più soggetti, tutti titolari di diritti sui dati del defunto secondo le disposizioni e i principi appena menzionati, che intendano esercitare diversamente tali diritti, con scelte "gestorie" anche, in ipotesi, radicalmente opposte (un esempio molto banale: si può immaginare che più figli dell'utente defunto intendano scegliere destini diversi per i suoi dati). In questi casi, in mancanza di indicazioni espresse dal *de cuius*, non può ipotizzarsi una soluzione univoca, ma semmai solo, volta a volta, una valutazione e un bilanciamento degli interessi delle parti, con uno sguardo attento agli eventuali indizi che il contesto possa offrire sulla volontà dell'utente defunto.

3.4. Il mandatario del *de cuius*

Posto che nel sistema italiano è la tutela della privacy a giocare un ruolo decisivo, spicca nella disciplina riformata il ruolo del mandatario incaricato all'uopo dall'utente di proteggere i suoi interessi digitali dopo la morte (32).

---

(29) L'universalità implica che la successione interessi l'intero patrimonio del defunto, senza alcuna distinzione sulla natura dei beni coinvolti; l'erede è immesso in tutto il — o in una quota del — patrimonio del *de cuius*.

(30) Così F.P. Patti, *Identità digitale e circolazione dei dati* post mortem, cit., 469; ma v. anche S. Deplano, *La successione a causa di morte nel patrimonio digitale*, cit., 430 ss.; G. Marino, *La "successione digitale*, cit., 180. Diversamente, V. Barba, *Contenuto del testamento e atti di ultima volontà*, cit., 290 ss.

(31) V. anche per rilievi comparatistici, F. Padovini, *Rapporto contrattuale e successione per causa di morte* Milano, 1990, 81 ss.; Id., *Le posizioni contrattuali*, in *Trattato di diritto delle successioni e donazioni*, diretto da Bonilini, I, Milano, 2009, 525 ss.

(32) Art. 2-*terdecies*, comma 1, d.lgs. n. 196 del 2003 riformato dal d.lgs. n. 101 del 2018. L'incarico al mandatario è vantaggioso rispetto alla nomina di un esecutore testamentario — sulla cui figura, v., recentemente, A.M. Benedetti, *Privato e pubblico nell'ufficio di esecutore testamentario*, in *Dir. successioni famiglia*, 2023, 1 ss. —: per rapidità (non occorre attendere la pubblicazione del testamento), per semplicità (non ci sono vincoli di forma), per sicurezza (le credenziali possono essere usate da chiunque abbia a disposizione il testamento).

Questa scelta di politica legislativa persegue due obiettivi. Anzitutto, legittimare la prassi contrattuale, in uso per le più comuni piattaforme social, di consentire all'utente di incaricare un "contatto erede" per la gestione dell'account dopo la morte: in tal senso, le regole si allineano alla prassi dei rapporti utente/social network.

In secondo luogo, incrementare il grado di protezione dell'autonomia testamentaria degli utenti, consentendo di ampliare il novero degli strumenti di gestione dei propri asset digitali dopo la morte (33); si tratta senza dubbio di un passo avanti nel riconoscimento della libertà testamentaria (34).

I commentatori che si sono misurati con questa scelta dei provider dopo l'entrata in vigore della disciplina di "attuazione" del GDPR hanno tentato, da una parte, di chiarire la natura di questo incarico, dall'altra, di qualificare la posizione giuridica del mandatario (35).

Quanto al primo aspetto, ci si è riferiti al "mandato *ad mortem exequendum*", un mandato i cui effetti giuridici si realizzano alla morte del mandante (l'interessato) (36). In dottrina questa figura si considera senz'altro compatibile, da un lato, con il divieto dei patti successori di cui all'art. 458 c.c. (37) e, dall'altro, con la natura fiduciaria del rapporto di mandato (38).

V., sui modi di trasmissione del patrimonio digitale, S. Stefanelli, *Destinazione* post mortem *dei diritti sui propri dati personali*, in *MediaLaws*, 1/2019, 136 ss.

(33) Negli ultimi anni il diritto successorio italiano ha dimostrato un crescente interesse verso la libertà testamentaria. Un esempio si trae dalle vicende relative alla diseredazione, sulla quale può vedersi, anche in una prospettiva di confronto con altri sistemi, F. Bartolini, F.P. Patti, *The freedom to disinherit children*, in *ZEuP*, 2018, 428.

(34) Cfr. G. Resta, *Chi controlla la nostra identità digitale dopo la morte?*, in *Giust. civ.*, 2018, 5.

(35) V. L. Vizzoni, *Mandato post mortem e c.d. eredità digitale*, in C. Granelli (a cura di), *I nuovi orientamenti della cassazione civile*, III ed., Milano, 2019, 149 ss.

(36) Che secondo G. Marino, *La "successione digitale*, cit., 197 va qualificato come atto unilaterale (una sostanziale autorizzazione) mentre V. Barba, *Interessi post mortem tra testamento e altri atti di ultima volontà*, in *Riv. dir. civ.*, 2017, 343 lo annovera nella categoria degli atti unilaterali *mortis causa* diversi dal testamento. Altri esempi di atti riferibili all'area del mandato *post mortem exequendum* si trovano in G. Resta, *La "morte" digitale*, cit., 919. Per una ricognizione degli atti sostitutivi del negozio testamentario, v. G. Christandl, *Will-Substitutes in Italy*, in A. Braun, A. Röthel (a cura di), *Passing Wealth on Death. Will-Substitutes in Comparative Perspective*, Oxford, 2016, 147.

(37) La compatibilità con il divieto dei patti successori deriva dalla non patrimonialità dell'incarico al mandatario (mentre l'art. 458 c.c. vieta solo le attribuzioni patrimoniali).

(38) Natura che parrebbe significare che i poteri dovrebbero cessare con la morte del mandante, secondo il disposto dell'art. 1722 n. 4 c.c.: ma, da un lato, esistono già eccezioni (ad es. il mandato nell'interesse del mandatario o di terzi), e, dall'altra, natura e *ratio* della disposizione non paiono impedirne una deroga pattizia. Sul punto v. C. Camardi, *L'eredità digitale*, cit., 92.

L'incarico, conferito in vita dall'utente *de cuius*, genera effetti che comprendono il potere del mandatario di chiedere e ottenere l'accesso all'account social per realizzare specifiche attività. Quanto alle modalità di conferimento, in genere, l'interessato si limita a reagire a una richiesta del provider, identificando il contatto erede, che quindi viene autorizzato a gestire l'account nei limiti predisposti dal provider stesso. Come si è condivisibilmente osservato, i diritti sull'account non integrano in alcun modo un'obbligazione del mandatario (che potrebbe anche non essere a conoscenza dell'incarico fino al momento della morte dell'utente/mandante). Del resto, i diritti del mandatario sull'account vanno bilanciati con altri possibili interessi meritevoli di protezione: con quelli, espressi dallo stesso utente/*de cuius* nel testamento, ovvero con interessi di matrice pubblicistica di terzi.

In definitiva, dunque, all'agente è inibita ogni azione in casi nei quali sia la legge a proibirla, o lo stesso interessato a manifestare una diversa volontà (ad esempio quella di cancellare l'account) (39).

3.5. Autonomia privata "negativa" sull'account

Per preciso dettato normativo — art. 2-*terdecies*, commi 2-5 del riformato codice della privacy — è consentito all'autonomia privata vietare la successibilità del rapporto fra social network e utente. Quando l'utente della piattaforma è una persona fisica emerge il problema della forte asimmetria di potere contrattuale fra l'utente e il gestore del social network (40), perché l'esclusione della trasmissibilità *mortis causa* della posizione è tendenzialmente imposta dal gestore, con una scelta che in realtà non realizza l'interesse dell'utente (41). L'effetto è che ai data controller e i provider è consentito l'accesso a un grande contenitore di dati e contenuti digitali, dei quali possono avvalersi per usi diversi (42).

In effetti nel caso tedesco, il social network fa valere l'accordo con

(39) V. G. Resta, *La successione nei rapporti digitali*, cit., 101.

(40) Sulle dinamiche asimmetriche nel rapporto gestore della piattaforma/utente — con riferimento ai gestori di servizi di natura patrimoniale —, v. F. Foltran, *Professionisti, consumatori e piattaforme online: la tutela delle parti deboli nei nuovi equilibri negoziali*, in *MediaLaws*, 3/2019, 162 ss.

(41) Le clausole in esame nascondono una scelta di policy operata unilateralmente dal provider informatico: v. F.P. Patti, *Identità digitale e circolazione dei dati* post mortem, cit., 472.

(42) Sui dati personali come beni v. G. Resta, *Personal Data and Digital Assets*, cit., 204 e Id., *I dati personali oggetto di contratto. Riflessioni sul coordinamento tra la direttiva (UE) 2019/770 e il regolamento (UE) 2016/679*, in *Annuario del Contratto 2018*, Torino, 2019, 125 ss.

l'utente per l'esclusione della trasmissibilità, attraverso la cd. memorializzazione dell'account (43).

La Corte tedesca afferma che quella con la quale si esclude la trasmissibilità *mortis causa* può considerarsi una clausola vessatoria ai sensi del § 307, par. 2, n. 1 del BGB, laddove incompatibile con i principi fondamentali espressi nelle norme dalle quali intende discostarsi (nello specifico, con il principio di universalità della successione) (44); la memorializzazione dell'account appare altresì incompatibile con il § 307, par. 2, n. 2 del BGB perché limita i diritti fondamentali e gli obblighi inerenti alla natura del contratto, al punto da pregiudicare il conseguimento dello scopo perseguito dalle parti del contratto.

Gli artt. 33-36 del codice del consumo, è noto, (45) sono applicabili ai soli rapporti fra consumatori e professionisti, e identificano come vessatorie le clausole, non negoziate, che determinino un eccessivo squilibrio fra diritti e obblighi delle parti, a svantaggio del consumatore; si è posto dunque il problema dell'applicabilità del controllo di vessatorietà alle clausole che escludano la successione nei rapporti fra utenti e piattaforme social e si è giustamente sostenuta la soluzione affermativa (46).

Al Codice civile può farsi riferimento per il problema delle condizioni

---

(43) Peraltro la Corte tedesca afferma che le clausole sulla memorializzazione dell'account non possono ritenersi vincolanti per l'utente, perché contenute nella sezione « supporto » del portale Facebook, e non all'interno del testo contrattuale secondo quanto invece disposto dal § 305, par. 2 del BGB.

(44) BGH, 12 luglio 2018, III ZR 183/17, cit., par. 30.

(45) Naturalmente in caso di applicabilità della legge italiana. Il problema è l'identificazione della legge applicabile, che il social network può scegliere determinando il contenuto della clausola sulla scelta di legge. Come noto, l'art. 6 (1) del Regolamento (CE) 593/2008 del 17 giugno 2008 sulla legge applicabile alle obbligazioni contrattuali — Roma I — pone un limite all'autonomia privata per i contratti con i consumatori, statuendo che « [f]atti salvi gli articoli 5 e 7, un contratto concluso da una persona fisica per un uso che possa essere considerato estraneo alla sua attività commerciale o professionale (« il consumatore ») con un'altra persona che agisce nell'esercizio della sua attività commerciale o professionale (« il professionista ») è disciplinato dalla legge del paese nel quale il consumatore ha la residenza abituale, a condizione che il professionista: *a*) svolga le sue attività commerciali o professionali nel paese in cui il consumatore ha la residenza abituale; o *b*) diriga tali attività, con qualsiasi mezzo, verso tale paese o vari paesi tra cui quest'ultimo; e il contratto rientri nell'ambito di dette attività ». Sul punto v. S. Fulli-Lemaire, *La tutela del consumatore alla luce delle regole sulla competenza giurisdizionale di fonte europea*, in A.M. Benedetti, I. Queirolo (a cura di), *Il consumatore di servizi finanziari nella crisi globale*, Roma, 2016, 55 ss., e con specifico riferimento ai social network, P.A. De Miguel Asensio, *Social Networking Sites: An Overview on Applicable Law Issues*, in *AIDA*, 2011, 3 ss.

(46) F.P. Patti, *Identità digitale e circolazione dei dati* post mortem, cit., 474; S. Deplano, *La successione a causa di morte nel patrimonio digitale*, cit., 441-442.

generali di contratto e dei contratti conclusi mediante formulario, perché il Codice offre regole soggettivamente neutre (artt. 1341 e 1342), e perciò applicabili anche ai contratti fra professionisti (47). Le condizioni generali di contratto predisposte da una sola parte — la piattaforma social —sono vincolanti solo se controparte ne ha conoscenza al momento della conclusione del contratto, ovvero se con l'ordinaria diligenza avrebbe dovuto conoscerle (48); ciò che pare arduo riscontrare laddove le clausole sulla memorializzazione sono contenute soltanto in sezioni dedicate al supporto, nella pagina delle FAQ o in altre "aree virtuali" poco frequentate.

La rinnovata disciplina in tema di data privacy (d.lgs. n. 101 del 2018) impone, si diceva, anche una valutazione sulle modalità di manifestazone del consenso: l'interessato infatti può espressamente vietare l'esercizio dei diritti di cui al GDPR (artt. 15-22) con una dichiarazione scritta consegnata o comunicata al responsabile del trattamento dati (49). La disposizione mira a proteggere non solo la volontà della persona, ma anche, e prima ancora, la persona stessa da indesiderabili intrusioni, posta la potenziale carica intima dei dati contenuti nei social (50); si prescrive poi che la volontà di vietare l'esercizio di questi diritti sia espressa in modo chiaro, specifico, che sia libera e consapevole, per garantire che si tratti di manifestazione dell'effettiva volontà dell'interessato (51).

L'effettività della protezione è affidata anche alla scelta di mantenere l'impianto letterale prescelto dal GDPR all'art. 4, par. 1, n. 11, che contiene una definizione di « consenso » (52). Si è ritenuta una strategia apprezzabile, che mira a scongiurare il pericolo di un procedimento di mera adesione a modelli generici predisposti da controparte per esprimere la volontà dell'in-

---

(47) V. G. Gorla, *Standard Conditions and Form Contracts in Italian Law*, in *Am. J. Comp. L.*, 1962, 1; E. Roppo, *Contratti standard. Autonomia e controlli nella disciplina delle attività negoziali di impresa*, Milano, rist. 2017, 173 ss., nonché da ultimo, nella prospettiva di una riforma del diritto interno, F.P. Patti, *Le clausole abusive nei contratti tra professionisti*, in *Annuario del contratto 2018*, cit., 86 ss.

(48) Art. 1341, comma 1, c.c.

(49) Secondo l'art. 2-*terdecies*, comma 2, d.lgs. n. 196 del 2003 può esercitare i menzionati diritti chi agisce nell'interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione.

(50) G. Resta, *La successione nei rapporti digitali*, cit., 102.

(51) Art. 2 *terdecies*, par. 3, d.lgs. 10 agosto 2018, n. 101.

(52) L'art. 4, comma 1, n. 11, GDPR definisce così il consenso: « "consenso dell'interessato": qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento ». Cfr. sul punto I.A. Caggiano, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *ODCC*, 2018, 78-82.

teressato (53). Il GDPR offre un ulteriore strumento efficace nei poteri del *Garante per la protezione dei dati personali*, che, quale autorità amministrativa indipendente, può, tra l'altro, adottare linee guida e "buone pratiche" di settore atte a contrastare abusi da parte dei provider; la soglia di protezione della volontà dell'interessato può allora saggiarsi attraverso le decisioni del Garante (54). D'altra parte, l'art. 7, comma 4, GDPR, dispone che « nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto » (55), perché il consenso in tal caso non sarebbe libero e deve quindi restare improduttivo di effetti (56).

In definitiva, la nuova regola prefigura un controllo rigido sull'effettiva volontà di vietare l'esercizio dei diritti di cui agli artt. 15-22 GDPR; coerentemente, stabilisce che l'interessato resti sempre libero di cambiare idea sul divieto, potendo revocarlo o modificarlo in qualsiasi momento, nel rispetto dei medesimi requisiti previsti per la manifestazione della volontà.

3.6. I diritti dei terzi

L'account social, pare ovvio segnalarlo, "appartiene" all'utente registrato sulla piattaforma (il cd. *data subject*), ma chiaramente coinvolge anche i terzi con i quali l'utente instauri relazioni (virtuali).

Si tratta di un aspetto importante, sottolineato da Facebook nel caso tedesco come argomento per negare ai genitori della ragazza defunta l'accesso all'account: si è infatti invocata la segretezza della corrispondenza dei terzi in relazione alle comunicazioni destinate all'account.

La Corte tedesca nega che la protezione dei dati personali di terzi possa costituire un valido argomento per impedire l'accesso degli eredi all'account

(53) F.P. Patti, *Identità digitale e circolazione dei dati* post mortem, cit., 475.

(54) Ad esempio, con riferimento al requisito della libertà, il Garante ha chiarito che l'offerta di un servizio non può essere condizionata al consenso per il trattamento dei dati (qualora questo non sia strettamente necessario all'adempimento della prestazione contrattuale).

(55) Sull'interpretazione della disposizione, v. G. Resta, *I dati personali oggetto del contratto*, cit., 134 ss.

(56) V. sul punto S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa dir. priv.*, 2016, 530-543; Id., *I requisiti del consenso al trattamento dei dati personali*, Santarcangelo di Romagna, 2016, 43-58. Sul problema del condizionamento del servizio al consenso al trattamento dei dati personali, v. ancora G. Resta, *I dati personali oggetto di contratto*, cit., 128 ss.

dell'utente defunto (57), sulla base di tre argomenti. Anzitutto, la natura dei contenuti digitali, intrinsecamente legati all'account, rende ininfluenti le dinamiche relative alla data privacy dei terzi. Gli eredi, ottenuto l'accesso *mortis causa*, non possono gestire l'account su base personale, ma saranno abilitati alle stesse azioni disponibili per l'utente in vita; perciò, esattamente come accade per l'utente, è impossibile verificare l'identità della persona con la quale si comunica; una volta che il contenuto digitale è stato "postato" sul profilo o sulla pagina Facebook, non è più gestibile da chi ha postato. Del resto la dinamica pare la stessa nel mondo della comunicazione analogica, ove chi trasmette una comunicazione non può certo impedire che il messaggio venga poi condiviso con un più ampio gruppo di persone. Inoltre, il principio di segretezza delle comunicazioni (§ 88 del *Telekommunikationsgesetz*) non può dirsi applicabile al caso di specie — e dunque non può considerarsi argomento utile a negare l'accesso all'account —, perché gli eredi non possono considerarsi « terzi » estranei all'utente defunto. Infine, lo stesso GDPR non impedisce il diritto degli eredi di accedere ai dati, perché il trattamento da parte di terzi è consentito dall'art. 6, par. 1, lett. (*b*) 1° ipotesi e lett. (*f*) (58).

Nel contesto nazionale la disciplina in materia di privacy autorizza i terzi che agiscano nell'interesse proprio o dell'utente deceduto a esercitare i diritti di cui agli artt. 15-22 GDPR, sempre che l'interessato non lo abbia espressamente vietato. Peraltro, lo stesso d.lgs. n. 101 del 2018 statuisce che il divieto non può nuocere alla posizione di terzi che intendano far valere un proprio diritto in giudizio (59). Allora, la disciplina della data privacy riformata non si riferisce agli interessi non patrimoniali dei terzi per impedire l'accesso ai contenuti digitali relativi all'account, ma, al contrario, per consentire loro la piena realizzazione della volontà di proteggere la propria posizione giuridica in giudizio.

Questa prospettiva ben emerge nei casi italiani che si sono misurati con il problema dell'accesso all'account del defunto, pur se nell'ambito di

(57) L. Wüsthof, *Germany's Supreme Court Rules*, cit., 206.

(58) Secondo l'art. 6, par. 1, lett. (*b*) del GDPR, Il trattamento è lecito se « è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso ». Secondo l'art. 6, par. 1, lett. (*f*), il trattamento è lecito se « il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore ». V. il commento di G. Resta, *Personal Data and Digital Assets*, cit., 204.

(59) Art. 2-*terdecies*, comma 5, d.lgs. n. 101 del 2018.

decisioni rese in sede cautelare (60): la domanda volta a ottenere un ordine nei confronti del provider di « fornire assistenza ai ricorrenti nel recupero dei dati personali dagli account del figlio deceduto » è accolta sulla base della sostanziale allegazione di un'esigenza dei terzi di proteggere una loro "legittima" posizione giuridica. Manca — ma per il tipo di procedimento nel quale la giurisprudenza finora ha avuto modo di cimentarsi non si tratta di una manchevolezza — una posizione di problemi pur inesorabili, quali una identificazione esatta del novero dei terzi cui la disciplina faccia riferimento e, soprattutto, i criteri di soluzione degli eventuali conflitti fra più terzi legittimati.

La liceità del trattamento « necessario per l'adempimento di un contratto del quale l'interessato è parte » [lett. (*b*)] rende l'accesso senz'altro possibile agli eredi per via del principio della universalità della successione, ma, nel quadro della rinnovata disciplina, anche ai soggetti indicati dal d.lgs. n. 101 del 2018 (61).

Del resto, il trattamento di questi dati è consentito se necessario per tutelare gli interessi di terzi [lett. (*f*)], ove per terzi senz'altro si intendono i soggetti menzionati nel decreto legislativo.

Infine il principio di segretezza della corrispondenza: la Costituzione protegge la libertà, la segretezza e l'inviolabilità di ogni forma di comunicazione (art. 15) contro possibili interferenze e intrusioni dell'autorità pubblica, in quanto diritto fondamentale della persona. Diritto che si è sempre inteso meritevole di protezione contro il pericolo di *disclosure* non autorizzate dal soggetto interessato. Pare molto difficile adattare questo principio e il suo significato profondo all'area dei contenuti digitali, perché le comunicazioni virtuali, e specialmente quelle sui social network, nascono destinate naturalmente alla condivisione e alla circolazione. La possibile applicabilità del menzionato principio alle comunicazioni social potrà semmai essere valutata caso per caso (e per adesso mancano riferimenti giurisprudenziali sul punto), tenendo presenti le specificità della piattaforma digitale e l'adeguatezza del livello di privacy prefigurato nelle condizioni contrattuali (62).

---

(60) Si tratta, anzitutto, di Trib. Milano, sez. I, ord. 10 febbraio 2021, resa in relazione a fatti molto simili a quelli del caso tedesco, Trib. Bologna, ord. 25 novembre 2021 e Trib. Roma, 10 febbraio 2022, per una disamina complessiva delle quali v. V. Confortini, *Persona e patrimonio*, cit., 118, anche per la condivisibile impressione critica.

(61) Art. 2-*terdecies*, comma 1, d.lgs. n. 101 del 2018.

(62) Sull'applicabilità dell'art. 15 Cost. alle nuove forme di comunicazione, v. C. Caruso, *La libertà e la segretezza delle comunicazioni nell'ordinamento costituzionale*, in *Forum Quaderni Costituzionali*, 2013.

3.7. Prospettive

La disciplina, seppur scarna, volta a proteggere i dati personali della persona defunta, offre un primo set di regole funzionali a veicolare un'idea politica: quella del controllo sulla versione digitale dell'identità personale anche dopo la morte. Offre anche un'indicazione di politica legislativa: governare il fenomeno non attraverso le regole successorie, intervenendo a estendere l'ambito di applicazione di quelle pensate per i beni non digitali, ma attraverso la protezione del dato, che si valorizza nella sua intrinseca natura; del resto questa attitudine è generalizzata, non puntuale per il dato "successibile". La disciplina successoria resta con i suoi principi, più che con le regole tecniche, a "supportare" l'interprete.

Peraltro, manca del tutto, fra questi plessi, un coordinamento. L'unica disposizione rilevante si trova nel comma 5 dell'art. 2-*terdecies*, d.lgs. n. 196 del 2003, ove si statuisce che il divieto di esercitare diritti di cui agli artt. 15-22 del GDPR non può pregiudicare l'esercizio da parte di terzi di diritti patrimoniali derivanti dalla morte dell'interessato (63). Se c'è un valore patrimoniale, l'esercizio di questi diritti cade in successione (64), ma per le situazioni di natura personale è più difficile identificare le interferenze fra le regole successorie applicabili e discipline diverse (65).

Difficile pare altresì trovare strumenti per gestire i possibili conflitti fra i vari soggetti ai quali, in virtù della nuova disciplina, è consentito esercitare diritti sui dati digitali della persona defunta (*iure proprio* o per tutelarne gli interessi, ad es. per ragioni familiari). Oppure identificare quale scelta, fra quella espressa sulla piattaforma social (ad es., per la memorializzazione dell'account) e quella eventualmente espressa nel testamento (ad es., per la cancellazione di tutti i dati relativi all'account), debba prevalere (66). Il che, da una parte, innesca il bisogno di un giudice particolarmente accorto nel valutare, per decidere, la specificità del caso concreto; dall'altra apre a una valutazione sull'adeguatezza del nostro diritto successorio ad affrontare questioni legate a una realtà totalmente nuova.

---

(63) Art. 2-*terdecies*, comma 5, d.lgs. n. 101 del 2018.

(64) V. G. Marino, *La successione digitale*, cit., 182, con riferimento a software, fotografie, app etc.

(65) Ad. esempio, l'area dei diritti di proprietà intellettuale: v. gli artt. 20 e 23 della legge sul diritto d'autore (l. 22 aprile 1941, n. 633). Per altri esempi, v. A. Zaccaria, *Diritti extrapatrimoniali e successione. Dall'unità al pluralismo nelle trasmissioni a causa di morte*, Padova, 1988, 171-196; A. Zoppini, *Le « nuove proprietà » nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni)*, in *Riv. dir. civ.*, 2000, 229-232.

(66) Sull'espressione della volontà testamentaria, con riferimento ai contenuti digitali, v. M. Cinque, *La successione nel "patrimonio digitale"*, cit., 654.

Ancora, il trend pare quello di recepire la prassi in uso alle dinamiche contrattuali utente/piattaforma, a tratti addirittura cristallizzandola; questo atteggiamento, giustamente ritenuto apprezzabile (67) — forse inevitabile, data la forza contrattuale delle condizioni studiate, formulate e veicolate fra gli utenti dalle grandi piattaforme — non può peraltro appiattirsi su quelle dinamiche: il controllo sulla conoscibilità, sulla comprensibilità, sull'eventuale vessatorietà delle clausole va operato, e adeguato al contesto.

Su questo dovrà essere la Corte di Giustizia dell'Unione Europea a identificare i punti fermi di un'interpretazione che dovrà poi svilupparsi in seno alle Corti nazionali. Mentre si lavora per una disciplina uniforme in ambito UE, quantomai necessaria data la trasversalità della materia e dei soggetti coinvolti, sono gli ordinamenti nazionali — la loro dottrina, la loro giurisprudenza — a misurarsi con i primi casi e a offrire le prime soluzioni e impostazioni teoriche. Ciò che induce a identificare un altro problema non secondario, ovvero la legge applicabile ai conflitti generati dai fenomeni della eredità digitale.

(67) V. F.P. Patti, *Identità digitale e circolazione dei dati* post mortem, cit., 478.

IV.

L'"OBLIO DIGITALE": STRUMENTI DI TUTELA DINANZI AL GIUDICE CIVILE

di *Martina Flamini*

Sommario: 4.1. Premessa. — 4.2. Il contenuto del diritto all'oblio digitale nella giurisprudenza. — 4.3. Gli strumenti di tutela del diritto all'oblio digitale e le "misure necessarie" *ex* art. 10, comma 10, d.lgs. 150 del 2011. — 4.3.1. La tutela cautelare. — 4.3.2. La deindicizzazione. — 4.3.3. La cancellazione. — 4.3.3.1. La cancellazione delle c.d. copie *cache*.

4.1. Premessa

Il tema del diritto all'identità personale digitale, declinato con riferimento al diritto all'oblio (1), coinvolge questioni assai complesse e impone al giurista approfondite riflessioni sulla qualificazione della situazione giuridica soggettiva protetta e sulle relative forme di tutela, nella selezione di rimedi che non sempre riescono a conformarsi al principio di effettività.

Autorevole dottrina (2) ha sottolineato come all'identità digitale si faccia comunemente riferimento declinandola in merito a due aspetti fondamentali: quello della tutela dell'identità personale in rete e quello delle tecniche di identificazione della persona a mezzo di strumenti informatici. Nel presente contributo, ci si soffermerà soltanto sul primo dei due profili, per indagare, attraverso l'esame delle posizioni della giurisprudenza di merito e di legittimità, quali forme di tutela possono essere invocate dinanzi al giudice

(1) Nel presente contributo non potranno essere esaminati i numerosi profili teorici di una categoria giuridica complessa, difficilmente definibile in modo unitario, sulla quale la dottrina si è a lungo soffermata. Con specifico riferimento ai profili relativi al diritto all'oblio ed alle questioni poste dalla rete, cfr. P. De Marinis, *Oblio, Internet e tutele. L'inibitoria*, Napoli, 2021; G. Cirillo, *La deindicizzazione dai motori di ricerca tra diritto all'oblio e identità personale*, in *Nuova giur. civ. comm.*, 2020, 1242; R. Pardolesi-S. Bonavita, *Diritto all'oblio e buio a mezzogiorno*, in *Foro it.*, 2018, I, 1151; Aa.Vv., *Il diritto all'oblio su internet dopo la sentenza Google Spain*, a cura di G. Resta-V. Zeno-Zencovich, Roma, 2015.

(2) G. Resta, *Dignità, persone e mercati*, Torino, 2014, 327 e ss.

civile (3). Nella prassi applicativa, infatti, accade sovente che chi agisce in giudizio lamenti la lesione del diritto all'onore o alla reputazione e proponga, altresì, domande volte ad ottenere tutela per un (asserito) illecito trattamento dei dati personali. Qualificare correttamente il diritto controverso rileva ai fini dell'individuazione del quadro normativo di riferimento, delle possibilità di bilanciamento tra diritti confliggenti (che possono tra loro concorrere e trovarsi, appunto, in conflitto con altri diritti) e della scelta dei rimedi previsti a tutela della lesione di un determinato diritto.

4.2. Il contenuto del diritto all'oblio digitale nella giurisprudenza

Prima di passare ad esaminare come il diritto all'oblio digitale sia stato ricostruito dalla giurisprudenza, nella prospettiva sopra indicata, appare significativo ricordare la vicenda che ha portato al primo riconoscimento di tale diritto, nella sua accezione tradizionale, da parte della giurisprudenza di legittimità.

Con la sentenza 9 aprile 1998 (4), n. 3679, la Suprema Corte si è pronunciata sul ricorso proposto dal giornalista e dalla società editrice di un settimanale avverso la decisione della corte territoriale che aveva accolto la domanda volta ad ottenere il risarcimento dei danni non patrimoniali, conseguenti alla seconda pubblicazione, a distanza di sei anni dalla prima, di una notizia relativa all'incriminazione dell'attore per gravi fatti di mafia (fatti in relazione ai quali, tra la prima e la seconda pubblicazione, era intervenuto un provvedimento di archiviazione in sede penale). Nella decisione in esame, la Corte, pronunciandosi su una domanda volta ad ottenere la tutela del diritto all'onore e alla reputazione, nel bilanciamento tra tali diritti e il diritto di cronaca, si è soffermata sul requisito dell'attualità della notizia, per affermare che l'attualità dell'interesse pubblico "non è strettamente collegato all'attualità del fatto pubblicato, ma permane finché resta o quando ridiventa attuale la sua rilevanza pubblica". In tal modo, ha osservato la Corte, viene

(3) L'oggetto del presente contributo, volto a fornire spunti di riflessione in merito alle forme di tutela dell'oblio digitale dinanzi al giudice civile, non consente l'esame dell'art. 64-*ter* disp. att. c.p.p., introdotto dal d.lgs. 10 ottobre 2022, n. 150, (in attuazione dell'art. 1, comma 25, della l. 27 settembre 2021, n. 134, legge delega della cd. riforma Cartabia) relativo al diritto all'oblio degli imputati e delle persone sottoposte ad indagini di chiedere l'inibitoria dell'indicizzazione di un provvedimento non ancora diffuso, ovvero un titolo che consenta di ottenere, *ex post*, la deindicizzazione di dati personali già oggetto di divulgazione (per un attento esame della nuova disposizione normativa e dei rapporti con l'art. 52, d.lgs. 30 giugno 2003, n. 196, cfr. Relazione n. 46 dell'Ufficio del Massimario e del ruolo della Corte di Cassazione).

(4) Cass., sez. III, Sentenza 9 aprile 1998, n. 3679 (Rv. 514405-01).

in considerazione "un nuovo profilo del diritto di riservatezza — recentemente definito anche come diritto all'oblio — inteso come giusto interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore e alla sua reputazione la reiterata pubblicazione di una notizia in passato legittimamente divulgata".

Il primo riconoscimento, in via giurisprudenziale, del diritto all'oblio avviene, pertanto, nel tradizionale campo della tutela dei diritti della personalità, in una vicenda caratterizzata dalla dedotta lesione del diritto alla reputazione, con una decisione che, nel bilanciamento tra libertà di informazione e dignità della persona, riconosce un nuovo profilo del diritto alla riservatezza, rappresentato dal diritto ad essere rappresentati per quello che attualmente si è e non più (o non solo) per quello che non si è più (5).

A questa prima dimensione del diritto all'oblio, se ne affianca una seconda (oggetto del presente contributo) che, muovendo dallo sviluppo delle nuove tecnologie (sviluppo che incide sui modi e tempi di acquisizione, diffusione e permanenza in rete delle informazioni, inverando un diverso atteggiarsi del rapporto tra tempo ed attualità dell'interesse pubblico), si traduce in un diritto che guarda alla contestualizzazione delle informazioni (6), all'aggiornamento della notizia (con riferimento ad altre informazioni che potrebbero aggiornare o cambiare il quadro fornito dalla notizia originaria), alla sua conservazione e circolazione in rete. Più che un autonomo diritto della personalità, l'oblio digitale costituisce un aspetto "funzionale" del diritto all'identità personale, segnatamente il diritto alla disassociazione del proprio nome da un dato risultato di ricerca, che si traduce nel c.d. ridimensionamento della propria visibilità telematica.

Il fondamento normativo dell'oblio digitale può essere ricondotto all'art. 2 della Costituzione, all'art. 10 del codice civile, all'art. 8 della CEDU, agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea, mentre

---

(5) La necessità di un interesse effettivo e attuale alla diffusione della notizia è stato poi successivamente ribadito da Cass., sez. III, 26 giugno 2013, n. 16111, Rv. 626952-01, che afferma il seguente principio di diritto: "In tema di diffamazione a mezzo stampa, il diritto del soggetto a pretendere che proprie, passate vicende personali non siano pubblicamente rievocate (nella specie, il cd. diritto all'oblio era invocato in relazione ad un'antica militanza in bande terroristiche) trova limite nel diritto di cronaca solo quando sussista un interesse effettivo ed attuale alla loro diffusione, nel senso che quanto recentemente accaduto (nella specie, il ritrovamento di un arsenale di armi nella zona di residenza dell'ex terrorista) trovi diretto collegamento con quelle vicende stesse e ne rinnovi l'attualità, diversamente risolvendosi il pubblico ed improprio collegamento tra le due informazioni in un'illecita lesione del diritto alla riservatezza".

(6) G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Il diritto all'oblio su internet dopo la sentenza Google Spain*, cit., 30-35; Id., *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. Inf.*, 2012, 391-392.

l'unica disposizione che si riferisce esplicitamente all'oblio, sebbene nella sola rubrica, è l'art. 17 del Regolamento UE 2016/679 (di seguito, GDPR). Tale norma, peraltro, non definisce il diritto all'oblio, né indica i criteri da utilizzare per valutare l'attualità della notizia, ma si limita a prevedere che l'interessato "ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano", disponendo che, in tali casi, "il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli...adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato a cancellare qualsiasi *link*, copia o riproduzione dei suoi dati personali". La norma in esame, al suo paragrafo 3, precisa che tale diritto non può essere invocato qualora il trattamento di cui trattasi sia necessario per uno dei motivi in esso elencati, tra i quali compare, alla lettera *a*) di quest'ultimo paragrafo, l'esercizio del diritto relativo, in particolare, alla libertà d'informazione.

La Suprema Corte, con sentenza III Sez., 5 aprile 2012, n. 5525 (Rv. 622169-01), accogliendo il ricorso proposto da un uomo politico che, imputato di corruzione e successivamente assolto, aveva chiesto l'aggiornamento dei dati personali presenti in un articolo confluito nell'archivio *on line* di un giornale (dal quale risultava la sola notizia dell'imputazione), aveva già riconosciuto tale nuova dimensione del diritto all'oblio. In particolare, con riferimento alla disciplina antecedente all'entrata in vigore del GDPR), richiamati i principi di liceità, correttezza, esattezza e aggiornamento dei dati personali in relazione alla finalità del loro trattamento, la Corte ha precisato che: "in riferimento alla rete *internet,* non si pone...un problema di pubblicazione o ripubblicazione dell'informazione, quanto bensì di permanenza della medesima nella memoria delle rete *internet* e, a monte, nell'archivio del titolare del sito sorgente".

L'aggiornamento delle notizie presenti nella rete, pertanto, consente di tutelare e rispettare "la proiezione sociale dell'identità personale del soggetto" che costituisce "essenzialmente lo scopo che fonda l'interesse pubblico, a sua volta a base della finalità del trattamento, alla persistente conoscenza della notizia".

La questione della tutela dinamica dell'identità digitale, lesa a causa della permanenza nella rete *internet* di informazioni per le quali il tempo può aver affievolito l'interesse pubblico, è stata esaminata dalla Corte di Giustizia nella nota sentenza del 13 maggio 2014 (7), con la quale è stato riconosciuto il

(7) Corte di Giustizia UE 13 maggio 2014, C-131/12, *Google Spain/AgenciaEspañolas de Protecciòn de Datos (AEPD)/Mario Costeja Gonzales*.

diritto alla deindicizzazione (8) con riferimento ad un *link* che, partendo da una ricerca effettuata attraverso l'inserimento del nome del ricorrente, consentiva di risalire ad un articolo (reperibile nell'archivio *on line* di un quotidiano) che riferiva l'episodio di un pignoramento subito dal detto ricorrente, dodici anni addietro, per il mancato pagamento di debiti previdenziali. Nella decisione in esame (che tocca questioni cruciali, tra le quali la possibilità di qualificare il gestore del motore di ricerca quale titolare del trattamento e la valutazione relativa ai tipi di trattamento che possono essere ritenuti "effettuati nel contesto di uno stabilimento" del responsabile del trattamento in un determinato Stato membro), la Corte di Giustizia, muovendo dalla considerazione in forza della quale il trattamento dei dati personali potrebbe divenire inadeguato, non pertinente o eccessivo anche in ragione del mancato aggiornamento o della conservazione dei dati per un tempo superiore a quello necessario, ha affermato la necessità di cercare un giusto equilibrio tra l'interesse degli utenti di *internet* all'informazione ed i diritti fondamentali della persona che, in linea di principio, prevalgono, salvo che il ruolo ricoperto dalla persona cui l'informazione si riferisce nella vita pubblica non giustifichi il sacrificio di tali diritti in favore del "preponderante" interesse pubblico.

Nella giurisprudenza nazionale, il mutamento della stessa morfologia del diritto all'oblio, dovuta all'avvento delle nuove tecnologie, è stato poi riaffermato dalla Suprema Corte nell'ordinanza (Sez. I, n. 7559 del 27 marzo 2020, Rv. 657424-01) (9) che, dopo aver precisato che tale diritto deve essere concepito come "diritto al controllo delle diffusione delle scelte fatte in passato", ha sottolineato come, pur non potendosi riconoscere una vera e propria pretesa alla cancellazione del proprio passato, la questione attiene alla "distorsione dell'immagine del soggetto, costruita nel tempo dopo la vicenda ormai dimenticata, provocata dalla riemersione della notizia".

Sul contenuto del diritto all'oblio digitale è tornata ancora la Suprema Corte con l'ordinanza Sez. I, 19 maggio 2020, n. 9147 (Rv. 657638-01), per

(8) Nella versione inglese della sentenza, il termine utilizzato è "*indexing*".

(9) Nel caso portato all'attenzione della Corte, la prima vicenda giudiziaria aveva ad oggetto la pubblicazione, nell'archivio *online* del « Corriere della Sera » di due articoli del 1994 relativi alla condanna, in primo grado, del padre degli attori. I ricorrenti avevano proposto ricorso al Garante, sostenendo che gli articoli avevano riferito solo della condanna in primo grado del defunto padre, un importante imprenditore nel campo tipografico, senza dar conto del successivo proscioglimento dell'imputato, in tal modo ledendo l'onore e la reputazione di tutta la famiglia. Per tali motivi hanno chiesto la rimozione degli articoli dall'archivio del giornale e, in via subordinata, l'aggiornamento della notizia e la deindicizzazione. Avverso il rigetto del Garante, i ricorrenti hanno proposto ricorso dinanzi al Tribunale di Milano, che ha rigettato le domande proposte.

affermare che il diritto all'oblio consiste nel non rimanere esposti, senza limiti di tempo, ad una rappresentazione non più attuale della propria persona con pregiudizio alla reputazione ed alla riservatezza, a causa della ripubblicazione, a distanza di un considerevole intervallo temporale, di una notizia relativa a fatti del passato.

Negli stessi termini si è da tempo espressa anche la giurisprudenza di merito, chiarendo che il diritto della persona al rispetto della verità della propria identità digitale — e cioè a non veder ulteriormente divulgate notizie di cronaca che lo riguardino ove le stesse non rivestano più alcun interesse pubblico — si traduce nell'affermazione del suo diritto "all'aggiornamento della notizia, al fine di ripristinare la completezza e quindi la verità stessa della informazione e di non reiterare la diffusione di informazioni sull'identità personale o morale non più rispondenti alla realtà del momento, al contempo garantendo l'interesse del lettore a ricevere una completa e corretta informazione" (10).

Ancora la giurisprudenza di merito ha chiarito che la rete *internet* costituisce una realtà nella quale le informazioni non sono archiviate (e cioè organizzate e strutturate) ma solo memorizzate senza limiti e senza tempo, poste tutte al medesimo livello, senza una valutazione del relativo peso, prive di contestualizzazione e di collegamento con altre informazioni pubblicate: di qui, appunto, il diritto del soggetto cui le informazioni si riferiscono ad ottenerne la cancellazione, pur lecitamente diffuse, se inutilmente lesive in ragione della loro perdita di attualità (11).

4.3. Gli strumenti di tutela del diritto all'oblio digitale e le "misure necessarie" *ex* art. 10, comma 10, d.lgs. n. 150 del 2011

Sinteticamente delineato il contenuto del diritto all'oblio digitale (tema non ricompreso nel perimetro di indagine delle Sezioni Unite nella sentenza 22 luglio 2019, n. 19861), occorre soffermarsi sul concreto atteggiarsi della relativa tutela dinanzi al giudice civile.

L'interessato che assume leso il suo diritto può chiedere la rettifica dei dati inesatti o l'integrazione di quelli incompleti (art. 16 del GDPR), la cancellazione (art. 17) e la "limitazione" del trattamento (18), potendosi altresì opporre alla protrazione del trattamento (art. 21). Tali diritti dell'interessato sono coerenti con i principi generali cui dev'essere informato il trattamento dei dati personali, in particolare del principio di "minimizzazione" (per cui gli stessi devono essere "adeguati, pertinenti e limitati a

(10) Trib. Milano, 4 giugno 2013 (RG n. 1232 del 2010).
(11) Trib. Mantova, 26 ottobre 2016.

quanto necessario rispetto alle finalità per le quali sono trattati": art. 5, comma 1, lett. *c*), di "esattezza" (per cui devono essere "esatti e, se necessario, aggiornati", sicché "devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati": art. 5, comma 1, lett. *d*), e di "limitazione della conservazione" (per cui devono essere "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati": 5, comma 1, lett. *e*).

L'art. 152, d.lgs. 30 giugno 2003, n. 196, (così come modificato dal d.lgs. 1 settembre 2011, n. 150 e dal d.lgs. 10 agosto 2018, n. 101) attribuisce alla competenza dell'autorità giudiziaria ordinaria "tutte le controversie che riguardano le materie oggetto dei ricorsi giurisdizionali di cui agli articoli 78 e 79 del Regolamento e quelle comunque riguardanti l'applicazione della normativa in materia di protezione dei dati personali, nonché il diritto al risarcimento del danno ai sensi dell'art. 82 del medesimo regolamento", prevedendo che il processo si svolga nelle forme di cui all'art. 10 del d.lgs. n. 150 del 2011.

Oggetto del processo dinanzi al giudice civile è rappresentato, anche laddove sia stata esperita dall'interessato la tutela alternativa dinanzi al Garante per la protezione dei dati personali (12), dal diritto soggettivo che l'interessato assume leso, e che il giudice ordinario può tutelare anche attraverso la prescrizione delle "misure necessarie anche in deroga al divieto di cui all'art. 4 della legge 20 marzo 1865, n. 2248, allegato *e*)" (art. 10, comma 10, del d.lgs. n. 150 del 2011). La genericità dell'espressione "misure necessarie" impone all'interprete di chiarire il contenuto dei provvedimenti che il giudice può adottare, con la precisazione che l'indagine dovrà essere condotta tenendo presente che il principio di alternatività (che né nell'impostazione della direttiva 95/46/CE, né in quella del Regolamento 2016/679 rappresentava una scelta obbligata (13)) non può tradursi in un *vulnus* per la tutela dell'interessato. Nell'interpretazione delle "misure necessarie", pertanto, dovrà guardarsi, da un lato, ai poteri di cui dispone l'Autorità indipendente, disciplinati dall'art. 58 del GDPR, dall'altro, ai diritti che il Regolamento riconosce all'interessato (si pensi, ad esempio all'art. 21 "Diritto di opposizione"), per concludere che una tutela effettiva dei diritti

(12) Sul tema dell'alternatività tra tutela amministrativa e tutela giurisdizionale, cfr. Cass. 20 maggio 2002, n. 7341; Cass. 25 giugno 2004 n. 11864; Cass. 25 maggio 2017 n. 13151 e Cass. 18 giugno 2018 n. 16061. Sullo stesso tema, per la giurisprudenza europea, cfr. CGUE, sentenza del 27 settembre 2017, *Puškár*, C-73/16.

(13) Sul punto, cfr. F. Cafaggi, *Tutela amministrativa, tutela giurisdizionale e principio di effettività*, in *Effettività delle tutele e diritto europeo. Un percorso di ricerca per e con la formazione giudiziaria*, a cura di P. Iamiceli, Trento, 2020, 68.

dell'interessato dovrebbe comprendere, in primo luogo, la tutela inibitoria (individuale) del diritto al lecito trattamento dei dati personali.

Per quanto riguarda la tutela inibitoria collettiva, le disposizioni della Direttiva (UE) 2020/1828 del Parlamento europeo e del Consiglio, del 25 novembre 2020, come attuata dal d.lgs. 10 marzo 2023, n. 28, forniscono chiare indicazioni, prevedendo, per le "azioni rappresentative", la possibilità del giudice di concedere provvedimenti inibitori, definiti dall'art. 1, lett. *i*) del cit. d.lgs. come provvedimenti con il quale "il giudice ordina la cessazione o il divieto di reiterazione della condotta omissiva o commissiva posta in essere in violazione delle disposizioni di cui all'allegato II-*septies* e ordina la pubblicazione del provvedimento, integralmente o per estratto, su uno o più quotidiani a diffusione nazionale o locale ovvero la pubblicazione di una rettifica".

In merito alla tutela inibitoria collettiva, importanti indicazioni sono fornite, inoltre, dalla Corte di Giustizia nella sentenza del 28 aprile 2022 (*Meta Platforms Ireland Limited c. Bundesverband der Verbraucherzentralen*). Nella decisione in esame, i giudici di Lussemburgo — esaminando la domanda di pronuncia pregiudiziale, proposta dalla Corte federale di giustizia della Germania, nell'ambito di una controversia che opponeva *Meta Platforms Ireland Limited,* già *Facebook Ireland Limited,* la cui sede sociale si trova in Irlanda, all'Unione federale delle centrali e delle associazioni di consumatori in merito alla violazione, da parte della Meta, della normativa tedesca in materia di protezione dei dati personali — dopo aver richiamato il contenuto dell'art. 80, par. 2, del GDPR (14), hanno osservato che riconoscere legittimazione ad agire (a prescindere dal conferimento di un mandato) ad un'associazione di tutela degli interessi dei consumatori, allo scopo di far cessare trattamenti di dati contrari alle disposizioni del Regolamento "indipendentemente dalla violazione dei diritti di una persona individualmente e concretamente pregiudicata da tale violazione, contribuisce incontestabilmente a rafforzare i diritti degli interessati e ad assicurare loro un elevato livello di protezione" (par. 74). Ad avviso della Corte, pertanto, l'esercizio di siffatta azione rappresentativa consente di "prevenire un gran numero di violazioni dei diritti degli interessati a seguito del trattamento dei loro dati personali" e si potrebbe rivelare un mezzo più efficace rispetto a quello che un'unica persona, concretamente pregiudicata da una violazione del suo diritto alla protezione dei dati personali, potrebbe esperire contro l'autore di tale violazione.

(14) Norma che riconosce legittimazione ad « un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali ».

4.3.1. *La tutela cautelare*

In merito alla questione relativa alla possibilità che il giudice civile, adito per la tutela del diritto all'identità personale, *sub specie* di diritto all'oblio digitale, possa concedere provvedimenti cautelari atipici d'urgenza (15), occorre sottolineare l'importanza del rimedio cautelare per garantire l'effettività della tutela dei diritti che, in ragione della velocità di circolazione delle informazioni nella rete (nonché nella loro "immanenza" nella stessa), potrebbero essere definitivamente compromessi nelle more di un procedimento di merito (16).

La tutela cautelare per i contenuti illeciti memorizzati dall'*hosting provider* è poi espressamente prevista dall'art. 16, comma 3, del d.lgs. 9 aprile 2003, n. 70 (17).

Ancora in via generale, nella prospettiva della selezione del rimedio esperibile in ragione della situazione giuridica soggettiva che si ritiene lesa, occorre precisare che l'esclusione della tutela cautelare per i diritti all'onore e alla reputazione lesi in conseguenza dell'esercizio della libertà di informazione a mezzo stampa (18) non può riguardare i casi in cui il soggetto interessato invochi tutela in conseguenza di un illecito trattamento dei dati personali.

---

(15) Provvedimenti cautelari che non si esauriscano nella mera sospensione dell'efficacia esecutiva del provvedimento del Garante impugnato, prevista dall'art. 10, comma 7, d.lgs. 1 settembre 2011, n. 150.

(16) Sulla necessità della tutela cautelare cfr. Corte Cost. 28 giugno 1985, n. 190 e Corte cost. 23 giugno 1994, n. 253, laddove il giudice delle leggi ha esplicitamente sottolineato il « valore » della tutela cautelare in genere in funzione di garanzia della effettività della tutela giurisdizionale, osservando che la « disponibilità » di misure cautelari, il potere, cioè, che le parti hanno di invocare — *ante causam* e nel corso di svolgimento del giudizio di merito — provvedimenti di cautela tipica od atipica, costituisce espressione del principio (chiovendiano) per cui la durata del processo non deve andare a danno dell'attore che ha ragione.

Conclusioni a cui è giunta da tempo anche la Corte di Giustizia, nella sentenza del 19 giugno 1990, causa C-213/89: "...la piena efficacia del diritto comunitario sarebbe del pari ridotta se una norma di diritto nazionale potesse impedire al giudice chiamato a dirimere una controversia disciplinata dal diritto comunitario di concedere provvedimenti provvisori allo scopo di garantire la piena efficacia della pronuncia giurisdizionale sull' esistenza dei diritti invocati in forza del diritto comunitario. Ne consegue che in una situazione del genere il giudice è tenuto a disapplicare la norma di diritto nazionale che sola osti alla concessione di provvedimenti provvisori".

(17) La norma in esame dispone che: "L'autorità giudiziaria o quella amministrativa competente può esigere, anche in via d'urgenza, che il prestatore, nell'esercizio delle attività di cui al comma 1, impedisca o ponga fine alle violazioni commesse".

(18) Esclusione affermata da una risalente e consolidata giurisprudenza della Corte Costituzionale (sentenza 9 luglio 1970, n. 122) e della Corte di Cassazione (Sez. I, Sentenza 27 maggio 1975, n. 2129, Rv. 375881-01).

In particolare, con riferimento al giornale *on-line*, le Sezioni Unite, con sentenza 18 novembre 2016, n. 23469 (Rv. 641537-01) hanno ribadito che i diritti all'onore e alla reputazione sono, nella fase cautelare, recessivi rispetto alla tutela della libertà di stampa, potendo la valutazione di prevalenza espressa dal dettato costituzionale essere sovvertita solo all'esito del giudizio di cognizione. La Suprema Corte ha peraltro chiarito che: "tale conclusione è limitata al caso in cui si invochi una tutela civilistica cautelare preventiva contro il giornale (in tale espressione ricondotto anche il settimanale) telematico con cui sia commessa una lesione all'onore o alla reputazione, cioè che si prospetti come connotato da un contenuto diffamatorio, mentre non è estesa a diversi casi di conflitti con altri diritti assistiti da differenti e specifiche normative, come quella in materia di protezione dei dati personali, ogni questione relativa all'interazione con le quali essendo lasciata esplicitamente impregiudicata".

Con riferimento alla posizione dei *social network*, la giurisprudenza di legittimità ha da tempo escluso che *Facebook* possa essere considerata giornale *on line* (consentendone anche il sequestro preventivo tramite oscuramento) (19).

Una possibile soluzione alla questione in esame è stata fornita dal Tribunale di Milano (20), all'esito di un ricorso *ex* art. 700 c.p.c., promosso da due avvocati al fine di inibire la diffusione di un articolo *online* ritenuto lesivo del proprio onore e della propria reputazione.

Dopo la prima fase, conclusasi con una pronunzia di inammissibilità fondata proprio sul principio affermato dalle Sezioni Unite del 2016, i ricorrenti hanno proposto reclamo, lamentando l'erronea qualificazione, da parte dei giudici della cautela, dell'oggetto della lesione e correlando quest'ultimo non già al diritto alla reputazione e all'onore ma piuttosto al diritto alla riservatezza, estraneo — secondo quanto sancito dagli stessi giudici di legittimità — al contemperamento con la libertà di stampa, in quanto ritenuto sempre prevalente. Il Collegio, pur avendo rigettato nel merito la domanda, ha ritenuto, tuttavia, ammissibile il reclamo e, valorizzando il principio di effettività della tutela ed il principio di proporzionalità nel giudizio di bilanciamento tra diritti di rango costituzionale in ipotesi di loro conflitto, ha affermato che "mentre un provvedimento volto ad impedire la

(19) In particolare, la Cassazione penale ha affermato che la diffusione di un messaggio diffamatorio attraverso l'uso di una bacheca *Facebook* non può dirsi posta in essere "col mezzo della stampa", non essendo i *social network* destinati ad un'attività di informazione professionale diretta al pubblico (Cass. pen., Sez. V, Sentenza 25 gennaio 2021, n. 13979, Rv. 281023-01; Cass. pen., Sez. V, Sentenza 14 novembre 2016, n. 4873; Rv. 269090; Cass. pen., Sez. I, Sentenza 28 aprile 2015, n. 24431, Rv. 264007).

(20) Tribunale di Milano del 25 gennaio 2018 (RG. n. 889/2018).

diffusione e la permanenza della pubblicazione contenente le notizie ritenute diffamatorie avrebbe avuto un effetto corrispondente a quello del sequestro (in violazione, dunque, del divieto posto dall'art. 21 III comma Cost.) un rimedio dall'oggetto più ristretto — idoneo a comporre tale conflitto consentendo allo stesso tempo di garantire il rispetto del principio di effettività e di proporzionalità della tutela giurisdizionale — sarebbe quello della richiesta in via d'urgenza di un aggiornamento della notizia contenente le precisazioni e le contestazioni dei diretti interessati". Tale strumento di tutela — secondo il Collegio — potrebbe essere infatti assimilato all'esercizio del diritto di rettifica disciplinato dall'art. 8 della l. 8 febbraio 1948, n. 47, e, in quanto tale, compatibile con l'attenuata tutela cautelare di cui godono l'onore e la reputazione rispetto alla libertà di stampa. La richiesta di rettifica in via d'urgenza non determina, infatti, alcuna limitazione alla formazione dell'opinione pubblica ma, al contrario, consente di informare il fruitore della notizia dell'esistenza di "voci contrarie", della "verità soggettiva" del soggetto "protagonista" della notizia, svolgendo al tempo stesso un ruolo di promozione del pluralismo *ex* art. 21 Cost. Si realizza, in tal modo, una tutela urgente del diritto leso, attraverso un aggiornamento della notizia (e non una sua eliminazione dalla rete), volta ad informare il lettore, in un tempo molto contenuto (e non a distanza di anni) dell'esistenza di aggiornamenti della vicenda, che ne rivelino il carattere ancora non definitivo.

4.3.2. *La deindicizzazione*

Nella scelta del rimedio necessario a tutelare il diritto all'oblio digitale, e in ossequio al principio di proporzionalità nel bilanciamento tra diritti contrapposti, il giudice può privilegiare l'adozione di un mezzo di tutela che si riveli coerente con il principio di proporzionalità (21) nel bilanciamento tra contrapposti diritti, da realizzare anche attraverso l'individuazione di criteri che consentono di privilegiare, in taluni casi, rimedi meno "radicali" rispetto alla cancellazione (criteri che, in assenza di indicazioni normative, sono stati demandati alla giurisprudenza).

Viene in esame, in primo luogo, l'adozione di un rimedio che precluda l'accesso ad un determinato contenuto attraverso motori di ricerca esterni rispetto all'archivio nel quale il detto contenuto si trovi. Attraverso la deindicizzazione (c.d. *de-listing*) dei contenuti presenti sul *web*, l'informazione non viene eliminata dalla rete, ma può essere attinta raggiungendo

(21) In materia di trattamento dei dati personali, con argomentazioni che ben possono essere applicate nel caso di specie, v., del pari, Corte di Giustizia, sentenza del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, C-92/09 e C-93/09, punto 48.

il sito sorgente o attraverso altri metodi di ricerca (quali, ad esempio, l'utilizzo di parole chiave), in tal modo conferendo al diritto all'oblio digitale il nuovo volto caratterizzato dal "*right not to be found easily*" (22).

In tale caso, come da tempo chiarito dal decisivo arresto della Corte di Giustizia, viene in rilievo il diritto dell'interessato "a che l'informazione in questione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome" (23). Sin dalle Linee-guida sull'attuazione della citata sentenza della Corte di Giustizia, il Gruppo di lavoro "Articolo 29" ha ricordato come la Corte non abbia ipotizzato la necessità di una cancellazione completa delle pagine degli indici del motore di ricerca-pagine che dovrebbero restare accessibili attraverso ogni altra chiave di ricerca. Tale distinzione tra la cancellazione di un particolare contenuto in una ricerca effettuata a partire dal nome dell'interessato e la possibilità di accedere a quel determinato contenuto all'esito di una ricerca effettuata mediante altri criteri è poi espressamente prevista dalla Linee-guida 5/2019 che dettano "criteri per l'esercizio del diritto all'oblio nel caso dei motori di ricerca, ai sensi del RGPD", adottate il 7 luglio 2020 (24).

Attraverso la deindicizzazione, pertanto, "si elimina una particolare modalità di ricerca del dato, che rimane presente in rete e che continua ad essere raggiungibile, ma con una ricerca più complessa e più lunga" (25).

Affinché la domanda dell'interessato, volta ad ottenere la deindicizzazione, possa ritenersi determinata, la stessa, come chiarito dalla Suprema Corte, deve contenere "la precisa individuazione del risultato che l'attore intende rimuovere e, quindi, normalmente, l'indicazione degli indirizzi telematici (o URL) dei contenuti rilevanti" (26).

Con riferimento all'onere della prova, la Corte di Giustizia ha chiarito che spetta alla persona che richiede al motore di ricerca la deindicizzazione per l'inesattezza di un contenuto indicizzato dimostrare tale inesattezza, fornendo gli elementi di prova che, tenuto conto delle circostanze del caso di specie, possono essere ragionevolmente richiesti al fine di dimostrare tale inesattezza manifesta (non potendosi invece pretendere che il richiedente debba produrre, sin dalla fase precontenziosa, una decisione giurisdizionale

---

(22) A. Palmieri-A. Pardolesi, *Dal diritto all'oblio all'occultamento in rete: traversie dell'informazione ai tempi di Google*, in *Foro it. - Nuovi Quaderni*, 1, 2017, 15.

(23) Sentenza del 13 maggio 2014, cit., par. 99.

(24) Consultabili al seguente link: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_it.pdf.

(25) Cass., Sez. I, n. 3952 del 8 febbraio 2022 (Rv. 664161-02).

(26) Cass., Sez. I, n. 20861 del 21 luglio 2021 (Rv. 662180-02).

in suo favore) (27). Nel caso in cui l'inesattezza di tali informazioni incluse nel contenuto indicizzato non appaia in modo manifesto alla luce degli elementi di prova forniti dall'interessato, il gestore del motore di ricerca non è tenuto, in mancanza di una decisione giudiziaria, ad accogliere siffatta richiesta di deindicizzazione. Nella decisione in esame, i giudici di Lussemburgo hanno altresì precisato come gravi sull'interessato un onere di attivazione (sempre che il contenuto originariamente pubblicato fosse lecito), non potendosi pretendere dal motore di ricerca un obbligo di cercare di chiarire i fatti al fine di accertare l'esattezza o meno delle informazioni asseritamente inesatte ivi contenute (28).

Il GDPR stabilisce una presunzione in favore dell'interessato e obbliga il titolare del trattamento a dimostrare l'esistenza di "motivi legittimi cogenti per procedere al trattamento (art. 21, paragrafo 1).

Quando un motore di ricerca (soggetto al quale, per primo si rivolge tale istanza) riceve una richiesta di deindicizzazione fondata sulla situazione particolare dell'interessato, è tenuto ora a cancellare i dati personali ai sensi dell'articolo 17, paragrafo 1, lettera *c*), del GDPR, a meno che non possa dimostrare che sussiste un « motivo legittimo prevalente » per l'inclusione in un elenco dello specifico risultato di ricerca che, in combinato disposto con l'articolo 21, paragrafo 1, configuri « motivi legittimi cogenti (...) che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato ».

Quando, invece, alla richiesta di deindicizzazione si contrappone l'esercizio del diritto alla libertà di espressione e di informazione (eccezione prevista dall'articolo 17, paragrafo 3, lettera *a*), così come indicato dalle Linee guida del 2020, occorrerà prendere in esame la natura dell'informazione, il suo carattere sensibile, l'interesse degli utenti di *internet* ad avere accesso all'informazione in ragione del ruolo che la persona interessata riveste nella vita pubblica.

Con riferimento ai dati relativi a procedimenti giudiziari, la Corte di Giustizia, nella sentenza n. 24 settembre 2019, causa C-136-17 (cd. Sentenza Google 2), ha precisato che il motore di ricerca, nel valutare una richiesta di deindicizzazione, deve considerare: "la natura e la gravità dell'infrazione di cui trattasi, lo svolgimento e l'esito di tale procedura, il tempo trascorso, il ruolo rivestito da tale persona nella vita pubblica e il suo comportamento in passato, l'interesse del pubblico al momento della richiesta, il contenuto e la forma della pubblicazione nonché le ripercussioni della pubblicazione per tale persona".

---

(27) Corte di Giustizia UE, Grande Sezione dell'8 dicembre 2022 - C-460/20.

(28) A medesime conclusioni giunge anche Cass. Sez. 1, n. 6806 del 7 marzo 2023 (Rv. 667165-01).

Dal suo canto, la giurisprudenza della Corte EDU da tempo ha cercato di trovare un equilibrio tra il diritto al rispetto della vita privata di cui all'art. 8 CEDU e il diritto alla libertà d'espressione di cui al successivo art. 10, individuando, a tal fine, precisi criteri per la ponderazione dei diritti concorrenti, e in particolare: il contributo della notizia a un dibattito di interesse generale, il grado di notorietà del soggetto, l'oggetto della notizia; il comportamento precedente dell'interessato, le modalità con cui si ottiene l'informazione, la sua veridicità e il contenuto, la forma e le conseguenze della pubblicazione (29).

L'esame delle decisioni di merito e di legittimità della giurisprudenza nazionale rivela come, ai fini dell'accoglimento di una domanda di deindicizzazione che il motore di ricerca ha ritenuto di non accogliere, nel bilanciamento tra contrapposti diritti (tra la tutela della vita privata e della dignità dell'interessato e l'interesse pubblico alla conoscenza del contenuto informativo), assumano rilievo i seguenti criteri: il ruolo pubblico della persona interessata (nelle linee guida elaborate nel 2014 si sottolinea come solitamente possa ritenersi che abbiano un ruolo nella vita pubblica "politici, alti funzionari pubblici, uomini di affari e professionisti, iscritti agli albi") e il tempo trascorso (30).

In particolare, come affermato dalla Suprema Corte nell'ordinanza Sez. I, 20 marzo 2018, n. 6919 (Rv. 647763-01) il diritto all'oblio può essere recessivo, rispetto al diritto di cronaca (con considerazioni che rilevano anche nel bilanciamento tra diritto alla deindicizzazione e libertà di espressione degli utenti della rete), solo in presenza di determinate condizioni, fra le quali il contributo arrecato dalla diffusione della notizia ad un dibattito di interesse pubblico, l'interesse effettivo ed attuale alla diffusione, la grande notorietà del soggetto rappresentato, le modalità in concreto impiegate e la preventiva informazione dell'interessato finalizzata a consentirgli il diritto di replica prima della divulgazione.

La giurisprudenza, nazionale e sovranazionale, si è dovuta misurare altresì con domande volte ad ottenere la c.d. deindicizzazione globale, vale a dire con richieste volte ad ottenere il c.d. *delisting* dai risultati della ricerca

---

(29) Corte EDU19 ottobre 2017, *Fuchsmann c. Germania*, 32; Corte EDU 10 novembre 2015, *Couderc et Hachette Filipacchi c. Francia*, 93: sulla necessità del giusto equilibrio tra il diritto al rispetto della vita privata, da un lato, e la libertà di espressione e la libertà di informazione del pubblico, dall'altro, cfr. pure Corte EDU 28 giugno 2018, M.L. e W.W. c. Germania, 89.

(30) Con riferimento al tempo trascorso, il Garante ha più volte ribadito che devono considerarsi recenti e di pubblico interesse notizie risalenti a "meno di dieci anni fa" (riportando a titolo di esempio, i provvedimenti 27 gennaio 2021, n. 32; 29 ottobre 2020, n. 210; 9 novembre 2017, n. 472).

non solo all'interno dei Paesi membri dell'Unione Europea, ma anche al di fuori dei confini dell'Unione. Come osservato dalla Corte di Giustizia, infatti, in un mondo globalizzato "l'accesso da parte degli utenti di *internet*, in particolare quelli localizzati al di fuori dell'Unione, all'indicizzazione di un *link*, che rinvia ad informazioni concernenti una persona il cui centro di interessi si trova nell'Unione, può quindi produrre effetti immediati e sostanziali sulla persona in questione anche all'interno dell'Unione". Tanto premesso, però, i giudici di *Kirchberg*, muovendo dal presupposto in forza del quale l'equilibrio tra il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali, da un lato, e la libertà di informazione degli utenti di *internet* dall'altro, può variare notevolmente nel mondo, hanno affermato che il legislatore dell'Unione non ha effettuato tale bilanciamento per quanto riguarda la portata di una deindicizzazione al di fuori dell'Unione (né ha previsto strumenti a tal fine) ed hanno pertanto concluso che non sussiste, allo stato, per il gestore di un motore di ricerca che accoglie una richiesta di deindicizzazione presentata dall'interessato, eventualmente, a seguito di un'ingiunzione di un'autorità di controllo o di un'autorità giudiziaria di uno Stato membro, un obbligo, derivante dal diritto dell'Unione, di effettuare tale deindicizzazione su tutte le versioni del suo motore (31).

A diverse conclusioni è giunta la Corte di Cassazione (32) che, muovendo proprio da un passaggio della pronuncia della Corte di Giustizia appena citata (il par. 72, laddove si legge che: "il diritto dell'Unione, pur se non impone, allo stato attuale, che la deindicizzazione accolta verta su tutte le versioni del motore di ricerca in questione, neppure lo vieta"), ha affermato che "il diritto alla protezione dei proprie dati personali e il suo fondamento costituzionale non tollerano limitazioni territoriali all'esplicazione della sfera di protezione, tanto più che nella specie tale diritto si sovrappone e si accompagna ai diritti all'identità, alla riservatezza e alla contestualizzazione delle informazioni", così ritenendo configurabile una condanna alla deindicizzazione di contenuti pubblicati *on line* su versioni extra UE del motore di ricerca (33).

---

(31) CGUE, Grande Sezione, C-507/17, *Google LLC* contro *Commission nationale de l'informatique et des libertés (CNIL).*

(32) Anche il Garante per la *privacy* aveva ritenuto ammissibile un'attività di rimozione degli URL anche alle versioni extraeuropee del motore di ricerca (provvedimento n. 557 del 21 dicembre 2017).

(33) Cass., Sez. I, 24 novembre 2022, n. 34658 (Rv. 666447-02), chiamata a pronunciarsi sul ricorso promosso da un soggetto con interessi professionali extraeuropei, il quale aveva richiesto l'effettiva rimozione degli URL con materiali a lui pertinenti anche nelle versioni non europee del motore di ricerca, dato che la sua attività professionale aveva Dubai come principale centro di interessi.

Tale questione (che non può essere esaminata *funditus* nel presente contributo) chiama l'interprete a confrontarsi con l'importanza di individuare la situazione giuridica soggettiva per la quale si invoca tutela e con i problemi relativi all'attuazione della tutela riconosciuta. Con riferimento al primo aspetto, infatti, si osserva come decisiva sia la qualificazione del diritto asseritamente leso e la corretta individuazione della disciplina normativa applicabile. La stessa Corte di Giustizia, infatti, chiamata a pronunciarsi in una controversia proposta dalla deputata *Eva Glawischnig-Piesczek* contro *Facebook Ireland Limited* in merito alla pubblicazione, sulla pagina di un'utente ospitata sul sito del *social network* Facebook, di un messaggio contenente dichiarazioni lesive dell'onore della ricorrente, ha utilizzato la disciplina sul commercio elettronico (in particolare, l'art. 18, par. 1, Dir. 2000/31/CE), per osservare che tale disciplina non prevede alcuna limitazione, segnatamente territoriale, alla portata dei provvedimenti che gli Stati membri hanno diritto di adottare conformemente alla direttiva in parola, che sanziona le violazioni avvenute in ogni luogo e in ogni lingua, così riconoscendo che il giudice nazionale può ordinare a un prestatore di servizi di *hosting* di rimuovere le informazioni oggetto dell'ingiunzione (nel quadro del diritto internazionale pertinente) (34). Nello stesso modo appare orientata la giurisprudenza di merito che, già da tempo, applicava alla diffamazione via *internet* la disciplina di cui alla Direttiva 31/2000 e al d.lgs. 9 aprile 2003, n. 70 (35).

In merito al secondo aspetto, ci si limita ad osservare come, a fronte di un ordine rivolto alla deindicizzazione anche al di fuori dei confini dell'Unione Europea, si pone un problema di attuazione del diritto così riconosciuto e di strumenti volti a verificare come e se il motore di ricerca abbia dato attuazione all'ordine del Tribunale.

4.3.3. *La cancellazione*

Rimedio volto, invece, all'eliminazione dalla rete del contenuto informativo è rappresentato dalla cancellazione, previsto dal richiamato art. 17 del GDPR.

La giurisprudenza ha esaminato i casi nei quali al diritto all'oblio digitale si contrappone l'interesse pubblico alla conoscenza di una determinata notizia, soffermandosi altresì su fattispecie in cui il diritto in esame deve essere bilanciato con l'interesse generale alla conservazione di notizie con

(34) Corte di Giustizia UE 3 ottobre 2019, *Eva Glawischnig Piesczek* contro *Facebook Ireland Limited*.

(35) Trib. Roma 15 febbraio 2019, n. 3512; Trib. Napoli Nord ord. 4 novembre 2016.

funzione di documentazione storica e culturale. In tale ultimo caso, infatti, si delinea un conflitto tra diritti contrapposti e si pone il problema del necessario bilanciamento fra il diritto all'informazione, declinato nella forma della conservazione dell'archivio storico delle informazioni pubblicate, da un lato, e il diritto degli interessati a veder calare il velo dell'oblio sulle vicende giudiziarie che li avevano coinvolti, dall'altro.

Con riferimento agli archivi giornalistici, in una risalente pronuncia, il Tribunale di Milano (36), decidendo sulla domanda di cancellazione dall'archivio telematico di un giornale di un articolo che recava informazioni (in parte inesatte) relative ad un'indagine per usura, condotta nel 1985, a carico di un privato cittadino (poi risultato estraneo alla predetta indagine), ha ritenuto prevalente il diritto all'oblio digitale dell'attore, condannando la testata giornalistica alla cancellazione del predetto articolo dall'archivio telematico. Il rimedio in esame è stato riconosciuto anche in ragione della prova dell'infruttuoso esito relativo alla c.d. deindicizzazione di tale articolo da parte dei motori di ricerca (sulla quale ci si soffermerà in seguito). Con riferimento alle finalità di conservazione, il Tribunale ha affermato che le finalità di archivio di una notizia così risalente avrebbero potuto essere assicurate attraverso la conservazione di una copia cartacea del detto articolo.

La Suprema Corte, interrogandosi sull'esistenza di una "sorta di primato" degli archivi storici *on line*, garantito dalla libertà di stampa e di informazione, ha affermato che, in forza dell'art. 21 della Costituzione, può riconoscersi un "generale diritto alla conoscenza di tutto quanto in origine lecitamente veicolato al pubblico, con conseguente liceità del fine del trattamento dei dati personali contenuti in un articolo", precisando tuttavia che tale diritto incontra un limite, in applicazione dell'art. 11 del d.lgs. n. 196 del 2003, nei casi in cui la permanenza del dato negli archivi informatici, per la sua generale accessibilità, "comporti un tale *vulnus* alla riservatezza dell'interessato (con conseguente ed immediata ripercussione sulla propria reputazione) da minarne in misura apprezzabile l'esplicazione dei diritti fondamentali della persona in ambito relazionale" (37).

Cass., Sez. I, 19 maggio 2020, n. 9147 (Rv. 657638-01) ha poi precisato che la tutela del diritto a non rimanere esposti senza limiti di tempo ad una rappresentazione non più attuale della propria persona deve essere posta in bilanciamento con l'interesse pubblico alla conoscenza del fatto, espressione del diritto di manifestazione del pensiero e quindi di cronaca e di conservazione della notizia per finalità storico-sociale e documentaristica (affer-

(36) Trib. Milano, 26 aprile 2013 (RG n. 5820/2013).

(37) Cass., Sez. I, 27 marzo 2020, n. 7559 (Rv. 657424-01).

mando, infine, come tale diritto ben potrebbe trovare adeguata tutela attraverso un rimedio quale la deindicizzazione).

4.3.3.1. *La cancellazione delle c.d. copie* cache

Diversa dalla deindicizzazione e dall'eliminazione dalla rete del contenuto informativo (la cancellazione trattata al punto che precede) è l'ordine di cancellazione delle c.d. copie *cache*. Come osservato da attenta dottrina, i dati presenti nella memoria *cache* dei motori di ricerca, "sono i contenuti delle pagine web esplorate dagli agenti software (denominati *web crawler*, *bot*, o *spider*), che possono essere comunque presentate all'utente a seguito di una sua interrogazione, anche se esse non sono aggiornate o non più disponibili perché rimosse dal *server* che le aveva originariamente caricate sulla rete. In questo modo, grazie alla memoria *cache*, un utente può pur sempre visualizzare una pagina *web* che, per una qualche ragione, non è più attiva. Così facendo, il motore di ricerca conserva sempre una copia dei siti *web* che esplora per mezzo dei propri agenti *software*, ma questa copia non è immanente, ma risiede nella memoria *cache*, fino al successivo passaggio degli agenti software che fotograferanno e registreranno il contenuto informativo più attuale, che sostituirà quello precedente" (38).

La questione è stata specificamente esaminata dalla giurisprudenza di merito e di legittimità. Il Tribunale di Milano (39), chiamato a decidere sul ricorso proposto da un motore di ricerca avverso il provvedimento del Garante per la protezione dei dati personali che gli aveva ordinato la rimozione (anche delle copie *cache*) dai risultati delle ricerche su *internet* effettuate con l'utilizzazione dei servizi di ricerca del predetto motore di ricerca di diversi URL, specificamente individuati, che collegavano il nome dell'interessato a una vicenda giudiziaria che si asseriva non più interessare il diritto di cronaca, ha confermato il provvedimento dell'Autorità, osservando come l'art. 17 del GDPR abbia previsto il diritto ad una cancellazione estesa dei propri dati personali, comprendente anche "qualsiasi *link*, copia o riproduzione" riferibile a tali dati.

La decisione in esame è stata cassata dalla Suprema Corte che, con ordinanza Sez. I, dell'8 febbraio 2022, n. 3952 (Rv. 664161-02), ha affermato che la copia *cache* dei siti *internet* indicizzati consente al motore di ricerca di fornire una risposta più veloce ed efficiente all'interrogazione posta dall'utente attraverso una o più parole chiave, e che la cancellazione di esse

(38) P. Sammarco, *Diritto all'oblio e cancellazione delle copie cache del motore di ricerca*, in *Dir. Inf.*, 2, 2022, 383 e ss.

(39) Trib. Milano, sentenza del 15 gennaio 2016.

preclude al motore di ricerca, nell'immediato, di avvalersi di tali copie per indicizzare i contenuti attraverso parole chiave anche diverse da quella corrispondente al nome dell'interessato. In forza di tali premesse, la Corte ha concluso che: "la cancellazione delle copie *cache* relative ad una informazione accessibile attraverso il motore di ricerca, in quanto incidente sulla capacità, da parte del detto motore di ricerca, di fornire una risposta all'interrogazione posta dall'utente attraverso una o più parole chiave, non consegue alla constatazione della sussistenza delle condizioni per la deindicizzazione del dato a partire dal nome della persona, ma esige una ponderazione del diritto all'oblio dell'interessato col diritto avente ad oggetto la diffusione e l'acquisizione dell'informazione, relativa al fatto nel suo complesso, attraverso parole chiave anche diverse dal nome della persona".

Tale conclusione, ad avviso di parte della dottrina (40), si espone ai seguenti rilievi critici: l'ordine di cancellazione delle copie *cache* disposto dall'autorità giudiziaria (o amministrativa) non incide sul contenuto informativo originario presente su *internet,* che resta visibile ai suoi utenti che dovranno solamente raggiungerlo attraverso una ricerca mirata e diretta; la direttiva 2000/31/CE lascia impregiudicata la possibilità di emettere nei confronti dei prestatori intermediari azioni inibitorie volte all'eliminazione dell'informazione ritenuta illecita da un'autorità (amministrativa o giurisdizionale) o alla disabilitazione dell'accesso alla stessa; il motore di ricerca è solo uno strumento per la fruizione di informazioni che svolge un "ruolo di facilitatore per il reperimento di una informazione", il che "non significa essere il destinatario della tutela costituzionale della libertà di espressione e di manifestazione del pensiero" (41).

Nella difficoltà di indicare delle prime conclusioni sul tema della tutela del diritto all'oblio digitale, ci si limiterà a ricordare le parole di un Maestro del diritto alla dignità della persona il quale, nel commentare il nuovo codice sulla *privacy*, aveva sottolineato l'importanza di arginare la tendenza ad utilizzare qualsiasi innovazione tecnologica per trattare dati personali. In particolare, ha osservato che: "la protezione dei dati personali appare sempre più stretta tra esigenze di sicurezza ed interessi dell'impresa, e dunque, a rischio continuo d'essere compressa per il puro fatto dell'offerta crescente di tecnologie che rendono sempre più agevoli forme generalizzate di controllo

(40) P. Sammarco, *op. cit.*

(41) P. Sammarco, *op. cit*. Da tempo, acutamente, V. Zeno-Zencovich, nella sua *La libertà di espressione*, Bologna, 2004, 135 aveva osservato come si fosse venuta a creare una sovrapposizione fattuale tra manifestazione del pensiero ed esercizio dell'attività di impresa delle comunicazioni.

e di raccolta d'informazioni personali" (42). L'utilizzo di tecnologie che moltiplicano le ipotesi di trattamento dei dati, la inevitabile permanenza degli stessi nella rete, il coinvolgimento, nel primo bilanciamento tra diritti contrapposti, di soggetti, quali i motori di ricerca, animati da interessi economici, rende ancora più evidente come spetti al giudice la tutela effettiva di quel "corpo elettronico" che si rivela un presidio della stessa libertà personale.

(42) S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo codice sulla privacy*, in *Europa e diritto privato*, 2004, 1 e ss.

V.

IDENTITÀ DIGITALE DELL'IMPRESA: RICOSTRUZIONE CONCETTUALE, FORME E TECNICHE DI PROTEZIONE

di *Luca Boggio*

Sommario: 5.1. Identità, organizzazione d'impresa ed interessi protetti: dalla tutela del valore oggettivo dell'impresa a quella della personalità dell'imprenditore. — 5.2. Il problema dell'identità personale tra nozione e confini concettuali. — 5.3. Identità personale e soggetti diversi dalle persone fisiche: il caso particolare delle imprese. — 5.4. *Segue*: identità dell'imprenditore, identità delle imprese, identità delle organizzazioni delle imprese. — 5.5. L'identità tra diritto privato e diritto dell'impresa: approccio alla disciplina. — 5.6. L'identità dell'organizzazione d'impresa a fronte della trasformazione digitale: l'individuazione nel mercato virtuale. — 5.7. *Segue*: il contributo di *domain names*, *user names*, *nicknames* e *alias* alla tutela (o alla violazione) dell'identità digitale dell'organizzazione d'impresa. — 5.8. L'identità (digitale) dell'organizzazione d'impresa può circolare? — 5.9. Qualche considerazione sull'identità digitale degli *influencers* (e dei *content creators*): a cavallo del confine tra diritto privato e diritto dell'impresa. — 5.10. *Segue*: il caso dei *virtual influencers*. — 5.11. Il problema dell'identità digitale dell'utilizzatore commerciale dei *marketplaces*. — 5.12. L'identità digitale dell'Intelligenza Artificiale che sia parte del ciclo produttivo. — 5.13. Le (molto) prossime frontiere: l'identità digitale dell'organizzazione d'impresa nel *metaverso*.

5.1. Identità, organizzazione d'impresa ed interessi protetti: dalla tutela del valore oggettivo dell'impresa a quella della personalità dell'imprenditore

L'identità è ciò che individua una persona; la persona che svolge attività d'impresa si individua e si definisce tradizionalmente attraverso l'uso della ditta o nome commerciale. L'imprenditore crea e sviluppa un'organizzazione di risorse produttive e attraverso l'esercizio dell'impresa — e, quindi, il funzionamento dell'organizzazione — si rivolge ed opera nel mercato. L'impresa più cresce, più tende ad oggettivizzarsi ed a emergere come qualcosa di altro rispetto all'imprenditore che l'ha creata e la sta sviluppando (1). Que-

(1) Che la componente organizzativa dell'impresa tenda ad assegnarle, "nel rapporto con i terzi, un carattere, in un certo modo, impersonale" è già stato riconosciuto da M. Proto,

st'oggettivizzazione, che via via assume rilievo, tende a favorire l'individuabilità di un valore anche "distaccabile" dall'imprenditore-creatore; perciò, sul piano del diritto, ha richiesto l'elaborazione di strumenti giuridici di protezione di quel valore attraverso la promozione della sua circolazione come mezzo per la più efficiente allocazione in capo a chi meglio possa e voglia mettere a frutto quel valore. Su questa linea il Codice Civile, che disciplina l'azienda né nella sua dimensione statica né nel suo sfruttamento dominicale, si cura di esclusivamente di regolare gli atti di disposizione di cui sia oggetto (2) affinché sia più agevole quella riallocazione presso chi disponibile a riconoscere al dante causa — tendenzialmente il creatore dell'organizzazione — un plusvalore che travalica la somma dei valori delle singole componenti isolatamente considerate. Quel plusvalore è l'avviamento, generalmente definito "qualità" dell'azienda. Come una qualità di una persona, anche l'avviamento contribuisce a definire non solo l'azienda come insieme di "beni", ma anche l'impresa come fenomeno dinamico e potenzialmente idoneo a produrre ulteriore valore concreto. Tuttavia, quando ci riferiamo all'avviamento, siamo di fronte ad una qualità di beni funzionalmente organizzati; l'individualità — e, quindi, le qualità — dell'organizzatore sono fuori gioco. L'abilità di chi ha prodotto l'organizzazione non è componente dell'avviamento, restando "esterno" ad esso; pure la reputazione dell'impresa, come organizzazione di cui è elemento anche il titolare (individuale o collettivo non importa), resta "esterna" a quell'avviamento.

Il diritto commerciale, in quanto settore dell'ordinamento focalizzato sullo sviluppo e sul governo delle attività economiche nella prospettiva della crescita sostenibile, da lungo tempo protegge però i creatori di avviamento e lo fa innanzi tutto attraverso la tutela delle loro creazioni (in senso ampio). Per questo: sono stati riconosciuti nei secoli diritti di uso esclusivo per l'insegna che contraddistingue il luogo fisico di esercizio dell'impresa, per il marchio che contraddistingue il prodotto o il servizio offerto al mercato; con la registrazione si può conseguire da tempo la protezione delle invenzioni di prodotto o di procedimento produttivo, del *design* industriale; ma vige anche il divieto di far uso del segreto industriale altrui non legittimamente acquisito e, più in generale, di far concorrenza sleale, divieto questo al quale si riconducono la proibizione di sfruttare slogan, format operativo, di stornare gruppi significativi di collaboratori (.... e molto altro). Tutte esclusive e forme di limitazioni dell'attività dei terzi funzionali a tutelare gli investimenti che

---

Il diritto e l'immagine. Tutela giuridica del riserbo e dell'icona personale, Milano, 2012, 134 s., rifacendosi a C. Angelici, *Diritto commerciale*, I, Roma-Bari, 2002, 34 e 64.

(2) Sul punto, limitando le citazioni, M. Cian, *Dell'azienda*, in *Commentario Schlesinger*, Milano, 2018, 16.

stanno a monte dei valori facenti parte del patrimonio organizzato per lo svolgimento dell'attività d'impresa. E gli investimenti, è noto, sono spese dirette a generare profitto; quindi, non per godere in sé dell'uso di un fattore della produzione, ma per incamerare il reddito netto prodotto dall'attività svolta per mezzo dell'insieme dei fattori di produzioni organizzati dall'imprenditore (3).

La giurisprudenza è andata anche oltre e tutela anche interessi più "personali" dell'imprenditore, come la reputazione nel mercato (4) che oggi, in tempi di responsabilità sociale, è componente di valore via via crescente in termini di importanza relativa e di quantificazione oggettiva del valore d'impresa (5). Una buona reputazione — soprattutto in epoca di intensa *tertiary communication* prodotta dai *social networks* (6) — è molto utile per operare efficacemente nel mercato e, conseguentemente, contribuisce alla produzione di migliori risultati economici, dal momento che — per un verso — orienta positivamente la scelta dei clienti (7) e — per altro verso —

---

(3) La sintesi esposta nel testo affonda le radici nella concezione del diritto dell'impresa come normazione di una serie di fatti e atti funzionalmente collegati ai fini della produzione di un guadagno e da considerarsi, perciò, da un punto di vista unitario e in una prospettiva finalistica. Come scriveva Ascarelli a proposito della disciplina della concorrenza, dei segni distintivi e delle creazioni dell'ingegno (v. T. Ascarelli, *Teoria della concorrenza e dei beni immateriali*, Milano, 1960, 899 s.), v'è "costanza di interesse tutelato, se pur poi diversamente tutelato nei vari istituti", che, per "comunanza di problemi", giustifica "la ricorrenza di uno stesso quadro generale" diretto alla "tutela della probabilità di guadagno ritraibili da un'attività economica"; sul piano dell'attuazione delle norme ciò determina "la rilevanza di una attività esercitata o esercitabile quale criterio di riferimento per l'applicabilità della tutela" (ancora, T. Ascarelli, *Teoria della concorrenza e dei beni immateriali*, cit., 890).

(4) Tra le più recenti v. Cass., ord., 18 novembre 2022, n. 34026; Cass., 22 ottobre 2013, n. 23933, in *Foro it.*, 2013, I, 3419 ss. con nota di M. Manenti, *Il punto sulle vertenze risarcitorie conseguenti al disastro di Ustica*; App. Catania, 28 giugno 2014, in *Onelegale*. La giurisprudenza tende a richiedere allegazione e prova del pregiudizio alla reputazione commerciale, ma non nelle ipotesi di lesione alla reputazione personale.

(5) V., *ex multis*, A. Caruana, *Corporate reputation: concept and measurement*, in *Journ. Product & Brand Man*., 1997, 109 ss.; B. Iannone, *La* Corporate Reputation *quale risorsa (intangibile) strategica. Dinamiche di sviluppo e strumenti di misurazione*, Roma, 2009, *passim*.; M.T. Cuomo-G. Metallo-D. Tortora, Corporate reputation management. *Analisi e modelli di misurazione*, Torino, 2014, 4 ss.

(6) L'ampliamento della base di soggetti che valutano positivamente un'impresa è frutto delle cc.dd. *reputational relationships* le quali contribuiscono a diffondere un'opinione sull'organizzazione presso pubblici con cui non ha contatti diretti. I soggetti appartenenti a queste ultime platee finiscono per formulare una valutazione di apprezzamento sulla sola base di quanto hanno sentito dire da altri (v. J. Grunig-L. Grunig, *A New Definition & Measure of Reputation*, in *Research. A Supplement of PR Report*, 16 maggio 2002).

(7) H.T. Keh-Y. Xie, *Corporate reputation and customer behavioral intentions. The roles of trust, identification and commitment*, in *Ind. Marketing Man.*, 2009, 38; H.M. Shamma-S.S.

contribuisce all'attrazione di risorse umane di qualità superiore, di maggiori investimenti e può altresì accrescere l'appetibilità nel mercato di capitali, migliorando la sua organizzazione interna e la sua struttura finanziaria (8). In sostanza, una migliore reputazione rispetto alle imprese concorrenti determina vantaggi competitivi, assicurando una più solida posizione di mercato (9) e maggiore resilienza in caso di crisi (10). Tuttavia, il livello reputazionale dell'impresa non dipende soltanto dalla qualità organizzativa, ma anche dalla qualità delle scelte operate da chi la organizza (11). L'orientamento alla sostenibilità, per esempio, è fattore di accrescimento della reputazione (12), ma è anche componente delle scelte imprenditoriali trasfuse in decisioni gestorie rispetto a cui le caratteristiche oggettive dell'azienda (13) sono la conseguenza ed il riflesso, non un fattore di determinazione. In questo senso, emerge un elemento soggettivo dipendente dal modo in cui si

---

HASSAN, *Customer and non-customer perspectives for examining corporate reputation*, in *Journ. Product & Brand Man.*, 2009, 5; R.P. NELLI, Corporate reputation*: valore per l'impresa, garanzie per il consumatore*, in *Cons. dir. merc.*, 2012, 96 ss.

(8) V. J. SABATE-E. PUENTE, *Empirical Analysis of the Relationship Between Corporate Reputation and Financial Performance. A Survey of the Literature*, in *Corp. Reputation Rev.*, 2003, 161 ss.; G. GABBI-A. PATARNELLO, *Il valore della reputazione bancaria tra "risk management" e scelte strategiche*, in *Banca impr. soc.*, 2010, 340; A. SIANO (A. VOLLERO-M. SIGLIOCCOLO), Corporate communication management. *Accrescere la reputazione per attrarre risorse*, Torino, 2015, 4; J. LEE-HB. KWON, *The synergistic effect of environmental sustainability and corporate reputation on market value added (MVA) in manufacturing firms*, in *Intl' Journ. Production Res.*, 2019, 7123 ss. Analogamente, rispetto al mercato digitale, G. D'ALFONSO, *Recensioni 'diffamatorie' in rete e lesione della reputazione digitale d'impresa. Illecito aquiliano e valutazione comparativa degli interessi dell'impresa e degli internauti, alla luce degli indirizzi giurisprudenziali sui limiti all'esercizio del diritto di critica*, in *Dir. merc. tecn.*, 15 ottobre 2019, 2; HB. KWON-J. LEE, *Exploring the differential impact of environmental sustainability, operational efficiency, and corporate reputation on market valuation in high-tech-oriented firms*, in *Intl' Journ. Production Econ.*, 2019, Maggio, 1 ss.

(9) Per tutti, si rinvia a J.M.T. BALMER-E.R. GRAY, *Corporate identity and corporate communications: creating a competitive advantage*, in *Ind. Comm. Training*, 2000, 256 ss.

(10) Sul punto N. DAWAR-M.M. PILLUTLA, *Impact of product-harm crises on brand equity. The moderating role of consumer expectations*, in *Journ. Mark. Research*, 2000, 215; D.H. DEAN, *Consumer reaction to negative publicity: Effects of corporate reputation, response, and responsibility for a crisis event*, in *Journ. Bus. Comm.*, 2004, 192; Y. SOHN-R.W. LARISCY, *A "Buffer" or "Boomerang"? The Role of Corporate Reputation in Bad Times*, in *Comm. Research*, 2015, 237 ss.

(11) Che la reputazione sia il prodotto dei comportamenti passati e delle aspettative sulle condotte future è ben messo in luce in G. DAVIES-R. CHUN-R. DA SILVA-S. ROPER, *Corporate Reputation and Competitiveness*, London, 2003, 58 ss.

(12) V. M. BONUZZI-G. COVASSI, *La sostenibilità, cardine della reputazione aziendale. Un caso di studio*, in *Tendenze nuove*, 2013, 383 ss.

(13) In ordine alla caratterizzazione oggettiva dell'azienda, per tutti, G.E. COLOMBO, *L'azienda*, in *Trattato Galgano*, III, Padova, 1979, 2.

comporta la persona dell'imprenditore che, per l'apprezzamento via via riscosso nel mercato, accresce e consolida un livello più o meno alto di reputazione della sua organizzazione imprenditoriale (14); questa reputazione, proprio attraverso quel consolidamento, tende ad oggettivizzarsi e a diventare valore riconoscibile e valutabile (15).

Tutto ciò rende evidente come gli elementi dell'impresa tendono a distaccarsi dell'imprenditore, ad assumere valore oggettivo in sé, almeno potenzialmente idoneo a circolare nel mercato in funzione, se il mercato reagisce efficientemente, di allocarsi presso chi meglio dovrebbe saperla gestire e far produrre il massimo profitto. Di qui si può già intuire come pure l'identità del titolare dell'impresa possa essere qualcosa con connotati parzialmente differenti — probabilmente più complessi — rispetto all'identità del non-imprenditore e suggerisce di verificare quali risposte possa avere una serie di interrogativi che ruotano attorno all'identità digitale. Il primo e più complesso è di certo volto a comprendere se quel grado di oggettivizzazione a cui più sopra s'è fatto cenno permei anche l'identità digitale dell'imprenditore tanto da distaccarsi da quest'ultimo risultando idonea a circolare nel mercato (16). Altri, forse più spiccioli sul piano teorico, riguardano l'attività degli *influencers*, dei *marketplaces*, dell'intelligenza artificiale, come pure la

---

(14) Riguardo alla connessione tra qualità del rapporto con gli *stakeholders* e la crescita della *corporate reputation* in funzione di migliorare la sostenibilità del *business* si rinvia a R. Rensburg-E. de Beer-E. Coetzee, *Linking Stakeholder Relationships and Corporate Reputation. A Public Relations Framework for Corporate Sustainability*, in *Public Relations Research*, a cura di A. Zerfass, B. van Ruler e K. Sriramesh, Wiesbaden, 2008, 385 ss.

(15) V. E. Black-T. Carnes-V. Richardson, *The Market Valuation of Corporate Reputation*, in *Corp. Reputation Rev.*, 2000, 31 ss.; K. Taken Smith-M. Smith-K. Wang, *Does brand management of corporate reputation translate into higher market value?*, in *Journ. Strat. Marketing*, 2010, 201 ss.; S. Raithel-M. Schwaiger, *The effects of corporate reputation perceptions of the general public on shareholder value*, in *Strat. Man. Journ.*, 2015, 945 ss.; I. Corradini-E. Nardelli, *La reputazione aziendale. Aspetti sociali, di misurazione e di gestione*, Milano, 2015, 47 ss.; R. Lamboglia, *Il controllo della reputazione finanziaria nel sottosistema delle relazioni azienda-banche*, Torino, 2017, 121 ss. In particolare, riguardo alla reputazione nel contesto digitale, si segnalano i recentissimi R.A. Abdelkhalik, *The effect of investment in the brand value chain on profitability and market value of the firm: lesson of success taken from Amazon*, in *Future Bus. Journ.*, 2023, 29 aprile, 2 ss. e *La reputazione è asset aziendale, vale 10 mld di fatturato annuo*, in *IlSole-24Ore*, 17 maggio 2023.

(16) Se così fosse, oggetto di circolazione tenderebbe ad essere l'impresa, più che il mero complesso di beni organizzati per il suo esercizio (ossia dell'azienda). Quindi, anche quelle caratteristiche riconducibili alle scelte imprenditoriali e operative derivanti da linee guida che l'imprenditore si sia dato ed alle quali i componenti dell'organizzazione siano tenuti ad uniformarsi nell'esercizio dell'attività (riguardo al valore reputazionale della partecipazione delle banche al consorzio "Patti Chiari" e alla possibilità di utilizzare tale adesione come tratto distintivo della banca v. A. Scotti, *I codici di condotta fra mercato, impresa e contratto*, Milano, 2019, 276 s.). Per concretizzare, codici di comportamento e atti di programmazione a

conduzione di attività imprenditoriali nel metaverso. Ma il punto di partenza sta nell'indagine sul significato dell'espressione "identità digitale delle imprese".

5.2. Il problema dell'identità personale tra nozione e confini concettuali

L'identità personale è un concetto complesso che esprime molteplici significati. In linea di principio, si riferisce alla percezione che ogni individuo ha di sé stesso, cioè della propria coscienza di esistere come persona in relazione con altri individui, con i quali forma un gruppo sociale; dunque, sta ad indicare una relazione tra il singolo e la società, sia nella prospettiva del singolo che, in una misura più o meno intensa, si identifica nel riconoscimento sociale dei suoi caratteri distintivi, ossia nel riconoscimento dell'individualità di costui da parte degli altri componenti della società. L'identità personale è frutto, in sostanza, di una prospettiva di tendenziale convergenza biunivoca tra la visione del singolo e quella degli altri componenti della società, che ha una componente psicologica ad un tempo individuale e sociale. Pertanto, esprime una soggettività che rileva in quanto oggettivizzata nella società attraverso il riconoscimento dell'individuo nella sua identificazione e nella sua continuità. Quindi, essa si connota per il carattere duraturo, sebbene si tratti di una persistenza che non significa immutabilità (17), piuttosto prosecuzione del soggetto riconosciuto.

Il diritto dà certamente rilievo all'identità come strumento di sussunzione dell'identificazione della persona rispetto agli altri componenti del

---

medio-lungo periodo potrebbero costituire mezzo per assicurare all'organizzazione imprenditoriale connotati determinati suscettibili di dare ad essa o consolidare in capo alla medesima una specifica immagine, dignità, reputazione. Si torna alla domanda posta nel testo: l'organizzazione nella misura in cui si distacchi da chi ne è titolare può presentare un grado di autonomia tale da renderla atta ad essere trasferita a terzi senza mutare quei connotati?

(17) Così V. Zeno-Zencovich, voce *Identità personale*, in *Dig. Comm. Sez civ.*, IX, Torino, 1993, 300; A. Putignano, *Abuso dell'immagine della persona nota: "e io pago..."*, in *Danno Resp.*, 2013, 886; G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 2017, 724; E. Tosi, *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, 2023, 53; D.G. Ruggiero, *Persona e identità digitale*, Napoli, 2023, 79 ss. La natura evolutiva dell'identità è presupposto anche delle indagini degli psicologi sociali; v., ad esempio, M. Mura-M. Martini, *Identità sociale e comunicazione in rete*, in *DiPAV Quaderni*, Milano, 2009, n. 25, 35, secondo i quali "l'identità è (...) l'esito di un processo, mai concluso, di costruzione di un'immagine di sé che è particolarmente significativa sia per l'individuo, in quanto ne sostiene il benessere — fondamentalmente, l'autostima e il senso di controllo —, che per la società, in quanto guida il comportamento individuale".

corpo sociale e nel tempo, ma non ne sono del tutto pacifiche forma e misura. Negli anni si è discusso, anche nel contesto del dibattito sulla ricostruzione della categoria dei diritti della personalità, se il diritto all'identità personale presenti o meno caratteri di autonomia sufficienti a qualificarlo come un diritto autonomo oppure se la tutela identità si esaurisca nel complesso delle protezioni assicurate agli (altri) diritti della personalità (18). Da tempo si confrontano i sostenitori di concezioni cc.dd. moniste e pluraliste (19) e non pare che il dibattito si sia ancora del tutto sopito, avendo peraltro tratto nuova linfa dalla trasposizione o dalla diretta applicazione delle regole eurounitarie sopravvenute (20). La ragione delle divergenze interpretative

(18) Dopo i primi studi sin dai primi anni Sessanta del Novecento, il dibattito si sviluppa in Italia soprattutto a partire dalla metà degli anni Settanta con l'emergere di una varietà di posizioni che vanno dal riconoscimento pieno di un autonomo diritto della persona sulla propria identità a quelle di chi nega siffatta autonomia propendendo per la riconduzione della protezione dell'identità personale all'alveo di tutela di altri diritti come quelli su nome, immagine, onore, reputazione, ecc. In merito a quel dibattito, al di là del primo e fondamentale studio di A. De Cupis, *I diritti della personalità*, in *Trattato Cicu-Messineo*, IV, 1, 1961, *passim* (di seguito si cita, però, dalla seconda edizione ossia da A. De Cupis, *I diritti della personalità*, in *Trattato Cicu-Messineo*, IV, 1982, 399 ss.), si segnalano, senza pretese di completezza, A. De Vita, *Art. 10*, in *Persone fisiche*, in *Comm. Scialoja-Branca*, Bologna-Roma, 1988, 627 ss.; V. Zeno-Zencovich, voce *cit.*, 294 ss.; M. Dogliotti, *Le persone fisiche*, in *Trattato Rescigno*, 2, Torino, 1999, 145 ss.; G. Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003, 152 ss.; I. Gonnelli-S. Pagliantini, *Art. 10*, in *Delle persone fisiche*, a cura di A. Barba e S. Pagliantini, 1, in *Comm. Gabrielli*, Assago, 2012, 677 ss. L'almeno parzialmente ambivalente approccio della giurisprudenza è reso palese dal confronto tra due note sentenze della corte di legittimità (v. Cass., 22 giugno 1985, n. 3769, in *Giust. civ.*, 1985, I, 3049 ss. con nota di F. Macioce, *L'identità personale in Cassazione: un punto di arrivo e un punto di partenza*, nonché Cass., 7 febbraio 1996, n. 978, in *Riv. dir. inf. informatica*, 1997, 115 ss. con nota di G. Cassano, *Contenuto e limiti del diritto all'identità personale (in margine allo sceneggiato sul caso "Re Cecconi"*; per una puntuale ricostruzione dell'itinerario giurisprudenziale — avviato cinquant'anni fa con Pret. Roma, 6 maggio 1974, in *Giur. it.*, 1975, I, 2, 514 ss. — si rinvia nuovamente a G. Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, cit., 55 ss.; cui *adde* M. Dogliotti, *Le persone fisiche*, cit., 148 ss.; nonché al più datato studio monografico di F. Cionti, *Segni distintivi della persona e segni distintivi della personalità*, Milano, 1994, 104 ss., nel contesto del quale si contestava la correttezza dell'impostazione fatta propria con la giurisprudenza del 1985 per lo "sdoppiamento" — v. la sintesi della critica alla pag. 173 — che avrebbe impresso al concetto di identità tutelata).

(19) Per tutti, G. Pino, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, cit., 139 ss.

(20) V. S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 583 ss.; V. Zeno-Zencovich, *Una lettura comparatistica della l. n. 675/96 sul trattamento dei dati personali*, in *Riv. trim. dir. proc. civ.*, 1998, 733 ss.; A. Mantelero, *Il diritto alla riservatezza nella l. n. 675 del 1996: il nuovo che viene dal passato*, ivi, 2000, 973 ss.; G. Pino, *Teorie e dottrine dei diritti della personalità. Uno*

sembra dipendere dalla difficoltà di fissare con precisione i contorni concettuali del diritto all'identità rispetto ad altri (relativi a nome, pseudonimo, immagine, reputazione, onore, ecc.), soprattutto se espressamente previsti dalle norme positive. I rischi sono due e opposti: da un lato, sovrapporre concetti e confondere tipologie e confini alle tutele (è la preoccupazione della concezione "pluralista"); dall'altro, lasciare scoperte aree bisognose di protezione in una società in costante evoluzione (è la preoccupazione della concezione "monista") (21). Dunque, il punto è trovare l'equilibrio tra le opposte esigenze che si vien dal menzionare, compito non facile, ma che può trovare concreta attuazione se si riesce a perimetrare il concetto di identità in modo complementare a quelli di nome, immagine, reputazione, ecc. senza sovrapposizioni.

Chiaramente, non è questa la sede per un compito così ambizioso, ma qualche spunto può essere offerto e, pur senza poter adeguatamente argomentarne i fondamenti (22), una linea definitoria può e deve essere comunque tracciata in modo tale da consentire di traslare i concetti sul piano della pratica attuazione della tutela rimediale. Il diritto all'identità personale, sul presupposto dell'autonoma tutela, si può definire come il diritto ad essere sé stessi (23), inteso come riconoscimento e rispetto della propria singolarità all'interno del corpo sociale (diritto alla verità di sé) (24) e, dunque, all'autonomia della partecipazione alla vita associata con la fisicità della persona e le acquisizioni ideologiche, morali, comportamentali (25) e sociali che qualificano l'individuo per il suo essere intellettuale (26), ivi comprese le connesse

---

studio di meta-giurisprudenza analitica, in *Materiali per una storia della cultura giuridica*, 2003, 271 ss.

(21) V. in tal senso F. Tozzi, *La circolazione dei diritti della persona*, Torino, 2013, 15.

(22) Lo stesso è costretto a fare, trattando la tematica dei diritti della personalità delle persone giuridiche, ad esempio A. Zoppini, *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati)*, in *Riv. dir. civ*., 2002, I, 861.

(23) Così A. De Cupis, *I diritti della personalità*, cit., 399.

(24) Sempre A. De Cupis, *I diritti della personalità*, cit., 399; cui *adde* F. Cionti, *Segni distintivi della persona e segni distintivi della personalità*, cit., 81 e 178 ss.; G. Pino, *L'identità personale*, in *Gli interessi protetti nella responsabilità civile*, a cura di P. Cendon, II, Torino, 2005, 383, che sottolinea i diversi (ed imprevedibili) gradi in cui la giurisprudenza ha mostrato di proteggere l'esigenza di verità; più recentemente E. Tosi, *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, cit., 53.

(25) Il profilo comportamentale — ed, in particolare, per quanto attiene al profilo del comportamento economico — è sottolineato da G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, cit., 726 ove la menzione della c.d. *transaction identity* quale "identità commerciale virtuale".

(26) V. Corte Cost., 3 febbraio 1994, n. 13, in *Foro it.*, 1994, I, 1668 ss.

esternazioni nel contesto del predetto corpo sociale (27). Senza dubbio — e qui stanno anche le basi della critica del riconoscimento dell'autonomia — il bene giuridico dell'identità personale (28) è protetto dal diritto positivo in via indiretta mediante l'attribuzione alla persona fisica di una serie di diritti che, per quanto non esclusivamente riconducibili all'identità, vi si rivelano strumentali (29): il diritto al nome ed allo pseudonimo (30); sulla propria immagine (31); alla reputazione (32); alla riservatezza (33) contribuiscono a tracciare

(27) Sulla rilevanza del riflesso della personalità dell'individuo nella realtà sociale ai fini della tutela dell'identità, in particolare, A. De Cupis, *I diritti della personalità*, cit., 399; F. Macioce, *Tutela civile della persona e identità personale*, Padova, 1984, 19; M. Proto, *Il diritto e l'immagine. Tutela giuridica del riserbo e dell'icona personale*, cit., 31.

(28) Sull'identità come bene giuridico v., ancora, A. De Cupis, *I diritti della personalità*, cit., 399.

(29) Sul punto, tra le altre, Cass., 29 gennaio 2016, n. 1748, secondo la quale nome e diritto sull'immagine sono da includere tra i "numerosi aspetti dell'identità di un individuo". Analogo rapporto di strumentalità fu ravvisato tra segni distintivi (commerciali) dell'impresa e azienda da F. Ferrara Jr., *La teoria giuridica dell'azienda*, Milano, 1945 (rist. 1982), 138, ove l'osservazione che "la legge difende l'organizzazione anche a mezzo della protezione dei segni distintivi, per cui si ha una localizzazione della tutela in questi mezzi di individuazione, una specie di decentramento della protezione in queste entità che dell'organizzazione fanno parte" (l'idea della strumentalità si ritrova nella dottrina successiva; v., ad esempio, M. Are, *Interesse alla qualificazione e tutela della personalità*, in *Riv. dir. comm*., 1965, I, 107; G. Bavetta, voce *Identità*, in *Enc. dir*., XIX, Milano, 1970, 955 nota 14; F. Cionti, *Segni distintivi della persona e segni distintivi della personalità*, cit., 207). Al di là della condivisibilità dell'idea che i segni distintivi siano "inclusi" nell'azienda, il punto sta nella configurabilità di una protezione dell'interesse sottostante all'azienda *attraverso* il riconoscimento di specifici diritti, che non escludono, comunque, la proteggibilità dell'insieme aziendale per sé, ma senza sovrapposizioni con la tutela di quei diritti suscettibili di svolgere anche una funzione "strumentale" (v., ancora, F. Ferrara Jr., *La teoria giuridica dell'azienda*, cit., 284 s.).

(30) Nome e pseudonimo identificano — secondo la giurisprudenza di legittimità (v. Cass., 7 febbraio 1996, n. 978, *cit.*, 115 ss.) — il soggetto sul piano dell'esistenza materiale e della condizione civile.

(31) Essa evoca le mere sembianze fisiche (v., ancora, Cass., 7 febbraio 1996, n. 978). Che l'immagine costituisca un segno distintivo essenziale della persona e vada comunque inquadrata nell'ambito — più generale — della tutela della identità di quest'ultima, quale apparenza fisica così come — allo stesso tempo — quale espressione e modo di essere della personalità nel suo complesso è idea acquisita tra gli interpreti (v. M. Dogliotti, *Le persone fisiche*, cit., 177 ss.; G. Alpa-A. Ansaldo, *Le persone fisiche*, in *Commentario Schlesinger*, Milano, 1996, 309 s.; Putignano, *Abuso dell'immagine della persona nota: "e io pago..."*, cit., 886 nota 4). Pertanto, v'è il divieto di introdurre nella riproduzione dell'immagine alterazioni che compromettano la comunicazione delle reali caratteristiche fisiche dell'individuo e ciò non soltanto quando l'immagine venga riprodotta fedelmente, ma anche allorché siano alterati elementi morali e sociali relativi alla personalità dell'individuo a cui quell'immagine appartiene (in tal senso Cass., 10 novembre 1979, n. 5790, in *Foro it.*, 1980, I, 81 con nota di R. Pardolesi; ripresa da A. Putignano, *Abuso dell'immagine della persona nota: "e io pago..."*, cit., 887).

l'identità del titolare di quel bene giuridico (34). Tuttavia, nome, eventuale pseudonimo, immagine, reputazione, ecc. descrivono e/o sono caratteristiche dell'individuo, ma, di per sé, non assicurano alla persona di essere trattata come distinta da altri nel corpo sociale e con la valorizzazione di tutti i connotati suscettibili appunto distinguerla, avendo la garanzia di poterli vedere imputare a sé medesima nella società (e non ad altri che ne siano

(32) Come messo in luce da G. PINO, *L'identità personale*, cit., 370, "l'integrità della proiezione sociale della propria personalità [ossia l'identità personale] può essere lesa anche tramite l'attribuzione di opinioni e idee che non sono in sé offensive, illecite ecc., ma sono semplicemente diverse da quelle realmente professate dall'interessato. La tutela dell'identità personale non coincide quindi con quella dell'onore e della reputazione, che presuppone invece l'attribuzione al diffamato di fatti offensivi"; secondo A. RICCI, *La reputazione: dal concetto alle declinazioni*, Torino, 2018, 58, l'identità della persona va tutelata, quando nel contesto sociale vi sia "un'alterazione della proiezione" della persona stessa, a prescindere "da un giudizio altrui di disvalore" invece necessario perché sia applicabile la tutela della reputazione. Rispetto ai profili caratteriale e morale dell'immagine il rischio di sovrapposizione con la tutela della reputazione è serio e frequente; quest'ultima esprime il valore sociale attribuito alla persona dai componenti della società in cui è inserita, mentre l'immagine rappresenta elementi morfologici della persona stessa anche di natura morale, intellettuale, religiosa a prescindere dal giudizio di valore espresso dalle componenti della società in cui la persona è inserita. L'immagine è la risultanza di un'apparenza oggettiva; la reputazione di un giudizio soggettivo. Ciò si evince dall'impostazione sottesa alle previsioni, in tema di immagine, contenute negli artt. 10 c.c. e 96 l. aut. (v. R. CARMINA, *La parabola del danno all'immagine degli enti*, in *Riv. IANUS*, 2015, 12, 111), non senza trascurare che la giurisprudenza di legittimità in qualche occasione ha, assai riduzionisticamente, confinato la protezione dell'immagine nei limiti delle mere "sembianze fisiche" (Cass. 22 giugno 1985, n. 3769, cit., 3049 ss.).

(33) La riservatezza esprime un dominio sulla conoscibilità esterna alla persona delle proprio caratteristiche intellettuali e comportamentali; pertanto, incorpora un obiettivo, definito "negativo" ossia alla "non rappresentazione all'esterno di proprie vicende personali" (così, prima dell'introduzione del *Codice della Privacy*, Cass. 20 aprile 1963, n. 990; Cass., 27 maggio 1975, n. 2129, in *Foro it.*, 1976, I, 2895 ss.; la posizione è sintetizzata nei medesimi termini da PUTIGNANO, *Abuso dell'immagine della persona nota: "e io pago..."*, cit., 886).

(34) Il disconoscimento del nome o l'imputazione di una reputazione diversa da quella appartenente alla persona sono annoverabili tra i fattori di offuscamento — se non di cancellazione — dell'identità che può finire per confondersi con quella di altri. Dunque, essi costituiscono contrassegni essenziali dell'individuo nel corpo sociale (analogamente A. PUTIGNANO, *Abuso dell'immagine della persona nota: "e io pago..."*, cit., 887), ma le relative tutele rimediali si prestano ad integrare e rafforzare quella dell'identità (detta strumentalità emerge chiara per quanto scrive A. FUSARO, *Nome e identità personale degli enti collettivi. Dal diritto all'identità uti singuli al diritto all'identità* uti diversi, in *Nuova giur. civ. comm.*, 2002, 51 ss., secondo la quale "il diritto che l'ente ha sul proprio nome non esaurisce la sua funzione nel permetterne l'identificazione e la differenziazione rispetto agli altri, ma assolve anche l'esigenza di tutelare l'identità del soggetto collettivo complessivamente considerata ed è perfettamente simmetrico rispetto al diritto al nome della persona fisica").

sprovvisti) (35). In altre parole, il nome ecc. sono elementi di individuazione della persona, ma non la esauriscono; sotto questo profilo, in linea con la ricostruzione "monista", il diritto all'identità contribuisce a garantire la piena realizzazione della persona prevista dalla Costituzione, giustificandosi così il richiamo giurisprudenziale all'art. 2 della Carta fondamentale. D'altro canto, se si limita il campo di azione del diritto all'identità alla protezione contro la confusione del singolo con altri individui e/o con la massa indistinta di cui è composto il corpo sociale e attraverso l'imputazione a sé delle proprie caratteristiche fisiche e morali, si evita di condannarlo ad una sorta di amorfismo, che può finire per determinare contraddizioni nelle tutele legali sia per effetto della difficoltà di delinearne il contenuto in presenza di vaghezza concettuale, che in ragione dei conflitti di disciplina che potrebbero sorgere in ragione delle sovrapposizioni con gli altri diritti della personalità. Questo, però, conduce a concludere che, innanzi tutto, il diritto all'identità si sostanzia e si esaurisce nel diritto di ciascuno di far uso della propria identità, precludendo ad altri di fare lo stesso (è uno *ius excludendi alios*); in secondo luogo, il diritto all'identità finisce per non essere il solo ad assicurare protezione al bene giuridico dell'identità personale nel corpo sociale, ma, pur non coprendo tutta la proiezione del bene giuridico dell'identità personale, contribuisce alla sua tutela con altri diritti rispetto ai quali si trova in rapporto di complementarità.

5.3. Identità personale e soggetti diversi dalle persone fisiche: il caso particolare delle imprese

Quando si riferisce alla persona fisica in quanto tale, l'identità personale attiene ad aspetti fisici e morali, questi ultimi se intellettualmente rappresentavi della personalità (36). Più complesso il discorso se si tratta dell'identità di soggetti giuridici privi — come fondazioni, associazioni, società, ecc. — di fisicità e spesso attivi attraverso una pluralità di individui non sempre espressivi di una medesima linea di pensiero e comportamentale. Per questa tipologia di soggetti non sono mancate proposte interpretative tese a negare l'attribuzione di diritti della personalità di contenuto coincidente con quello

(35) Il profilo sociale è decisivo ma qui non è inteso nel senso limitato (e limitativo) a cui si riferisce parte della dottrina (v. F. Cionti, *Segni distintivi della persona e segni distintivi della personalità*, cit., 201).

(36) A. Putignano, *Abuso dell'immagine della persona nota: "e io pago..."*, in *Danno Resp.*, 2013, 886.

riconosciuto alle persone fisiche (37); tuttavia, si può dire che è prevalsa l'idea opposta dell'attitudine delle persone giuridiche — e, più in generale, di tutte le entità soggettivizzate — ad essere titolari di detti diritti, seppur con la precisazione che il riconoscimento legale spiegherebbe effetti nei limiti della funzione del soggetto creato dall'ordinamento giuridico (38). In sostanza, i soggetti giuridici possono godere dei diritti della personalità *intra vires* e così il contenuto del diritto finisce per conformarsi entro il perimetro fissato dalla *ratio* della loro istituzione (39). Questo, quando il soggetto giuridico eserciti un'attività d'impresa, lascia margine per coprire eventuali aree di interesse

(37) V., nel senso che la tutela della ditta e del marchio (quindi, dei segni distintivi dell'impresa), sia fuori del perimetro dei diritti della personalità M. Dogliotti, *Le persone fisiche*, cit., 182.

(38) Per una ricostruzione del dibattito con gli opportuni riferimenti dottrinali si rinvia, per tutti, a A. Fusaro, *I diritti della personalità dei soggetti collettivi*, Padova, 2002, 116 ss. e A. Zoppini, *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati)*, cit., 887 ss.; cui *adde*, più recentemente, S. Landini, *Identità digitale tra tutela della persona e proprietà intellettuale*, in *Riv. dir. ind.*, 2017, I, 184.

(39) L'affermazione esposta nel testo non trova il consenso di quella dottrina che — in contrasto con l'orientamento prevalente in giurisprudenza (*ex pluribus* Cass., 9 giugno 2016 n. 11875; Cass., 11 agosto 2009 n. 18218, secondo la quale "la persona giuridica è portatrice di diritti della personalità compatibili con l'assenza di fisicità e quindi del diritto all'esistenza, all'identità, al nome, all'immagine e alla reputazione", riprendendo Cass., 29 ottobre 2002, n. 15233) — rifiuta la possibilità di riconoscere ai soggetti giuridici diritti della personalità, potendo essi intestarsi soltanto diritti patrimoniali attesa la loro funzione meramente economica; non potendo negare però la necessità di salvaguardare, ad esempio, l'onore o la reputazione del gruppo delle persone fisiche componenti il soggetto giuridico, pena una lesione indiretta dell'interesse di queste ultime, la dottrina in questione conclude che "il c.d. onore dell'associazione non riconosciuta altro non è, se non l'onore dei suoi membri, in quanto concerne quella particolare posizione della persona che è costituita dall'appartenenza ad un'associazione" (così D. Rubino, *Le associazioni non riconosciute*, Milano, 1952, 223 s.; F. Galgano, *Delle persone giuridiche*, in *Comm. Scialoja-Branca*, Bologna-Roma, 2006, 73 s.). Tuttavia, si può osservare, in contrario, che, se si riconosce che i soggetti giuridici collettivi sono forme di realizzazione della persona caratterizzate — in conformità con il principio di cui all'art. 2 Cost. — dalla espressione della persona stessa attraverso relazioni con altri, attribuire direttamente a ciascun componente del soggetto collettivo — con potere di autonoma azione a tutela — diritti in conseguenza di fatti o atti collettivi significa disconoscere in una qualche misura il valore della partecipazione al soggetto collettivo; in sostanza, si finisce per sminuire il carattere sociale dell'espressione della persona nelle collettività organizzate nelle quali avrebbe deciso di realizzarsi. Ciò non inficia quanto esposto nel testo in ordine ai confini del riconoscimento di diritti della personalità ai soggetti giuridici individuati nella struttura, nella funzione e nelle finalità assegnate dall'ordinamento a detti soggetti, confini che definiscono l'area dell'applicabilità delle norme giuridiche e della titolarità delle situazioni giuridiche (v. C. Rabitti Bedogni, *Nome sociale e disciplina della concorrenza*, Milano, 1984, 114 e 193; A. Zoppini, *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati)*, cit., 869 nota 83 F. Galgano, *Delle persone giuridiche*, cit., 77 s.; conf. con riferimento all'assenza di

meritevole non protette attraverso il riconoscimento di diritti tipici della disciplina dell'impresa e che si riconnettono alla sua individuazione ed alla sua azione nel mercato, dovendosi respingere l'idea che i diritti sulla ditta e sugli altri segni distintivi, nonché i rimedi contro la concorrenza sleale esauriscano le forme di protezione del valore dell'impresa accordate dall'ordinamento (40).

5.4. *Segue*: identità dell'imprenditore, identità delle imprese, identità delle organizzazioni delle imprese

In chiusura del primo paragrafo di questo studio si è anticipata la domanda se il crescente grado di oggettivizzazione della reputazione dell'impresa permei l'organizzazione e l'identità digitale dell'imprenditore in misura così rilevante da distaccarle da quest'ultimo risultando idoneo a farle circolare nel mercato. Prima di rispondere a questo quesito, più oltre, è necessario stabilire ora se quel crescente grado di oggettivizzazione sia innanzi tutto sufficiente ad autonomizzare l'organizzazione e i suoi caratteri identificativi rispetto al proprietario/titolare.

In linea di principio, più che di identità dell'impresa, mi pare opportuno trattare infatti di identità dell'organizzazione utilizzata per l'esercizio dell'impresa, dal momento che i terzi — quindi, il corpo sociale — entrano in

---

"fisicità" delle entità dotate di soggettività giuridica, come le associazioni non riconosciute, Cass., 16 novembre 2015, n. 23401).

(40) Analogamente Trib. Milano, 11 giugno 1994, in *Foro it.*, Rep. 1995, voce *Persona fisica*, n. 31, ove si qualifica espressamente quello all'identità come un "diritto dell'impresa" (sebbene poi, nella ricostruzione teorica sottostante alla decisione, sembri sovrapporsi al diritto all'immagine commerciale dell'impresa medesima); A. Zoppini, *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati)*, cit., 869 ss. In senso opposto rispetto a quanto riportato nel testo e, quindi, escludendo tutele diverse da quelle indicate si segnala Cass. 2 maggio 1991, n. 4785, in *Foro it.*, 1992, I, 841, con nota di M. Chiarolla, che esclude la configurabilità di un diritto all'identità personale a favore di soggetti diversi dalle persone fisiche, laddove statuisce che "notizie non vere che riguardino una società-imprenditore possono concretare tutt'al più atti di concorrenza sleale; ma sempre alla condizione che la diffusione della notizia provenga da un concorrente e che la diffusione stessa sia idonea a danneggiare l'altrui azienda"; in dottrina, tra i molti che affrontano il tema, si segnalano per gli accenti critici utili a meglio precisare il rapporto tra soggetti diversi dalle persone fisiche e diritti della personalità M. Nuzzo, voce *Nome (dir. vig.)*, in *Enc. dir.*, XXVIII, Milano, 1978, 310; C. Rabitti Bedogni, *Nome sociale e disciplina della concorrenza*, cit., 39 ss.; G. Tamburrino, *Persone giuridiche. Associazioni non riconosciute. Comitati*, in *Giur. Sist. Bigiavi*, Torino, 1997, 285; L. Bozzi, *Le denominazioni sociali tra tutela civile e tutela mercantile*, in *Riv. dir. comm.*, 1999, II, 150 ss.; A. Fusaro, *I diritti della personalità dei soggetti collettivi*, Padova, 2002, 116 ss.; A. Zoppini, *I diritti della personalità delle persone giuridiche (e dei gruppi organizzati)*, cit., 869.

rapporto e percepiscono le caratteristiche delle componenti dell'organizzazione (dei dipendenti con cui parlano, dei macchinari che distribuiscono il prodotto, del sito *web* che intermedia l'offerta commerciale, dei *softwares* che concludono lo *smart contract* o prestano il servizio, ecc.) nonché quelle dell'organizzazione nel suo complesso. Considerato in questi termini l'oggetto concreto rispetto al quale gioca il *principium individuationis*, si può meglio comprendere la possibilità di riferire caratteristiche individualizzanti a un qualcosa di oggettivamente percepibile, come è l'organizzazione, perché costituita appunto da determinate persone, mezzi materiali, beni immateriali, ma non solo; essa è, anche, plasmata da direttive gestorie, codici di condotta (41), procedimentalizzazioni operative, caratteristiche, tutte queste, senza dubbio potenzialmente mutevoli — anzi normalmente mutevoli nel tempo — ma dotate comunque di una certa stabilità, almeno nel breve-medio periodo, tanto da offrire uno specifico profilo esistenziale e comportamentale all'organizzazione: in altre parole, si tratta di caratteristiche identitarie e, cioè, di particolari atti a distinguere la singola organizzazione nell'ambito del corpo sociale costituito da tutte le organizzazioni imprenditoriali operanti nel mercato. Dunque, l'identità dell'organizzazione d'impresa esiste e può presentare connotati che è necessario stabilire se siano rilevanti anche giuridicamente, in quanto distinguano un qualcosa di riconosciuto anche socialmente.

Il dubbio che si potrebbe profilare è se, nel quadro del fenomeno di oggettivizzazione sul quale mi sono ripetutamente soffermato, quest'identità dell'organizzazione d'impresa sia un qualcosa di più e di diverso — dal punto di vista dell'ordinamento — rispetto all'identità dei beni destinati all'esercizio dell'impresa. La risposta non può che essere affermativa nella misura in cui l'identità di quell'organizzazione derivi anche da caratteri di natura comportamentale come direttive gestorie, codici di condotta, procedimentalizzazioni operative. Infatti, questi caratteri non possono costituire componenti dell'azienda, perché non riconducibili alla categoria dei "beni" pur nell'ampio senso al quale talora vi si è fatto riferimento ai fini dell'applicazione degli art. 2555 ss. c.c. (42). Se siamo dinanzi a qualcosa di diverso, oggettivamente percepibile dal corpo sociale, che contribuisce autonomamente a delineare un profilo identitario e che per questo rappresenta pure un

(41) Sulla rilevanza dei codici di condotta ai fini della "costruzione" della reputazione dell'impresa e della sua identità v. A. Scotti, *I codici di condotta fra mercato, impresa e contratto*, cit., 276 s.

(42) In proposito A De Martini, *L'usufrutto di azienda*, Milano, 1950, 61 ss.; G.E. Colombo, *L'azienda*, cit., 20 s.; G. Cottino-G. Bonfante, *L'imprenditore*, in *Trattato Cottino*, I, Padova, 2001, 613 s.; F. Martorano, *L'azienda*, in *Trattato Buonocore*, I, 3, Torino, 2010, 11 s., ove anche riferimenti giurisprudenziali.

valore per (il titolare del)l'impresa, allora abbiamo a che fare con una situazione in cui è applicabile il *principium individuationis* e in cui v'è un'utilità della sua utilizzazione per dare rilevanza giuridica e protezione a quel valore.

Si può chiudere ora un primo cerchio e, cioè, si può osservare che, caratterizzandosi funzionalmente, al titolare dell'impresa — sia esso in forma individuale o collettiva non rileva — deve riconoscersi sì uno specifico diritto alla protezione della propria identità di operatore organizzato e professionale nel mercato distinto dagli altri e con caratteristiche proprie e riconosciute ma nei limiti di quanto utile all'esercizio dell'attività d'impresa: cioè, il diritto all'identità (dell'organizzazione) dell'impresa è funzionale all'attività. Sul piano normativo, l'impresa — o, meglio, l'imprenditore — si differenzia dal non-imprenditore per la soggezione alla speciale disciplina dell'attività che contiene norme sconosciute al diritto privato come quelle che istituiscono e regolano la ditta, l'insegna, il marchio, il segreto industriale/commerciale, vietano la concorrenza sleale, ecc. Quindi, il diritto all'identità dell'organizzazione dell'impresa si confronta con un *parterre* di regole protettive della corretta individuazione dell'identità stessa — e della consequenziale disciplina — diverso e più composito di quello applicabile al non-imprenditore, ma "funzionalizzato". Tutto questo porta, poi, a porsi il quesito se, nel prisma dell'oggettivizzazione di ciò che concerne l'impresa come fenomeno economico e come organizzazione, le sue caratteristiche ed il loro riconoscimento sociale possano costituire fattore di individuazione delle stessa anche a prescindere dalla persona dell'imprenditore e così "seguire" quest'ultima se trasferita dal titolare ad altri (43). Il punto, si vedrà, è stabilire se l'ordinamento consenta una tal "sequela" oppure se vi ostino ragioni d'interesse generale.

5.5. L'identità tra diritto privato e diritto dell'impresa: approccio alla disciplina

Il diritto commerciale, sin dai tempi lontani del Medio Evo, si è giustificato come disciplina giuridica autonoma per la sua ispirazione a principi parzialmente diversi dal diritto civile: quest'ultimo è incentrato sulla proprietà fondiaria e sulla conservazione del valore attraverso il dominio statico sui beni; il diritto commerciale si pone, diversamente, nella prospettiva dinamica dell'uso produttivo dei beni e della facilitazione della loro circolazione in funzione della realizzazione di un mercato atto a riconoscerne

(43) Lo stesso dovrebbe dirsi di alcuni connotati del soggetto, tra i quali la reputazione.

il valore attraverso corrispettivi. Anche di questa diversa prospettiva (funzionale) si deve tenere conto allorché s'intende analizzare l'identità delle imprese e costruirne un regime giuridico consono alle esigenze delle imprese stesse come entità di un mercato nel quale debbono muoversi oggi in modo responsabile con una precisazione: la funzione non può incidere sull'oggetto da disciplinare, ma sulla sua disciplina. Cioè, l'esistenza dell'identità dell'organizzazione d'impresa è un fatto e la normativa ne regola la protezione in prospettiva di attuarne la funzione, ma anche nei limiti di questa. La domanda è: l'identità "civile", quindi, differisce concettualmente dall'identità "commerciale"?

L'identità non può essere che una, perché individua un soggetto, uno, e ciò sia "dentro" che "fuori" dal mercato. Il soggetto, infatti, è sempre lo stesso, che, magari, decide di presentarsi in modi diversi o, meglio, decide di presentare aspetti diversi della propria (unica) identità (44). Per il carattere sociale che si è ravvisato tipico dell'identità, il titolare aspira a far valere la propria individualità rispetto agli altri consociati — cioè, ad essere riconosciuto per chi è — ma anche costoro aspirano a ritrovare sia nell'identità "civile" che in quella "commerciale" il medesimo soggetto, senza inganni. Si tratta del principio di verità consustanziale al diritto all'identità (45), che trova, peraltro, un suo specifico, ma generale riconoscimento pure nel diritto commerciale nella misura in cui quest'ultimo tende a prevenire e rimuovere confusioni tra operatori, come pure sulla provenienza dei prodotti e dei servizi, ma anche assicurare trasparenza in ordine alla titolarità delle imprese, ecc. (46).

Piuttosto, è la disciplina che varia a seconda che il soggetto faccia valere la sua identità — o, meglio, il suo diritto all'identità — nel mercato o meno. Quando spende la sua identità nel mercato, è sottoposto alla relativa disciplina che, in ragione della sua funzionalità nel mercato stesso, devia rispetto a quella di diritto civile e, in questa prospettiva, il diritto civile è residuale rispetto al diritto dell'impresa. Se, per convenzione e per agevolare semanticamente l'indicazione dei contesti di spendita (dentro/fuori del mercato), si può distinguere tra identità "civile" e identità "commerciale", ma con l'accortezza di ricordare che ambedue sono espressioni, appunto in contesti differenti, del medesimo bene giuridico e che, perciò, si pongono in rapporto di *species* a *genus* rispetto all'identità "generale".

---

(44) Un'utile esemplificazione della mutevolezza della persona rispetto all'unicità dell'identità si trova in F. CIONTI, *Segni distintivi della persona e segni distintivi della personalità*, cit., 76 ss.

(45) Sul punto si rinvia agli AA. citati alla nota 23.

(46) Il divieto di concorrenza sleale confusoria, il registro dei marchi, il registro delle imprese rispondono chiaramente a quell'esigenza di verità.

Sul piano pratico, per la complementarità e la connessione che esiste tra diritto all'identità e altri diritti (nome, immagine, reputazione, ecc.) come il primo "reagisce" ai secondi, questi "reagiscono" alle lesioni del primo; più un'impresa ha reputazione, più anche la sua identità merita protezione, in quanto mezzo di tutela del valore non meramente economico-patrimoniale che essa esprime (47). Tuttavia, proprio per quanto esposto nella pagine immediatamente precedenti, quando sia lamentata la lesione dell'identità dell'impresa piuttosto che la sua reputazione, è opportuno fare grande attenzione a verificare su quale profilo concreto abbia inciso o incida l'evento allegato; infatti, può ben essere che, in ipotesi di pregiudizio per una società, sia leso il diritto all'adeguata diversificazione della ditta o della denominazione sociale e non quello alla distinzione dell'identità, lesione che si avrebbe se, invece che un uso di una ditta o di una denominazione troppo simile, il danneggiante abbia fatto passare l'idea nel mercato di una coincidenza soggettiva tra sé e la società in questione. E questo cosa significa? Significa che, nel caso di lesione dell'identità dell'impresa, non possono di certo invocarsi le forme di protezione previste dall'art. 2564 c.c. in quanto inapplicabili a ciò che non esplichi una funzione distintiva in senso proprio, ma sia, piuttosto, indicativo delle caratteristiche di un soggetto o di un'organizzazione imprenditoriale (48); però, similmente a quanto accade in caso di violazione del diritto altrui sulla ditta, potrà farsi ricorso alla disciplina della concorrenza sleale confusoria di cui all'art. 2598, n. 1, c.c., cosa che peraltro sembrerebbe smentire la necessità di una tutela autonoma dell'identità dell'impresa anche in funzione di evitare sovrapposizione di regole. Sarebbe però una conclusione affrettata, perché, se la disciplina della concorrenza sleale può indubbiamente contribuire ad offrire protezione, i presupposti per la sua applicazione ne escludono l'utilità in caso di identità

(47) Non mancano riconoscimenti giurisprudenziali della meritevolezza della protezione di interessi non meramente economici in capo a soggetti collettivi v. Cass., 16 novembre 2015, n. 23401, ove l'affermazione che "il diritto alla tutela del nome e dell'identità (...) non spetta solo alle persone fisiche o giuridiche, ma anche alle associazioni non riconosciute"; Trib. Napoli, 27 febbraio 2004, in *Foro it*., 2004, I, 1557; meno recentemente Pret. Firenze, ord., 3 giugno 1986, in *Foro it*., 1987, I, 287 ss., secondo la quale deve salvaguardarsi "l'individualità morale della persona fisica o dell'associazione, acquisita attraverso le affermazioni di essa nel contesto delle relazioni sociali, con opere meritorie, o con atteggiamenti del più vario contenuto". V. anche Cass., 28 gennaio 1997, n. 832, in *Foro it.*, 1997, 2537 ss., con nota di C. Bellomunno e N. Colombo, *La tutela della sigla nelle associazioni non riconosciute.*

(48) Tuttavia, come accennato più oltre, la tutela della ditta (o dell'insegna con il rinvio a quella della ditta) può entrare in gioco per segni che si pongono in rapporto di strumentalità con l'identità dell'organizzazione d'impresa (*domain names*, *nicknames*, ecc.).

dell'impresa violata da parte — ad esempio — di un non-concorrente (49). L'esempio aiuta altresì a chiarire un profilo decisivo: il diritto all'identità, anche dell'impresa, non si confonde con le forme di tutela che lo presidiano, ma "viene prima"; cioè, il diritto è riconosciuto al suo titolare come tale e tale diritto è poi tutelato diversamente in ragione del contesto in cui è fatto valere (dentro al mercato o meno). Per quanto l'esistenza di una tutela del diritto assicuri a quest'ultimo l'effettività, non viene meno la distinzione di piani tra quello del suo riconoscimento da parte dell'ordinamento e quello della tutela che l'ordinamento stesso gli accorda.

Tornando al piano del contenuto della protezione, si è chiarito sin dal primo paragrafo di questo studio che l'identità dell'impresa è tutelata non soltanto per gli investimenti finanziari che incorpora e il valore che rappresenta, dovendosi superare il confine della mera capacità di produrre profitto per includervi anche l'attitudine a soddisfare gli interessi della vasta gamma di *stakeholders* che all'impresa fanno oggi riferimento nel contesto di un mercato in cui ha rilievo non soltanto l'attività economica ma anche l'agire sociale dell'impresa stessa (50). Costoro fanno affidamento sull'impresa non per i guadagni che può produrre per i suoi proprietari, ma per le utilità che può mettere a loro disposizione. Nel valutare il ricorrere di pregiudizi in capo alla medesima, si deve tenere conto di questa più ampia prospettiva e fissare il perimetro delle azioni di tutela preventiva e/o successiva in modo da soddisfare tutta la gamma di interessi in gioco di cui si fa carico la legislazione commerciale.

Tutto ciò conduce a constatare prima d'altro che il diritto all'identità dell'impresa gode di una tutela "speciale" (quella offerta della correttezza professionale di cui all'art. 2598 cit.) e si accompagna ad un insieme di interessi meritevoli che travalica la posizione del titolare dell'impresa, cosicché la tutela "civile" finisce per essere residuale (51), in ragione del rapporto di specialità esistente tra diritto dell'impresa e diritto privato. Come per ditta,

---

(49) Il punto critico evidenziato nel testo emerge chiaro per la diversa (e non condivisibile) soluzione adottata da Cass. 2 maggio 1991, n. 4785, *cit.*, 841, che — come riportato alla nota — sottolinea la necessità della provenienza della condotta pregiudizievole da un concorrente.

(50) L'impresa non può essere più concepita soltanto come un'utilità per il suo titolare, ma riveste una rilevanza sociale, oltre che per lavoratori, creditori, fornitori, ecc. anche per l'intero sistema economico nel quale è inserita; nella misura in cui può essere produttiva per la società.

(51) V. per tutti in ordine alla possibilità di dover ricorrere alla tutela civile per i segni distintivi dell'impresa R. Costi, *Il nome della società*, Milano, 1964, 74 ss.; d'altronde, anche chi argomenta l'applicazione analogica della disciplina di prevenzione e repressione della concorrenza sleale oltre il novero degli imprenditori, non giunge a superare il confine segnato

insegna, marchio, che hanno tutele proprie diverse da quelle dei segni distintivi "civili", anche l'identità dell'impresa trova quantomeno nella disciplina della concorrenza sleale una tutela speciale rispetto a quella di diritto privato, salvo verificare la possibilità di estenderle pure talune regole speciali relative ai segni distintivi "commerciali". La conclusione non è tanto teorica, ma fa emergere una chiara regola applicativa della tutela accordata dall'ordinamento all'identità delle imprese.

Ma anche una seconda regola può enunciarsi. L'impresa sempre quella (e non altra) è, quando subisce la violazione della propria identità, sia che l'azione illecita provenga da un imprenditore concorrente così come da un non-imprenditore; ciò che muta è la protezione accordata dall'ordinamento all'identità in contesti differenti. Nel secondo caso, difettando i presupposti per la tutela speciale "commerciale", il carattere residuale del diritto privato assicura comunque l'applicabilità delle protezioni previste dalle norme ordinarie.

Su un piano generale può concludersi che, in sostanza, l'identità è una sola, ma che beneficia e soggiace a diversa disciplina a seconda che la situazione in discussione sia "di mercato" o meno.

5.6. L'identità dell'organizzazione d'impresa a fronte della trasformazione digitale: l'individuazione nel mercato virtuale

La trasformazione digitale ha modificato e continua a determinare la modifica delle scelte d'impresa, dei settori di attività, delle tendenze di mercato, ecc., influendo sui comportamenti e sugli equilibri tra gli interessi in gioco (52). La digitalizzazione offre a tutti — e, pertanto, anche alle imprese — possibilità operative molto più estese di quelle tradizionali,

---

dall'intrapresa, quantomeno, di iniziative economiche nel senso fatto proprio dall'art. 41 Cost. (così C. Rabitti Bedogni, *Nome sociale e disciplina della concorrenza*, cit., 193).

(52) Esempio lampante degli effetti strutturali sul mercato della trasformazione è quanto accaduto — ma anche in corso di evoluzione — nel rapporto tra produttori, intermediari e clienti finali, laddove entrino in gioco i cc.dd. *marketplaces* (Amazon, Alibaba, Ebay, ecc.) che hanno rovesciato i tradizionali rapporti di forza. Questa non è la sede per accennare neppure minimamente il tema, ma, per quanto di analogo fenomeno siano visti i prodromi nei decenni passati allorché i grandi operatori GDO iniziarono a commissionare a produttori — tendenzialmente già loro fornitori di prodotti a marchio degli stessi — speciali forniture da marchiare con marchi nuovi o meno di titolarità degli stessi operatori GDO, la posizione di intermediazione dei *marketplaces* pone significativi problemi, ancor prima che di *antitrust*, di concorrenza sleale in ragione della quantità di informazioni sulla clientela (esistente e potenziale), sui costi, sulla capacità produttiva, ecc. di cui gli stessi *marketplaces* godono di fatto senza costi o a costi proporzionalmente molto contenuti, mentre detti fornitori ne sono per lo più all'oscuro.

perché riduce — quando non azzera — le distanze fisiche e i tempi di comunicazione, incrementa le capacità di elaborazione (di informazioni, di offerte commerciali, di prodotti e servizi al mercato, ecc.) e quelle di comparazione, impone spesso un più rapido rinnovamento della produzione e delle relative offerte commerciali.

La propensione produttivistica del diritto commerciale, alla quale s'è fatto cenno nel paragrafo precedente, trova un fattore di accelerazione delle dinamiche che regola e, al tempo stesso, si presta ad assecondare quell'accelerazione proprio per meglio realizzare le finalità che il legislatore ha assegnato alla legislazione in materia d'impresa. In questo quadro evolutivo, si deve riconoscere all'identità digitale dell'impresa una funzione non diversa, proprio per l'unicità concettuale dell'identità, ma più "orientata" rispetto a quella del non-imprenditore; cioè, l'identità digitale dell'impresa ha un profilo "commerciale", perché è spesa nel mercato. Il punto di partenza resta fissato, chiaramente, nel concetto di identità digitale, che è ormai riconosciuta come un diritto fondamentale della personalità (53), ma va declinato in capo all'imprenditore nel mercato in funzione di ricostruirne la specifica disciplina.

Per quanto anche il non-imprenditore si stia a digitalizzando sempre più per accedere a prodotti e servizi, l'imprenditore, per un verso, dispone — o può dotarsi — di risorse tendenzialmente maggiori per far fronte ai costi della digitalizzazione e incrementare il grado di quest'ultima nella propria attività, ma, per altro verso, è addirittura costretto alla trasformazione digitale pena l'uscita dal mercato (54). Cresce, infatti, il mercato digitale e l'identità digitale sta, quindi, diventando per l'impresa un fattore chiave non

---

(53) Volendo limitare al minimo le citazioni si segnala Cass., 27 agosto 2020, n. 17894, ove la sottolineatura che "i diritti fondamentali della persona costituiscono senz'altro un "catalogo aperto", (...) sicché è ben possibile che diritti in passato considerati secondari assurgano col tempo al rango di diritti fondamentali (è stato il caso, ad esempio, del diritto all'identità personale; del diritto all'oblio; del diritto alla riservatezza, e da ultimo del diritto all'identità digitale)".

(54) La garanzia di accesso al mercato digitale pone spesso questioni rilevanti sul piano *antitrust* (v. Trib. UE, 14 settembre 2022, T-604/18, *Google* e *Alphabet* c. *Commissione*), ma si estende, più in generale, a tutti in una prospettiva di parità di opportunità di accesso ad *internet* come porzione fondamentale del mercato, a prescindere dai casi (eccezionali) di abuso. V., per quanto attiene alla protezione dei diritti della personalità attraverso la garanzia di accesso ad *internet*, G. Guzzardi, *L'abuso di posizione dominante nel mercato dei servizi digitali*, in *Nuova giur. civ. comm.*, 2023, 316, il quale sottolinea come ormai "indubbia è la capacità di *internet* di soddisfare bisogni essenziali per lo sviluppo della persona", rendendo fondamentale la c.d. *net neutrality* (a proposito del principio di neutralità della rete in rapporto alla tutela della concorrenza nel mercato v., tra gli altri, M. Orofino, *La declinazione della net-neutrality nel Regolamento europeo 2015/2120. Un primo passo per garantire un'Internet aperta?*, in *Federalismi.it*, 2, 2016; L. Belli-C. Mardsen, *European net neutrality, at*

tanto di competizione, ma di sopravvivenza. Più il mercato tradizionale è soppiantato da quello digitale, più l'identità digitale acquisisce rilevanza rispetto quella tradizionale.

Digitalizzandosi la società — e, più specificamente, l'economia — nuovi profili di estrinsecazione dell'impresa sono emersi e, in quanto meritevoli di tutela perché rappresentativi di ulteriore valore, hanno beneficiato di protezione da parte degli ordinamenti giuridici (55). Ormai da più di due decenni, *domain names*, *softwares*, *data bases* e altre "creazioni" dell'innovazione digitale sono assurti a oggetto di tutela sia a livello nazionale che globale. Nella crescita e trasformazione innovativa delle imprese la percentuale di "nuovo valore digitale" va progressivamente incrementandosi e, per molte di esse, è diventata la parte preponderante del valore nel mercato. Dunque, ricostruire adeguatamente il regime dell'identità digitale dell'impresa è un passaggio fondamentale per comprendere in quale misura oggi (e domani) il diritto sia (e sarà) in grado di assicurare protezione alla creazione di valore e, quindi, agli investimenti che stanno a monte di detta creazione. Garantire tutela agli investimenti in parola è fattore chiave per promuoverli e per offrire agli investitori prospettive concrete in ordine alla percezione dei ritorni degli investimenti medesimi. L'investitore commerciale, è scontato, rischia aspirando non solo a recuperare quanto speso, ma anche a incassare un *surplus*. Per questo, fondamentale è pure la garanzia di poter far circolare nel mercato il valore acquisito.

Posto che l'identità di un soggetto si manifesta necessariamente anche attraverso il riconoscimento della medesima da parte del contesto sociale in cui è collocato, per l'identità digitalelo "spazio sociale" più rilevante è il *web* e, più precisamente, quei "luoghi" del *web* nei quali v'è possibilità d'incontro tra ciascuna impresa e le sue controparti (clienti e fornitori, in senso ampio). Il *web*, grazie ad *internet*, è luogo di contatti e, perché i contatti siano potenzialmente forieri di affari, è necessario che ciascuno sia individuabile in

---

last?, in *MediaLaws*, 12 ottobre 2016); G. D'IPPOLITO-M. MONTI, Net neutrality *e "tariffe zero": la convergenza delle esigenze democratiche e di mercato*, in *Riv. dir. media*, 2021, 261 ss.; A.M. GAMBINO-R. GIARDA, *L'accesso ad Internet come diritto*, *ibidem*, 112 ss.).

(55) La giurisprudenza di legittimità ha riconosciuto che i "sistemi informatici" rappresentano "un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost. e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615 (relazione al disegno di l. n. 2773, poi trasfuso nella L. 23 novembre 1993, n. 547), involgendo profili che — oltre la tutela della riservatezza delle comunicazioni — attengono alla definizione ed alla protezione dell'identità digitale *ex se*" (v. la recente Cass., 31 dicembre 2020, n. 29978).

modo univoco. Anche in quello spazio virtuale che è il *web* (56), quindi, è essenziale per l'imprenditore-titolare dell'identità che la stessa gli sia riconosciuta e tutelata, in quanto nel *web*, quale "mercato virtuale" (*on-line*), l'identità soddisfa la medesima esigenza sottesa al riconoscimento nel "mercato fisico" (*off-line*) e richiede protezione analoga (57). Il contesto del *web* è ormai una sorta di semplice partizione della società — e, quindi, del mercato — con la conseguenza che i principi di protezione extra-*web* ben debbono essere applicati, *mutatis mutandis*, nel *web*.

Riprendendo la conclusione esposta nel precedente paragrafo in ordine alla protezione accordata all'identità nel nostro ordinamento, essa è una, ma beneficiaria di tutele diverse a seconda del contesto di mercato o extra-mercato. Anche il *web* può essere mercato oppure no. Dunque, in linea di principio, quella conclusione deve applicarsi anche alle situazioni che si presentano nel *web*, sia nei casi di fatti o atti virtualmente contestualizzabili in siti, sia nelle ipotesi delle medesime tipologie di fatti o atti riferibili all'uso di *app*.

Gli strumenti di individuazione — e, dunque, il modo di identificazione — dei soggetti nel *web* tecnicamente sono gli *user names* (58), i *nicknames* (59) o gli *alias* (per i soggetti) e i *domain names* (per i siti dei soggetti) (60); similmente alle esigenze presenti nel mercato *off-line* è necessaria sia l'indi-

---

(56) Nel senso che la pagina web è un "luogo virtuale" o un "ambiente" di incontro tra domanda ed offerta di prodotti o servizi Trib. Roma, ord., 22 dicembre 1999, in *AIDA*, 2000, 711; Trib. Cagliari, ord., 23 dicembre 2000, *ivi*, 2001, 795.

(57) Come si vedrà più oltre, nel mercato digitale sono più stringenti i limiti di utilizzo dell'identità digitale come mezzo espressivo alternativo legittimante anche la creazione di connotati di fantasia (quanto alla legittimità per ricorso alla *fictio* in ordine alla propria personalità come forma di manifestazione del pensiero v. D.G. Ruggiero, *Persona e identità digitale*, cit., 135).

(58) Tra gli *usernames* debbono essere annoverati gli strumenti come il c.d. SPID che consente un'identificazione sicura dell'utente, ma non è la sua identità nel senso che si è dato in questo studio; infatti, l'art. 1, n. 1, lett. *o*),dD.P.C.M. 24 ottobre 2014 definisce lo SPID quale "*rappresentazione informatica della corrispondenza biunivoca tra un utente ed i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale*", ponendolo su un piano del tutto diverso rispetto a quello della personalità. Riguardo al fatto che lo SPID costituirebbe una "declinazione (...) più risalente e restrittiva" dell'identità digitale della persona rispetto ad un'accezione "più recente ed estensiva" incentrata sul "complesso di dati, informazioni, attività che servono non solo ad individuare ma a rappresentare compiutamente la storia personale di un dato soggetto" v. E. Tosi, *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, cit., 51.

(59) Analogamente, nel perimetrare il diritto anonimato in rete, A. La Spina, *Complessità e identità personale*, Napoli, 2022, 309 ss.; secondo D.G. Ruggiero, *Persona e identità digitale*, cit., 134 nota 148, invece, il *nickname* non avrebbe valore identificante.

(60) Infatti, con i *domain names* si contraddistinguono i propri siti *web*, attraverso i quali sono svolte anche attività d'impresa; con gli *usernames* ci si distingue — e questo vale

viduazione degli operatori che dello spazio da cui operano. Rispetto all'identità digitale delle imprese *domain names* e *user names* (o *nicknames* e *alias*) rappresentano, senza dubbio, tasselli fondamentali: servono ad attuare il cd. *principium individuationis* che sta alla base dell'identità (anche delle organizzazioni d'impresa) e, pertanto, a salvaguardare quel valore ad essa riconnettibile. E ciò, si badi bene, è emerso sin dai primi anni di utilizzo dei *domain names*, in particolare (61). Si tratta di segni che presentano analogie concrete sia con la ditta che con l'insegna per la capacità di identificazione (ossia il carattere distintivo) di una specifica impresa e per la funzionalità (tecnica) alla riconduzione del cliente al punto di contatto con l'impresa medesima; pertanto, analogamente a ditta e insegna, sia il *domain name* che lo *user name* (come pure il *nickname* o l'*alias*) si pongono in un rapporto di strumentalità rispetto all'identità (digitale) dell'impresa che operi nel *web* o, più specificamente, all'interno di *social media*.

Questa prospettiva d'indagine muove dal punto di vista dell'esigenza dell'organizzazione d'impresa ad essere individuata digitalmente e, quindi,

---

anche per le imprese — nell'accesso, per quanto qui rileva, anche a siti *web* altrui e, soprattutto, ai *social media* quali *Facebook*, *Instragram*, *Telegram*, *Tiktok*, *X* attraverso i quali pure sono svolte anche attività d'impresa.

(61) Infatti, sin dalla seconda metà degli anni Novanta, si sono diffusi fenomeni di *cybersquatting* come il *domain name grabbing* e il *typosquatting*. Tutte pratiche implicanti la registrazione di *domain names* contenenti in tutto o con lievi modificazioni segni distintivi altrui, molto spesso assai noti; ciò in funzione di rivendere il *domain name* o di pregiudicare gli interessi del titolare legittimo del segno originale oppure ancora per, più semplicemente, sfruttare la notorietà del segno per scopi non autorizzati dal titolare stesso. Mentre negli Stati Uniti d'America fu preso introdotta una disciplina diretta a contrastare il *cybersquatting* (con *l'ACPA — Anticybersquatting Consumer Protection Act* del 1999 come estensione del *Lanham Act* in materia di marchi), in Italia il problema fu affrontato soltanto a livello giurisprudenziale con molte decisioni (v., tra le altre, Cass., 18 agosto 2017, n. 20189; Trib. Milano, ord., 26 febbraio 2008, in *AIDA*, 2010, 654 ss.; Trib. Bologna, 29 agosto 2007; Trib. Napoli, 7 luglio 2005; Trib. Milano, 7 agosto 2001, in *AIDA*, 2003, 901; in dottrina, senza pretese di completezza ma per ulteriori riferimenti, G.E. Sironi, *Art. 20*, in *Codice della proprietà industriale*, a cura di A. Vanzetti, Milano, 2013, 409; D. Lindsay, *International Domain Name Law. ICANN and the UDRP*, Oxford-Portland, 2007, 95 ss.; A. Schwabach, *Internet and the Law: Technology, Society, and Compromises*, Santa Barbara, 2023, 58 ss.; per un commento degli effetti dell'*ACPA* e riferimenti giurisprudenziali nord-americani W.R. Towns, *United States of America ('.us')*, in *Domain Name Law and Practice. An International Handbook*, a cura di T. Bettinger e A. Waddell, Oxford, 2015, 1028 ss.). Negli anni successivi, in caso di *domain names* abusivamente registrati, l'Organizzazione mondiale per la proprietà industriale ha poi introdotto, unitamente all'*Internet Corporation for Assigned Names and Numbers* (ICANN), una specifica procedura rimediale a beneficio dei legittimi titolari dei diritti sui segni incorporati nei *domain names* che prevede la sospensione del loro utilizzo (v. T. Bettinger-A. Waddell-H. Xue, *Rights Protection Against Registration and Use of Domain Names within a New gTLD*, in *Domain Name Law and Practice. An International Handbook*, cit., 1237 s.).

anche nel mondo virtuale. In altre parole, si cura del diritto a scegliere di avere ed utilizzare un'identità anche digitale. La ricerca sarebbe, però, carente se non si considerassero i limiti a quel diritto di scelta. È noto che il contenuto concreto dei segni distintivi commerciali non è del tutto libero, perché ci sono esigenze — spesso contrapposte — dei concorrenti, dei clienti e, più in generale, di funzionamento del mercato che sono meritevoli di tutela; ciò, peraltro, è vero pure per i segni distintivi civili non necessari, come lo pseudonimo. Dunque, ma nel successivo paragrafo il tema è più dettagliatamente affrontato, il diritto alla scelta della propria identità digitale ha confini dettati dalla speciale disciplina che la governa nella prospettiva dell'attività esercitata nel mercato.

5.7. *Segue*: il contributo di *domain names*, *user names*, *nicknames* e *alias* alla tutela (o alla violazione) dell'identità digitale dell'organizzazione d'impresa

Come la pratica insegna, spesso i *domain names* — che sono più idonei a svolgere una funzione distintiva rispetto a *usernames*, *nicknames* e *alias* — incorporano la parte letterale di altri segni distintivi dell'impresa, da questa utilizzati extra-*web* in una logica di coerenza dell'immagine aziendale nel mondo virtuale rispetto a quello fisico. Questa scelta di coerenza, sulla scia di prese di posizione della giurisprudenza (62), ha trovato recezione a livello normativo nel testo dell'art. 22 c.p.i. con la specificazione che i *domain names* ricadono nell'area di applicazione del principio di unitarietà dei segni distintivi. Peraltro, già prima dell'espressa menzione normativa nel 2005, l'uso di *domain names* confondibili era ritenuto integrare, comunque, una condotta di concorrenza sleale vietata ai sensi dell'art. 2598, n. 1, c.c.; ancor oggi quest'ultima disciplina può ben trovare applicazione, dal momento che il legislatore ha non ha introdotto un esaustivo regime speciale per i *domain names* (63).

---

(62) V. in modo esplicito — ad esempio — Cass., 18 agosto 2017, n. 20189; Trib. Milano, ord., 26 febbraio 2008, in *AIDA*, 2010, 654 ss.; Trib. Bologna, 29 agosto 2007; Trib. Napoli, ord., 7 luglio 2005, in *AIDA*, 2005, Rep. IV.4. Prima dell'entrata in vigore dell'art. 22 c.p.i., la tutela del *domain name* era stata ricavata talora dalla disciplina del marchio (Trib. Milano, 7 agosto 2001, *cit.*, 901; Trib. Modena, ord., 23 agosto 2000, in *AIDA*, 2001, 777), talaltra dalle norme codicistiche sulla ditta (Trib. Napoli, ord., 27 maggio 2000, *ibidem*, 769) o sull'insegna (Trib. Milano, ord., 3 giugno 1997, *ivi*, 1998, 531; Trib. Milano, ord., 13 aprile 2000, *ivi*, 2000, 728; Trib. Reggio Emilia, ord., 30 maggio 2000, *ibidem*, 733), talaltra, ancora, dai principi a protezione della testata (Trib. Padova, ord., 14 dicembre 1998, *ibidem*, 672; Trib. Viterbo, ord., 24 gennaio 2000, in *ivi*, 2001, 756).

(63) Così, recentemente, P. Di Tullio, *Art. 2598*, in *Commentario Ubertazzi*, Milano, 2019, 2531.

D'altro canto, vista la funzione di mezzo tecnico di reperimento ed individuazione di un sito *web* soddisfatta dal *domain name*, la tutela che l'ordinamento gli accorda, ben si presta a contribuire alla salvaguardia dell'identità del suo titolare, distinguendolo da altri imprenditori nel mercato. Dunque, se vale l'assimilazione del *domain name* all'insegna, vale anche il richiamo alla regola dell'art. 2564, comma 1, c.c., che assicura l'uso esclusivo del segno nel mercato stesso. Tutela questa che è completata dal divieto di adozione di segni confusori da parte di concorrenti in virtù del disposto dell'art. 2598, n. 1. Ma non basta. Come non è lecita l'adozione anche da parte di non-concorrenti di segni confondibili con ditta ed insegna altrui, così neppure è lecito riportare il contenuto del *domain name* di altri pur se in segni distintivi diversi (64) o nell'ambito di comunicazioni di tipo pubblicitario, realizzando forme di agganciamento vietate ai sensi dell'art. 2598, n. 2 (65). Dunque, la tutela accordata a questi segni, in quanto distintivi dell'identità dell'organizzazione d'impresa, ben si presta ad assicurare l'univoca individuazione di quest'ultima. Unica eccezione si configura, quando l'uso (legittimo) del segno altrui è fatto con funzione meramente descrittiva delle caratteristiche della identità di un terzo.

Usernames, *nicknames* e *alias* più difficilmente si prestano a svolgere una funzione distintiva dell'impresa, sebbene non la si possa escludere in radice (66). Non mancano casi di inserimento di componenti verbali dei segni distintivi già utilizzati *off-line* in *usernames*, *nicknames* e *alias* necessari per aprire e mantenere profili in *social media* — quali *Instagram*, *Facebook*, *TikTok*, ecc. — e di utilizzo degli stessi da parte dell'utente-cliente (attuale o potenziale) per ricercare informazioni ed offerte commerciali di un'impresa, appunto, attraverso i *social media*. In caso di un tale uso di *usernames*, *nicknames* o *alias*, non ci sono ragioni che escludano l'applicazione della regola che impone la differenziazione del segno propria dei *domain names*; lo impone, ancora una volta, il principio di unitarietà dei segni distintivi ormai normativamente esteso anche ad ogni "*altro segno distintivo*" (67). Parimenti, l'uso di *usernames*, *nicknames* e *alias* confondibili costituisce condotta di

(64) Si pensi, ad esempio, alla denominazione di un'associazione che eserciti o meno attività d'impresa non importa.

(65) La concorrenza sleale "per agganciamento" è infatti vietata ai sensi dell'art. 2598, n. 2, c.c. (Cass., 13 luglio 2021, n. 19954); in ordine alla repressione della pubblicità per agganciamento come attività tesa all'appropriazione di pregi v. M. Ammendola, *L'appropriazione di pregi*, Milano, 1991, 92 ss.

(66) Sul punto S. Landini, *Identità digitale tra tutela della persona e proprietà intellettuale*, cit., 182.

(67) Sul punto G.E. Sironi, *Art. 22*, in *Codice della proprietà industriale*, cit., 471.

concorrenza sleale vietata ai sensi dell'art. 2598, n. 1 (68). Per converso, come per i *domain names*, se non è fatto con funzione meramente descrittiva, è illecito che il terzo riporti in propri segni il contenuto di *usernames*, *nicknames* e *alias* che individuano un determinato imprenditore e ciò sia che lo faccia un concorrente, così come un non-concorrente; soltanto differisce la norma repressiva.

Concludendo, un aspetto va rimarcato per evitare fraintendimenti, perché è il presupposto della tutela. *Domain names*, *usernames*, *nicknames* e *alias*, ma, in realtà, anche gli indirizzi di posta elettronica (69) — similmente a ditta ed insegna *off-line* — contribuiscono a garantire al titolare il rispetto della propria identità, evitando l'ingenerarsi di confusioni nei terzi — ed, in particolare, in clienti e fornitori — in ordine alla sua identificazione in quella "parte virtuale" del mercato che è il *web* (70). È vero però che, specularmente, il titolare soprattutto di *usernames*, *nicknames* o *alias*, a sua volta, non può utilizzarli per confondere i terzi e sfruttare l'identità altrui (71). Sebbene non manchi chi ha segnalato l'interesse delle persone a "costruirsi" delle identità digitali con caratteri perfino di fantasia (72), sostenendo come ciò

---

(68) V., con specifico riguardo ai "nomi di *account*", G.E. Sironi, *Art. 22*, cit., 471.

(69) Che l'indirizzo di posta elettronica possa esplicare anche una funzione distintiva è implicito nella sua qualificazione come "strumento di comunicazione commerciale per la vendita dei prodotti" (così Trib. Bologna, ord., 20 novembre 2013, in *GADI*, 2013, 1272), in quanto consente di veicolare l'offerta commerciale ad una specifica impresa.

(70) Che la libertà di creazione di nuove identità digitali incontri il limite dell'inganno dei terzi è sottolineato da S. Landini, *Identità digitale tra tutela della persona e proprietà intellettuale*, cit., 198. Peraltro, in campo sociologico è stato sottolineato con riferimento a *nicknames*, *alias*, *avatars*, come "la relativa stabilità nel tempo che essi hanno, nonostante la facilità con cui li si può cambiare, ne tradiscono la funzione identitaria e, se si considera che vengono pensati ed utilizzati anche quando gli interlocutori conoscono l'identità reale, è chiaro il loro ruolo di presentazione, più che di falsificazione dell'identità (così, ancora, M. Mura-M. Martini, *Identità sociale e comunicazione in rete*, cit., 45).

(71) La giurisprudenza esclude che sia lecita "la condotta di colui che crei ed utilizzi un 'account' ed una casella di posta elettronica servendosi dei dati anagrafici di un diverso soggetto, inconsapevole, con il fine di far ricadere su quest'ultimo l'inadempimento delle obbligazioni conseguenti all'avvenuto acquisto di beni mediante la partecipazione ad aste in rete" (v. Cass. pen., 15 dicembre 2011, n. 12479; più recentemente, Cass. pen., 22 giugno 2018, n. 42572).

(72) Si pensi alle possibilità di "costruzione" anche di più identità aggiuntive offerte da *social media* come *Second Life*, che viene così descritto: "realtà virtuale e tridimensionale fruibile attraverso la rete Internet mediante un *software*", che "offre la possibilità di costruire virtualmente personaggi e situazioni che sostituiscono forme di vita reale creando una "seconda vita" nella quale ci si colloca come fosse autentica, rappresentando un vero e proprio spazio abitativo costruito dagli utenti che, oltre alla propria identità, possono realizzare oggetti di qualsiasi tipo, sviluppare una propria storia, condividere emozioni, fare affari" (così la voce *Second Life* in Treccani, *Enciclopedia online*, reperibile all'indirizzo https://www.treccani.it/

possa contribuire alla piena realizzazione della loro personalità (73), una tal prospettiva non è lecita nei medesimi termini per le imprese, perché a rischio di conflitto con il principio di trasparenza che ne governa la partecipazione al mercato ed una cui espressione fondamentale è la pubblicità nel registro delle imprese. Analoga esigenza di trasparenza è perseguita delle regole che presidiano l'adozione e l'uso di tutti i segni distintivi dell'impresa. Pertanto, non solo è preclusa l'adozione di *domain names*, *usernames*, *nicknames* e *alias* confondibili con segni altrui in funzione di tutelare l'identità si terzi, ma addirittura è vietata l'adozione di *domain names*, *usernames*, *nicknames* e *alias* che, semplicemente, non consentano l'individuazione o la corretta individuazione dell'imprenditore titolare (74). Il titolare non può utilizzarli per operare di nascosto nel mercato digitale, perché ciò, oltre a porsi in conflitto con il principio generale di trasparenza che impone la riconoscibilità dell'imprenditore nell'esercizio dell'impresa (75), viola la specifica regola stabilita dall'art. 7 Decreto Legislativo 9 aprile 2003, n. 70 attuativo della c.d. Direttiva *e-commerce*. Per questo e perché confliggente con il divieto di concorrenza sleale denigratoria è preclusa la creazione — sotto *domain names*, *usernames*, *nicknames* e *alias* appositamente registrati — di profili apparentemente imputabili ad un imprenditore, ma, in realtà, creati da un concorrente per diffondere informazioni false sull'apparente titolare; per tale via si assicura anche tutela all'identità digitale violata di quest'ultimo.

Neppure è ammissibile l'utilizzo del contenuto di *domain names*, *usernames*, *nicknames* e *alias* altrui in *metatag*, *hashtag*, ecc., ossia in quelle stringhe verbali che sono il mezzo di individuazione dei contenuti nel *web* e nei *social media*; infatti, salve le ipotesi — eccezionali — in cui se ne possa

---

enciclopedia/second-life/#:~:text=Realt%C3%A0%20virtuale%20e%20tridimensionale%20fruibile,a%20circa%20900.000%20nel%202017); in sostanza, è uno strumento per disconnettere l'identità virtuale da quella reale (v. T. Boellstorff, *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*, Princeton, 2015, 187) mediante la creazione di un *avatar*, che si presenta e può svolgere molteplici attività virtuali, celando la personalità reale.

(73) S. Landini, *Identità digitale tra tutela della persona e proprietà intellettuale*, cit., 190.

(74) Peraltro, per quanto concettualmente vi sia differenza tra anonimato (ignoranza) e pseudonimo (dissimulazione) del titolare (così T. Boellstorff, *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*, cit., XVII), sul piano delle conseguenze materiali per i terzi il risultato pregiudizievole tende a coincidere, poiché l'ostacolo all'identificazione dell'imprenditore rende arduo in entrambi i casi attivare strumenti preventivi o esercitare rimedi successivi nei suoi confronti.

(75) V., per tutti, in ordine all'interesse generale alla conoscibilità delle principali informazioni relative alle imprese C. Ibba, *Il registro delle imprese*, in *Trattato Iudica-Zatti*, Milano, 2021, 8; con riferimento alla trasparenza nella trasformazione digitale G. Cabras, *Via della impresa*, Torino, 2023, 71.

invocare l'uso in funzione descrittiva, non è lecito far ricorso alle varie tipologie di *tag* per realizzare forme di agganciamento alla notorietà altrui (76). Principi analoghi si applicano anche con riferimento alle attività di *linking* (77), *framing*, ecc. quando tendano a realizzare o realizzino situazioni di confusione o di vera e propria sostituzione di identità digitali di un'organizzazione d'impresa (78).

Comunque, come ditta ed insegna non sono l'identità del soggetto nel mercato (e il "nome civile" non coincide con quella del suo titolare), non corrispondono all'identità del soggetto, così pure *domain names*, *usernames*, *nicknames* e *alias* non corrispondono con l'identità digitale dell'organizzazione d'impresa, sebbene contribuiscano alla sua individuazione ed alla protezione indiretta della stessa.

5.8. L'identità (digitale) dell'organizzazione d'impresa può circolare?

È pacifico che i segni distintivi dell'impresa possano essere ceduti a terzi. Ciò vale per ditta, insegna, marchio utilizzati nel mercato tradizionale; parimenti si ritiene per *domain names* e *user names* utilizzati nel mercato digitale. Si è scritto qualche pagina addietro che ciò che attiene all'organizzazione dell'impresa ha registrato negli anni un fenomeno di oggettivizza-

---

(76) Non necessariamente gli *hashtag* svolgono una funzione distintiva, ma quest'ultima può risultare e si deve accertare di volta in volta se, appunto, un *hashtag* sia utlizzato per contraddistinguere un prodotto, un servizio, un'impresa o il luogo — anche virtuale — da cui esercita l'attività (a tal proposito Corte giust. UE, 12 settembre 2019, C-541/18, *AS*, ECLI: EU:C:2019:725, punto 18 commentata da T. Fuchsberger, *Unterscheidungskraft einer Marke nach der Richtlinie 2008/95/EG*, in *ÖZK*, 2019, 183 s.). Anche per ulteriori riferimenti si rinvia a G.E. Sironi, *Art. 20*, cit., 412; in giurisprudenza le diverse modalità d'uso nel *metatag* hanno condotto ad inquadrare la condotta dell'utilizzatore per lo più nella fattispecie di cui al n. 1 (Trib. Bologna, 12 giugno 2012, in *Foroplus*; Trib. Bologna, 30 luglio 2002, in *Giuraemilia.it*) o al n. 3 (Trib. Monza, 15 luglio 2008, in *Foroplus*; Trib. Milano, 8 febbraio 2002, in *Corr. giur.*, 2002, 1607 ss. con nota di S. Meani, *Possibili tutele contro l'uso distorto di termini corrispondenti a marchi altrui nei* Meta-Tag *dei siti* web; Trib. Napoli, 28 dicembre 2001, in *Dir. inf. informatica*, 2002, 94 nota di P. Sammarco, *Atti di concorrenza sleale attraverso* Internet *e responsabilità del* provider; Trib. Roma, 18 gennaio 2001, in *Riv. dir. ind.*, 2002, 189 ss. nota di R. Sciaudone, *L'uso del marchio altrui come* metatag).

(77) L'idoneità del *linking* ad integrare fattispecie confusorie o appropriative è affermata da Trib. Bologna, 9 settembre 2015, in *Foroplus*.

(78) In tali casi possono cumularsi le tutele offerte dalla disciplina autorale che s'incentrano sul diritto morale dell'autore e che, si ricorda, è funzionale alla protezione della personalità dell'autore, quale creatore dell'opera e, pertanto, all'individuazione di uno dei caratteri della sua identità. In ordine al potenziale cumulo della tutela del diritto morale in caso di *linking* v., ad esempio, S. Scalzini, *« Hyperlinking » e violazione del diritto d'autore nell'evoluzione giurisprudenziale europea*, in *A.G.E.*, 2017, 639 nota 3.

zione in funzione della sua circolazione in ragione della riconnessione ad esso di un autonomo valore, reso così suscettibile di scambio nel mercato. Questo perché la possibilità della circolazione agevola la futura liquidazione degli investimenti e, a monte, incrementa la propensione ad effettuarli. Tutto ciò, contribuendo alla promozione della crescita dell'economia, è utile all'interesse generale e, quindi, va favorito nei limiti del possibile.

Si è cercato di chiarire nel precedente paragrafo 5.4 che, più che all'identità dell'impresa, è utile fare riferimento all'identità dell'organizzazione d'impresa. La domanda cruciale è: l'identità digitale dell'organizzazione imprenditoriale è sufficientemente oggettiva da poter circolare? Nel diritto privato, essendo l'identità la concretizzazione della singolarità della persona nel corpo sociale, essa è inscindibile dalla persona e, perciò, inalienabile (79). È lo stesso nel contesto del mercato per quella "parte" di identità che individua l'impresa come organizzazione con i suoi connotati individualizzanti? In altre parole, è ammissibile una scissione tra l'identità "privatistica" e l'identità "commercialistica" del titolare dell'impresa intesa come identità della sua organizzazione?

La diversità dei principi del diritto delle imprese rispetto al diritto privato suggerisce di considerare non scontata la risposta tanto più alla luce dell'orientamento emerso negli ultimi decenni favorevole alla commerciabilità di almeno taluni diritti della personalità, come quello sulla propria immagine (80). È vero che l'identità è strumento di individuazione del titolare dell'impresa e ciò potrebbe escludere ragioni di deviazione dal principio di inalienabilità. Tuttavia, ci si deve chiedere: l'identità dell'organizzazione d'impresa (e, in particolare, di quella "digitale") è distaccabile dal suo titolare e così tanto da essere suscettibile di trasferimento ad altri senza lesione — anzi, con adeguata realizzazione — degli interessi protetti dall'ordinamento? Una volta concluso, come ai precedenti paragrafi 5.4 e 5.5, per la configurabilità di un'identità dell'organizzazione d'impresa, come

(79) V. in tal senso F. Tozzi, *La circolazione dei diritti della persona*, Torino, 2013, 13; con riferimento più generale a tutti i diritti della personalità A. De Cupis, *I diritti della personalità*, cit., 88; G. Resta, *I diritti della personalità*, in *Trattato Sacco*, 1, Torino, 2006, 661 ss.; per una ricostruzione del dibattito si rinvia anche a M. Proto, *Il diritto e l'immagine. Tutela giuridica del riserbo e dell'icona personale*, cit., 171 ss. Non è così, invece, per l'immagine o il ritratto, rispetto ai quali l'interpretazione dominante riconosce ormai un *coté* patrimoniale commerciabile e risarcibile in caso di violazioni da parte di terzi non autorizzati al loro utilizzo (in proposito si rinvia nuovamente all'ampio studio di F. Tozzi, *La circolazione dei diritti della persona*, cit., 130 ss.).

(80) V. ancora, anche per ulteriori riferimenti, F. Tozzi, *La circolazione dei diritti della persona*, cit., 130 ss., il quale sottolinea l'emergere di una concezione "bipolare" dei diritti della personalità che vedono diritti — trasferibili — di sfruttamento economico affiancarsi a diritti — intrasferibili — della personalità.

species del *genus* identità del titolare di quest'ultima (il soggetto imprenditore), quantomeno si è dinanzi ad un bene giuridico individuabile e distinguibile rispetto al quale è questione di stabilire se sia meritevole di "distaccabilità" dal suo titolare. Per i diritti "civili" della personalità la risposta degli interpreti è, come poc'anzi ricordato, negativa per la non troncabile connessione con una determinata persona che ne è titolare, ma questo affonda le radici nel rapporto tra ciò a cui sono connesse le caratteristiche giuridicamente rilevanti e la loro sintesi nell'identità. Si tratta però, nel diritto privato, di caratteristiche della persona non disgiungibili dalla stessa, cioè soggettive.

Diverso è il discorso per le caratteristiche dell'organizzazione d'impresa, che non si riferiscono ad una persona, ma ad un qualcosa che ad una persona (o, più in generale, ad un soggetto giuridico) fa capo, cioè la possiede in un rapporto di alterità. Orbene, l'oggettivizzazione dell'organizzazione dell'impresa consente di considerare questa "altro" rispetto al titolare dell'impresa, all'imprenditore. Dunque, almeno sul piano materiale, si ha una *species* dell'identità che potrebbe, almeno astrattamente, essere distaccato dal titolare del *genus* senza che quest'ultimo veda compromessa la possibilità di essere soggettivamente identificato; infatti, quel titolare mantiene necessariamente le caratteristiche identitarie soggettive, ma può anche mantenere quelle altre oggettive di cui non intenda spogliarsi.

L'ammissibilità astratta del distacco dell'identità dell'organizzazione d'impresa non ne implica peraltro la legittimità nel nostro ordinamento positivo. Sempre nel paragrafo 5.4, si è concluso che l'identità dell'organizzazione d'impresa è qualcosa di diverso e, come tale, oggettivamente percepibile dal corpo sociale, funzionale a distinguere quell'organizzazione da altre e che per questo rappresenta un valore economico, ancora una volta, oggettivo. Se non si disconosce che il diritto dell'impresa mira a favorire e proteggere la creazione di valore economico oggettivo e che fa ciò anche favorendone la circolazione in funzione della migliore allocazione ai fini del suo sfruttamento, è giocoforza ribaltare il principio tradizionale privatistico dell'inalienabilità ed affermare la cedibilità dell'identità delle organizzazioni imprenditoriali (81). La questione è, piuttosto, se sia "libera" oppure se vi siano vincoli legali. Il dubbio si risolve a favore di quest'ultima soluzione,

(81) Siffatta conclusione sembrerebbe poter trovare conferma nell'idea della cedibilità degli attributi immateriali della personalità oggetto di interessi patrimoniali (così E. Tosi, *Circolazione dei dati personali tra contratto e responsabilità. Riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, cit., 83; sul punto anche G. Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005, 213); tuttavia, quell'idea è stata argomentata prendendo a riferimento il modello dei diritti d'autore, sottolineando che, nonostante i diritti non siano riferiti ad un'opera ma alla persona,

perché il "sistema" di diritto delle imprese protegge valori come la fiducia dei terzi (82), la correttezza del gioco concorrenziale, la trasparenza del mercato in sé (83), ecc.

Molte sono le ricadute in termini di disciplina delle situazioni concrete. Come già anticipato, ed ora offrendo una più argomentata riflessione sul punto, l'identità dell'organizzazione imprenditoriale può circolare, ma nel rispetto — ad esempio — dell'art. 2598 c.c., escludendo che il cessionario possa presentarsi come fondatore dell'organizzazione d'impresa (84) per accreditarsi maggiormente presso il pubblico a svantaggio dei concorrenti. Altra ipotesi di possibile ricorso alla tutela contro la concorrenza sleale si profila allorché il cedente, che abbia ceduto l'azienda con patto di non-applicazione del divieto di concorrenza ai sensi dell'art. 2557, possa comunque "ricostruire" un'identità di una nuova organizzazione d'impresa ricalcando pedissequamente (o, meglio, parassitariamente) quella ceduta e ciò in linea con la ritenuta ammissibilità dell'uso del patronimico che coincida con quello del concorrente preveniente eccetto quando "sia giustificato, in una ambito strettamente delimitato, dalla sussistenza di una reale esigenza descrittiva inerente all'attività, ai prodotti o ai servizi offerti" (85). All'identità dell'organizzazione d'impresa dovrebbero applicarsi, poi, per *analogia iuris* i principi che impongono al concorrente successivo l'onere di differenziazione, pena la violazione del *principium individuationis*. Ancora, similmente a quanto si sostiene per l'identità "civile", fuori dei casi di applicabilità dell'art. 2598 cit. il cessionario può far valere nei confronti del cedente o di

---

la cessione investirebbe il diritto di utilizzarli per costruire profilazioni o entrare a far parte di *databases* senza, quindi, spogliare la persona di connotati che effettivamente la caratterizzano. In altre parole, la cessione sarebbe più propriamente qualificabile come licenza d'uso. Ciò rende evidente come la dottrina citata si ponga su una linea argomentativa diversa da quella esposta nel testo, posto che lo sfruttamento dalla medesima ipotizzato avviene mediante un atto che non spoglia la persona di un qualche connotato della sua identità, ma si limita a consentirne l'utilizzo ad altri; nel testo, invece, si sostiene la cedibilità in senso proprio di fattori identificanti, dal momento che la cessione dell'identità d'impresa segue la cessione dell'impresa stessa, spogliandone l'(ex)titolare.

(82) V. C. Rabitti Bedogni, *Nome sociale e disciplina della concorrenza*, cit., 61.

(83) Per tutti, evidenziando come l'interesse alla trasparenza debba essere contemperato con quello dell'imprenditore interessato, C. Santagata, *Concorrenza sleale e trasparenza del mercato*, Padova, 1979, 72 s.

(84) La "fondazione" di un'impresa può, per molti versi, assimilarsi alla discendenza per nascita di una persona fisica da determinati avi (per la tutela in ambito civile della verità della discendenza v., in particolare, A. De Cupis, *I diritti della personalità*, cit., 405 s.).

(85) Testualmente dalla recente Trib. Milano, 22 dicembre 2021, in *www.giurisprudenzadelleimprese.it*; cui *adde* Trib. Torino, 23 luglio 2019, *ibidem*.

terzi la tutela generale inibitoria prevista dagli artt. 7 e 10 c.c. (86), sempre salvo il diritto al risarcimento dei danni ai sensi dell'art. 2043 c.c. in assenza di inadempimento di eventuali pattuizioni contrattuali; se la lesione sia prodotta da violazione dell'identità perpetrata via *web* o *social network*, possono anche ricorrere i presupposti per pretendere la rettifica ai sensi dell'art. 8, legge 8 febbraio 1948, n. 47 (87).

Quanto finora esposto in ordine alla commerciabilità dell'identità dell'organizzazione d'impresa suggerisce di pervenire alla medesima conclusione anche per l'identità digitale di quest'ultima. Senza dubbio, sono trasferibili a terzi (i diritti su) *domain names*, *usernames*, *nicknames* e *alias*, così come lo sono (i diritti su) ditta, insegna e nome sociale. Ma, al di là della possibilità di cedere questi segni e così di agevolare il trasferimento ad altri di elementi di individuazione dell'organizzazione d'impresa (normalmente, monetizzandone il valore), l'aspirazione di ciascun imprenditore a vedersi fare concorrenza soltanto con modalità corrette, quella dei clienti a non essere ingannati sul titolare dell'impresa fornitrice, quella di tutti a conoscere chi operi nel mercato ed certo numero di informazioni veritiere che lo riguardino segnano il confine di legittimità della cessione d'identità — anche digitale — dell'organizzazione d'impresa.

5.9. Qualche considerazione sull'identità digitale degli *influencers* (e dei *content creators*): a cavallo del confine tra diritto privato e diritto dell'impresa

Prima di concludere questo studio è opportuno dedicare qualche osservazione a proposito del ruolo che l'identità di un'organizzazione d'impresa, come ricostruita nelle pagine che precedono, può giocare nel mercato digitale rispetto ad una serie di situazioni tipiche dello stesso. Un primo insieme di questioni sono poste da quelle figure che spesso stanno a cavallo del confine tra il non-imprenditore, il lavoratore autonomo e l'imprenditore (88). Si tratta dei cc.dd. *influencers* (89) ovvero di coloro che, normal-

(86) In ordine al carattere generale della tutela civile prevista per i singoli diritti della personalità e, tra questi, del diritto all'identità si segnalano A. De Cupis, *I diritti della personalità*, cit., 413.

(87) A riguardo M. Dogliotti, *Diritto all'identità personale, garanzia di rettifica e modi di tutela*, in *Giust. civ.*, 1981, I, 632 ss.; A. De Cupis, *I diritti della personalità*, cit., 413.

(88) Nel senso che sarebbe imprenditore — secondo Trib. Torino, 7 luglio 2011, in *Foro It.*, 2013, I — chi "avvia i contatti e calamita le amicizie virtuali di un gruppo costituito all'interno del *social network Facebook*". Secondo un'indagine della Commissione UE, i cui risultati sono stati resi noti il 14 febbraio 2024, il 97% dei *post* degli *influencers* ha "contenuto commerciale", ma soltanto il 78% degli *influencer* esercitano "attività commerciale" e, ancor

mente mediante profili *social* (90), presentano problemi/soluzioni d'interesse, opportunità di acquisto/investimento, forniscono notizie su ogni genere di tema, diventano personaggi di successo, popolari nei *social network* e, quindi, in grado di influire sui comportamenti e sulle scelte di un determinato pubblico. Ovviamente, ci sono *influencers* con un vasto seguito di *followers*, mentre altri hanno un più limitato impatto sul pubblico (i cc.dd. *micro-influencers* e *nano-influencers*) (91), ma, ciò nonostante, possono rappresentare comunque un canale comunicativo per raggiungere gruppi d'interesse (*target*). Perciò, le imprese si stanno sempre più avvalendo della collaborazione di *influencers* nell'attività di comunicazione per migliorare il proprio grado di penetrazione nel mercato digitale, sfruttando anche la presa di costoro sui rispettivi *followers*. Il punto è la tecnica di approccio dell'*influencer* ai propri *followers*, che è spesso caratterizzata dall'instaurazione di un rapporto comunicativo incentrato sulla compartecipazione dei secondi alle esperienze di vita del primo, una compartecipazione che, come tale, si fonda sull'interattività potenziale attraverso i canali *social* e, per lo più, su un'esposizione diretta di "esperienze di vita" — più o meno genuine (92) — dell'*influencer* condivise con i propri *followers* attraverso i *social media* di riferimento. Questo genera normalmente — e sta proprio in ciò la "forza"

---

meno, il 36% sono registrati come "commercianti a livello nazionale" (v. il comunicato stampa della Commissione UE reperibile all'indirizzo https://ec.europa.eu/commission/presscorner/detail/en/ip_24_708). Il problema qualificatorio va affrontato, innanzi tutto, in coordinamento tra diritto delle persone, diritto del lavoro e diritto commerciale ed in questa (amplissima) prospettiva ci si limita a segnalare, anche per ulteriori riferimenti, qualche saggio recente (v. E. Raimondi, *Il lavoro nelle piattaforme digitali e il problema della qualificazione della fattispecie*, in *LLI*, 2019, 2, 69; P. Iervolino, *Sulla qualificazione del rapporto di lavoro degli* influencers, *ivi*, 2021, 2, 34 ss.; L. Torsello, *Il lavoro degli* influencers*: percorsi di tutela*, *ibidem*, 58).

(89) Nella pratica si tende a distinguere tra *influencers* e *content creators* in funzione di mettere in luce l'imputazione della produzione di contenuti originali. I primi, anche se spesso lo fanno, non necessariamente producono contenuti originari, ricorrendo ad altri "creatori"; i secondi, non necessariamente si rivolgono direttamente al pubblico a mezzo di *social networks*, ma non è escluso che lo facciano effettivamente. Tuttavia, le due attività (produzione di contenuti e diffusione via *social network*) spesso si cumulano in capo al medesimo soggetto (v. D. Biondini-B. Lomaglio, Influencer Marketing*: tra diritto e pratiche*, Milano, 2023, 4 s.). Di seguito nel testo il riferimento agli *influencers* prescinde dal fatto che essi creino effettivamente i contenuti, ma non esclude che lo facciano.

(90) Normalmente, operano attraverso *accounts* attivati nei *social media* (*Instragram*, *TikTok*, *Youtube*, ecc.) presentandosi sotto *usernames*, *nicknames* o *alias* che talvolta corrispondono con il loro nome civile o commerciale, talaltra sono di fantasia (v. S. Landini, *Identità digitale tra tutela della persona e proprietà intellettuale*, cit., 190).

(91) V. D. Biondini-B. Lomaglio, Influencer Marketing*: tra diritto e pratiche*, cit., 9.

(92) Cfr. D. Biondini-B. Lomaglio, Influencer Marketing*: tra diritto e pratiche*, cit., 8.

dell'*influencer marketing* — una commistione tra "personale" e "commerciale", che gioca — come accade in generale per la comunicazione pubblicitaria — sul tendenziale abbassamento delle difese del *target* rispetto ad un'offerta "commerciale" proposta in modo accattivante per le ragioni più disparate; in pratica, il *follower* si ritrova più propenso a far proprio il suggerimento dell'*influencer*, quando vi sia l'evocazione di "esperienze di vita" di natura "personale" di quest'ultimo che è considerato una modello cui ispirarsi, talora quasi un *maitre-à-penser* che detta il gusto e le scelte altrui (93).

Il carattere abituale ed economico dell'attività di molti *influencers* giustifica la loro riconduzione alla categoria dell'imprenditore, quando abbiano creato quel minimo di organizzazione idoneo ad integrare tutti i requisiti di cui all'art. 2082 c.c. (94). Quindi, può essere imprenditore chi incarica un *influencer*, ma può essere tale anche l'*influencer* medesimo.

Volendo qui restringere il campo alle tematiche che riguardano gli *influencers* più organizzati — e, perciò, normalmente anche più "influenti" — mi limiterò ad esaminare qualche questione riguardante gli *influencers*-imprenditori. Il problema, che il modo di proporsi al pubblico degli *influencers* più frequentemente pone, attiene di certo alla qualificazione della loro attività, onde stabilire se sia commerciale oppure privata (95). L'attrattività dell'*influencer* e l'attitudine a determinare le scelte del c.d. *target* è spesso correlata alla capacità/abilità di ciascun *influencer* di presentarsi — almeno per certi aspetti — somigliante al proprio *target* e/o di apparire per quest'ultimo, appunto, come un modello al quale potersi ispirare; dunque, qualcuno

---

(93) Che il successo del ricorso all'*influencer marketing* si giochi sul piano della credibilità dell'*influencer* rispetto alla promozione di un contenuto per la sua prossimità ai propri *followers* è dato assodato che ha condotto negli ultimi anni l'AGCM ad aprire una pluralità di procedimenti in ragione dell'occultamento di attività di promozione pubblicitaria (v.; in dottrina C. Goanta-S. Ranchordás, *The regulation of social media influencers: an introduction*, in *The Regulation of Social Media Influencers*, a cura di C. Goanta e S. Ranchordás, Cheltenham, 2020, 5 mettono in evidenza come i "*social media influencers play the role of a trusted individual in the online community in a certain way; they are trusted because they present themselves as authentic, approachable and relatable individuals*").

(94) Analogamente L. Torsello, *Il lavoro degli* influencers*: percorsi di tutela*, cit., 58. Può non essere agevole stabilire se un *influencer* stia promuovendo commercialmente un prodotto o un servizio e, quindi, se stia agendo come persona o come impresa (v. per un riferimento alle difficoltà di qualificazione C. Goanta-S. Ranchordás, *The regulation of social media influencers: an introduction*, cit., 9, sebbene i risultati esposti dalla Commissione UE e citati alla nota 88 potrebbero suggerire di pervenire a conclusioni diverse).

(95) Non stupiscono, anzi confermano proprio il problema attinente al tentativo — più o meno colpevole — di tacere o, peggio, dissimulare il carattere di promozione commerciale del messaggio veicolato con *posts*, *reels*, ecc. i risultati della già citata indagine della Commissione UE.

di "meglio", ma comunque "apparentemente emulabile" dal destinatario del messaggio. In sostanza, la forza dell'*influencer* sta nell'impressione di prossimità che ingenera in ciascuno dei suoi *followers*, ma proprio questa può rappresentare un problema, perché implica un rischio di sviamento in ordine al reale oggetto della comunicazione dell'*influencer* ed alla finalità della medesima. In questo "gioco" a rischio l'identità dell'*influencer* costituisce elemento centrale della comunicazione, perché proprio le caratteristiche dell'*influencer* sono lo strumento di creazione e sfruttamento della "prossimità". Da un lato, pertanto, l'identità (necessariamente) digitale dell'*influencer* va tutelata come mezzo di realizzazione dell'attività di *marketing* e, quindi, come strumento di esercizio dell'impresa (se in capo all'*influencer* ricorrano i requisiti di cui all'art. 2082 cit.); dall'altro, quell'identità deve essere rappresentata in tutta la sua realtà (e verità), senza l'occultamento delle finalità commerciali che potrebbero non solo sviare il *follower* inconsapevole, ma anche costituire mezzo di concorrenza sleale. Dunque, mentre per quanto attiene al primo profilo possono semplicemente richiamarsi le osservazioni svolte nei paragrafi 5.6 e 5.7 in tema di protezione dell'identità dell'organizzazione d'impresa, di certo applicabili pure all'identità dell'*influencer*-imprenditore, un cenno di approfondimento merita il profilo del rischio di sviamento dei *followers* anche nel gioco concorrenziale.

Si è messo in luce che nel mercato digitale vale la regola propria del mercato "generale" secondo la quale non è ammissibile — perché qualificabile come condotta contraria alla correttezza professionale — né l'uso di profili *fake*, né, tantomeno, quello di profili ingannevoli. Ciò traslato sul piano della peculiarità degli *influencers*, più sopra menzionata e costituita dallo sfruttamento della "prossimità", comporta che non sia lecito non solo non rendere palese al *follower* il carattere promozionale di determinate azioni — quali *posts*, *reels*, ecc. — ma anche la costruzione e il mantenimento di un'identità non chiaramente commerciale, quando l'*account* sia utilizzato prevalentemente a tal fine. Lo impone, oltre alla disciplina della concorrenza, il principio di verità che sta alla base della tutela dell'identità, alla quale si ha diritto, ma della quale non si può abusare. Concludendo, sono illegittime quelle forme di comunicazione degli *influencers* che, facendo leva sulla loro persona come presenza nel mondo virtuale, tendano a far credere di non svolgere, in realtà, attività di natura commerciale (96). Ciò che è chiaro è che

(96) Sebbene il problema sia solo analogo, perché relativo alle regole sulle modalità della pubblicità e non alla verità in ordine all'identità dell'*influencer* in termini di tipologia delle condotte che contribuiscono a delineare la personalità (e, quindi, l'identità) del soggetto, è utile ricordare i recenti provvedimenti di chiusura di istruttorie da parte dell'AGCM in materia di *influencer marketing* soltanto dopo l'assunzione di impegni — da parte degli

non è ammissibile l'invocazione di una sorta di scriminante di illustrare — con *posts*, *reels*, ecc. — semplicemente momenti della propria esistenza personale per sfuggire alle regole di governo del mercato, allorché si operi professionalmente nel mercato stesso (97). Dunque, l'esposizione del proprio "privato" da parte degli *influencers* non consente loro di sfuggire alle regole dell'impresa; anzi, il tentativo di occultare attraverso quell'esposizione il carattere commerciale dell'attività promozionale svolta può essere ragione di connotazione in termini di maggiore illiceità di condotte a prima vista del tutto riconducibili alla sfera privata. Peraltro, nelle ipotesi in cui l'attività effettivamente promozionale sia "mascherata" sotto le vesti dell'esposizione della vita privata dell'*influencer*, ma diretta a promuovere il prodotto o il servizio di un'impresa, possono presentarsi le condizioni per imputare/estendere eventuali responsabilità anche a quest'ultima (98).

5.10. *Segue*: il caso dei *virtual influencers*

Il discorso sugli *influencers* non sarebbe completo se non si dedicasse attenzione anche al caso di quelli "virtuali" e, cioè, di quei personaggi di fantasia che sembrano persone e ne simulano i comportamenti potenziali. Sono il frutto della convergenza tra diverse tecnologie e discipline, come l'intelligenza artificiale, la *computer* grafica, la realtà aumentata, il *motion capture* e il *machine learning* (99). Sono presenti su canali *social* su *Instagram*,

---

influencers e dei loro committenti — tesi a ristabilire condizioni di trasparenza nel mercato (v., tra le altre quelle relative ai casi *Alitalia* e *Barilla*, AGCM, *Insanity Page-Pubblicità occulta Barilla*, Provvedimento n. 28167, in *Boll. AGCM*, 16 marzo 2020, 124 ss.; AGCM, *Aeffe-Alitalia*, Provvedimento n. 27787, in *Boll. AGCM*, 10 giugno 2019, 12 ss.). Peraltro, talune piattaforme, a prescindere da imposizioni normative, includono nelle proprie condizioni generali di prestazione dei servizi digitali il divieto, a carico degli *influencers*, di adottare pratiche di *marketing* irresponsabili o, comunque, in contrasto con taluni canoni etici (v. F. Pflücke, *The Case for Increased Responsibility and Liability of Brands in Social Media Influencer Marketing*, in *J. Eur. Cons. Mark. Law*, 2024, 6).

(97) Un tale tentativo è stato respinto, chiaramente, da Trib. Genova, 4 febbraio 2020, reperibile all'indirizzo https://www.dekuzu.com/dl/docs/Ferrari-v-Phillip-Plein.pdf e comm entata da G. Cassano, *Quanto l'influencer non può fare brumbrum. A proposito dell'illecito uso del marchio altrui*, reperibile all'indirizzo https://dirittodiinternet.it/quanto-linfluencer-non-puo-brumbrum-proposito-dellillecito-uso-del-marchio-altrui-tribunale-genova-4-febbraio-2020/.

(98) In tema di coinvolgimento della responsabilità del committente v. F. Pflücke, *The Case for Increased Responsibility and Liability of Brands in Social Media Influencer Marketing*, cit., 8.

(99) In tal senso L. Tedesco, *La carica degli influencer virtuali: che cosa fanno e quali sono i più famosi*, in *Wired*, 2 dicembre 2023, reperibile all'indirizzo https://www.wired.it/gallery/influencer-virtuali/.

YouTube, *TikTok* o *Twitch* dove pubblicano foto, video, *stories*, *live*, *reels*, ecc. e sviluppano "una propria identità, una storia, una personalità, uno stile e valori che li rendono unici e riconoscibili" (100). Ci sono *influencers* virtuali creati da imprese-persone giuridiche (101) ed altri anche da pubbliche amministrazioni (102), che sono più seguiti di tante persone "reali". L'utilizzo di *virtual influencers* è favorito dal fatto che non hanno limiti fisici o temporali e, quindi, possono anche "lavorare" 24 ore su 24, 7 giorni su 7. Si prestano a promuovere i prodotti in modo creativo e coinvolgente su molteplici piattaforme e canali, risultando più adatti a raggiungere un pubblico internazionale senza doversi preoccupare delle barriere linguistiche o culturali, proprio grazie alla loro natura fittizia. A differenza degli *influencers* reali, possono essere personalizzati in modo da rispecchiare perfettamente i valori e lo stile dell'impresa committente o titolare dei diritti esclusivi su di essi, permettendo di creare una forte connessione con il pubblico di riferimento (103) e di evitare altresì eventuali scandali — e, quindi, il conseguente

(100) V., ancora, L. Tedesco, *La carica degli influencer virtuali: che cosa fanno e quali sono i più famosi*, in *Wired*, cit. Esempi ne sono *Nobody Sausage* con oltre 21,4 milioni di *followers* su *TikTok*, *Lu of Magalu* creata nel 2009 per promuovere *iBlogTV* e con oltre 6,8 milioni di *followers* oggi su *Instagram*, *Lil Miquela* con oltre 2,6 milioni, *Leya Love* con oltre 560 mila. Va segnalata, poi, la *virtual influencer* italiana *Rebecca Galani*, definita nel profilo *Instagram* come "Modella Virtuale AI", la quale si caratterizza per la capacità di rispondere ai messaggi dei suoi *followers* e, infatti, è stata intervistata sfruttando la sua abilità *Gpt* (v. D. Polidoro, *Intervista alla prima* influencer *virtuale italiana*, in *Wired*, 6 gennaio 2024, reperibile all'indirizzo https://www.wired.it/article/prima-ai-influencer-italiana-rebecca-galani/).

(101) Tant'è vero che la nuova legge francese n. 2023-451 del 9 giugno 2023 "*visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux*" si estende anche alle persone giuridiche — cfr. l'art. 1 — che si servono di *virtual influencers* [a riguardo E. Calzolaio, *L'attività pubblicitaria dell'*influencer *nel diritto francese* (Loi *n. 451 del 9 giugno 2023)*, in *Dir. inf. inform.*, 2023, 914].

(102) È il caso dell'avatar della "Nuova Venere" con il profilo @*venereitalia23*, realizzato dal Governo italiano, per la campagna "*Italia: Open to Meraviglia*" (per il sito ufficiale si rinvia all'indirizzo https://www.ministeroturismo.gov.it/italia-open-to-meraviglia/ e per la presentazione si veda il filmato reperibile all'indirizzo https://www.youtube.com/watch?v=4zwXqqSPEOI&t=45s).

(103) V. D. Biondini-B. Lomaglio, Influencer Marketing*: tra diritto e pratiche*, cit., 13 e 170 s.; M. Piccinali, *Influencers e virtual social media*, in *Il metaverso. Modelli giuridici e operativi*, Milano, 2023, 57 s. In linea di principio si è appurato che i *virtual influencers* hanno gli stessi effetti positivi degli *influencer* umani (V.L. Thomas-K. Fowler, *Close encounters of the AI kind: Use of AI influencers as brand endorsers*, in *J. Adv.*, 2021, 11 ss.; cui *adde* C. Lou-S.T.J. Kiew-T. Chen-T.Y.M. Lee-J.E.C. Ong-Z. Phua, *Authentically fake? How consumers respond to the influence of virtual influencers*, in *J. Adv.*, 2023, 540 ss.). Peraltro, si deve segnalare che v'è chi ha osservato che i *followers* su *Instagram* hanno reazioni tendenzialmente negative se l'*influencer* virtuale si presenta come eccessivamente indistinguibile da un essere umano, ma con la percezione che resti un prodotto digitale (v. J. Arsenyan-A. Mirowska, *Almost human?*

pregiudizio reputazionale — legati a condotte delle persone fisiche non in linea con gli *standard* etici attesi dal pubblico (104). Chiaramente, la creazione di un/una *virtual influencer* è uno strumento che molto si presta ad operare nel *metaverso* (105).

Pertanto, il/la *virtual influencer* non è un soggetto, una persona, ma appunto uno "strumento" creato per interagire con i *followers*. È basato su un *software*, nel senso che è il risultato del funzionamento di un *software* (106), e, come tale, non ha una personalità propria. Si tratta di un prodotto; tuttavia, considerato che simula le persone umane e delinea delle caratteristiche analoghe a quelle della personalità pur difettando di quest'ultima, i tratti peculiari di ciascuna creazione, che esprime anche un dinamismo, sono frutto di investimenti di risorse imprenditoriali e meritano tutela nel quadro della protezione del valore oggettivo d'impresa del quale si va discorrendo sin dal primo paragrafo di questo lavoro.

Orbene, qualificandosi come un prodotto, una creazione, d'impresa ed a prescindere dalla tutela accordata al *software*, il (creatore del/)la *virtual influencer* può godere della tutela autorale e beneficia di certo della protezione contro la concorrenza sleale e, quindi, contro l'imitazione servile, l'appropriazione di pregi da parte di chi utilizzi un altro *virtual influencer* che per profilo identitario potrebbe ingenerare confusione nel pubblico non riguardo alla riconduzione della proposta commerciale ad una persona-*influencer*, che non c'è, quanto, piuttosto, ad un imprenditore proprietario o titolare di licenza d'uso del *software* generatore del *virtual influencer* obbiettivo dell'attività confusoria (107).

In sintesi, le caratteristiche della personalità virtuale, che corrispondono all'identità virtuale di questa tipologia di *influencers*, sono protette non come elementi di una personalità, ma dalle norme sui "segni distintivi atti ad

---

A comparative case study on the social media presence of virtual influencers, in *Intl' J. Human-Computer Studies*, 2021, 155).

(104) V. M. Mrad-Z. Ramadan-L. Issam Nasr, *Computer-generated influencers: the rise of digital personalities*, in *Mark. Intell. Planning*, 2022, 1; K. Jiang-J. Zheng-S. Luo, *Green power of virtual influencer: The role of virtual influencer image, emotional appeal, and product involvement*, in, in *J. Retail. Cons. Services*, 2024, 1; M.H.E.E. Gerrath-H. Olya-Z. Shah-H. Li, *Virtual influencers and pro-environmental causes: The roles of message warmth and trust in experts*, in *J. Bus. Res.*. 2024, 1.

(105) Sul punto si rinvia, oltre che a M. Piccinali, *Influencers e virtual social media*, cit., 58, all'ultimo paragrafo di questo contributo.

(106) Che si tratti di *software* proprietario o in licenza d'uso è confermato da M. Piccinali, *Influencers e virtual social media*, cit., 58.

(107) A proposito dell'imputazione della responsabilità per atti compiuti dal *virtual influencer*, v. D. Biondini-B. Lomaglio, Influencer Marketing*: tra diritto e pratiche*, cit., 180.

identificare i prodotti o i servizi di un'impresa" (108) o per via di privativa in quanto dotate del necessario gradiente di creatività richiesto dalla l. aut. e, comunque, contro la copia grossolana ai sensi del Codice civile. Ma v'è pure un rovescio della medaglia nel senso che la simulazione dell'identità umana, che idealmente va in parallelo con la simulazione dell'intelligenza umana tipica dell'intelligenza artificiale, pone problemi sul piano pubblicitario e di trasparenza in ordine alla provenienza del messaggio. Da un lato, anche l'attività a mezzo di *virtual influencer* simulando l'esposizione di una "vita privata" (109) che, in realtà, neppure esiste, non consente a chi se ne serva di sfuggire alle regole dell'impresa (110) e ciò ancor più che nel caso degli *influencers*-persone "reali"; dall'altro, ai *virtual influencers* si devono applicare le prescrizioni che impongono agli utilizzatori di rendere palese agli *end-users* che sono in contatto con un *bot*, per quanto sofisticato possa essere (111).

5.11. Il problema dell'identità digitale dell'utilizzatore commerciale dei *marketplaces*

Nelle ultime due decadi, con lo sviluppo dei nuovi modelli di intermediazione *online*, abbiamo assistito ad una rivoluzione rispetto al paradigma tradizionale secondo il quale il "produttore-venditore" è soggetto forte nelle operazioni di mercato, mentre intermediari e clienti, spesso, sono soggetti deboli (o meno forti), ma comunque meritevoli di tutela contro pratiche abusive del primo. Di quell'approccio tradizionale sono prova, tra le altre, le regolamentazioni delle condizioni generali di contratto, di protezione del consumatore, dell'agente di commercio, del cliente bancario, nonché di limitazione delle obbligazioni fideiussorie *omnibus*, ecc. Per quanto quest'approccio mantenga un'utilità in determinati settori economici, appunto, tradizionali, non è così in *internet*. Infatti, la dimensione assunta, ma soprattutto la centralità nelle contrattazioni di mercato ormai ravvisabile in capo a taluni operatori (*Amazon*, *Ebay*, per citare i più significativi *marketplaces*) comportano il sostanziale capovolgimento di quel paradigma assegnando a costoro la

(108) Così, D. Biondini-B. Lomaglio, Influencer Marketing*: tra diritto e pratiche*, cit., 180. Nel medesimo senso il *decisum* di US District Court, Northern District California, 9 marzo 2023, *Roblox Corp.* v. *Wowwee Group Ltd.*, reperibile all'indirizzo https://www.loeb-.com/en/insights/publications/2023/03/roblox-corporation-v-wowwee-group-limited.

(109) In proposito R. Lanzo, *L'*influencer marketing *nell'era del Metaverso*, in *Metaverso*, a cura di G. Cassano e G. Scorza, Pisa, 2023, 247.

(110) V. M. Piccinali, *Influencers e virtual social media*, cit., 61.

(111) V. R. Lanzo, *L'*influencer marketing *nell'era del Metaverso*, cit., 252; M. Piccinali, *Influencers e virtual social media*, cit., 61.

posizione di contraente forte rispetto al quale anche il produttore, oltre al cliente, finisce per essere meritevole di una protezione a contemperamento di una debolezza negoziale strutturale (112).

Di certo, in questa sede non è opportuno un ragionamento in termini generali e mi limito a qualche osservazione su aspetti connessi con l'identità del produttore-venditore e la sua tutela. Molta parte dell'*e-commerce* passa oggi attraverso i *marketplaces* e taluni di questi (113) si pongono spesso in concorrenza con coloro che si avvalgono di essi come canale distributivo, i cc.dd. utenti commerciali (114). Ciò pone una serie di problemi e, tra questi, in particolare quelli di natura concorrenziale sia sul piano della rigidità delle forme di presentazione dell'offerta da parte dell'utente commerciale, che dell'offuscamento della sua identificazione soggettiva come venditore nel *marketplace* (115). Vediamoli distintamente, sebbene non manchino profili di collegamento e di comunanza.

---

(112) Relativamente al conflitto di interessi tra piattaforma e utente, nonché alla conseguente concentrazione di vantaggi in capo alla prima ai danni dei secondii L. KHAN, *The Separation of Platforms and Commerce*, in *Col. Law Rev*., 2019, 973 ss.; cui *adde* R.J. GILBERT, *Separation: A Cure for Abuse of Platform Dominance?*, in *Inform. Econ. Pol.*, 2021, 100876.

(113) *Amazon*, probabilmente, rappresenta il caso più evidente e, comunque, le modalità di azione di *Amazon* costituiscono senza dubbio un interessante ipotesi di studio in funzione di valutare le problematiche identitarie e concorrenziali che possono presentarsi nei "grandi" *marketplaces*, modalità che, allo stato, non paiono tutte specificamente affrontate a livello normativo neppure con il *Digital Market Act* (Regolamento UE/2022/1925). Tuttavia, con l'art. 6, paragrafo 2, comma 1, il legislatore europeo ha affrontato almeno uno dei temi di concorrenza sleale che l'attività dei *marketplaces* solleva e, cioè, quello dell'utilizzo di informazioni non pubbliche per far concorrenza agli utenti commerciali, così tendendo a neutralizzare la posizione di privilegio informativo che il *marketplace* potrebbe avere rispetto agli utenti commerciali.

(114) La definizione si trova, ad esempio, nel Regolamento UE/2019/1150, che promuove per gli "utenti commerciali" dei servizi di intermediazione *online* equità e trasparenza da parte delle relative piattaforme, nonché nel *Digital Market Act*. Tali sarebbero coloro che sarebbero riconducibili al concetto di "*privato che agisce nell'ambito delle proprie attività commerciali o professionali o una persona giuridica che offre beni o servizi ai consumatori tramite servizi di intermediazione online per fini legati alla sua attività commerciale, imprenditoriale, artigianale o professionale*" (art. 1, n. 1, Reg. n. 1150) o di "*qualsiasi persona fisica o giuridica che, nell'ambito delle proprie attività commerciali o professionali, utilizza i servizi di piattaforma di base ai fini della fornitura di beni o servizi agli utenti finali o nello svolgimento di tale attività*" (art. 2, n. 21, *Digital Market Act*).

(115) Il novero dei problemi potenziali concorrenziali è, comunque, molto più ampio di quello delineato nel testo perché — ad esempio — critico è anche il sistema di indirizzo delle scelte tra le proposte di prodotti da parte dell'*end user*, posto che il gestore del *marketplace* può utilizzare molte "leve" per orientare quelle scelte (per qualche indicazione v. C. FARRONATO-A. FRADKIN-A. HAGIU-D. LOMAX, *Understanding the Tradeoffs of the Amazon Antitrust Case*, in *Harv. Bus. Rev.*, 11 gennaio 2024, reperibile all'indirizzo https://hbr.org/2024/01/understanding-the-tradeoffs-of-the-amazon-antitrust-case).

Almeno in apparenza, per ragioni di standardizzazione dei contenuti tese ad agevolare più ampie comparazioni tra le offerte commerciali, il singolo utente commerciale si trova ad accettare, tra le altre, due imposizioni: da un lato, se offre un prodotto non ancora censito nel *marketplace*, deve redigere una scheda di presentazione e costruire l'offerta secondo parametri e vincoli predefiniti dal *marketplace*, che si concretizzano in una scheda-prodotto, perché, diversamente, quest'ultimo rifiuta di consentire l'utilizzo della propria piattaforma; dall'altro, se offre un prodotto già censito, deve adeguarsi alla scheda-prodotto preesistente — cioè, predisposta da altri utenti commerciali — ed utilizzare quest'ultima. Al di là di altre problematiche che la regolamentazione contrattuale pone rispetto all'abdicazione di diritti di proprietà industriale ed intellettuale a favore del *marketplace* (116), tutto ciò non solo elide le diversità di presentazione e di offerta dei prodotti nel *marketplace* (117), ma impedisce di beneficiare — sul piano dell'identità dell'impresa — delle diverse caratterizzazioni delle presentazioni e delle offerte, omologandole agli occhi del pubblico e, quindi, del corpo sociale presso il quale l'identità dovrebbe invece acquistare forma e costituire in pari misura valore proprio. Chiaramente, nella misura in cui il diritto all'identità è ritenuto disponibile, la scelta dell'utente commerciale di tendere ad annichilirla è accettabile da parte dell'ordinamento, salvo che non entrino in gioco i superiori interessi dell'ordinamento stesso sottesi alla disciplina *antitrust* (e i relativi rimedi), a quella che pone un argine all'abuso di dipendenza economica e non solo. Infatti, pur a fronte del carattere tendenzialmente disponibile del diritto sull'identità digitale alla cui creazione un soggetto — almeno in astratto — ben potrebbe rinunciare stando sempre *offline*, imperative esigenze di tutela degli *end-users* (consumatori o meno) impongono la riconoscibilità dell'utente commerciale e la sua non-confondibilità con terzi in una prospettiva sia di generale trasparenza nel mercato *online*, che di adeguata individuabilità della controparte contrattuale. In altre

(116) Infatti, i contratti per adesione al servizio di *marketplace* stabiliscono — ad esempio — che al venditore si applichi la regola secondo la quale "*you grant us a royalty-free, non-exclusive, worldwide, perpetual, irrevocable right and license to use, reproduce, perform, display, distribute, adapt, modify, re-format, create derivative works of, and otherwise commercially or non-commercially exploit in any manner, any and all of Your Materials, and to sublicense the foregoing rights to our Affiliates and operators of Amazon Associated Properties*" (così l'art. 4 - *Licence* dell'*Amazon Services Business Solutions Agreement - General Terms*).

(117) V. in proposito la *Guida per principianti alla vendita su Amazon* reperibile all'indirizzo https://sell.amazon.it/vendere-online/guida-per-principianti, nella quale, alla sezione "Pubblicazione della prima offerta", si chiarisce la necessità di provvedere all'"associazione ad un'offerta esistente", quando un altro utente commerciale già offra il medesimo prodotto nel *marketplace*.

parole, l'esigenza di verità sottostante all'identità richiede l'effettività del più volte menzionato *principium individuationis*.

Dalla prospettiva del predisponente la scheda-prodotto la possibilità che altri ad essa si rifacciano per promuovere e vendere il prodotto proprio pone un problema di pubblicità per agganciamento, mentre dall'opposta prospettiva del *new comer*, il quale è spinto ad avvalersi di quella medesima scheda-prodotto senza significative differenziazioni, la necessità di agganciamento reprime le potenzialità di vendita riconnettibili ad innovazioni della proposta commerciale. In altre parole, la standardizzazione tende all'omologazione delle offerte, anche se di prodotti non coincidenti, con la conseguenza che il gioco concorrenziale rischia di esaurirsi in un numero ben minore di variabili — quali prezzo, disponibilità del prodotto, rapidità della consegna, *rating* del fornitore nel *marketplace* e poche altre — con pregiudizio della concorrenza sulle caratteristiche e la qualità della merce. Quest'omologazione dell'offerta espone gli utenti commerciali al rischio di appiattimento delle reciproche differenze, incidendo negativamente sulla loro caratterizzazione individuale e, pertanto, sulla delineazione della loro identità dentro e fuori del *marketplace*. Nel contesto della disciplina della concorrenza sleale ciò è accettabile, in quanto frutto di una libera determinazione dell'utente commerciale, ma nella sola misura in cui non conduca ad un'eccessiva opacità rispetto alla necessità d'individuazione di ciascuno di essi. L'eventuale pregiudizio dell'interesse del pubblico alla trasparenza e, cioè, all'identificazione dell'utente commerciale/fornitore del prodotto è limite all'annacquamento degli elementi differenziali delle singole identità (118).

5.12. L'identità digitale dell'Intelligenza Artificiale che sia parte del ciclo produttivo

Oggi, anche al centro del dibattito giuridico si collocano numerose questioni relative all'intelligenza artificiale, che investono molti settori del diritto e, tra questi, quello dei diritti della personalità. La domanda è, dunque, se l'Intelligenza Artificiale (con le iniziali maiuscole) sia o meno "soggetto" e, conseguentemente, potenziale titolare di diritti. Così, si finisce per lambire la questione dell'identità digitale dell'Intelligenza Artificiale ed, in particolare, di quella che contribuisce a cicli di produzioni destinate al mercato; pertanto, è da chiedersi se debba essere riconosciuta un'identità

(118) Per quanto attiene al profilo della trasparenza in ordine alla persona del fornitore a beneficio dell'*end user* giova ricordare il disposto del già citato art. 7, decreto legislativo 9 aprile 2003, n. 70.

propria — e, cioè, autonoma — all'Intelligenza Artificiale che, ad esempio, concluda contratti nel mercato finanziario, apra linee di credito, scriva articoli di commento su quotidiani, individui potenziali acquirenti di beni o servizi, stabilisca limiti operativi ai clienti di una banca, interpreti un elettrocardiogramma patologico, formuli previsioni in ordine all'esito di una determinata attività, ecc. In tutte queste ipotesi, ed in altre ancora, l'Intelligenza Artificiale simula attività, che, quando compiute dalla persona umana, contribuirebbero a delinearne le caratteristiche e, perciò, l'identità. La pubblicazione di una serie di saggi e di commenti in quotidiani, riviste, *blog*, ecc. fa del redattore un giornalista o uno scrittore e, come tale, sarebbe identificato nel corpo sociale; analogamente potrebbe dirsi per chi giochi a scacchi, partecipando a tornei, vincendone anche attraverso l'elaborazione di nuove tattiche. Tutte queste attività possono essere svolte da parte dell'Intelligenza Artificiale e, talora, anche meglio della persona umana. Il quesito filosofico, prim'ancora che giuridico, è se, quando compiute dall'Intelligenza Artificiale, queste attività siano ancora imputabili alla persona umana. Il tema generale può, in definitiva, essere affrontato da due opposte prospettive: quella della persistente riconducibilità dell'atto alla persona umana, quando posto in essere dall'Intelligenza Artificiale; quella — alternativa — dell'imputabilità di detto atto all'Intelligenza Artificiale in quanto soggetto di diritto.

Premesso che questa non è la sede per risolvere una questione di portata così generale, un'osservazione, tuttavia, può essere fatta in relazione alla partecipazione dell'Intelligenza Artificiale al ciclo produttivo nella prospettiva dell'identità dell'impresa. La persona umana può essere fattore di produzione e i diritti rispetto alle prestazioni della persona umana acquisire rilievo nella valutazione di un'impresa. Posto che l'impresa è attività e che nell'ambito della sua organizzazione — come per le persone fisiche — l'Intelligenza Artificiale rileva per le prestazioni che fornisce, quest'ultima contribuisce a tracciare il profilo identitario dell'organizzazione d'impresa in modo non dissimile dalle persone che ne siano parte, poiché ne determina gli atti e, in tal modo, ne segna il profilo. Seguendo quest'impostazione, il dubbio in ordine alla soggettività dell'Intelligenza Artificiale non rileva ai fini della identificazione delle caratteristiche dell'organizzazione d'impresa, giocando un ruolo esclusivamente il risultato del prodotto dall'Intelligenza Artificiale. Quest'oggettivizzazione consente di affermare la rilevanza dell'Intelligenza Artificiale ai fini dell'identità dell'impresa e anche dell'identità digitale della stessa, se e quando la prima contribuisca ad un ciclo produttivo interamente digitale della seconda o a quella parte del suo ciclo produttivo che si svolga in "ambiente" digitale. *Providers* di servizi di *data mining online* o *chatbots* in grado di simulare conversazioni in un linguaggio simile a quello

umano o, ancora, *softwares* per la negoziazione algoritmica nel mercato finanziario o per la conclusione di *smart contracts* possono rispondere a questa funzione, connotando l'organizzazione dell'impresa. In quanto parte di questa, possono circolare assieme ad essa nel mercato e, se *softwares* e *databases* alla base dell'Intelligenza Artificiale sono oggetto di esclusive/privative, l'identità digitale dell'impresa ne risulta in pari misura — ma per via mediata — protetta; ciò in modo del tutto analogo a quello in cui nome commerciale, *domain names* ed altri diritti immateriali contribuiscono alla protezione di detta identità. In difetto di questa protezione "mediata", che impedisce a terzi di assumere le caratteristiche oggetto di privative, comunque la tutela dell'identità deve essere assicurata in via "diretta" all'impresa per quelle altre caratteristiche perché esse restano decisive nel tracciare il profilo identitario dell'organizzazione. Quella tutela va, in tal caso, ricercata nella disciplina più volte citata della concorrenza, che ne vieta la slealtà.

Considerata la rilevanza che rivestono oggi nel mercato digitale le attività di profilazione dei destinatari di prodotti e servizi compiute dai fornitori, un altro aspetto emergente è già stato analizzato da attenti studiosi. L'uso degli strumenti di profilazione può sconfinare nell'abuso tanto da tramutarsi da mezzo (legittimo) di individuazione dell'offerta più interessante e congeniale al cliente in mezzo (illecito) di limitazione della sua autonomia contrattuale, in quanto si risolve in una limitazione dell'accesso ad offerte alternative (119). In sostanza, gli strumenti di profilazione sono suscettibili di imprimere una connotazione del tutto conservativa all'identità digitale in contrasto con l'idea che, invece, questa sia destinata ad evolversi nel tempo in ragione anche delle condotte del titolare, senza che questi sia "imprigionato" un profilo identitario non più rispondente al vero (120). Il tema è stato studiato, come accennato, in ambito privatistico, ma ha rilievo anche nel gioco concorrenziale tra imprese, perché, se un cd. utente commerciale si trova categorizzato in un qualche modo — ad esempio — sotto il profilo del *rating*

(119) È il risultato identificato come *filter bubble* — e, cioè, della "bolla di filtraggio" — che "condanna" il profilato ad essere identificato più che altro con le caratteristiche manifestate nel passato e fino al momento presente, riducendo le possibilità di ostensione di nuove offerte disomogenee rispetto al profilo elaborato. Sul tema, affrontato in Italia soprattutto nella prospettiva della limitazione del pluralismo informativo e della libera formazione del consenso democratico, v. in ottica più orientata alla tutela della persona Mi. Bianca, *La* filter bubble *e il problema dell'identità digitale*, in *Riv. dir. media*, 2019, 2, 1 ss.

(120) Ciò non accade quando la profilazione finisca per tracciare un'identità reale, ma prima sconosciuta perché non "voluta" o ricostruibile solo attraverso informazioni non immediatamente evidenti (in proposito, ancora, Mi. Bianca, *La* filter bubble *e il problema dell'identità digitale*, cit., 12). Si tratta della identità cd. catturata, che, tuttavia, nella misura in cui esprima la verità delle caratteristiche del titolare — se lecitamente conosciute — non sembra presentare profili di illegittimità.

ESG, rischia di avere accesso più limitato ad opportunità di mercato. Chiaramente, il tutto dipende dalla dinamicità dell'algoritmo di valutazione, ma non si possono escludere abusi suscettibili di ledere — oltre alla reputazione commerciale dell'organizzazione d'impresa — pure la sua identità come attore nel mercato digitale. Ciò considerato, è ancora una volta alla disciplina del divieto di concorrenza sleale (ed alla sua attitudine ad includere nuove condotte concrete tra quelle precluse) alla quale, in particolare, ci si deve rifare per porre argine e rimedio agli abusi in questione. Ma non si può neppure escludere che talune situazioni più gravi, di abuso, possano trovare rimedio nel diritto *antitrust* o nel divieto di abuso di dipendenza economica.

5.13. Le (molto) prossime frontiere: l'identità digitale dell'organizzazione d'impresa nel *metaverso*

Il *metaverso*, inteso come spazio virtuale nel quale si entra con un *avatar* e si compiono azioni analoghe a quelle proprie del mondo reale, sta diventando anche mercato. Con i *metaversi* la rete non sarà più fatta di siti, ma di mondi digitali in 3D in cui si potrà immergere in tempo reale un numero potenzialmente illimitato di utenti. È vero che il *metaverso* è uno spazio virtuale — e, quindi, immaginario — dove ciò che accade simula quanto potrebbe accedere nel mondo reale; è pure verso che ciò che accade nel *metaverso* può avere effetti al di fuori di esso e, perciò, nel mondo reale (121). A differenza di *Second Life*, che include anche una prospettiva ludica (122), il *metaverso* è una dimensione virtuale della realtà effettiva, che, dunque, travalica il gioco e richiede una regolamentazione analoga a quella della dimensione fisica pur con gli adattamenti necessari alle peculiarità di quella virtuale.

---

(121) Lo ha ben messo in evidenza A.C. Nazzaro, *Le regole del* metaverso *tra legge esistente e progetti futuri*, reperibile all'indirizzo https://dirittodiinternet.it/wp-content/uploads/2022/12/Nazzaro-La-relazione.pdf, 2, la quale puntualizza che "il metaverso, nelle idee dei suoi sviluppatori, non è un mondo virtuale completamente avulso dalla realtà fisica, ma dovrebbe collegarsi ad essa creando quella che in gergo si chiama interconnessione"; analogamente V. Falce, *Metaverso, metaversi o realtà aumentata?*, reperibile all'indirizzo https://dirittodiinternet.it/wp-content/uploads/2022/12/Falce-La-relazione.pdf, 1.

(122) A *Second Life* s'è fatto riferimento anche alla precedente nota 66. Spesso è presentata come una piattaforma attraverso la quale condurre giochi di ruolo, sebbene all'interno di *Second Life* siano state sviluppate e persistano numerose attività economiche (in vari settori *fashion*, immobiliare, ecc.) tanto da rendere utile l'introduzione di una "moneta" virtuale (il *Linden $*) convertibile da e in valuta "reale" per regolare scambi effettivi.

Come in *internet*, nel *metaverso* si svolgono quindi attività sociali, economiche, individuali, collettive attraverso esperienze immersive (123) e ciò pone problemi di protezione giuridica sotto molti profili di rilievo anche per il diritto dell'impresa (violazione di segni distintivi, copia di opere intellettuali, inadempimento di obbligazioni contrattuali, frodi commerciali, ecc.). La connessione oggettiva tra *metaverso* e realtà fisica può, peraltro, determinare lesione dei diritti sia di chi vi operi, sia di chi non vi operi. Ora, a prescindere da altri problemi, è opportuno sottolineare che, proprio per quella connessione appena ricordata, chi svolge attività economica nel contesto virtuale del *metaverso* non può sfuggire alle regole applicabili nel mondo fisico (124). La natura virtuale dell'ambiente, già sperimentata con *internet*, non lo sottrae alle regole sulla tutela dei segni distintivi, della concorrenza, sulla trasparenza degli operatori verso il mercato, ecc. Come a suo tempo, dunque, sono state applicate alle attività *online* regole pensate e costruite per operare nel mondo *offline*, così pure si deve e si dovrà ragionare per il *metaverso* nella misura in cui non apparterrà ad una dimensione di gioco o fantasia, ma ad una reale analoga a quella fisica.

Concentrandoci sul profilo dell'identificazione dei soggetti nel *metaverso*, proprio per la connessione tra ambiente virtuale ed ambiente reale è necessario che essa sia possibile ed efficace per assicurare la verità di ciò che appare nel *metaverso* (125). Quindi, chi compra e chi vende nel *metaverso* deve essere identificabile e deve avere un'identità digitale spendibile nel *metaverso* stesso, un'identità digitale anche tutelata perché, come quella non-digitale, rappresenta un valore per il suo titolare ed una garanzia di identificabilità per i terzi. La regola dell'art. 7, d.lgs. n. 70 del 2003 deve applicarsi anche alle attività economiche svolte nel *metaverso* al fine di assicurare l'individuazione del fornitore del servizio virtuale. La disciplina tesa a garantire la lealtà della concorrenza parimenti si applica, così come vanno applicate le norme di tutela dei segni distintivi e dei diritti di autore onde consentire — da un lato — la protezione di chi operi fuori del *metaverso* da violazione dei suoi diritti nell'ambiente virtuale, ma — dall'altro — anche tutelare segni distintivi, creazioni e attività economiche presenti nel solo *metaverso*, assicurando così la salvaguardia degli investimenti fatti

(123) C'è chi ne ha sottolineato, molto criticamente, il prevalere della dimensione economica peraltro fortemente influenzata dalla disciplina contrattuale che l'utente accetta, quando decida di entrare nel *metaverso* (a riguardo recentemente, L. Di Maio, *L'art. 2 della Costituzione e il "Metaverso"*, in *Riv. dir. media*, 2023, 61).

(124) Conf. A.C. Nazzaro, *Le regole del* metaverso *tra legge esistente e progetti futuri*, cit., 2.

(125) Il tema è affrontato in M. Iaselli, *L'identità digitale nel* metaverso, in *Dem. dir. soc.*, 2023, 43 s.

per promuovere e condurre iniziative economiche in tale ambiente. Ciò posto, è evidente che quanto esposto nei paragrafi precedenti con riferimento all'identità digitale delle imprese può trovare piena applicazione anche con riferimento alle attività condotte da queste nel solo *metaverso*.

VI.
DA OPERAIO AD AVATAR? IDENTITÀ DIGITALE E PRIVACY DEL LAVORATORE

di *Giuseppe Sigillò Massara*

Sommario: 6.1. L'introduzione di nuove tecnologie nei luoghi di lavoro. — 6.2. L'identità digitale del lavoratore e prime prospettazioni di metaverso. — 6.3. I controlli a distanza del datore di lavoro e il diritto alla *privacy* del lavoratore. — 6.4. Alcune considerazioni conclusive.

6.1. L'introduzione di nuove tecnologie nei luoghi di lavoro

Non è un mistero che le nuove tecnologie rivestano un ruolo primario dei diversi ambiti della vita quotidiana, ivi incluso il rapporto di lavoro. Come nelle precedenti Rivoluzioni Industriali, le imprese hanno ormai assorbito il frutto del progresso tecnologico all'interno della loro organizzazione, nell'intento di aumentare la produttività, riducendo i costi e le dispersioni energetiche; a differenza delle precedenti Rivoluzioni Industriali, la Rivoluzione Digitale comporta un'interiorizzazione delle macchine non solo nei processi produttivi, ma anche nella gestione del personale, nell'organizzazione aziendale e nell'interazione con la clientela.

In particolare, è la seconda fase della Rivoluzione Digitale [1], caratterizzata dall'imporsi dei sistemi di intelligenza artificiale, dell'*internet of things* e dei *social media*, a portare ad una modifica nel modo di fare e concepire l'impresa, sempre più globalizzata, da un lato, e dematerializzata, d'altro.

---

[1] Si possono distinguere tre diverse fasi della Rivoluzione Digitale. Una prima, caratterizzata da mail e utilizzo di siti "immobili", con l'interazione individuale tra soggetto e macchina; una seconda, quella attuale, più dinamica e caratterizzata dal diffondersi dei social media, dall'intelligenza artificiale e dell'*internet of things* e *ubiquous computing*, che vede l'interazione tra soggetti mediata dal digitale, nonché un'interazione attiva tra persone e digitale e finanche un'interazione tra macchine (dietro impulso umano); una terza, potenzialmente caratterizzata dal diffondersi del metaverso e della realtà virtuale, su cui *infra*, con l'interazione tra persone e tra persone e cose realizzata nel mondo virtuale "come se" fosse realizzata nel mondo reale. In questo senso cfr., M. Ferraris, *La biblioteca di Abele*, AIB Studi, 2022, 62, 1, 105 ss.

Contrariamente a quanto potrebbe ritenersi di primo acchito, peraltro, tali mutamenti non riguardano una parte marginale di imprese di nuova generazione (come le piattaforme di lavoro) o caratterizzate da grandi dimensioni o diffusione transnazionale. Ad uno sguardo attento, difatti, non sfugge come anche le imprese di dimensioni più tradizionali e ridotte siano coinvolte dall'ondata di riunioni online, rassegna dei *social network* per selezionare il personale di nuova assunzione (2), sponsorizzazione sul web dei prodotti e servizi offerti, *mail-list* e archiviazione elettronica.

Non c'è, dunque, da stupirsi che l'introduzione di nuove tecnologie porti ad uno stravolgimento generalizzato del mercato del lavoro: come anticipato, lo stesso è avvenuto con le precedenti Rivoluzioni Industriali e, a ben vedere, si concretizza ogni qualvolta l'umanità venga in possesso di un nuovo strumento attraverso il quale agire nella realtà modificandola. Senza perdersi nell'elaborazione di futuri scenari distopici, tuttavia, occorre prendere atto che i riflessi della Rivoluzione Digitale nel mondo del lavoro si caratterizzano per alcune peculiarità di rilievo rispetto al passato.

Come rilevato da attenta dottrina (3), se gli anni del boom economico sono stati caratterizzati per una fiducia nel progresso e per la diffusione di opinioni che legavano l'introduzione delle nuove tecnologie a un miglioramento delle condizioni lavorative, ad esempio attraverso la sostituzione delle persone con le macchine per la realizzazione delle attività più usuranti o pericolose, la concretizzazione odierna di tali proiezioni non è sempre così rosea. Detto altrimenti, alla robotizzazione, "piattaformizzazione", diffusione del *machine learning* (4)*, crowdsourcing*, *social organization*, *internet of things*, *ubiquous computing* e in generale digitalizzazione del mercato del lavoro non sempre corrisponde una maggior tutela dei lavoratori, tanto da portare la citata dottrina a parlare di un « pericoloso percorso verso un vero e proprio baratro riguardo la sfera dei diritti della persona » (5). Permane e si rafforza, dunque, l'esigenza di tutelare questi ultimi, attraverso una legislazione che,

---

(2) Per la fase successiva all'assunzione, alcune informazioni possono giungere al datore di lavoro in maniera causale, anche per il tramite dei *social network*. Per un approfondimento in merito alla loro utilizzabilità, cfr. A. Topo, *Circolazione di informazioni, dati personali, profilazione e reputazione del lavoratore*, in C. Pisani, G. Proia, A. Topo, (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Torino, 2022, 389 ss.

(3) C. Romeo, *L'avatar, il metaverso e le nuove frontiere del lavoro: traguardo o recessione*, in *Il lavoro nella Giurisprudenza*, n. 5, 2023, 472 ss.

(4) Per un approfondimento in merito al rapporto tra *machine learning* e tutela della privacy dei lavoratori, cfr. A. Sitzia, B. Lopes, *Le più avanzate modalità di controllo sul lavoratore: machine learning e social media*, in C. Pisani, G. Proia, A. Topo, (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, cit., 358 ss.

(5) C. Romeo, *L'avatar, il metaverso e le nuove frontiere del lavoro: traguardo o recessione*, cit., la citazione è di p. 472.

anche nel mercato digitalizzato, continui a muoversi lungo le due direttrici tradizionali del sistema costituzionale volto alla realizzazione dell'eguaglianza sostanziale delle parti del rapporto di lavoro attraverso un riequilibrio dei poteri di forza: « quella della limitazione dei poteri imprenditoriali e della procedimentalizzazione-controllo del loro esercizio; nonché quella della valorizzazione dell'autonomia privata collettiva, sia in chiave di contro-potere sindacale, che in chiave di partecipazione negoziale alla produzione normativa e alla politica dei redditi » (6). Per chi indossa le lenti del giuslavorista non è difficile individuare il diritto alla dignità personale e la tutela della *privacy* del lavoratore tra quelli posti maggiormente a rischio e, dunque, più di altri bisognosi di tutela.

Ancora una volta, non è una novità la sussistenza di un nesso inscindibile tra evoluzione tecnologica e diritto alla *privacy* (7), non a caso sorto sul finire del '800 in risposta alla diffusione delle prime manifestazioni della potenzialità dell'informatica (anche in termini di diffusione di notizie personali, non più affidato al passa parola, ma alla ben più potente diffusione della stampa giornalistica) e delle banche dati di raccolta delle informazioni.

Al contempo, è di tutta evidenza che le potenzialità di raccolta, conservazione ed elaborazione dei dati sono sempre maggiori, sia in considerazione del numero sempre maggiore di interazioni tra persone e macchine (che tali interazioni registrano), sia in considerazione della potenza sempre maggiore di tali macchine (8).

A tale processo, non sfugge il mondo del lavoro, nell'ambito del quale la raccolta, conservazione ed elaborazione dei dati è sempre più presente, quale effetto collaterale di nuove modalità di esecuzione della prestazione (si pensi ai lavoratori agili) e di organizzazione e funzionamento dell'impresa (oramai inimmaginabile priva di strumenti di archiviazione online o collegamenti da remoto) ovvero quale espressa introduzione dell'intelligenza artificiale per la concretizzazione di moderne tecniche di gestione del personale e distribuzione del lavoro (con i sistemi di *management by algorithmics*, di *people*

(6) R. Pessi, A. D. Zumbo, *Mercato globale, nuove tecnologie e diritto del lavoro*, in *ADL*, vol. 2, 2021, 267 ss.

(7) Per la ideazione del diritto alla privacy, si veda S. D. Warren, L. D. Brandei, *The right to privacy*, in *Harvard Law Review*, 1890, 4, 193; per una qualificazione dello stesso, cfr. S. Scagliarini, *La riservatezza e i suoi limiti*, Roma, 2013.

(8) Non è un caso che negli ultimi anni, a livello globale, si è imposto il mercato dei Big Data, su cui cfr. C. Batini, *"Big Data". "Big Challenges and Big Concerns"*, in *Gnosis*, 2017, fasc. 2, 40 ss.; G. Buttarelli, *Le sfide del "Big Data" tra evoluzione tecnologica, etica e interessi collettivi*, in *Gnosis*, 2017, fasc. 2, 30 ss.; E. Dagnino, *"People Analytics": lavoro e tutele al tempo del "management" tramite "big data"*, in *LLI*, 2017, fasc. 1, 31 ss.

analytics practices e di *electronic performance monitoring* (9)) o strategie di tutela del patrimonio aziendale (come i software che, attraverso la scansione di mail e indirizzi web, operano per evitare la diffusione di virus o il compimento di *cybercrimes* a danno dell'impresa).

6.2. L'identità digitale del lavoratore e prime prospettazioni di metaverso

Dalla digitalizzazione dell'impresa, in breve, deriva la manipolazione di un quantitativo esponenziale di dati personali, afferenti a clienti e fornitori (anche potenziali), nonché, per quel che qui rileva, ai lavoratori.

Collezionati e ordinati insieme, tali dati consentono di identificare il lavoratore, offrendo un complesso di informazioni su quest'ultimo idoneo a rappresentarne le caratteristiche d'insieme e a fornire una sua immagine "non corporea". Peraltro, a seconda della sofisticatezza dei sistemi di rilevazione utilizzati nell'impresa, i dati raccolti possono giungere fino a descrivere le modalità di interazione del lavoratore con colleghi e clienti, rilevando finanche il suo stato d'animo e la sua condizione di salute.

Al contempo, sempre più spesso entra a far parte dell'oggetto del contratto di lavoro l'interazione del lavoratore con altri soggetti (clienti, colleghi, fornitori) mediata da strumenti digitali, che consente di aggiungere ai dati raccolti "surrettiziamente" la collezione di informazioni sui comportamenti volontari realizzati sul web.

Per il lavoratore (a diversi livelli) digitalizzato, in altre parole, all'identità personale (10) "tradizionale" si accompagna una identità digitale, che, facendo ricorso ad una definizione fornita in altro ambito eppure utile a fini didascalici, potremmo definire come « rappresentazione informatica della corrispondenza biunivoca tra utente ed i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale » (11).

---

(9) Per un maggior approfondimento della questione, si rinvia a G. Sigillò Massara, *Privacy e controlli nel lavoro autonomo*, in C. Pisani, G. Proia, A. Topo, (a cura di), *Privacy e lavoro. La circolazione dei dati e personali e i controlli nel rapporto di lavoro*, cit., 816 ss.

(10) Da intendersi come l'interesse del singolo ad avere una rappresentazione di sé nella vita di relazione che coincida con la sua vera identità, il suo agire, le sue convinzioni. Per un approfondimento in merito ai profili costituzionali, cfr. S. Scagliarini, *Identità digitale e tutela della privacy*, atti del Convegno annuale Associazione Gruppo di Pisa - Genova 18/19 giugno 2021: *Il diritto costituzionale e le sfide dell'innovazione tecnologica*, disponibile al link https://gruppodipisa.it/images/convegni/2021_Convegno_Genova/Simone_Scagliarini_-_Identità_Digitale_e_Tutela_della_privacy.pdf.

(11) La definizione è presa dal d.P.R. 24 ottobre 2014, art. 1, comma 1, lett. *o*). In merito, cfr. S. Scagliarini, *Identità digitale e tutela della privacy*, cit.

Si tratta, in altre parole, della personalità associata al lavoratore che opera virtualmente e che a quest'ultimo viene associata dagli altri operatori della rete. Se di essa si parla già adesso, è possibile immaginare uno sviluppo del suo rilievo in relazione alle potenzialità derivanti dal diffondersi del metaverso, allo stato ancora embrionale, ma potenzialmente prorompente nel prossimo futuro (12).

È per tali ragioni che, un cenno alle possibili interazioni tra metaverso e mercato del lavoro pare doveroso.

Nell'assenza di una definizione legale, è possibile descrivere il metaverso come « una tecnologia che, impiegando sistemi di intelligenza artificiale di ultima generazione, è in grado di generare un ambiente digitale, virtuale, immersivo e sociale. E che, attraverso l'impiego di realtà virtuale e aumentata, simulatori di visione, tattili e di movimento, è in grado di riprodurre l'esperienza dell'essere e del sentirsi presente, per il tramite di una propria rappresentazione (c.d. avatar), all'interno di una scena digitale tridimensionale, in maniera tale da potere interagire con persone e cose, secondo modalità quanto più possibile somiglianti a quelle reali » (13). Si tratta, in altre parole, di una realtà virtuale, in quanto tale simulazione del mondo reale, in cui, a differenza delle esperienze precedenti, il soggetto fisico si immerge completamente attraverso la stimolazione contemporanea dei diversi sensi, interagendo in essa in maniera tridimensionale.

Per poter agire nella realtà virtuale e interagire con gli altri operatori, il soggetto fisico ha un doppio ordine di necessità: in primo luogo, occorre avere la disponibilità della strumentazione informatica necessaria per "entrare" nella realtà virtuale, quali i già citati simulatori visivi, uditivi e tattili; in secondo luogo, occorre un avatar, ossia una proiezione dell'individuo persona fisica all'interno della realtà digitale.

La descrizione che precede racchiude in sé una prospettiva essenziale per il corretto inquadramento delle problematiche giuridiche connesse alle interazioni tra metaverso e mondo del lavoro. La concezione, cioè che, sebbene il metaverso rappresenti una realtà parallela e simulata abitata

(12) Nella pratica attuale, i maggiori esempi di realtà virtuale si registrano in ambito militare, nel design o architettura e in relazione alla medicina predittiva; al contempo, il primo esempio di metaverso, quale luogo virtuale e tridimensionale di interazione e scambio interamente digitale di beni anch'essi digitali si registra in ambito artistico con i *Non Fungible Token* (NFT).

(13) V. Maio, *Diritto del lavoro e metaverso. Se il lavoro non è un (video)gioco*, in *LLI*, vol. 8, n. 2, 2022, 42 ss. In merito alla definizione di metaverso, in relazione alle problematiche connesse con il diritto del lavoro, cfr. anche M. Nogueira Guastavino, D. Mangan, *The metaverse matrix of labour law*, in *Italian Labour Law e-Journal*, fasc. 1, vol. 16, 2023, 13 ss.; P. Sipka, *Potential challenges of working in a virtual space*, *ivi,* 53 ss.

esclusivamente da soggetti virtuali, quali appunto gli avatar, l'avanzamento di tale realtà virtuale e i suoi effetti nella "realtà reale" sono il frutto delle scelte dell'operatore persona fisica associato al singolo avatar, che a quest'ultimo dà gli impulsi per muoversi e interagire con gli altri operatori.

È evidente, allora, che anche ove dovessero diffondersi imprese destinate a rendere servizi esclusivamente nel metaverso, funzionanti per il tramite di contratti di lavoro aventi ad oggetto prestazioni da rendere interamente e necessariamente nell'ambito del metaverso attraverso il ricorso ad avatar (14), i lavoratori andrebbero pur sempre individuati nelle persone fisiche che, operando attraverso gli input dal mondo reale, controllano tali avatar. In altre parole, preliminare a qualsiasi considerazione in merito al rapporto tra lavoro e metaverso è la necessità di resistere alla tentazione di individuare negli avatar i nuovi lavoratori. Essi, sono piuttosto la proiezione digitale del lavoratore persona fisica che, secondo una metafora proposta da autorevole dottrina (15), agisce da marionettista (16).

---

(14) Il che ha già generato un ambio dibattito in merito alla possibilità o meno di qualificare il metaverso come luogo di lavoro (con le ripercussioni che ne conseguono in termini, ad esempio, di salute e sicurezza sul lavoro, tutela antidiscriminatoria, proprietà intellettuale), per cui si rinvia a C. Romeo, *L'avatar, il metaverso e le nuove frontiere del lavoro: traguardo o recessione*, cit., e ai diversi contributi di *Labour and Law Issues*, vol. 8, n. 2, 2022, e, in particolare, A. Donini, M. Novella, *Il metaverso come luogo di lavoro. Configurazione e questioni regolative*, 1 ss. Accolgono, *sic et simpliciter*, il metaverso come luogo di lavoro V. De Stefano, A. Aloisi, N. Countouris, *The metaverse is a labour issue*, pubblicato il 1° febbraio 2022 su *Social Europe*, disponibile al link https://www.socialeurope.eu/the-metaverse-is-a-labour-issue#:~:text=This%20is%20already%20a%20complex,lead%20to%20their%20account%20being.; M. Biasi, M. Murgo, *The virtual space of the Metaverse and the fiddly identification of the applicable labor law*, in *Italian Labour Law e-Journal*, fasc. 1, vol. 16, 2023, 1 ss.

(15) C. Romeo, *L'avatar, il metaverso e le nuove frontiere del lavoro: traguardo o recessione*, cit.

(16) Evidentemente, le considerazioni che precedono non si applicano agli avatar interamente digitali, il cui funzionamento dipende dall'applicazione dell'intelligenza artificiale e le cui "mosse" nel metaverso non sono, dunque, frutto delle scelte di singoli operatori. Al contempo, in relazione a tali ipotesi, tornano alla mente le considerazioni già svolte in merito alla imprescindibilità dell'intervento umano, foss'anche solo nella fase preparativa, nel funzionamento delle macchine intelligenti, in relazione alle quali si rinvia a G. Sigillò Massara, *Tecnologie, diritto e lavoro (anche) agile*, in R. Pessi, P. Matera, G. Sigillò Massara (a cura di), *Diritto, lavoro, nuove tecnologie e blockchain*, Roma, 2021, 65 ss. Al contempo, occorre rilevare che, nonostante all'apparenza il funzionamento dell'intelligenza sia interamente automatizzato ed esclusivamente basato sulla rielaborazione dei dati raccolti, spesso dietro ai servizi offerti dall'intelligenza artificiale si celano lavoratori in carne e ossa, c.d. lavoratori del *click*, per lo più reclutati nel sud del mondo, al fine di garantire l'efficienza dei servizi offerti ai Paesi del nord, su cui *amplius* cfr. V. De Stefano, A. Aloisi, *Il tuo capo è un algoritmo. Contro il lavoro disumano*, Roma, 2020; A. Casilli, *Schiavi del click. Perché lavoriamo tutti per il nuovo capitalismo?,* Milano, 2020.

Data per assodata tale premessa, sono molteplici le interazioni che il metaverso potrebbe avere con il mercato del lavoro. In primo luogo, l'attenzione va alla creazione di uffici virtuali, in cui i lavoratori possano operare tramite degli avatar, agendo da remoto, e interagendo nella realtà immersiva sia con colleghi che con clienti e fornitori. Si tratterebbe, in altre parole, di una evoluzione del lavoro agile che consenta non solo di lavorare e interagire a distanza, ma di immergersi interamente nel luogo virtuale di lavoro, anche sperimentando in versione tridimensionale i prodotti o servizi aziendali. Molteplici sono i pro, altrettanti sono i contro, di una scelta di tal fatta (17).

Partendo dai primi, per lo più in comune con il lavoro agile, vi sono i diversi vantaggi derivanti dalla assenza di un luogo di lavoro fisico distinto rispetto alla propria abitazione: vantaggio per l'impresa consistente nella riduzione dei costi di gestione degli stessi; un vantaggio per il lavoratore consistente nella riduzione dei tempi di spostamento da e per il luogo di lavoro, con effetti ambigui nell'ambito della conciliazione della vita professionale e lavorativa che, se da un lato tende ad essere agevolata, d'altro lato trascina in sé i rischi di una iper-connessione; un vantaggio sociale e ambientale consistente nella riduzione di inquinamento e di traffico.

Rispetto allo *smart working*, tuttavia, vi sono dei vantaggi aggiuntivi, come quelli derivanti dalle interazioni intuitive con gli avatar e la comodità per la clientela di sperimentare tridimensionalmente il prodotto o il servizio prima di acquistarlo. Al contempo, il ricorso alla realtà aumentata e immersiva con la sua flessibilità e velocità/variabilità di interazione, tende a favorire un apprendimento più celere e un miglior rendimento dei lavoratori, anche grazie a diverse applicazioni della teoria dei giochi e di tecniche di *gamification* (18).

Dal lato opposto, vi sono le problematiche attinenti all'esercizio dei diritti collettivi (19) e i rischi connessi alla prolungata permanenza nella realtà virtuale, con le conseguenze in termini di stress, problemi visivi, difficoltà di concentrazione e problematiche relazionali nella "realtà reale", già noti in relazione ai lavori impiegatizzi o che comunque richiedono lunghe ore

(17) Per un maggior approfondimento, si rinvia a M. Lombardi, *Il lavoro nel metaverso: uno spazio indefinito possibile*, in *LLI*, vol. 8, n. 2, 2022, 28 ss.

(18) Come evidenziato da V. Maio, *Diritto del lavoro e metaverso. Se il lavoro non è un (video)gioco*, cit., uno degli obiettivi dell'applicazione del metaverso al luogo di lavoro consiste proprio nella diffusione delle tendenze, già presenti, alla c.d. *gamification*, ossia all'applicazione di meccanismi tipici dei giochi (come la raccolta di punti o il superamento di livelli) ai rapporti di lavoro, al fine di stimolare la produttività. In merito, cfr. anche M. Biasi, *Guest Editorial. The Labour Side of the Metaverse*, in *Italian Labour Law e-Journal,* fasc. 1, vol. 16, 2023, I ss.

(19) Su cui, v. F. Pisani, *Collective labour relations in the metaverse*, in *Italian Labour Law e-Journal,* fasc. 1, vol. 16, 2023, 41 ss.

davanti a uno schermo, ma amplificati dall'immersione totale del soggetto nella realtà virtuale (20).

Ad essi, si aggiungono i rischi di violazione della dignità personale e della *privacy* dei soggetti coinvolti, chiamati a operare costantemente in un luogo virtuale soggetto a monitoraggio e controllo continuo da parte dell'imprenditore (21), peraltro attraverso strumentazioni potenti e sempre più pervasive di raccolta dati — anche dati biometrici, ad esempio attraverso il tracciamento dei movimenti facciali e la profilazione comportamentale ed emozionale — e di loro rielaborazione a fini decisionali.

Lo "sdoppiamento" del lavoratore in una personalità digitale da muovere nel metaverso operando da remoto nel mondo reale, peraltro, comporterebbe un doppio ordine di problemi specifici in ordine al *right to privacy* e ai poteri datoriali.

Da un lato, occorrerebbe individuare il confine in merito alla sostituzione del lavoratore nella gestione di un avatar unilateralmente imposta dal datore di lavoro, circostanza che pone alla luce il dubbio in merito al se e in che modo sia rivendicabile da parte del lavoratore il diritto all'identità dell'avatar gestito nel corso del tempo e, dunque, associato alla sua personalità (22).

Di converso, peraltro, sussiste l'esigenza datoriale di ottenere la certezza che "dall'altro lato dello specchio" vi sia effettivamente il lavoratore e che quest'ultimo non si sia fatto sostituire nella gestione dell'avatar. A tal fine, il ricorso alla verifica dell'identità per il tramite di dati biometrici potrebbe accentuarsi. E tale raccolta di dati, d'altronde, potrebbe espandersi anche ai comportamenti, modi di fare, tono della voce del lavoratore, al fine di garantirsi la possibilità di sostituirlo nella gestione dell'avatar storicamente associatogli, senza creare turbamenti tra i colleghi o perdere la fidelizzazione della clientela (23).

In breve, sebbene la disciplina del controllo a distanza da parte del datore di lavoro, così come quella della *privacy* dei lavoratori, abbia conosciuto notevoli modifiche destinate ad un adattamento al progresso tecnologico in un passato relativamente recente, con il continuo avanzare della digitalizzazione dell'impresa, l'imporsi degli strumenti di gestione algorit-

---

(20) In merito alla salute e sicurezza dei lavoratori del metaverso, cfr. I. Rácz-Antalm, *Labour law and Metaverse - can they fit together?,* in *Italian Labour Law e-Journal,* fasc. 1, vol. 16, 2023, 29 ss.

(21) In merito, cfr., F. Lamberti, *Il metaverso: profili giuslavoristici tra rischi nuovi e tutele tradizionali*, in *Federalismi.it*, fasc. 4, 2023, 205 ss.

(22) La situazione, peraltro, andrebbe a complicarsi ove il ricorso a tale sostituzione sia utile, ad esempio, a "coprire" un lavoratore scioperante (c.d. crumiraggio tecnologico).

(23) In questo senso, cfr. M. Peruzzi, *"Almeno tu nel metaverso". Il diritto del lavoro e la sfida dei nuovi spazi digitali*, in *LLI*, vol. 8, n. 2, 2022, 64 22.

mica del personale e connessa elaborazione dei dati, le potenzialità del diffondersi del lavoro reso nel metaverso, si prospettano "nuove sfide".

6.3. I controlli a distanza del datore di lavoro e il diritto alla *privacy* del lavoratore

Dato il contesto descritto nelle pagine precedenti, nel presente paragrafo ci si soffermerà sulla disciplina del controllo a distanza fissata dall'art. 4 dello Statuto dei Lavoratori (di seguito, *breviter*, "art. 4") a seguito delle modifiche apportate dal *Jobs Act* (24), cercando di evidenziare alcune interazioni con la disciplina di tutela della *privacy* (25).

Preliminare all'esame del contenuto precettivo dell'art. 4 è l'individuazione della sua *ratio legis*, utile per fornire una corretta interpretazione della disposizione.

A tal fine, il punto di partenza è la collocazione dell'art. 4 all'interno del Titolo I dello Statuto dei lavoratori, dedicato alla tutela « della libertà e della

---

(24) Per un commento più ampio, si vedano G. Proia, *Trattamento dei dati personali, rapporto di lavoro e l'« impatto » della nuova disciplina dei controlli a distanza*, in *RIDL*, fasc. I, 4, 2016, 560 ss.; M. T. Carinci, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D. Lgs. 151/2015): spunti per un dibattito*, in *LLI*, vol. 2, no. 1, 2016; I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della "privacy",* in *LLI*, 2016, fasc. 1, 45; R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, d.lgs. n. 151/2015*), in *RIDL*, 2016, fasc. 1, 77 ss.; R. Fabozzi, *I controlli a distanza (di cinquant'anni),* in *MGL*, fasc. 1, 2020, 59 ss.; R. Fabozzi, *Nuove tecnologie e potere di controllo*, in R. Pessi, P. Matera, G. Sigillò Massara, (a cura di), *Diritto, Lavoro, tecnologie e Blockchain*, Roma, 2020, 139 ss.; M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore) = The transfer of rest and holidays according to art. 24 of Legislative Decree no. 151/2015*, in *WP C.S.D.L.E. "Massimo D'Antona".IT,* 300/2016; E. Dagnino, *Tecnologie e controlli a distanza*, in M. Tiraboschi (a cura di), *Le nuove regole del lavoro dopo il Jobs Act*, in *Le nuove leggi civi*., Milano, 2016, 107 ss.; P. Lambertucci, *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs Act),* in *Wp CSDLE "MAssimoD'Antona".it*, n. 255, 2015; A. Stanchi, *Nel Jobs Act il nuovo articolo 4 dello Statuto dei Lavoratori,* in *GLav*, n. 38, 2015, 40 ss.; A. Stizia, *I controlli a distanza dopo il "Jobs Act" e la Raccomandazione R(2015)5 del Consiglio d'Europa,* in *LG*, 2015, 678 ss.; A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav*., in *RIDL*, fasc. 3, 2016, 513 ss.; P. Tullini, *Il controllo a distanza attraverso gli strumenti per rendere la prestazione lavorativa. Tecnologie di controllo e tecnologie di lavoro: una distinzione è possibile?,* in *Il Nuovo Diritto del Lavoro*, 2017, 94 ss.

(25) Per un raffronto tra la tutela della *privacy* e la disciplina dei controlli a distanza, cfr. G. Proia, *Controlli a distanza e trattamento dei dati personali: due discipline da integrare (ma senza far confusione),* in C. Pisani, G. Proia, A. Topo, (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, cit., 329 ss.; A. Ingrao, *Controlli a distanza e privacy del lavoratore*, in *LLI*, vol. 9, n. 1, 2023, I 103 ss.

dignità del lavoratore ». Nel procedimentalizzare e limitare la possibilità per il datore di lavoro di realizzare un controllo sull'attività lavorativa attraverso strumenti tecnologici, allora, l'art. 4 è volto a tutelare la dignità personale dei lavoratori nonché, di riflesso, la loro riservatezza e *privacy*. Si tratta, in altre parole, di una delle prime fattispecie incidenti sul diritto alla riservatezza ad essere oggetto di una specifica disciplina legale, ben prima dell'introduzione del Codice della *Privacy*. Già all'inizio degli anni '70, agli albori della rivoluzione tecnologica, si concretizza la necessità di tutelare la dignità dell'individuo che lavora, evitando che l'esecuzione della prestazione lavorativa lo esponga ad un rischio specifico di ingerenza datoriale incontrollata nella propria sfera intima individuale, nella consapevolezza dell'inevitabilità del ricorso a moderni mezzi di controllo all'interno delle imprese e della necessità di evitare il concretizzarsi di controlli occulti e continui.

La *ratio* dell'art. 4, allora, viene a concretizzarsi nel bilanciamento di due contrapposti interessi di rilievo costituzionale: da un lato essi attengono ad elementi di natura prettamente economica e imprenditoriale (tutelati dall'art. 41 della Costituzione); d'altro lato si scontrano con le necessità di tutela della persona in quanto tale e in quanto soggetto che, proprio attraverso il lavoro, si inoltra nel percorso di emancipazione individuale e sociale costruito dal combinato disposto dei primi quattro articoli della Carta Costituzionale, non a caso contenenti i « principi fondamentali » sui quali si fonda la Repubblica italiana.

È proprio in considerazione del "lavoro" inteso quale « principe dei diritti sociali » (26) e quale strumento primario di sviluppo della personalità, nella sua componente individuale e collettiva, tutelato in « tutte le sue forme e applicazioni » dall'art. 35 e riconosciuto come diritto e dovere dall'art. 4 della Costituzione, che acquista particolare rilievo la necessità di evitare l'esposizione del lavoratore alla succitata ingerenza incontrollata nella propria sfera personale per il semplice fatto di svolgere l'attività lavorativa.

In questo senso, acquista rilievo la collocazione dell'art. 4 nel Titolo I dello Statuto, destinato a proteggere la dignità del lavoratore, quale diritto a svolgere la propria attività in un ambiente sereno e scevro dai condizionamenti che inevitabilmente deriverebbero da ogni forma di controllo occulto e continuativo. Al contempo, ciò che viene tutelato è la libertà del prestatore;

---

(26) M. Mazziotti, *Il diritto al lavoro*, Milano, 1956, p. 87; il diritto al lavoro è stato definito anche come "archetipo" dei diritti sociali da W. Schmidt, *I diritti fondamentali sociali nella Repubblica Federale Tedesca*, in *Riv. trim. dir. pubbl.*, 1981; nonché come il "primo" dei diritti sociali da S. Giubboni, *Il primo dei diritti sociali. Riflessioni sul diritto al lavoro tra Costituzione italiana e ordinamento europeo*, in *WP C.S.D.L.E. "Massimo D'Antona" .IT* — 46/2006.

libertà che, tra le sue multiformi manifestazioni, comprende indubbiamente il *right to privacy* e, quindi, da un lato il diritto a che la raccolta, elaborazione e archiviazione dei dati circa l'attività (vieppiù ove estranea ai luoghi di lavoro) e la persona sia ridotta allo stretto indispensabile e, d'altro lato, il diritto al mantenimento di una sfera di "non ingerenza" dalle intrusioni della controparte negoziale (anche nel combinato disposto con l'art. 8 dello stesso S.L.).

Modellato sulle esigenze della fine degli anni '60, la versione originale dell'art. 4 sancisce in primo luogo un generale divieto di « uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori ». Il secondo comma prevede una deroga a tale divieto, consentendo l'introduzione di tali apparecchiature, qualora necessarie per ragioni organizzative e produttive o connesse alla sicurezza sul lavoro, previo accordo sindacale o, in mancanza, dietro autorizzazione dell'Ispettorato del Lavoro (27). La disciplina è di per sé chiara, impostata sul divieto generale di impiantare nelle aziende apparecchiature tecnologiche destinate ad un monitoraggio continuativo dell'attività lavorativa, "addolcito" dalla possibilità di far ricorso ad esse per le ragioni tipizzate (seppur attraverso clausole generali) dalla legge ed afferenti ad esigenze aziendali estranee all'esercizio del potere di controllo datoriale, dietro la garanzia che gli interessi dei lavoratori siano presi in considerazione attraverso il controllo sindacale o amministrativo.

È evidente come la dimensione aziendale di riferimento sia quella di un mercato del lavoro ancora coinvolto dal processo di terziarizzazione solo parzialmente e ancora fortemente legato alle fabbriche di stampo post-fordista. E, difatti, la norma ha originariamente ad oggetto le c.d. apparecchiature esterne (28) alla prestazione di lavoro, rivolgendosi soprattutto a quegli strumenti che, permettendo di controllare la continuità di un macchinario o di registrare le conversazioni dei dipendenti (29), consentono di ottenere informazioni utili sulla quantità e la continuità del lavoro e di ricostruire in tal modo l'attività svolta da ciascun prestatore. Nella lettera della legge, diversamente, non vengono in rilievo quegli strumenti costantemente utilizzati per rendere la prestazione lavorativa — e, talvolta, anche al

(27) I commi due e seguenti prevedevano una particolare disciplina per gli apparecchi già impiegati nei luoghi di lavoro al momento dell'emanazione della norma e una procedura di impugnazione dei provvedimenti dell'Ispettorato del Lavoro.

(28) I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della Privacy,* in *LLI,* 2016, 2, 1, 1.

(29) Sul punto si veda: C. Assanti, G. Pera, *Art. 4 (Impianti audiovisivi),* in *Commento allo Statuto dei diritti dei lavoratori,* a cura di C. Assanti, G. Pera, Padova, 1972, 26.

di fuori del contesto lavorativo — pur idonei ad una massiccia raccolta di dati e, quindi, all'esercizio di un incisivo controllo datoriale, si pensi, senza necessità di eccessivi sforzi immaginativi, agli indirizzi e-mail, computer, telefoni e tablet aziendali (30).

L'art. 4 pre-*Jobs Act*, in altre parole, finisce per disciplinare fenomeni divenuti via via di minor rilievo e, di converso, per lasciare privi di tutele le nuove fattispecie emergenti, con ciò impedendo *de facto* la realizzazione di quel necessario contemperamento tra l'interesse dell'azienda a controllare l'utilizzo degli strumenti tecnologici da parte del lavoratore e la necessità di tutelare la dignità e la riservatezza di quest'ultimo, che come visto deve essere individuato quale fine ultimo del dettato normativo.

Nonostante le clausole generali contenute nella lettera dell'art. 4 ne abbiano consentito una certa adattabilità, anche grazie alla definizione da parte della giurisprudenza della nozione di "controlli difensivi" (31), è evidente come, dopo oltre quaranta anni dalla sua emanazione, caratterizzati dalla Rivoluzione Digitale, si renda necessaria una riforma della disciplina che la renda "al passo coi tempi" adeguandone il contenuto precettivo all'evoluzione tecnologica intercorsa dal 1970 ad oggi (32).

---

(30) Di fronte a tali fattispecie e alle difficoltà applicative derivanti dall'eventuale estensione *sic et simpliciter* del disposto dell'originario art. 4, parte della dottrina avalla anche l'ipotesi di escludere gli strumenti da lavoro dall'area di applicazione della norma statutaria, sostenendo che per il ricorso a questi ultimi non sia necessario acquisire la preventiva autorizzazione. Cfr. P. Ichino, *Il contratto di lavoro*, Torino, 2003, III, 234; E. Gragnoli, *L'uso della posta elettronica sui luoghi di lavoro e la strategia di protezione elaborata dall'Autorità Garante,* in *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, P. Tullini (a cura di), Padova, 2010, 68. *Contra*, P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in *RIDL*, 2009, I, 329, secondo cui i controlli « difensivi non costituiscono una *species* estranea allo Statuto, ma sono riconducibili all'area del controllo preterintenzionale ».

(31) La giurisprudenza di legittimità, in particolare, identifica la fattispecie dei "controlli difensivi", ovvero i « *controlli diretti ad accertare condotte illecite del lavoratore* ». Cfr., *inter alia*, Cass. 4 aprile 2012, n. 5371 e Cass. 23 febbraio 2012, n. 2722, entrambe in *RIDL*, 2013, II, 113, con nota di G. Spinelli. Per il primo approdo giurisprudenziale con cui è affrontato il tema della inclusione o meno dei controlli difensivi nell'alveo dell'art. 4 Stat. Lav. è rinvenibile in Cass. 3 aprile 2002, n. 4746, con commento di L. Nogler in *G. Lav*., 2002, n. 21, 10. La prima pronuncia della Corte di Cassazione in tema di monitoraggio degli accessi ad internet è invece più recente: Cass. 23 febbraio 2010, n. 4375, in *RGL,* 2010, II, 462, commentata da A. Bellavista; Cass. 3 aprile 2002, n. 4746, in *G. Lav*., 2002, n. 21, 10, con nota di L. Nogler; Cass. 23 febbraio 2010, n. 4375.

(32) Esigenza già da tempo paventata, cfr. A. Trojsi, *Il comma 7, lettera* f), *della legge delega n. 183/2014: tra costruzione del Diritto del lavoro nell'era tecnologica e liberalizzazione dei controlli a distanza sui lavoratori*, in M. Rusciano, L. Zoppoli (a cura di), *Jobs Act e contratti di lavoro dopo la legge delega 10 dicembre 2014 n. 183, WP CSDLE "MassimoD'Antona" -*

Si giunge, così, attraverso le modifiche apportate dal *Jobs Act*, ad una nuova formulazione dell'art. 4 (33), in cui è possibile identificare due nuclei essenziali, corrispondenti ai primi due commi e destinati a regolare due momenti distinti (seppur intimamente connessi), che vengono in considerazione in caso di utilizzo da parte del datore di strumenti da cui deriva la possibilità di controllare l'attività di lavoro e acquisire dati relativi ad essa e al dipendente (34).

Il primo nucleo contiene le norme destinate a disciplinare la possibilità per l'imprenditore di ricorrere a strumenti esterni all'attività lavorativa, da cui possa derivare più o meno indirettamente un controllo da parte del datore di lavoro. Vengono, così, definite (35) le condizioni di legittimità dell'installazione delle apparecchiature che potremmo definire di "controllo preterintenzionale", in quanto, pur destinate ad altri scopi, consentono alla parte datoriale di monitorare l'attività dei dipendenti quale effetto collaterale. Orbene, in relazione ad essi viene dettata una condizione sostanziale, tale per cui le apparecchiature in esame possono essere utilizzate « esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale » (36) (non, quindi, per monitorare l'attività dei dipendenti); una condizione formale/procedimentale tale per cui il ricorso ad esse deve essere preceduto da un accordo sindacale, ovvero da un'autorizzazione amministrativa (che, eventualmente, ne disciplini le modalità di utilizzo).

Collective volumes, 2014, n. 3, 119 ss.; C. Zoli, *Il controllo a distanza del datore di lavoro: l'art. 4 l. n. 300/1970 tra attualità ed esigenze di riforma*, in P. Tullini (a cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, Padova, 2010, 164 ss.; A. Levi, *Il controllo informatico sull'attività dei lavoratori*, Torino, 2013; A. Stizia, *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Padova, 2013.

(33) In merito alla riforma, cfr., *inter alia*, R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23, D. Lgs. 151/2015),* in *RIDL*, 2016, 77 ss.; M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore), WPCSDLE"MassimoD'Antona".it*, n. 300/2016; V. Maio, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *ADL*, 2015, 1186 ss.; E. Baletti, *I controlli a distanza dei lavoratori dopo il Jobs Act*, in F. Santoni, M. Ricci, R. Santucci (a cura di), *Il diritto del lavoro all'epoca del Jobs Act*, Napoli, 2016.

(34) I. Alvino, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della Privacy,* in *LLI,* 2016, 2, 1, 1.

(35) Senza più porre un divieto generale, che può, tuttavia, considerarsi ancora implicito nell'interpretazione complessiva della norma che, ponendo le condizioni di legittimità del ricorso agli strumenti di controllo da remoto, impedisce al contempo l'utilizzo di tali tecnologie al di fuori dei limiti legali. In tal senso si esprime anche il Comitato dei Ministri degli Stati Membri del Consiglio d'Europa nella Raccomandazione CM/REc (2015) 5 del 1° aprile 2015 in materia di trattamento dei dati personali nei rapporti di lavoro.

(36) Art. 4, c. 1.

Per espressa previsione del secondo comma dell'art. 4, detta disciplina non è applicabile « agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze » (37). Il secondo nucleo fondante l'art. 4, quindi, attiene alle apparecchiature "interne" alla prestazione, ossia utilizzate nell'attività lavorativa, e da cui possa conseguire un controllo datoriale. In relazione ad esse, viene superata l'esigenza di accordo sindacale o autorizzazione ammnistrativa, proprio in considerazione della strumentalità delle apparecchiature in esame alla prestazione lavorativa, della loro diffusione e delle difficoltà organizzative che deriverebbero dall'estensione della disciplina di cui al primo comma. Nonostante tale scelta sia condivisibilmente destinata a fluidificare i processi organizzativi aziendali con riferimento a tutta quella strumentazione oggi indispensabile (o, comunque, utile) per l'utile perseguimento degli obiettivi di impresa, il rischio è quello di mantenere un *vulnus* nelle necessità di tutela della dignità dei lavoratori.

In particolare, secondo una parte della dottrina, la riforma avrebbe liberalizzato la possibilità del datore di lavoro di sorvegliare il lavoratore attraverso gli strumenti informatici necessari per rendere la prestazione lavorativa (38). Deve rilevarsi, tuttavia, come tale paventata liberalizzazione sia fortemente circoscritta dall'imporsi di una nozione restrittiva di « strumenti utilizzati per rendere la prestazione lavorativa » (39), da intendersi come strettamente necessari alla prestazione (40), tanto da portare una parte della giurisprudenza a ritenere necessario verificare « caso per caso, a seconda del tipo di mansione e a seconda della organizzazione aziendale, se lo strumento affidato al lavoratore dal datore di lavoro sia oggettivamente necessario all'esecuzione della prestazione lavorativa e cioè se sia il mezzo

(37) Art. 4, c. 2.

(38) V. in questo senso A. Trojsi, *La sorveglianza digitale del datore di lavoro*, in A. Bellavista, R. Santucci, (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Torino, 2022, 71 ss.

(39) *Contra* v. G. Proia, *Controlli a distanza e trattamento dei dati personali*, cit. (p. 338) il quale sostiene che non sia « convincente la tesi secondo cui lo strumento di cui trattasi debba essere "necessario" e non semplicemente "utile", ai fini dell'esecuzione della prestazione. Così interpretando la norma, le si fa dire esattamente il contrario di quella che è la sua *ratio*, e non si considera che le innovazioni organizzative e tecnologiche, tanto più se considerate in relazione agli strumenti di lavoro, non si prestano mai ad essere valutate in termini di indispensabilità, ma sempre e solo in termini di utilità ».

(40) Garante per la Protezione dei Dati Personali, 13 luglio 2016, n. 303; Trib. Roma 24 marzo 2017, in *DRI*, n. 1, 2018, 264 ss., con nota di E. Gramano, *La rinnovata (ed ingiustificata) vitalità della giurisprudenza in materia di controlli difensivi*; Cass. 22 settembre 2021, n. 25731, a quanto consta non annotata.

utilizzato dal lavoratore per svolgere le sue mansioni » (41). Al contempo, tende ad imporsi anche una nozione restrittiva di "strumento" di lavoro, da intendersi quale mezzo strettamente funzionale all'esecuzione della prestazione stessa (42), tanto da portare ad affermare la necessità di distinguere tra le componenti *hardware* del computer aziendale, strettamente necessarie a rendere la prestazione e dunque escluse dalla necessità di accordo sindacale o autorizzazione amministrativa, ed eventuali *software* aggiunti dal datore per ragioni diverse, come la protezione dei dati aziendali o da crimini informatici, assoggettati alla disciplina ordinaria (43).

Il terzo e ultimo comma si occupa di un aspetto, estremamente rilevante, estraneo alla disciplina previgente: esplicitare la possibilità di utilizzare i dati legittimamente ottenuti — *i.e.* ottenuti nel rispetto dei limiti di cui ai primi due commi dell'art. 4, nonché, come vedremo, della disciplina sulla *privacy* — per « tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196 » (44).

Viene, di tal guisa, previsto un coordinamento espresso tra l'art. 4 e il Codice della *Privacy* (45), disposto all'evidente fine di creare una coerenza complessiva dell'ordinamento, affidando la tutela della dignità e libertà del lavoratore ad una sommatoria di discipline (46) estranea alla lettera della disposizione previgente.

Il coordinamento tra la legislazione lavoristica di limitazione dei controlli a distanza e la regolamentazione del diritto alla riservatezza, tuttavia, non è sempre immediato, anche in considerazione della differenza di approccio: se il legislatore italiano sin dagli anni '70 prevede una procedimentalizzazione e dei limiti alle modalità di acquisizione delle informazioni — *i.e.* gli strumenti

---

(41) Trib. Torino 18 settembre 2018, n. 1664, a quanto consta non annotata.

(42) Cfr. Min. Lav. 18 giugno 2015; Provvedimento Garante per la protezione dei dati personali 13 luglio 2016, n. 303.

(43) Trib. Torino 18 settembre 2018, n. 1664, cit.; Trib. Milano n. 2757 del 2017.

(44) Art. 4, c. 3.

(45) In questa sede, si danno per presupposto le principali innovazioni apportate alla disciplina della *privacy* dal d.lgs. 10 agosto 2018, n. 101, di attuazione del GDPR attraverso la redazione di un "codice nuovo" rispetto a quello precedente, con un cambio di impostazione — che dallo stampo autorizzatorio passa a quello dell'*accountability* e responsabilizzazione del titolare del trattamento dati, nella specie il datore di lavoro — da cui deriva una modifica profonda dell'impostazione complessiva. Per un maggiore approfondimento sul punto, G. Sigillò Massara, *Privacy e controlli nel lavoro autonomo*, cit.

(46) In questo senso, cfr. G. Proia, *Controlli a distanza e trattamento dei dati personali*, cit.; P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, in *RIDL*, fasc. I, 2009, 323 ss.

di controllo a distanza — quello europeo si concentra sul prodotto delle informazioni, i dati, impostando la disciplina sulla trasparenza e responsabilizzazione da un lato, limiti al loro trattamento dall'altro (47).

La differenza di approccio si spiega anche con la differenza di intenti: la disciplina del controllo a distanza, sin dalla sua origine, ha come effetto indiretto quello di limitare l'accesso datoriale ai dati personali ottenibili per il tramite di strumentazione informatica, ma non è questo lo scopo diretto della norma (48). Si tratta, piuttosto, di una limitazione dei controlli occulti e prolungati, appunto, degli strumenti a disposizione datoriale per realizzare altri scopi e da cui può derivare in maniera mediata l'acquisizione di dati e, dunque, la loro rielaborazione. Quello che in ambito *privacy* si definisce trattamento di dati, in altre parole, attiene ad un momento secondario rispetto a quello oggetto della disciplina dell'art. 4, che nella sua versione originaria non contiene alcuna informazione in merito ai dati ottenuti, mentre nella versione odierna consente un generico utilizzo « per tutti i fini connessi al rapporto di lavoro » purché tale trattamento avvenga nel rispetto della normativa sulla *privacy* (oltre che previa informativa adeguata).

Quest'ultima, difatti, si occupa espressamente del trattamento dei dati personali, da intendersi come qualsiasi raccolta o elaborazione di informazioni idonee a rendere una persona fisica identificata o identificabile da parte di un apparecchio tecnologico o conservazione presso un archivio cartaceo. Nell'attuale versione del Codice della *Privacy*, profondamente riformato dal d.lgs. 10 agosto 2018, n. 101 di attuazione del GDPR, la tutela della riservatezza individuale nei confronti di trattamenti sempre più invasivi viene impostata *in primis* attraverso la valorizzazione dell'*accountability*, ossia di responsabilizzazione del titolare del trattamento dati personali, nel caso di specie il datore di lavoro, che deve predisporre misure tecnico-organizzative di salvaguardia dei dati personali, trasparenza e correttezza, nel rispetto dei criteri di *privacy by design* e *privacy by defalut* (49) (50).

---

(47) Tale differenza viene evidenziata in chiave fortemente critica della disciplina sovranazionale da E. Gragnoli, *Il potere di controllo, le risorse digitali e gli algoritmi*, in A. Bellavista, R. Santucci (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Torino, 2022, 27 ss., il quale a sostegno dell'approccio italiano afferma che « poco importa che cosa si apprenda, ma che cosa si voglia scoprire e, soprattutto, perché » (pag. 32).

(48) Cfr. G Proia, *Controlli a distanza e trattamento dei dati personali*, cit.

(49) In merito, cfr. A. Stizia, *I limiti ai controlli tra giurisprudenza nazionale e CEDU*, in A. Bellavista, R. Santucci (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, cit., 109 ss.; A. Ingrao, *La protezione dei dati personali dei lavoratori*, *ibidem*, 127 ss.

(50) L'importanza del *principio di accountability* (che si sostanzia nella valorizzazione dell'assunzione di responsabilità dei singoli titolari e, in particolare, nella valutazione del

Come noto, peraltro, l'art. 88 del GDPR, nel disciplinare il trattamento dei dati personali nell'ambito dei rapporti di lavoro, lascia ampio spazio alla legislazione integrativa degli Stati Membri. Nel nostro ordinamento, la scelta è di non adottare norme specifiche, sicché la relativa disciplina finisce per risultare in gran parte coincidente con l'art. 4 di cui sopra, nonché con l'art. 8 dello Statuto dei Lavoratori che limita le informazioni che possono essere oggetto di indagine datoriale a quelle strettamente professionali (51).

Attraverso la sommatoria di discipline apparentemente a sé stanti, allora, si creano delle interconnessioni, che attengono alla legittima acquisizione di dati (attraverso strumenti elettronici) da parte datoriale subordinata al rispetto del doppio nucleo costituente l'art. 4, e al legittimo trattamento dei dati così ottenuti, subordinato al rispetto del Codice della *Privacy*, con particolare riferimento all'informazione preventiva (52) espressamente richiamata dall'ultimo comma dell'art. 4, ma anche agli altri principi, tra cui quello della coerenza tra le finalità indicate nell'informativa e le modalità effettive, della minimizzazione (53), di conservazione (54).

---

livello di rischio dei trattamenti e della conseguente necessità di adottare gli adempimenti previsti dalla normativa nonché dell'adeguatezza delle misure di protezione) determina un profondo cambiamento culturale, oltre che una forte cesura rispetto alla normativa precedente. Tale visione è ampiamente condivisa in dottrina, cfr. *ex multis*: G. Finocchiaro, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in *EAD.* (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017, 12 ss.

Ancora, F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ.*, 2017, II, spec. 375 ss. evidenzia come il GDPR non rappresenti una mera ricognizione aggiornata e sistematizzata della normativa e della giurisprudenza, ma determini delle scelte importanti in materia di politica del diritto.

(51) In questo senso, cfr. il provvedimento del Garante per la protezione dei dati personali del 28 ottobre 2021, n. 9722661, in cui si afferma che, per effetto del rinvio alla legislazione nazionale specifica operato dall'art. 88 del GDPR, il rispetto della disciplina di cui agli artt. 4 e 8 dello Statuto dei Lavoratori è condizione di legittimità del trattamento dei dati personali nell'ambito del rapporto di lavoro.

(52) Il ruolo determinante dell'informazione preventiva "adeguata" viene sottolineata a più battute dal Garante della *Privacy*, recentemente con il provvedimento del 13 maggio 2021, n. 9669974 e del 13 aprile 2021, n. 9670738.

(53) Ossia il principio per cui l'intrusione nella sfera personale altrui deve essere la minore possibile. Cfr. A. Stizia, *I limiti ai controlli tra giurisprudenza nazionale e CEDU*, cit.

(54) In base al quale la conservazione dei dati che consentano l'identificazione di un lavoratore deve essere effettuata dal datore di lavoro (così come da qualsiasi titolare di trattamento) per il tempo necessario alle finalità indicate, dovendosi poi procedere alla loro cancellazione. Cfr. A. Stizia, *I limiti ai controlli tra giurisprudenza nazionale e CEDU*, cit.

6.4. Alcune considerazioni conclusive

Come si è già avuto modo di rilevare (55), in conclusione, nonostante le (e forse in ragione delle) molteplici modifiche e successioni che la normativa ha vissuto nel corso del tempo, quello alla *privacy* si conferma come un diritto dal carattere fortemente dinamico che necessita di un adattamento che vada di pari passo col progresso tecnologico e quindi con le sempre mutevoli esigenze delle aziende che risentono fortemente dell'eco della digitalizzazione.

Nell'impostazione attuale, tale adattamento è primariamente affidato alla disciplina europea (56), lasciando al legislatore interno un ruolo, se non marginale, quantomeno integrativo e complementare rispetto a quello sovranazionale (57), in ossequio al principio di sussidiarietà. Principio di sussidiarietà che opera anche nell'ambito dell'ordinamento interno e nel rapporto tra pubblico e privato, in considerazione dell'apporto richiesto sia all'Autorità Garante (ormai per lo più soggetto regolatore e vigilante) che al singolo titolare del trattamento (in virtù del più volte richiamato principio di *accountability*), per la realizzazione effettiva dell'impianto legislativo e per la tenuta complessiva del sistema (58).

Con l'avanzare del progresso tecnologico, in altre parole, avanzano le

---

(55) G. Sigillò Massara, *Privacy e controlli nel lavoro autonomo*, cit.

(56) Sul tema dello spostamento della garanzia in sede sovranazionale, si veda: L. Califano, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in L. Califano, C. Colapietro, *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, 3 ss.

(57) La materia, peraltro, acquista rilievo anche nell'ambito della Carta Europea dei Diritti dell'Uomo e delle Libertà Fondamentali (CEDU), che all'art. 8 tutela il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza. Anche tale disciplina risulta applicabile alla delimitazione dei limiti al controllo dei lavoratori e alla tutela della loro riservatezza. Si veda, ad esempio, la recente sentenza Florindo de Almeida Vasconcelos Gramaxo, con cui la Corte EDU affronta per la prima volta la tematica dei controlli tecnologici realizzati tramite sistemi GPS, ritenendo utilizzabili a fini disciplinari i relativi dati per ragioni di tutela del patrimonio aziendale (Corte Europea dei Diritti dell'Uomo, 13 dicembre 2022, n. 26968, in *Diritto delle Relazioni Industriali*, fasc. 2, 2023, 551, con nota di M. Rosa, *Bilanciamento di interessi e giurisprudenza della Corte europea dei diritti dell'uomo sui controlli tecnologici tramite dispositivi di geolocalizzazione: l'affaire Florindo de Almeida Vasconcelos Gramaxo c. Portogallo*).

(58) Come osservato da S. Scagliarini, *Dal "vecchio" al "nuovo" Codice della privacy,* in *Il "nuovo" codice in materia di protezione dei dati personali, La normativa italiana dopo il d.lgs. n. 101 del 2018*, cit., difatti, l'attuale Codice della *privacy* tende ad attribuire all'autorità pubblica il ruolo di mero soggetto regolatore, accrescendo di converso, sotto il profilo sostanziale, le responsabilità del singolo titolare del trattamento, con l'intervento del Garante — non in chiave burocratica e autorizzatoria — bensì in un'ottica di controllo e di eventuale

esigenza di tutela del diritto alla riservatezza quale prerogativa intima della persona, legata alla sua dignità e libertà individuale, affidate in maniera progressivamente maggiore da un lato al livello sovranazionale, anche in ragione della dimensione transnazionale del fenomeno, d'altro lato a livello individuale, con la responsabilizzazione del singolo titolare di trattamento, individuato quale soggetto meglio di altri idoneo a garantire i beni protetti, in ragione della sua posizione di supremazia nella disponibilità effettiva dei dati.

E di tali dati, nell'ambito del diritto del lavoro, si possono fare diversi usi, dal più tradizionale ambito disciplinare, gli stessi acquistano una rilevanza fondamentale per le imprese che realizzino sistemi integralmente o parzialmente automatizzati di gestione del personale, ad esempio attraverso il *management by algorithmic* e gli *EPM* di cui si è detto in apertura. In entrambi i casi, il dato personale costituisce l'ingrediente principale per far funzionare le ricette organizzative mediate dall'intelligenza artificiale, elemento indispensabile senza il quale l'intero sistema viene a mancare.

Al contempo, occorre rilevare che la stretta interconnessione tra strumenti di gestione del personale e quindi di indirizzo dell'attività, i quali consentono anche di esercitare un controllo costante della stessa, comporta che « potere di indirizzo e potere di controllo convergono e si sincronizzano, consentendo al datore di lavoro di avere una pressocché continua conoscenza/ingerenza relativa all'adempimento della prestazione » (59).

In altre parole, le nuove tecnologie portano ad un rimodularsi dei poteri datoriali, in particolare del potere direttivo e di controllo, i quali tendono a sovrapporsi in un rapporto inscindibile, in cui lo stesso strumento con cui il datore di lavoro indirizza l'attività consente un controllo sul corretto adempimento della stessa (spesso fra l'altro eseguita per il tramite del medesimo strumento). Al contempo, sono le informazioni ottenute per il tramite del controllo digitale — i dati — a fungere da motore per il successivo esercizio del potere direttivo, creando un circuito organizzativo autoalimentato.

Il potere di controllo, in questo contesto, acquista un rilievo primario nell'etero-direzione datoriale quale elemento essenziale del rapporto di lavoro subordinato. Non è un caso che, nell'ambito di proposta di direttiva relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali (60), il potere di controllo diventa determinante per l'applicazione della presunzione di subordinazione.

---

sanzione *ex post*, nell'ipotesi in cui si sia verificato un abuso del margine di autovalutazione lasciato ai singoli.

(59) L. Zoppoli, *Lavoro digitale, libertà negoziale, responsabilità: ancora dentro il canone giuridico della subordinazione*, in *Diritto lavori Mercati*, fasc. I, 2022, 51 ss.

(60) COM/2021/762 final.

La tutela della *privacy* e della dignità personale dei lavoratori, in questo contesto, acquista un rilievo primario per evitare la concretizzazione dei futuri distopici immaginati dalla fantascienza letteraria e cinematografica caratterizzata da "individui privati della loro individualità" e della loro sfera di riservatezza in cui l'identità digitale finisce con il prevalere rispetto alla personalità del singolo ridotto ad avatar.

Pare, dunque, che obiettivo del legislatore, tanto nazionale quanto europeo, debba consistere nel combinare armoniosamente la disciplina della *privacy* e delle limitazioni all'esercizio del potere di controllo datoriale, nel difficile bilanciamento tra l'accompagnamento del progresso e la necessità di evitare che lo stesso vada a travolgere i diritti dell'individuo. Se la scelta di sommare le due discipline può sembrare condivisibile, così come l'ampliare il raggio di responsabilizzazione del singolo, più vicino alla realtà da regolare e quindi maggiormente in grado di gestirla, e il rilievo della trasparenza, utile al fine di rendere edotti i lavoratori del livello di monitoraggio cui sono sottoposti, talvolta i meccanismi adottati rischiano di essere eccessivamente improntati a formalismi poco efficaci.

Si pensi, in proposito, alla recente modifica in merito all'obbligo informativo gravante sul datore di lavoro nei confronti del lavoratore operata dal c.d. Decreto Trasparenza, per come modificato dal c.d. Decreto Lavoro. In merito, difatti, pare trattarsi di normative condivisibilmente dirette a ridurre le asimmetrie informative; il rischio, tuttavia, è che le stesse risultino poco idonee a incidere sul dislivello di poteri tra le parti contrattuali, inserite in un mercato del lavoro precario, con un'ampia percentuale di disoccupazione, inoccupazione e *working poors*. Una volta informato della sottoposizione ad un monitoraggio costante e delle relative conseguenze, il lavoratore accetterà di iniziare o proseguire il rapporto di lavoro, o preferirà proseguire la ricerca, con il rischio di ritrovarsi nella stessa situazione presso altri *competitors*? Rimane sullo sfondo la domanda di fondo, se cioè la trasparenza consenta una maggiore libertà di scelta tra il "divenire avatar" o "restare operaio", ovvero si esaurisca in una mera formalità, che, pur consentendo una maggiore consapevolezza del lavoratore non gli lascia altra scelta a quella di prendere atto delle nuove, mutate, condizioni generali del lavoro.

VII.
IDENTITÀ DIGITALE E RISERVATEZZA

di *Marco Rossetti*

Sommario: 7.1. Non siamo romantici. — 7.2. Alla ricerca dell'identità perduta. — 7.3. L'identità personale. — 7.4. L'*identità digitale* nella legislazione comunitaria. — 7.5. L'*identità digitale* nella legislazione nazionale. — 7.6. Mondo digitale e riservatezza: una *liaison dangereuse*. — 7.7. Identità digitale e tutela della riservatezza.

7.1. Non siamo romantici

"Ah, sciagurato! / Va', mi lascia! Scorda un nome ch'è infamato": così implora la disperata Violetta nel II atto della *Traviata*.

Scongiurando Alfredo di interrompere la loro relazione, Violetta non gli disse: "*dimenticami*"; gli disse "dimentica *il mio nome*".

Quanto fu felice quella metonimia pensata dal librettista! Nessun altro aspetto della persona, infatti, più del nome riesce a sintetizzare in un solo segno un intero vissuto: dal colore degli occhi alle inclinazioni morali.

Se la triste storia di Alfredo Germont e Violetta Valèry dovessimo ambientarla ai giorni nostri, quell'accorata implorazione non basterebbe più. Violetta probabilmente avrebbe dovuto implorare l'amato dicendogli: "*dimentica il mio account*". Anzi, "*i miei account*".

Un po' perché oggi siamo meno romantici; un po' perché oggi il nome è solo uno dei segni, e forse neanche il principale, che ci *identificano* nelle relazioni con gli altri. Tanto in quelle giuridiche, quanto in quelle sociali. Insomma, alla domanda: "*chi sei?*" il nome non è più una risposta obbligata.

Ma il nome (inteso come prenome e cognome *ex* art. 6 c.c.) è stato per secoli il segno di identificazione per eccellenza della persona, e dunque il mezzo di riconoscimento della sua *identità*.

La proliferazione dei segni di identificazione ha comportato quindi la proliferazione delle identità.

Nelle relazioni (tristemente) sorte o coltivate con la mediazione meccanica dei *social network*, il nome può essere sostituito dal *nomignolo* ("nickname", il quale giuridicamente parlando è uno pseudonimo *ex* art. 9 c.c.); nelle relazioni con fornitori di servizi o beni mediate dal *web* il nome

può essere sostituito da un codice alfanumerico chiamato con una strana parola che nella nostra bella lingua suonerebbe come "conto utente" (*account*); nei rapporti con le pubbliche amministrazioni il nome può essere sostituito da una coppia di credenziali (*userid* e *password*).

Per di più, mentre ognuno di noi ha un (solo) nome di cui all'art. 6 c.c., nelle relazioni mediate dal *web* o da qualsiasi applicazione informatica, una sola persona può avere plurimi e diversi segni identificativi: spesso uno per ogni relazione che deve intrattenere col suo "interlocutore" informatico. Avrò uno *UserId* ed una password per pagare le contravvenzioni, un altro per pagare le bollette, un altro ancora per consultare il registro elettronico dei voti scolastici dei miei figli, un quarto per leggere il quotidiano *on line,* e così via *ad libitum*.

E per ciascuno di questi usi il mio "nome" digitale potrà essere diverso, ed io sarò una persona diversa per ciascuna delle macchine che riceve le mie richieste. In tal modo l'individualità della persona in quanto tale si polverizza in una miriade di codici che ne identificano solo un aspetto, un'attività, un gesto. La persona scompare, sostituita dall'ombra delle azioni che compie.

Oggi, insomma, può dirsi realizzata la profezia di Vitangelo Moscarda: per il *web* sono uno, ma posso essere anche centomila, ed in definitiva non sono nessuno.

7.2. Alla ricerca dell'identità perduta

Se oggi una persona non si identifica più soltanto in base al nome, sorge il problema di stabilire se i nuovi ed ulteriori segni di identificazione possano ritenersi elementi costitutivi della sua identità.

Ed in caso di risposta affermativa al quesito che precede, sorge l'ulteriore problema di stabilire se questa "*identità digitale*" sia un diritto; di quale natura; che tipi di tutela riceva dalla legge.

Per rispondere a questi quesiti occorre muovere dalla nozione di *identità personale*. Se, infatti, non ci si accorda sui contenuti di questa nozione, diverrebbe impossibile stabilire quali elementi essa includa, e quali ne restino fuori.

Anticipando quanto si dirà meglio nel prosieguo del presente scritto, ai quesiti appena anticipati deve rispondersi che:

— l'identità personale è nozione multifattoriale, che non comprende solo il nome;

— l'identità personale include i segni di identificazione scelti od utilizzati per le attività mediate dal *web* o da *software* applicativi;

— anche questi segni identificativi diversi dal nome formano oggetto d'un *diritto della persona*, che per convenzione potremmo anche chiamare

"*identità digitale*", purché sia ben chiaro che questo sintagma è solo una convenzione terminologica, per designare uno dei tanti aspetti di cui si compone l'identità personale; e che ogni persona ha uno ed un solo diritto alla propria identità personale;

— il diritto all'*identità digitale* forma oggetto ormai di previsioni normative e di atti paranormativi copiosi, ridondanti e non sempre coordinati, sicché è complesso per l'interprete ricostruirne con certezza i confini e le forme di tutela;

— gli elementi identificativi della persona che formano oggetto del diritto all'*identità digitale* beneficiano in astratto della tutela prevista in linea generale per tutti i dati personali.

Tuttavia l'applicazione al diritto all'identità digitale, per come è stato conformato dal legislatore comunitario (1), delle regole dettate a tutela dei dati personali, presenta molti problemi, che discendono da tre contraddizioni irrisolte:

a) quello all'*identità digitale* è un diritto *della persona* assoluto, ma non indisponibile;

b) l'identità digitale è un segno di identificazione, ma si consente ad ogni persona di averne più d'una;

c) la legge nello stesso tempo pretende di tutelare le identità digitali, ma ne consente la *mercificazione*.

Nelle pagine che seguono affronteremo questi problemi nell'ordine in cui sono stati esposti.

Muoveremo quindi dal ripercorrere la nozione di "identità personale", per poi introdurre quella di "identità digitale", esaminarne i contenuti, i limiti, le forme di tutela sul piano della riservatezza, ed infine le suesposte contraddizioni irrisolte.

---

(1) Mi ostino a definire tale, piuttosto che "eurounitario", il diritto dell'Unione Europea. Anche a tacer, infatti, qualsiasi considerazione linguistico-semantica, credo che i lemmi entrati nell'uso sia meglio non toccarli, per evitare confusioni. Del resto chi discorre di "diritto eurounitario" appare più realista del re, posto che, anche dopo la trasformazione della Comunità Economica Europea in Unione Europea (disposta dal Trattato di Lisbona), la Commissione europea, il Consiglio, il Parlamento e la Corte di Giustizia hanno continuato ad usare tranquillamente nei loro atti le espressioni "*diritto comunitario*", "*regolamento comunitario*", "*azione comunitaria*", e via dicendo. Né meno significativo è che nel sito "Eurlex" il lemma "eurounitario" compare solo in 12 documenti su svariate centinaia di migliaia: e precisamente in 12 sentenze della Corte di Giustizia, pronunciate su questioni ad essa rimesse da giudici italiani, nelle cui motivazioni quell'aggettivo compare solo nella trascrizione delle questioni sollevate dal giudice rimettente.

7.3. L'identità personale

Secondo il più noto *thesaurus* della lingua italiana, l'identità è "*l'insieme delle indicazioni, delle generalità, dei caratteri individuali, dei dati anagrafici che consente il riconoscimento di una persona*" (2).

Il concetto di "identità" non esprime dunque solo il nome d'una persona, ma l'insieme delle caratteristiche che la rendono diversa da tutte le altre. L'identità personale, dunque, è l'insieme sia del nome, sia dei "caratteri morfologici, fisici, psichici, chimici, di rapporto e di proporzione" di quella persona (3).

Che la propria identità fosse un diritto (il diritto di "distinguersi e di essere distinto dagli altri" (4)), e che la sua lesione fosse un atto antigiuridico non si creda sia una novità dei nostri anni.

L'uso fraudolento del nome altrui era illecito già nel diritto romano classico (5), sia pure alla condizione che da esso fosse derivato pregiudizio ad un terzo. Spenta la grandezza di Roma e dispersa la capillare amministrazione imperiale, le signorie ed i feudatari altomedioevali si trovarono nell'impossibilità di *identificare* in modo certo ogni suddito, compito che fu assunto, ma senza coordinamento, dai registri in cui i parroci annotavano battesimi, matrimoni e funerali.

a) Con l'emersione degli Stati centralizzati moderni risorse l'interesse dello Stato alla conoscenza per nome dei cittadini, giustificato da esigenze militari, giudiziarie e fiscali (6).

Questa circostanza fece sorgere l'idea che fosse interesse soltanto dello Stato conservare i nomi e garantirne l'immutabilità, e che di conseguenza il

---

(2) S. Battaglia, *Grande Dizionario della Lingua Italiana*, vol. VII, 210, *ad vocem*. "Identità" deriva dall'avverbio latino *identidem*, a sua volta derivato dalla locuzione "*idem et idem*", e cioè "lo stesso, ripetutamente".

(3) Così già G. Falco, *Identità personale*, in *Nuovo digesto it*., vol. VI, 649, Torino, 1938-XVI, 649.

(4) È la definizione di G. Bavetta, *Identità (diritto alla)*, in *Enc. del dir*., vol. XIX, Milano, 1970, 953.

(5) Già Papiniano (II sec.) ammoniva che *falsi nominis vel cognominis asseveratio poena falsi coercetur* (Dig., XLVIII, 10, 13, pr.), ed infatti una legge di poco posteriore degli imperatori Diocleziano e Massimiano (tramandata da *Codex*, IX, 25) stabiliva che la scelta del nome è riservata ai privati, ma questi non possono mutarlo a loro piacimento se ciò rechi danni ai terzi ignari (*sicut in initio nominis, cognominis, praenominis, recognoscendi singulos, impositio libera est privatis; ita eorum mutatio innocentibus periculosa non est. Mutare itaque nomen, vel praenomen [sive cognomen] sine aliqua fraude licito iure, si liber es, secundum ea quae saepe statuta sunt, minime prohiberis; nullo ex hoc praeiudicio futuro*; concetto ribadito nelle Istituzioni di Giustiniano: II, 20, 29).

(6) E. Spagnesi, *Nome (storia)*, in *Enc. del dir*., vol. XXVIII, Milano, 1978, 290; A. De Cupis, *Nome e cognome*, in *Noviss. dig. it*., vol. XI, Torino, 1965, 299.

nome e l'identità personale non sarebbero altro che "*una istituzione di polizia civile*", una "*matricola*", necessaria ai fini di buona amministrazione (7), di qui sorse la c.d. *concezione pubblicistica* del nome e dei segni di identificazione, secondo cui la lesione del diritto al nome costituiva innanzitutto un illecito nei confronti dello Stato, mentre nei confronti dell'individuo poteva costituire un danno risarcibile soltanto in presenza di un pregiudizio ulteriore. Se, infatti, il nome costituiva "oggetto" di un interesse dello Stato, e non di un diritto dell'individuo, la sua lesione non poteva costituire danno di per sé, ma soltanto ove fosse allegato e dimostrato, giustappunto, un pregiudizio ulteriore (il che, sia detto incidentalmente, per la dottrina meno recente, era un merito per la concezione pubblicistica del diritto al nome).

In contrapposizione alla tesi pubblicistica del diritto all'identità si venne tuttavia sviluppando già alla fine del XIX sec. l'opposta concezione c.d. *privatistica*, secondo cui l'identità personale e *in primis* il nome, che di essa costituiva l'elemento più evidente, costituivano oggetto d'un diritto assimilabile a quello di proprietà. L'individuo, secondo questa concezione, era proprietario del suo nome e della sua identità, con la conseguenza che qualsiasi usurpazione, scambio, violazione, contestazione da parte di terzi poteva configurare un atto illecito, così come in tema di proprietà il pregiudizio è insito nella contestazione (8).

b) La dottrina moderna ha abbandonato sia la concezione pubblicistica dell'identità personale basata solo sul nome, a sua volta inteso quale "misura di polizia sociale", sia quella privatistica dell'identità personale quale oggetto di un diritto di proprietà, ogni vincolo tra il nome e la persona che lo portava (assimilando il primo ad una sorta di "placca d'immatricolazione"), in quanto il nome costituisce parte essenziale del patrimonio morale d'ogni individuo.

Alla concezione privatistica, invece, sono stati mossi due ordini di rilievi.

Il primo è che l'oggetto della proprietà è necessariamente esterno rispetto al titolare di essa, mentre l'identità non è un qualcosa di esterno all'individuo, ma costituisce parte integrante di quest'ultimo (9).

Il secondo rilievo è che le norme sulla proprietà sono inapplicabili ai segni identificativi della persona, in quanto talora inutili e talaltra eccessivamente rigorose. Ad esempio, il bene oggetto di proprietà non può essere usato da terzi senza la volontà del proprietario, mentre il nome altrui ben può essere usato da terzi, quando non se ne approprino o lo attribuiscano ad altri

---

(7) Per riferimenti, E. Capizzano, *La tutela del diritto al nome civile*, in *Riv. dir. comm.*, 1962, I, 249.

(8) E. Capizzano, *op. ult. cit.*, 252-253.

(9) A. De Cupis, *op. ult. cit.*, 300.

(come nel caso di citazione del nome in un'opera storica), ovvero nei casi di omonimia (10).

c) Bandite le teorie pubblicistica e privatistica, l'identità personale fu più rettamente intesa come "il patrimonio ideologico dell'individuo".

Non solo dunque il suo nome e il suo volto, ma il complesso delle opinioni politiche, sociali, religiose, professionali, e via dicendo, da lui professate e manifestate all'esterno.

L'identità personale è perciò anche definita "immagine sociale", formula che meglio esprime il carattere individualizzante di questo concetto (11).

L'identità personale forma oggetto di un diritto personalissimo ed inviolabile dell'individuo, pacificamente ricompreso tra i diritti inviolabili di cui è menzione nell'art. 2 Cost., e la sua lesione può essere fonte d'un danno non patrimoniale.

L'identità personale viene lesa quando ad una persona siano pubblicamente attribuite opinioni che non ha, oppure convinzioni che non nutre, od ancora stili di vita che non pratica, e che siano antitetici rispetto a quelli suoi propri. Così ad es., nella sentenza "capostipite" in tema di risarcimento del danno da lesione dell'identità personale, la Corte di Cassazione ritenne sussistente tale pregiudizio in un caso in cui una ditta produttrice di tabacchi, per avvalorare una campagna promozionale della vendita di sigarette c.d. "leggere", estrapolò alcune frasi da un'intervista concessa dal direttore dell'Istituto Nazionale per lo studio e la cura dei tumori, le quali presentate in modo avulso dal contesto in cui erano state pronunciate, lasciavano

---

(10) Così si esprimeva, su questi aspetti, la Corte di Cassazione di Torino già un secolo e mezzo fa: "*a tutelare* [il nome] *non sempre a proposito si potrebbe invocare l'applicazione di tutti quei principii di diritto che regolano e proteggono la proprietà delle cose materiali.*

Un nome può essere comune a più individui, a più famiglie, senza che ne venga scemato il pregio e il godimento a ciascuno di coloro che lo portano; il nome di una persona o di una famiglia può essere impunemente citato nella narrazione di un fatto storico, può servire d'indicazione di una località, di un fondo o di altra cosa qualunque, piaccia o non piaccia a coloro a cui appartiene; e in questi casi, come in altri consimili, che si ripetono all'infinito nei rapporti del giure civile, sarebbe inattuabile in termini assoluti il principio dell'inviolabilità, quale viene concessa al proprietario di una cosa immateriale" (Cass. Torino, 7 agosto 1883, in *Foro it*., 1883, I, 1052).

(11) Per tutti, su questi concetti, resta sempre valido V. Zeno-Zencovich, *Identità personale*, in Digesto civ., vol. IX, Torino 1993, 294 e ss.; più di recente, G. Mantovani, *Identità personale*, in *Encicl. bioetica e scienza giur*., Napoli, 2014, 43; M. La Torre, *Il nome: contrassegno dell'identità personale*, in Giust. civ., 2013, II, 443; F. D. Busnelli, *La persona alla ricerca dell'identità*, in E. Del Prato (a cura di), *Studi in onore di Antonino Cataudella*, Napoli, 2013, 317; G. Finocchiaro, *Identità personale (diritto alla) [aggiornamento-2010]*, in *Digesto civ*., Torino, 721; C. Honorati, *Diritto al nome e all'identità personale nell'ordinamento europeo*, Milano, 2010, *passim*; A. Cappelli, *Il diritto all'identità personale*, in *Vita not*., 2004, 1143.

intendere al lettore che lo scienziato, anziché dirsi contrario ad ogni uso di tabacco, si fosse espresso in senso favorevole al consumo di dette sigarette (12).

Perché sussista una lesione dell'identità personale ovviamente non è sufficiente che siano attribuite a taluno opinioni non sue, ma è necessario che tali opinioni siano radicalmente contrastanti con quelle del danneggiato, e soprattutto che siano tali da presentarlo agli occhi dell'opinione pubblica come persona diversa di convinzioni diverse da quelle effettivamente possedute. Così, ad esempio, è stata ritenuta sussistente tale lesione:

— nel sottacere al proprio figlio le vere generalità del padre biologico (13);

— nel pubblicizzare i propri prodotti (nella specie, capi di vestiario) mediante la diffusione non autorizzata di un noto attore (14);

— nell'attribuire ad un uomo politico, da sempre sostenitore della inderogabilità dello stato di diritto, della volontà di trattare con un gruppo di terroristi rapitori di altro uomo politico (15);

— nell'attribuire ad un pubblico ufficiale la qualità di massone (16);

— nell'attribuire a taluno l'adesione ad una manifestazione celebrativa del centenario della nascita di Benito Mussolini (17);

— nell'attribuire falsamente ad un uomo politico di opinioni contrastanti con quelle del proprio partito (18);

— nell'estrapolare brani letterari o musicali dal contesto originario per inserirli in altri contesti, quando ciò produca un risultato profondamente

---

(12) Cass., 22 giugno 1985, n. 3769, in *Giust. civ*., 1985, I, 3049. Curiosamente, quindici anni prima, la Corte aveva negato che i titoli nobiliari potessero rientrare nell'oggetto del diritto all'identità personale (Cass. civ., sez. I, 13 luglio 1971, n. 2242, in *Dir. fam*., 1973, I, 939, con nota di Liguori, *Rapporti familiari, segni distintivi della personalità e tutela degli attributi familiari*).

Dopo la sentenza "capostipite" del 1985, il "diritto all'identità personale" ha conosciuto straordinarie fortune, ed è stato riconosciuto anche ad associazioni non riconosciute, quali i partiti politici: anch'essi, si è stabilito, hanno il diritto di distinguersi ed essere distinti dagli altri enti consimili, e tale diritto si traduce nell'uso esclusivo della denominazione e del segno distintivo (Cass. civ., sez. I, ord. 16 giugno 2020, n. 11635).

(13) Trib. minorenni Caltanissetta, 30 novembre 2018, in *Dir. famiglia*, 2019, 679.

(14) Trib. Roma, 23 novembre 2007, in *Foro it*., 2008, I, 1711.

(15) Trib. Roma, 27 marzo 1984, in *Resp. civ*., 1984, 562. In quel caso l'autore dell'articolo, il direttore del giornale e la società editrice furono condannati in solido al risarcimento dei danni non patrimoniali, liquidati in 70 milioni di lire.

(16) Trib. Roma, 15 novembre 1983, in *Foro it*., 1985, I, 281.

(17) Pret. Roma, 3 ottobre 1986, in *Dir. informazione e informatica*, 1987, 244.

(18) Trib. Napoli, 21 marzo 1994 (ord.), in *Dir. informazione e informatica*, 1994, 1029.

divergente dal genere e dallo stile per i quali l'autore era conosciuto ed apprezzato (19);

— nell'attribuire la paternità d'una corrente artistica a persona diversa da quella effettiva, non adeguatamente motivata sul piano della critica letteraria e per di più in contrasto con l'opinione largamente condivisa della comunità scientifica (20).

In alcune decisioni si è arrivati ad ammettere che il diritto alla tutela dell'identità personale del membro della famiglia premorto costituisce un diritto fondamentale dei congiunti dello stesso, rientrante nel « catalogo aperto » di cui all'art. 2 cost., e la cui lesione genera un danno risarcibile (21).

d) In conclusione l'identità personale è:

1) quanto alla natura, un diritto della persona;

2) quanto ai contenuti, una *sfera* che include qualsiasi elemento caratterizzante l'individuo, e quindi sia caratteri giuridici (il nome), sia caratteri fisici (l'immagine fisica), sia caratteri spirituali (le opinioni), sia caratteri relazionali (l'appartenenza a gruppi).

7.4. L'*identità digitale* nella legislazione comunitaria

Il sintagma "*identità digitale*" è nato nella prassi, per poi essere utilizzato anche dalla legislazione nazionale ed europea. Non sempre è stato usato in modo univoco; spesso lo è stato in modo polisemico; ancor oggi non può dirsi che la nozione di "*identità digitale*" dettata dalla legge coincida con l'identica espressione usata nella prassi forense e giudiziaria.

Sarà dunque utile innanzitutto ricordare brevemente cosa sia per la legge l'identità digitale, per poi passare a stabilire se sia un diritto, di che tipo, e come si coniughi col diritto alla riservatezza.

La legislazione comunitaria non contempla atti normativi (Regolamenti e Direttive) che diano una definizione di "*identità digitale*".

Tuttavia la materia dei dati di identificazione personale attraverso strumenti elettronici è contemplata dal Regolamento (il Regolamento 23 luglio 2014 n. 910/14, c.d. "Regolamento eIDAS").

Questo Regolamento definisce e disciplina, per quanto qui rileva, "mezzi", "regime" e "dati" di identificazione digitale.

I mezzi di identificazione elettronica sono "*un'unità materiale e/o im-*

(19) *Ex multis*, Trib. Roma, 11 dicembre 2002, in *Dir. informazione e informatica*, 2003, 149; Trib. Milano, 18 luglio 1994, in *Annali it. dir. autore*, 1994, 606; Trib. Roma, 9 giugno 1993, in *Dir. informazione e informatica*, 1993, 972.

(20) Trib. Roma, 9 dicembre 2003, in *Dir. e giustizia*, 2004, fasc. 9, 100.

(21) Trib. Roma, 29 giugno 1998, in *Resp. civ.*, 1999, 477.

materiale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online": ad esempio, una password (art. 3, n. 2).

Il regime di identificazione è "*l'insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica*" (art. 3, n. 4).

I dati di identificazione elettronica, infine, sono definiti come "*un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona giuridica*" (art. 3, n. 3).

Stando al Regolamento eIDAS, pertanto, l'identità digitale dovrebbe definirsi e farsi coincidente con i "dati di identificazione".

Questo Regolamento tuttavia non ha una portata universale.

Esso venne concepito per garantire la c.d. "interoperabilità" tra i vari sistemi di identificazione adottati dai vari Stati membri. Il suo scopo era garantire il riconoscimento reciproco, non dettare una disciplina generale dell'identità digitale. Esso, inoltre, riguardava solo i mezzi di identificazione utilizzati dalle pubbliche amministrazioni, ma non quelli da privati in relazione a rapporti di diritto privato (22).

a) L'espressione "identità digitale" comparve per la prima volta (23) in un atto normativo dell'Unione Europea nell'Allegato I al Regolamento 11 dicembre 2013, 1291/13 (oggi abrogato), che istituì "*il programma quadro di ricerca e innovazione (2014-2020) - Orizzonte 2020*", e nella successiva Decisione del Consiglio del 3 dicembre 2013, che a quel Regolamento diede attuazione. Ma né nell'uno, né nell'altro di quei testi l'espressione "*identità digitale"* costituiva una definizione legale o se ne stabiliva il contenuto. Il Regolamento 1291/13 era infatti una specie di "libro dei sogni" di molte decine di pagine, contenente l'elenco di tutto quel che l'Unione avrebbe dovuto realizzare negli anni a venire (una specie di "piano quinquennale", insomma). Tra questi obiettivi si prevedeva [§ 3.7, lettera *a*), dell'Allegato] che l'Unione avrebbe dovuto garantire la sicurezza dei cittadini contro il rischio di attentati e frodi anche "*valutando del rendimento operativo delle tecnologie relative all'identità personale ("identità digitale")*".

Seguirono lunghi anni di silenzio normativo.

---

(22) Su tale regolamento si vedano, da ultimo ma *ex plurimis*, A. Ortalda e S. Leucci, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Riv. it. informatica e dir.*, 2022, 145.

(23) Tralascio gli atti nei quali tale espressione venne usata in senso aspecifico ed incongruo rispetto al tema qui in discussione: ad es., nell'allegato alla Rettifica della decisione 2009/767/CE della Commissione, del 16 ottobre 2009, in cui quel sintagma compare solo tra le istruzioni sulla compilazione di un modulo.

b) Poi, dal 2021, l'*identità digitale* inizia a comparire sempre più spesso nei lavori preparatori e nei testi normativi dell'Unione.

Innanzitutto il Regolamento 12 febbraio 2021, n. 2021/241 ("*che istituisce il dispositivo per la ripresa e la resilienza*", cioè il Regolamento che dispensò denari a fiumi per fronteggiare la crisi causata dalla pandemia da Covid-19) stabilì che gli Stati membri, per accedere ai fondi dell'unione, dovessero soddisfare vari requisiti, tra cui garantire nei propri progetti una adeguata transizione digitale, di cui doveva essere componente "l'*applicazione del regime europeo di identità digitale per uso pubblico e privato*" (all'Allegato VII, punto 011-*ter*; tale "regime europeo" tuttavia, come si dirò tra breve è ancora di là da venire).

Anche tale previsione, dunque, è sostanzialmente irrilevante ai nostri fini.

c) Pochi mesi dopo il Regolamento su "*ripresa e resilienza*" seguì la Comunicazione inviata dalla Commissione al Parlamento ed al Consiglio [del 9 marzo 2012, COM (2021)118], intitolata "*Bussola per il digitale 2030: il modello europeo per il decennio digitale*", o più brevemente *Digital Compass* (24).

Si tratta d'una corposa dichiarazione programmatica, che si prefigge, tra gli altri due obiettivi: aumentare le competenze informatiche (25) quelle della popolazione e dei professionisti, ed incrementare le infrastrutture digitali degli Stati membri. Per conseguire questi due obiettivi, la Commissione prevede (§ 3.3) che entro il 2030 dovrebbe (il condizionale è d'obbligo!) essere raggiunta "*un'ampia diffusione di un'identità affidabile e controllata dagli utenti, consentendo a ciascun cittadino di controllare le proprie interazioni e la propria presenza online.*

Gli utenti potranno utilizzare appieno e facilmente i servizi on line in tutta l'UE, preservando nel contempo la loro vita privata".

Ovviamente la "Comunicazione" del 9 marzo 2021 non è un atto normativo, e non ha introdotto alcuna norma cui l'interprete possa fare riferimento per delimitare il concetto di "identità digitale".

d) La Raccomandazione 3 giugno 2021, n. 2021/946 della Commissione. Questa Raccomandazione chiese agli Stati membri di adoperarsi per introdurre "*un'architettura tecnica e un quadro di riferimento che stabiliscano il*

---

(24) Sulla quale si veda M. R. Allegri, *Il futuro digitale dell'Unione europea: nuove categorie di intermediari digitali, nuove forme di responsabilità*, in *Riv. it. informatica e dir.*, 2021, 2.

(25) "*Competenze digitali*", le chiama il documento, con espressione purtroppo largamente diffusa. Ma in italiano dire "competenza digitale" fa venire in mente solo l'abilità del pianista o del prestigiatore.

funzionamento del quadro europeo relativo a un'identità digitale in conformità al regolamento eIDAS ([26])*, tenendo conto della proposta della Commissione su un quadro europeo relativo a un'identità digitale*".

Il senso della Raccomandazione possiamo così riassumerlo: "io Commissione sto lavorando ad una disciplina comune che consenta a tutti i cittadini dell'Unione di disporre di "*portafogli digitali personali autodeterminati che consentano un accesso sicuro e agevole a diversi servizi, sia pubblici che privati, sotto il totale controllo degli utenti*". In pratica, un meccanismo che consenta, con un solo identificativo, di accedere ai vari servizi offerti dalla rete o per mezzo della rete *web*, senza doversi registrare ogni volta che si chieda un servizio ad un diverso fornitore, lasciando a questo il possesso e la gestione dei dati dell'utente.

Un richiamo — talmente generico da far sorridere — alla necessità di introdurre nuove regole in tema di identità digitale è contenuto nella successiva Raccomandazione 3 ottobre 2023, n. 2023/2113 della Commissione, "*relativa ai settori tecnologici critici per la sicurezza economica dell'UE ai fini di un'ulteriore valutazione dei rischi con gli Stati membri*". In pratica, il richiamo all'identità digitale compare nell'Allegato alla Raccomandazione, che elenca "*i 10 settori tecnologici critici per la sicurezza economica dell'UE*".

Va da sé che tali Raccomandazioni non hanno alcun carattere vincolante, anzi, non sono nemmeno fonti di produzione.

e) La nozione di "identità digitale" acquista un (modesto) spessore ed un meno oscuro significato solo con la "*Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*", adottata dal Parlamento, da Consiglio e dalla Commissione il 23 gennaio 2023.

Il punto 7 della dichiarazione, rubricato "*Servizi pubblici digitali online*", impegna Parlamento, Commissione e Consiglio "*a garantire che a tutte le persone che vivono nell'UE sia offerta la possibilità di utilizzare un'identità digitale accessibile, volontaria, sicura e affidabile, che dia accesso a un'ampia gamma di servizi online*".

Badi il lettore a due circostanze: innanzitutto la suddetta dichiarazione di impegno è sussunta in un paragrafo dedicato ai "servizi pubblici", non alle transazioni tra privati; in secondo luogo essa riprende l'auspicio della Raccomandazione n. 2023/2113, già ricordata al § precedente. Insomma, negli intenti del legislatore comunitario, l'identità digitale si riduce a ciò: mettere in tasca a ciascun cittadino una chiave unica per accedere a una molteplicità di servizi.

([26]) È il Regolamento n. 910/14 "*in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno*", del quale si dirà meglio più oltre.

Anche la "Dichiarazione" qui in esame, tuttavia, non è certo una norma di diritto vincolante per gli Stati membri. Si tratta solo d'una bella promessa, inutile per l'interprete.

f) Se tuttavia l'Unione Europea sinora non ci ha dato norme rilevanti per la definizione del concetto di "identità digitale", ben altra è la conclusione cui pervenire se si bada al diritto *in itinere.*

Viene in rilievo sotto questo profilo la proposta di modifica del Regolamento n. 910/2014, recante "*l'istituzione di un quadro per un'identità digitale europea"* [COM/2021/281].

Ricordiamo che il Regolamento 910/14 (c.d. "Regolamento eIDAS", sul quale dovremo tornare tra breve) è l'importante fonte che disciplina l'identificazione elettronica ed i servizi fiduciari per le transazioni elettroniche nel mercato interno.

La proposta di modifica di tale Regolamento, presentata il 3 giugno 2021, si fonda su alcuni rilievi critici, e si prefigge alcuni obiettivi.

I rilievi su cui si fonda la proposta di introduzione di una "identità digitale europea" sono — detto molto semplicemente — essenzialmente tre: *a)* solo una parte dei cittadini europei può disporre di criteri di identificazione elettronici affidabili e sicuri, tanto nei rapporti con le amministrazioni, quanto nei rapporti con i privati; *b)* i sistemi di identificazione adottati dagli Stati membri non sono validi per tutti gli altri, con la conseguenza che "*pochissimi servizi pubblici online accessibili a livello nazionale sono raggiungibili a livello transfrontaliero attraverso la rete eIDAS"*; (c) gli utenti di servizi informatici non hanno il pieno controllo dei propri dati, una volta che questi siano stati affidati al gestore dei servizi.

L'obiettivo della proposta è "*il passaggio dalla dipendenza esclusiva da soluzioni di identità digitale nazionali alla fornitura di attestati elettronici di attributi validi a livello europeo*": in pratica, l'identificazione dell'utente eseguita da un fornitore di servizi digitali in Italia, dovrà essere valida e riconosciuta in tutti gli altri Stati membri.

Per realizzare questo scopo la proposta di Regolamento prevede che i fornitori di servizi digitali si dotino di "*portafogli europei di identità digitale*", vale a dire uno strumento "*che consente all'utente di conservare dati di identità, credenziali e attributi collegati alla sua identità, fornirli su richiesta alle parti facenti affidamento sulla certificazione e utilizzarli per l'autenticazione, online e offline, per un servizio*" (27).

In pratica, scopo del "portafoglio digitale europeo" è collegare i dati che

(27) L'esistenza e il concreto funzionamento dei "portafogli europei di identità digitale" sono dati per presupposti dalla coeva proposta di Regolamento sull'istituzione "dell'euro digitale", presentata il 28 giugno 2023 [COM/2023/369].

identificano informaticamente una persona nei rapporti con l'amministrazione finanziaria (ad es., la chiave di accesso al sistema SPID) ad altri servizi (per esempio, l'amministrazione dei trasporti, le università, le banche). Questi "portafogli", rilasciati dalla P.A. o da privati a ciò autorizzati, permetterebbero al titolare di accedere a servizi *on line* senza doversi ogni volta identificare presso il gestore di questi, e soprattutto — ecco la novità — senza affidare al gestore del servizio i propri dati personali, perdendone il controllo e restando all'oscuro dell'uso che di essi farà il gestore.

La proposta di Regolamento, dunque, non *definisce*, ma *presuppone* la nozione di identità digitale, e la intende come sinonimo dell'insieme di dati che consentano di identificare univocamente l'utente di un servizio o prodotto elettronico.

In ogni caso la proposta non sembra di pronta approvazione: dopo tre anni dalla sua presentazione, dal 7 dicembre 2022 è in discussione al Consiglio (procedura 2021/0136/COD).

7.5. L'*identità digitale* nella legislazione nazionale

Nell'ordinamento la prima definizione di "identità digitale" comparve più di dieci anni fa, in un testo regolamentare in attuazione del "Codice dell'amministrazione digitale" ([28]), contenente le regole tecniche per l'identificazione del titolare della casella di posta elettronica certificata. Si trattava dell'art. 1, lettera *h*), d.p.c.m. 27 settembre 2012, il quale definiva l'"identità digitale" come "*la rappresentazione informatica della corrispondenza biunivoca tra una persona fisica ed i suoi dati d'identità*".

Questa definizione fu ampliata negli atti normativi successivi, ed estesa ad ambiti ulteriori rispetto all'identificazione del titolare d'una casella di posta elettronica, ma a qualsiasi fine.

In particolare col d.l. 21 giugno 2013, n. 69, novellando il d.lgs. 7 marzo 2005, n. 82, fu introdotto il "Sistema Pubblico per la gestione dell'Identità Digitale di cittadini ed imprese" (SPID), definito come "*un insieme aperto di soggetti pubblici e privati che, previo accreditamento da parte dell'Agenzia per l'Italia digitale (...) gestiscono i servizi di registrazione e di messa a disposizione delle credenziali e degli strumenti di accesso in rete nei riguardi di cittadini e imprese per conto delle pubbliche amministrazioni, in qualità di erogatori di servizi in rete, ovvero, direttamente, su richiesta degli interessati*" ([29]).

([28]) D.lgs. 7 marzo 2005, n. 82.

([29]) Lo SPID ha avuto un grande successo. Prova ne sia che la legge finanziaria del 2020 (l. 30 dicembre 2022 n. 178), all'art. 1, comma 622, stabilì una elargizione (chiamata "indennità di architettura e di gestione operativa") ai gestori del servizio SPID, "*considerate*

In attuazione di tale previsione il successivo d.p.c.m. 24 ottobre 2014 stabilì le caratteristiche del sistema di identificazione SPID, ed all'art. 1, lettera *o*), definì l'identità digitale come "*la rappresentazione informatica della corrispondenza biunivoca tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità di cui al presente decreto e dei suoi regolamenti attuativi*".

Si noti come:

— la definizione del 2012 definisce l'identità digitale come la rappresentazione informatica d'una "persona fisica", quella del 2014 come la rappresentazione informatica d'un "utente";

— la definizione del 2012 fa riferimento ai "dati d'identità", quella del 2014 agli "attributi identificativi";

— la definizione del 2012 nulla dice sui criteri di riscontro, quella del 2014 stabilisce che gli attributi identificativi dell'identità digitale sono solo quelli "*raccolti e registrati in forma digitale*".

Pochi mesi dopo questi interventi, la definizione di "identità digitale" fu inserita nelle definizioni generali premesse al codice dell'amministrazione digitale, già ricordato (d.lgs. 82 del 2005). In particolare, il d.l. 26 agosto 2016, n. 179, modificò l'art. 1, d.lgs. n. 82 del 2005, inserendo la lettera *u-quater*) che definì l'identità digitale come "*la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme dei dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64*".

Come si noterà, nella definizione del 2016 scomparve l'aggettivo "biunivoca", che invece nelle definizioni precedenti qualificava la corrispondenza tra l'utente ed i suoi "attributi identificativi". È impossibile stabilire se fu mero errore degli addetti al *drafting* o scelta deliberata, ma va da sé che una "identità digitale" che non garantisca una corrispondenza "biunivoca", cioè esclusiva di altre possibili corrispondenze ed identificazioni, serve a ben poco.

a) La nozione di "identità digitale", per come definita dall'art. 1, lettera *u-quater*), d.lgs. n. 82 del 2005 è richiamata o presupposta da molti provvedimenti normativi e regolamentari regionali. Tralasciando le centinaia di provvedimenti che raccomandano o impongono il ricorso al sistema SPID per avanzare istanze alle amministrazioni regionali, meritano di essere ricordati innanzitutto alcuni provvedimenti di "tutela" dell'identità digitale.

---

le iniziative e le attività di singole pubbliche amministrazioni che comportano un incremento significativo del numero medio di accessi al secondo al sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), per assicurare la sostenibilità tecnica ed economica dello SPID".

È il caso dell'art. 9-*bis* della l. reg. Lombardia 28 ottobre 2003, n. 20 (come modificato dall'art. 10 della l. reg. Lombardia 6 giugno 2019, n. 9), che nel quadro del contrasto al c.d. *cyberbullismo* ha affidato al Comitato Regionale per le Comunicazioni" (CORECOM) il compito di "*promuovere e realizzare iniziative (...) di tutela della reputazione e della identità digitale in rete*".

La legge lombarda evidentemente ha fatto da apripista, perché norme esattamente identiche sinanche *ad litteram* poco dopo sono state adottate dal legislatore laziale (art. 21-*bis* della l. reg. Lazio 28 ottobre 2016, n. 13, come modificato dall'art. 12, comma 1, lettera *b*), della l. reg. Lazio 11 agosto 2021, n. 14) e da quello calabrese (art. 3-*bis* della l. reg. Calabria 22 gennaio 2001, n. 2, come modificato dall'art. 9 l. reg. Calabria 23 dicembre 2022, n. 52).

Non è in verità del tutto chiaro in che modo i Comitati Regionali per le Comunicazioni possano "*tutelare l'identità digitale*", sicché non è azzardato sospettare che norme di questo tipo possano alla prova dei fatti ridursi al rango di mere dichiarazioni di intenti, o poco più.

b) Conclusivamente: la definizione normativa di "*identità digitale*" è una sfera concentrica di dimensioni minori rispetto alla nozione emersa dal diritto vivente di "identità personale".

Questa si riferisce a qualsiasi carattere identificativo della persona; quella si riferisce ai soli "attributi identificativi" dell'utente di un servizio informatico, *raccolti e registrati in forma digitale*.

Apparentemente ci troveremmo dunque in presenza di un rapporto da *genus* a *species*. Ma i "dati identificativi" dell'utente di un servizio informatico, possono ritenersi anch'essi oggetto d'un diritto *della persona*? Chi compra un paio di scarpe *on line* può dirsi leso nei suoi diritti fondamentali se il venditore fa un uso non autorizzato del nome utente (per di più di fantasia ed usato solo per quel servizio) e della chiave di accesso forniti dall'utente?

Ecco i quesiti cui è giunto il momento di rispondere.

Come si è visto in precedenza, per più di un secolo la dottrina giuridica discusse sulla natura del diritto al nome: se si trattasse d'un diritto reale o d'un diritto della persona. Ebbene, è sorprendete che la dottrina contemporanea, immemore di quel dibattito stia specularmente replicando lo stesso dibattito (30).

---

(30) Se ne veda un esaustivo ed aggiornato *resumé* in G. Proietti, *Algoritmi e interesse del titolare del trattamento nella circolazione dei dati personali*, in *Contratto e Impr.*, 2022, 880; il dibattito è illustrato anche da V. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inform.*, 2018, 4, 698.

Secondo taluni i dati identificativi digitali sono assimilabili ai "beni", e possono essere liberamente ceduti o venduti (31).

Un secondo orientamento all'opposto ritiene che i dati identificativi della persona, in quanto oggetto d'un diritto personale, non possano essere trasferiti dietro compenso (32).

Una teoria intermedia ritiene poi che il diritto sui dati digitali identificativi della persona non possa essere trasferito a titolo definitivo, ma es ne può accordare il godimento temporaneo, sempre revocabile *ad nutum* (33).

Non è mancato, infine, chi — non senza una buona dose di cinismo — ha capovolto il problema, così ragionando: siccome i dati digitali servono a tutti gli operatori economici del *web* per la profilazione dei clienti, sarebbe "ingiustificabile" limitare il trasferimento o il godimento delle *identità digitali* e di tutti i *footprint* lasciati dagli utenti del *web*, perché una limitazione di tal fatta "*potrebbe tradursi in un ostacolo al funzionamento dell'economia digitale, visto che in tale contesto risulta estremamente importante il libero accesso ai dati al fine di garantire il corretto funzionamento dei mercati*" (34). Il che val quanto dire che quel che si deve garantire è il funzionamento del mercato, non la libertà delle persone.

L'importanza pratica del dibattito è tuttavia molto attenuata (ma non eliminata) dall'art. 1, § 3, del RGPD, il quale — non senza una certa contraddittorietà rispetto ai roboanti proclami di tutti gli organi comunitari sull'importanza delle persone e dei loro diritti alla riservatezza — proclama solennemente che "*la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*". Il che val quanto dire

---

(31) G. D'Ippolito, *Commercializzazione dei dati personali: dato personale tra approccio morale e negoziale*, in *Dir. inform*., 2020, 634; Resta e V. Zeno-Zencovich, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ*., 2018, 414 ss.; G. Pitruzzella, *Big Data, Competition and Privacy: A look from the antitrust perspective*, in *Concorrenza e Mercato*, 2016, 16; G. Resta, *Diritti esclusivi e nuovi beni immateriali*, Torino, 2011, 38; V. Zeno-Zencovich, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, in Cuffaro, V. Ricchiuto e V. Zeno-Zencovich (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, 169.

(32) G. Alpa, *L'intelligenza artificiale. Il contesto giuridico*, Modena, 2021, 73; Id., *Il diritto di essere sé stessi*, Milano, 2021, 264; il tema fu anticipato già un quarto di secolo fa da S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv*., 1997, 583.

(33) B. Parenzo, *Sull'importanza del dire le cose come stanno: ovvero, sul perché della necessità di riconoscere la natura patrimoniale dei dati personali e l'esistenza di uno scambio sotteso ai c.d. servizi digitali "gratuiti"*, in *Dir. fam*., 2021, 1462-1470.

(34) A. Stazi e F. Corrado, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. inform*., 2019, 450-455.

che in tema di identità digitale prima vengono gli interessi economici, e poi quelli delle persone (35).

La cedibilità dei dati personali *digitali* è stata invece ammessa entro limiti ben circoscritti dalla Corte di cassazione, la quale ha stabilito che è consentito al gestore di un sito internet, il quale somministri un servizio fungibile cui l'utente possa rinunciare senza gravoso sacrificio (nella specie servizio di *newsletter* su tematiche legate alla finanza, al fisco, al diritto e al lavoro), di condizionare la fornitura del servizio al trattamento dei dati per finalità pubblicitarie, ma solo a condizione che il consenso sia singolarmente ed inequivocabilmente prestato in riferimento a tale effetto, il che comporta l'obbligo per il gestore del sito di indicare all'interessato i settori merceologici cui i messaggi pubblicitari saranno riferiti (36). Sulla scia di tale decisione, anche Cass. civ., sez. II, 15 marzo 2023, n. 7555, (in questo caso, però, in un giudizio di opposizione a sanzione irrogata dall'Autorità garante per illecito trattamento di dati) ha ritenuto che l'art. 130, comma 4, del d.lgs. 30 giugno 2003, n. 196 va interpretato nel senso che non è necessario il consenso dell'interessato se il titolare del trattamento utilizza, ai fini della vendita diretta di propri prodotti o servizi le coordinate di posta elettronica fornite dal medesimo nel contesto della vendita, sempre che si tratti di servizi analoghi a quelli oggetto della vendita e l'interessato, adeguatamente informato, non rifiuti tale uso, inizialmente o in occasione di successive comunicazioni. In applicazione di tale principio, la S.C. ha rigettato il ricorso proposto da una s.r.l., titolare di un sito internet che offriva il servizio di comparazione di preventivi, alla quale il Garante aveva notificato ordinanza ingiunzione *ex* art. 162, comma 2-*bis* del d.lgs. cit. per avere trattato, senza la previa acquisizione del suo consenso, i dati personali di un cliente, che si era registrato sul sito internet riferibile alla predetta società, solo per provarlo, senza concludere alcun contratto di vendita di un bene o di un servizio).

7.6. Mondo digitale e riservatezza: una *liaison dangereuse*

Che il diritto alla riservatezza spesso entri in conflitto con altri diritti, pur essi tutelati, non è un mistero. Ma sui più frequenti di questi conflitti

(35) Ed infatti vi è stato chi ha dubitato della conformità di tale previsione al Trattato, sia pure per motivi ben più sottili di quello grossolanamente esposto nel testo: cfr. F. Bravo, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e Impr.*, 2018, 190.

(36) Cass. civ., sez. I, 2 luglio 2018, n. 17278, in *Giur. it.*, 2019, 530, con nota di S. Thobani, *Operazioni di tying e libertà del consenso.*

possediamo ormai o norme, o princìpi sufficientemente chiari. Tra il diritto di difesa in giudizio e quello alla riservatezza prevale il primo, tra il diritto alla riservatezza e quello all'informazione prevale il secondo solo se siano rispettate certe condizioni; tra il diritto alla riservatezza e l'iniziativa economica prevale il primo.

Nel mondo dell'identità digitale le cose vanno diversamente. Qui il diritto alla riservatezza del titolare dei dati identificativi, e conseguentemente le forme della sua tutela, è condizionato da tre contraddizioni implicite nel sistema che l'interprete non può sciogliere.

a) La prima delle contraddizioni che condiziona la tutela della riservatezza delle *identità digitali* è quella tra la funzione delle regole di *identificazione*, che è individuare in modo univoco una persona, e la riconosciuta (ed anzi proclamata da una corrente di pensiero che sembra considerare tale libertà alla stregua delle leggi mosaiche (37)) libertà dell'utente di dotarsi di quante identità volesse, fossero pure migliaia.

Come si vide a suo tempo, infatti, l'identità personale è un diritto della persona che viene violato quando le si attribuiscano idee, opinioni, titoli, attributi non suoi. Ma se la persona che fruisce di servizi o immette informazioni nella rete possiede tante identità quanti sono i servizi cui accede, quale sarà l'identità "giusta", dalla cui violazione scaturiscono conseguenze giuridiche? E se l'utente avesse mille identità diverse, potrebbe invocare mille risarcimenti, se i suoi dati fossero violati? E se l'utente avesse una identità con cui accede ai dibattiti sul sito web degli "*amici della caccia*", ed un'altra per accedere ai dibattiti sul sito web degli "*amici degli animali*", potrebbe lamentare una lesione della sua identità personale, se taluno lo definisse "*animalista*" piuttosto che "*cacciatore"*? (38)

---

(37) A tal riguardo mi piace ricordare come, tra le tante mediocrità che grazie al *web* vengono elevate e tenute in fama di tesori sapienziali (sì che "*un Marcel diventa ogni villan che parteggiando viene"*), vi sono i *blogger*. Uno di questi ha pensato addirittura di dettare "i dieci comandamenti" della c.d. "*Self-Sovereign Identity*", vale a dire la pretesa di usare segni identificativi per l'accesso ai servizi informatici che non vengono "affidati" al gestore del servizio, ma restano nella disponibilità e sotto il controllo del titolare (un po' come il portafoglio europeo dell'identità digitale, di cui si è detto in precedenza). Il presupposto comune di questi "comandamenti" è che ogni utente ha il "diritto" di crearsi quante identità voglia (Allen, *The Path to Self-Sovereign Identity*, in www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/). Questa straordinaria intuizione intellettuale non ha mancato di essere recepita e rilanciata anche da noi dai giuristi *à la page* (per tutti, M. MARTORANA, *Self-sovereign identity e tutela della privacy nell'identità digitale*, in *www.altalex.it* del 22 novembre 2022).

(38) Già diversi anni fa, in un contributo spesso citato, fu osservato che "*la capacità di assumere diverse identità in rete (e addirittura di trovarsi di fronte al proprio doppio, secondo l'esperienza di Sherry Turkle) è condizionata alla possibilità di mantenere una qualche forma di*

In punto di diritto il problema è dunque questo: a misura che cresce la possibilità di assumere più identità digitali, cresce specularmente la difficoltà di individuare il fatto illecito e di conseguenza il danno risarcibile, che ovviamente non potrebbe mai essere ritenuto *in re ipsa* per il solo fatto dell'attribuzione d'una qualifica o della manomissione di dati personali (39).

b) La seconda delle contraddizioni che condizionano la tutela della riservatezza delle *identità digitali* è quella tra l'interesse pubblico alla crescita dell'economia digitale, e l'interesse privato alla tutela della propria persona.

Si tratta dell'aspetto più delicato.

Lo possiamo riassumere così: se l'*identità digitale* forma oggetto d'un diritto fondamentale della persona, essa in teoria dovrebbe essere indisponibile. Così come non si potrebbe vendere o affittare il proprio nome, lo stesso dovrebbe dirsi dell'*identità digitale*.

Sappiamo tutti però che non è così. I dati che qualunque utente del *web* lascia (è costretto a lasciare) ogni volta che decida di utilizzare il *web*, a qualunque scopo, sono il carburante dell'economia del terzo millennio.

Sapere, ad esempio, quante persone tramite il *web* leggono quel giornale, acquistano quel vino o simpatizzano per quel partito sono informazioni preziosissime per chi fa soldi con l'attività di *profilazione* degli utenti. Quelle informazioni saranno pagate a peso d'oro dall'editore, dal vinaio e dal partito. Ai padroni del *web* non importa ovviamente chi siamo, ma importa cosa facciamo: e le tracce di quel che facciamo (*footprint*) giustamente sono state definite "*il petrolio dell'era digitale*" (*the oil of the digital era*) (40).

La parossistica acquisizione e gestione dei dati da parte dei grandi *internet provider* è un fenomeno così importante per l'economia mondiale, che ben pochi governi al mondo accetterebbero di impedirlo.

Dunque da un lato abbiamo un diritto della persona che, in quanto tale,

---

anonimato e dunque di non essere « identificati » per la propria identità reale. Per contro ammettere una tutela della identità "prescelta", e dunque della propria maschera virtuale (si pensi agli avatars creati dagli utenti di "Second Life"), come spesso si fa invocando ora la disciplina dello pseudonimo, ora quella del right of publicity o degli altri diritti di proprietà intellettuale, presupporrebbe una certa stabilità nell'uso dei segni distintivi, la quale potrebbe essere assicurata attraverso l'introduzione di più o meno sofisticati sistemi di identificazione" (G. Resta, *Identità personale e identità digitale*, in *Dir. inform. e informatica*, 2007, 511, ma specialmente 515-516).

(39) Sull'impossibilità di ammettere l'esistenza di danni *in re ipsa* si veda la fondamentale decisione di Cass. civ., sez. un., 15 novembre 2022, n. 33645, in *Giur. it*., 2023, 1273, con nota di Iuliani, *Lesione del potere di godimento e risarcimento del danno*.

(40) La metafora per cui i dati sarebbero il nuovo petrolio fu coniata dal matematico inglese Clive Humby, e divenne famosa dopo che *The Economist* nell'edizione del 6 maggio 2017 la usò per un commento (non firmato) dal titolo *The world's most valuable resource is no longer oil, but data* (traggo la citazione da Scagliarini, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *www.consultaonline.it*).

non dovrebbe essere commerciabile; dall'altro abbiamo una economia mondiale che ha bisogno di commercializzare quel diritto.

Il fenomeno è stato da tempo segnalato dalla dottrina.

Si è esattamente osservato che i dati (digitali) personali "*costituiscono al tempo stesso la risorsa sulla quale si basa l'economia digitale e l'oggetto del diritto alla protezione dei dati personali, riconosciuto dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea*" (41). Pertanto pretendere di consentirne l'uso alla sola condizione che l'utente del servizio digitale dia il consenso significa di fatto trasformare il consenso nel "prezzo" per ottenere in cambio la fornitura del servizio (42).

La contraddizione, poi, è aumentata dal fatto che è lo stesso legislatore comunitario a dichiarare solennemente di voler garantire la "libera circolazione" dei dati personali (art. 1 RGPD), aggiungendo che tale libera circolazione "*non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*".

Ed infatti secondo il RGPD il "*diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta*", ma va coordinato con altri diritti fondamentali », tra i quali la libertà d'impresa.

c) La terza delle contraddizioni che condizionano la tutela della riservatezza delle *identità digitali* è quella tra l'attribuzione al singolo della facoltà di concedere a terzi il trattamento dei propri dati digitali, e l'assoluta imperscrutabilità, per il concedente, dell'uso che verrà fatto dei dati così generosamente messi a disposizione.

Qualsiasi utente del web, infatti, dopo avere immesso i propri dati — ad esempio per registrarsi su un sito, ne perde di fatto il controllo. Questi dati potranno essere acquisiti, elaborati, trasmessi, venduti, dal fornitore del servizio digitale a qualunque terzo: ad un altro fornitore, ad un privato, ad una c.d. società di profilazione, persino ad un partito politico, senza che il titolare lo sappia (43).

---

(41) Finocchiaro, *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it*., 2019, 1657; A. Morace Pinelli, *La circolazione dei dati personali tra tutela della persona, contratto e mercato,* in *Nuova giur. civ*., 2022, 1322, ove si osserva: "*l'interconnessione digitale su larga scala (il 65% della popolazione mondiale è connesso ad internet, unitamente ad oltre cinquanta miliardi di oggetti) genera masse di dati che costituiscono una merce ed alimentano la* data driven economy. *In effetti, la sinergia tra* big data *e intelligenza artificiale genera ricchezza*".

(42) I. Rapisarda, *La* privacy *sanitaria alla prova del* mobile ecosystem. *Il caso delle* app mediche, in *Nuove leggi civ. comm*., 2023, 184.

(43) Il lettore probabilmente ricorderà la vicenda di *Cambridge Analytica,* una società di consulenza per il commercio *on line*, che nel 2018 fu accusata di avere usato in modo illecito milioni di dati prelevati dagli utenti di *Facebook* durante la campagna presidenziale americana del 2016. Secondo l'accusa, la società elaborò le informazioni raccolte mediante algoritmi il cui

Qualunque persona usi una *identità digitale* per servirsi del web non sa e non può sapere quali tracce digitali lascia, né da chi saranno raccolte e catalogate, né a quali fini. Aggiungasi che il complesso di tutte queste tracce digitali, che ha un valore commerciale inestimabile, è di fatto controllato solo da due categorie di enti: il gestore (*provider*) al quale i dati vengono affidati, e l'ente che li acquista o li usa per estrarne informazioni da vendere a terzi.

La raccolta e l'elaborazione di dati digitali su scala mondiale da parte di pochi soggetti, come ben s'intende, può diventare il terreno di coltura di ogni tipo di abuso. I dati infatti vengono classificati in base ad algoritmi, ma l'algoritmo è un modello matematico solo apparentemente scientifico ed oggettivo: esso in realtà riproduce le valutazioni e le priorità attribuite da chi lo ha creato; è una "*opinione radicata nella matematica*" (44).

Si è perciò giustamente osservato che "*anche malgrado la buona fede degli ideatori, il funzionamento dell'algoritmo coglie solo parzialmente la complessità di una situazione, finendo non solo per restituire risultati infondati, quando non addirittura palesemente discriminatori, ma anche, ove non costantemente aggiornato, per cristallizzare le situazioni individuali e sociali che prende in esame. È quanto accade, ad esempio, con molti modelli introdotti per la individuazione dei soggetti a maggior rischio di recidiva, laddove questi algoritmi, segnalando come più probabile la commissione di altri reati da parte di determinate categorie di persone (perlopiù di precise origini etniche ed inevitabilmente legate a specifici ambienti urbani più degradati ed in cui opportunità di istruzione e di lavoro appaiono maggiormente difficili a presentarsi), portino a concentrare controlli e indagini su quegli stessi soggetti, che a quel punto giocoforza con maggiore probabilità finiranno per risultare più propensi a delinquere. Cosicché il modello, apparentemente funzionante, in realtà esprime*

---

scopo era manipolare le preferenze degli elettori a favore del candidato alla presidenza Donald Trump (poi eletto), grazie alla diffusione di notizie false calunniose a carico dell'altro candidato, Hillary Clinton. La medesima società fu anche accusata di avere usato i dati degli utenti di *Facebook* per orientare l'elettorato in occasione del *referendum* svoltosi nel 2016 nel Regno Unito per favorirne l'uscita dall'Unione Europea.

Sulle implicazioni giuridiche della vicenda, tra i tanti contributi, si veda D. Sborlini, *Profilazione elettorale e protezione dei dati personali: prospettive di soluzione in ambito europeo,* in *Dir. informazione e inf.*, 2022, 1173.

(44) C. O'Neil, *Armi di distruzione matematica*, Firenze-Milano, 2017, 33. Secondo Soro, *Persone in rete*, Roma, 2018, 117, "*numerose applicazioni hanno dimostrato che gli algoritmi non sono matematica pura — come tale, infallibile e neutra — ma piuttosto opinioni umane strutturate in forma matematica che riflettono spesso [...] le precomprensioni di chi li progetta*".

semplicemente una profezia che si autoavvera, determinata da un equivoco alla base che porta a confondere una correlazione con un rapporto di causalità" (45).

d) In conclusione l'interprete ha il non agevole compito di sciogliere questi tre nodi:

1) se alla pluralità di identità digitali possa corrispondere una pluralità di tutele;

2) l'identità digitale è un diritto della persona, ma i dati che ne formano oggetto possono essere ceduti;

3) l'esercizio della libertà personale di cedere a terzi l'uso dei dati digitali personali ha generato enormi *Leviatani* che rischiano di soffocare quella libertà in nome della quale sono stati alimentati.

7.7. Identità digitale e tutela della riservatezza

I fenomeni appena descritti hanno reso evidente che la tutela dei dati identificativi dell'utente di servizi informatici, o *identità digitale* che dir si voglia, deve avvenire su tre piani.

Il primo piano, ovviamente, è quello della tutela dei dati. Se si ammette che l'identità digitale è un dato inerente la persona, deve ammettersi che gli elementi che la costituiscono non sfuggono alle tutele previste in linea generale per tutti i dati personali.

Come vedremo, però, paradossalmente proprio questo, che è l'aspetto più evidente della tutela da apprestare al titolare dei dati digitali, è anche quello che di fatto si è rivelato sinora meno efficace.

Il secondo piano è quello della tutela del consumatore contro le pratiche commerciali scorrette. Se, infatti, si ammette che i dati dell'identità digitale possano essere ceduti per scopi commerciali, ne viene di conseguenza che tale cessione non potrà essere imposta od estorta con condotte decettive o latamente estorsive.

Il terzo piano è quello della repressione delle condotte limitative della concorrenza.

Come s'è accennato il *web*, che sembrava agli albori del millennio la nuova democrazia, di fatto è nelle mani di pochi. E quando si è in pochi a gestire affari multimiliardari, la tentazione di costituire un *cartello* è dietro l'angolo.

---

(45) S. Scagliarini, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *Consulta OnLine*, 2021, 510.

a) A livello comunitario il testo normativo fondamentale sulla tutela dei dati personali è il Regolamento 27 aprile 2016, n. 679/16, altrimenti detto Regolamento Generale per la Protezione dei Dati Personali, o RGPD (46).

Chiediamoci dunque se esso si applichi alle identità digitali, e in che modo.

Il primo quesito è di agevole soluzione: l'art. 4, n. (1), del RGPD i dati personali come "*qualsiasi informazione riguardante una persona fisica identificata o identificabile (...); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

L'espressa menzione degli "*identificativi on line*" non consente dubbi sul fatto che qualsiasi elemento idoneo ad individuare l'utente di un qualsiasi servizio o prodotto offerto tramite il *web* rientra nell'ambito d'applicazione del RGPD.

L'identità digitale dunque è tutelata dalle norme del Regolamento.

b) Il RGPD — molto semplificando — non impone a chi tratta dati personali altrui "cosa" deve fare. Stabilisce piuttosto quale obiettivo il gestore deve garantire. Lo si potrebbe definire perciò un testo "*teleologicamente orientato*", come se dicesse al gestore: "*adotta le procedure che ritieni più opportune, ma garantisci almeno questi risultati*".

Ed i risultati che il RGPD impone di conseguire (art. 5, commi 1 e 2) sono sette, così riassumibili:

1) garantire il principio di "*liceità, correttezza e trasparenza*" (47); dunque — teoricamente — nessun trattamento può essere effettuato all'insaputa del titolare; il *Considerando XXXIX* del Regolamento chiarisce che il principio di trasparenza è soddisfatto se sono intelligibili e conoscibili dal titolare dei dati le modalità con cui questi sono raccolti, utilizzati, consultati o altrimenti trattati;

2) garantire il principio di "*limitazione della finalità*", e cioè raccogliere i dati solo per scopi determinati e dichiarati;

3) garantire il principio di "*minimizzazione*", e cioè non raccogliere alcun dato che non sia strettamente necessario per lo scopo del trattamento;

---

(46) Non pochi si ostinano a indicare il Regolamento con l'acronimo "GDPR", ovvero *General Data Protection Regulation*. Sarebbe doveroso far loro notare che delle quattro parole inglesi appena trascritte, non una ha una etimologia anglosassone, ma sono tutti puri etimi latini.

(47) Molto ci sarebbe da ironizzare su una legge che imponga di rispettare la legge, ma la nomopoietica moderna ci ha abituato a questi bizantinismi.

4) garantire il principio di "*esattezza*", e cioè dotarsi di una procedura per correggere tempestivamente i dati inesatti;

5) garantire il principio di "*limitazione della conservazione*", e cioè non conservare i dati quando siano esaurite le necessità per cui furono raccolti;

6) garantire il principio di "*integrità e riservatezza*", e cioè dotarsi di procedure idonee a prevenire il rischio che i dati possano essere perduti, manomessi o trafugati.

7) dotarsi di strutture e personale idonei a trattare i dati nel rispetto dei princìpi che precedono, e conservare le prove per dimostrarlo agli interessati e alle autorità di controllo (principio di "responsabilizzazione").

c) I sette princìpi di cui all'art. 5 del RGPD vanno poi coordinati coi sette presupposti stabiliti dal successivo art. 6. La prima di tali norme stabilisce "*come*" i dati personali debbono essere trattati, la seconda stabilisce "*quando*" debbano esserlo.

Questi sette presupposti (ovviamente) alternativi sono:

a) il consenso dell'interessato;

b) la necessità di eseguire un contratto di cui l'interessato è parte;

c) la necessità adempiere una obbligazione o di esigerla dall'interessato;

d) la necessità di salvaguardare "interessi vitali" d'una persona fisica;

e) la necessità di adempiere doveri pubblici;

f) la necessità di perseguire "*un legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano [sugli] interessi o [sui] diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore*".

Il primo e l'ultimo di tali presupposti hanno fatto molto discutere.

d) Dal punto di vista formale, la tutela dell'identità digitale parrebbe piena. Pure, la dottrina non ha mancato di rilevare diversi aspetti problematici delle tutele apprestate dal RGPD. In particolare, sia sul consenso al trattamento, sia sul "legittimo interesse".

Quanto al consenso, è stato osservato che esso è un ben misero baluardo, a fronte dell'enorme disparità di potere, cognizioni e posizioni tra l'interessato e il gestore, e ciò per più ragioni.

Innanzitutto, un vero consenso non può che essere libero ed informato. Ma la legge consente all'interessato di sapere molto poco sulla fine che faranno i suoi dati digitali, una volta che ne ha autorizzato l'uso. In particolare, l'interessato non sa con che tipo di procedimento saranno valutati e profilati, né quale algoritmo sarà utilizzato. Il RGPD non impone affatto al gestore di spiegare l'algoritmo all'interessato, ma parte della dottrina ha ritenuto di potere ricavare tale obbligo dal combinato disposto

degli artt. 12-15 e 22 del Regolamento (48). Un diverso orientamento, all'opposto, ritiene che il RGPD accordi all'interessato solo il diritto ad essere informato prima del consenso all'uso dei suoi beni sul fatto che saranno trattati con una procedura automatizzata, ma non ha alcun diritto a ricevere una spiegazione *ex post* sulla logica utilizzata (49).

In secondo luogo, la dottrina ha segnalato come il requisito del consenso possa riuscire velleitario, in un contesto economico-sociale nel quale le tecniche di profilazione diventano sempre più complesse e perciò inconoscibili, di conseguenza gli utenti diventano sempre più condizionati e — per ciò solo — impreparati, ed infine la dipendenza dal *web* diventa sempre più massificante ed irrinunciabile anche per i più banali gesti della vita quotidiana. E comunque, anche ad ammettere che il gestore del servizio digitale adempia certosinamente tutti gli obblighi informativi a suo carico, resterebbe il fatto che l'utente il quale volesse sapere che fine fanno i suoi dati avrebbe l'onere di leggere non solo l'informativa (*privacy policy*) del gestore, ma anche quelle di tutti i terzi cessionari che dal primo riceveranno i suoi dati insieme a quelli di altre migliaia di persone, in un infinito rimpiattino.

La cooperazione di tutti questi fattori ha generato un fenomeno studiato dall'economia comportamentale, secondo cui il titolare dei dati è indotto a cliccare sulle caselle di autorizzazione all'uso dei dati in modo sempre più inconsapevole (50). Questi sudi sono ormai così copiosi e generalizzati da indurre sinanche il Consiglio di Stato a ritenere che sia una pia illusione quella secondo cui il consumatore informato è persona razionale e libera nelle sue scelte: ed infatti con ordinanza 10 ottobre 2022, n. 8650, la Sesta Sezione ha sottoposto alla Corte di giustizia dell'Unione Europea la seguente

---

(48) B. Goodman e S. Flaxman, *European Union Regulations on algorithmic decision-making and a "right to explanation"*, in *AI Magazine*, 2017, fasc. 3, 6; Tabarrini, *Comprendere la "big mind": il gdpr sana il divario di intelligibilità uomo-macchina?*, in *Dir. inform.*, 2019, 2, 565; G. Malgieri e G. Comandè, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, fasc. 4, 2017, 243.

(49) Swachter, Bmittelstadt e L. Floridi, *Why a Right to explanation of automated decision-making does not exist in the general data protection regulation*, in *International Data Privacy Law*, 2016, fasc. 2, 76.

(50) Il Comitato Nazionale di Bioetica ha osservato nel parere *Mobile-health e applicazioni per la salute: aspetti Bioetici*, 12: "*già è stata sollevata la preoccupazione che il consenso informato visualizzato sullo schermo e non su carta, porti a cliccare in modo immediato senza il tempo sufficiente per una scelta consapevole e senza la possibilità di accertare la effettiva volontarietà. Inoltre la moltiplicazione dei consensi può portare ad una irritazione da parte dell'utente o spesso ad acconsentire solo per velocizzare la procedura, senza — anche qui — adeguata consapevolezza*".

In argomento si vedano anche Acquisti, L. Brandimarte e G. Loewensten, *Privacy and human behaviour in the age of information*, in *Science*, 2015, 347.

questione: se la nozione di "consumatore medio" di cui alla Direttiva 2005/29/CE, inteso come consumatore normalmente informato e ragionevolmente attento ed avveduto — per la sua elasticità ed indeterminatezza — non debba essere formulata con riferimento alla miglior scienza ed esperienza e di conseguenza rimandi non solo alla nozione classica dell'*homo oeconomicus,* ma anche alle acquisizioni delle più recenti teorie sulla razionalità limitata che hanno dimostrato come le persone agiscono spesso riducendo le informazioni necessarie con decisioni "irragionevoli" se parametrate a quelle che sarebbero prese da un soggetto ipoteticamente attento ed avveduto acquisizioni che impongono una esigenza protettiva maggiore dei consumatori nel caso — sempre più ricorrente nelle moderne dinamiche di mercato — di pericolo di condizionamenti cognitivi.

e) Infine, si rivelato in dottrina come le regole dettate dal RGPD non sono perfettamente coordinate con quelle del Regolamento eIDAS, sotto almeno tre aspetti:

1) la sovrapposizione tra il regime di responsabilità previsto da eIDAS e quello previsto dal RGPD;

2) l'incompatibilità dell'insieme minimo di dati previsto da eIDAS con il principio della minimizzazione dei dati previsto dal RGPD;

3) l'incompatibilità del requisito di ritirare il portafoglio europeo di identità digitale in caso di violazione o compromissione dello stesso con il principio di disponibilità dei dati previsto dal RGPD (51).

(51) Per l'illustrazione di questi problemi si veda A. Ortalda e S. Leucci, *Identità digitale e protezione dei dati personali: punti di incontro e rischi nelle discipline eIDAS e RGPD*, in *Riv. it. informatica e dir.*, 2022, 149 e ss.

Parte V
DOMICILIO DIGITALE NEL PROCESSO PENALE

I.
LE CATEGORIE GENERALI DI DOMICILIO E IL PROCESSO PENALE. IL DOMICILIO PER I DEPOSITI

di *Antonella Ciriello*

1.1. Le categorie generali di domicilio e il processo penale. Il domicilio per i depositi

Come visto nel capitolo introduttivo, dalla normativa generale primaria si evincono i concetti (del pari generali) di domicilio digitale generale, speciale e di piattaforma. (v. *supra* cap. 1 par. 1.3).

Con riguardo, in particolare, al domicilio digitale speciale, va evidenziato che il CAD si limita ad affermare, all'art. 3-*bis*, comma 4-*quinquies* (dopo aver declinato le figure dei domicili digitali generali obbligatori e facoltativi, collegati ai pubblici registri o elenchi) che "*È possibile eleggere anche un domicilio digitale speciale per determinati atti, procedimenti o affari. In tal caso, ferma restando la validità ai fini delle comunicazioni elettroniche aventi valore legale, colui che lo ha eletto non può opporre eccezioni relative alla forma e alla data della spedizione e del ricevimento delle comunicazioni o notificazioni ivi indirizzate*".

Nella stessa norma, in cui ci si preoccupa, sempre in chiave generale, di razionalizzare e individuare le modalità per raggiungere i cittadini con strumenti digitali, superando il cd. "divario digitale" (di cui parlava anche il d.l. 18 ottobre 2012, n. 179), viene stabilito che debbano essere "*determinate le modalità con le quali ai ...soggetti (n.d.r. che non hanno un domicilio digitale) è attribuito un domicilio digitale ovvero altre modalità con le quali, anche per superare il divario digitale, i documenti possono essere messi a disposizione e consegnati a coloro che non hanno accesso ad un domicilio digitale*".

In termini generali si evince dunque che l'ambizione normativa (in perfetta linea con l'Europa) è favorire la comunicazione digitale.

A livello definitorio, poi, una sistemazione di questi concetti si rinviene nel Decreto della Presidenza del Consiglio dei Ministri - Dipartimento per la Trasformazione Digitale, 8 febbraio 2022, n. 58, sia pure nell'ambito di una disciplina riguardante la piattaforma per la notificazione degli atti della Pubblica Amministrazione.

Ed infatti, in quel decreto nato per adeguare le sistemazioni emergenziali delle piattaforme che gestivano i certificati vaccinali e aprire la strada al futuro delle piattaforme digitali come strumenti di dialogo con i cittadini, in prospettiva evolutiva e di compliance con la descritta visione europea dell'EuWallet) si rinvengono le utili definizioni (del tutto in linea con il CAD) di:

1) « domicilio digitale generale »: l'indirizzo di posta elettronica certificata o di un servizio elettronico di recapito certificato qualificato inserito in uno degli elenchi di cui agli articoli 6-*bis*, 6-*ter* e 6-*quater* del CAD e previsto dall'articolo 26, comma 5, lettera *a*), del decreto-legge 16 luglio 2020, n. 76.

2) « domicilio digitale speciale »: l'indirizzo di posta elettronica certificata o di un servizio elettronico di recapito certificato qualificato, eletto ai sensi dell'articolo 3-*bis*, comma 4-*quinquies*, del decreto legislativo n. 82 del 2005 o di altre disposizioni di legge, come domicilio speciale per determinati atti o affari, se a tali atti o affari è riferita la notificazione, di cui all'articolo 26, comma 5, lettera *b*), del decreto-legge.

3) (n.d.r. per completezza) « domicilio digitale di piattaforma »: l'indirizzo di posta elettronica certificata o di un servizio elettronico di recapito certificato qualificato, appositamente eletto per la ricezione delle notificazioni delle pubbliche amministrazioni effettuate tramite piattaforma, di cui all'articolo 26, comma 5, lettera *c*), del decreto-legge 17 luglio 2020, n. 76, convertito, con modificazioni, dalla legge 11 settembre 2020, n. 120;

Tali figure generali trovano, almeno in parte, una propria declinazione nelle regole processuali civili e penali.

In particolare, anche sul versante penale, così come visto per il processo civile, ai fini delle comunicazioni e delle notifiche, la norma rilevante è costituita dall'art. 16-*ter* del decreto-legge 18 ottobre 2012, n. 179 [1] (v. *infra* sez. 1, cap. 1 e, più specificamente, cap. 2, paragrafo 2.2.

Per i depositi telematici, come già evidenziato nel capitolo introduttivo, le discipline sono differenti tra i due processi [2]: nel processo civile si utilizza

---

[1] Considerato il "testo unico del telematico" per lungo tempo è stato ripetutamente rimaneggiato e detta "misure per favorire la crescita, lo sviluppo dell'economia e della cultura digitali, attuare politiche di incentivo alla domanda di servizi digitali e promuovere l'alfabetizzazione informatica, nonché per dare impulso alla ricerca e alle innovazioni tecnologiche, quali fattori essenziali di progresso e opportunità di arricchimento economico, culturale e civile e, nel contempo, di rilancio della competitività delle imprese". Nonostante la razionalizzazione e la codificazione realizzata dai decreti legislativi 149 e 150 del 2022, resta ancora un punto di riferimento per il telematico con riferimento a vari settori della giurisdizione non solo ordinaria.

[2] E, considerando che le differenze si accentuano anche con riferimento ad altri processi telematici italiani di altre giurisdizioni, occorre chiedersi quando verrà acquisita la

esclusivamente lo strumento della PEC, anche se la normativa generale (e quella tecnica recentemente innovata, con il d.m. n. 217 del 2023, ne prospetta il superamento) mentre, sul versante del processo penale telematico il medesimo d.m. n. 217 n. 2023, emanato ai sensi dell'art. 87, comma 6-*bis*, decreto legislativo 10 ottobre 2022, n. 150, individua un regime differenziato.

In primo luogo è previsto per determinati atti in una determinata fase (3) l'upload presso il portale dei depositi telematici, PDP, la cui definizione è ora dettata nelle regole tecniche innovate con il medesimo decreto in commento.

L'art. 7-*bis* del regolamento (d.m. 21 febbraio 2011, n. 44, cit.), infatti, stabilisce che: "*Il portale dei depositi telematici consente la trasmissione in via telematica da parte dei soggetti abilitati esterni dei dati, atti e documenti del procedimento, secondo quanto previsto dall'articolo 51 del codice in materia di protezione dei dati personali*".

Per identificare correttamente poi, il domicilio digitale rilevante ai fini del deposito nel processo penale telematico su portale, occorre attingere alle specifiche tecniche del DGSIA, emesse ai sensi dell'art. 34 del citato regolamento n. 44, recentemente aggiornate e pubblicate in consultazione (4) sul portale dei servizi telematici.

In particolare, si legge all'art. 18 delle specifiche, che l'accesso al PDP è consentito unicamente "*ai soggetti iscritti nel ReGIndE con ruolo avvocato, praticante abilitato, nonché avvocato ente pubblico e funzionario ente pubblico, questi ultimi limitatamente agli appartenenti all'Avvocatura dello Stato*" (5).

Accanto, tuttavia, al deposito su portale resta tutt'ora ammesso il deposito introdotto durante il periodo emergenziale tramite PEC (6).

---

indispensabile consapevolezza che le differenze non imposte da peculiarietà delle rispettive discipline sono perniciose, in vista della interoperabilità richiesta dall'UE.

(3) Il Deposito telematico obbligatorio su PDP riguarda, ai sensi del citato d.m., i depositi nella fase delle indagini preliminari e nei procedimenti di archiviazione di cui agli articoli 408, 409, 410, 411 e 415 del codice di procedura penale, quelli nei procedimenti di riapertura delle indagini di cui al 414 cpp, la nomina del difensore, la rinuncia o revoca del mandato ex art. 107 c.p.p.

(4) Sul sito https://pst.giustizia.it/PST/resources/cms/documents/SPECIFICHE_TECNICHE_DM_44_2011REV_04.01.24.pdf

(5) Nelle specifiche tecniche del DGSIA, recentemente aggiornate e pubblicate in consultazione sul sito https://pst.giustizia.it/PST/resources/cms/documents/SPECIFICHE_TECNICHE_DM_44_2011REV_04.01.24.pdf si legge all'art. 18 che al PDP L'accesso al PDP è consentito unicamente ai soggetti iscritti nel ReGIndE con ruolo avvocato, praticante abilitato, nonché avvocato ente pubblico e funzionario ente pubblico, questi ultimi limitatamente agli appartenenti all'Avvocatura dello Stato.

(6) Prevede l'art. 3, d.m. n. 217 del 2023 cit. comma 8, che "*Rimane consentito il deposito mediante posta elettronica certificata come disciplinato dall'articolo 87*-bis *del decreto*

Ed infatti l'art. 3, d.m. 29 dicembre 2023, n. 217, cit., al comma 8, stabilisce che "*Rimane consentito il deposito mediante posta elettronica certificata come disciplinato dall'articolo 87*-bis *del decreto legislativo 10 ottobre 2022, n. 150 per tutti i casi in cui il deposito può avere luogo anche con modalità non telematiche*".

L'art. 87-*bis* del d.lgs. n. 150 del 2022, ai fini che interessano (ossia la modalità di deposito) prevede che: "*...è consentito il deposito con valore legale mediante invio dall'indirizzo di posta elettronica certificata inserito nel registro generale degli indirizzi elettronici di cui all'articolo 7 del regolamento di cui al decreto del Ministro della giustizia 21 febbraio 2011, n. 44. Il deposito con le modalità di cui al periodo precedente deve essere effettuato presso gli indirizzi di posta elettronica certificata degli uffici giudiziari destinatari, indicati in apposito provvedimento del Direttore generale per i sistemi informativi automatizzati, pubblicato nel portale dei servizi telematici del Ministero della giustizia. Con il medesimo provvedimento sono indicate le specifiche tecniche relative ai formati degli atti e alla sottoscrizione digitale e le ulteriori modalità di invio. Quando il messaggio di posta elettronica certificata eccede la dimensione massima stabilita nel provvedimento del Direttore generale per i sistemi informativi automatizzati di cui al presente comma, il deposito può essere eseguito mediante l'invio di più messaggi di posta elettronica certificata. Il deposito è tempestivo quando è eseguito entro le ore 24 del giorno di scadenza*".

Anche ai fini del deposito cd. "emergenziale prorogato" tramite PEC, rileva come domicilio digitale del mittente, ai sensi del cit. art. 87-*bis* del decreto legislativo n. 150 del 2022, quello che si evince dal ReGinDe. Per gli

---

legislativo 10 ottobre 2022, n. 150 per tutti i casi in cui il deposito può avere luogo anche con modalità non telematiche". L'art. 87-*bis* prevede poi:"*1. Sino al quindicesimo giorno successivo alla pubblicazione dei regolamenti di cui ai commi 1 e 3 dell'articolo 87, ovvero sino al diverso termine previsto dal regolamento di cui al comma 3 del medesimo articolo per gli uffici giudiziari e le tipologie di atti in esso indicati, per tutti gli atti, i documenti e le istanze comunque denominati diversi da quelli previsti nell'articolo 87, comma* 6-bis*, e da quelli individuati ai sensi del comma* 6-ter *del medesimo articolo, è consentito il deposito con valore legale mediante invio dall'indirizzo di posta elettronica certificata inserito nel registro generale degli indirizzi elettronici di cui all'articolo 7 del regolamento di cui al decreto del Ministro della giustizia 21 febbraio 2011, n. 44. Il deposito con le modalità di cui al periodo precedente deve essere effettuato presso gli indirizzi di posta elettronica certificata degli uffici giudiziari destinatari, indicati in apposito provvedimento del Direttore generale per i sistemi informativi automatizzati, pubblicato nel portale dei servizi telematici del Ministero della giustizia. Con il medesimo provvedimento sono indicate le specifiche tecniche relative ai formati degli atti e alla sottoscrizione digitale e le ulteriori modalità di invio. Quando il messaggio di posta elettronica certificata eccede la dimensione massima stabilita nel provvedimento del Direttore generale per i sistemi informativi automatizzati di cui al presente comma, il deposito può essere eseguito mediante l'invio di più messaggi di posta elettronica certificata. Il deposito è tempestivo quando è eseguito entro le ore 24 del giorno di scadenza".*

uffici destinatari, il domicilio digitale rilevante è indicato "in apposito provvedimento del Direttore generale per i sistemi informativi automatizzati, pubblicato nel portale dei servizi telematici del Ministero della giustizia".

Si tratta, chiaramente di una soluzione ponte, in attesa dell'adeguamento tecnologico del PPT, poiché il deposito tramite un messaggio di PEC non integrato con gli applicativi non determina l'afflusso diretto dell'atto nel fascicolo informatico, ma impone una attività manuale.

In termini generali, come visto, la norma dell'art. 3-*bis*, comma 4-*quinquies* del CAD, sopra ricordata, attribuisce rilievo al domicilio digitale speciale per determinati atti, procedimenti o affari, stabilendo valore legale per lo stesso e precludendo la proposizione di eccezioni da parte di colui che lo abbia eletto.

Nel disciplinare in termini sempre generali, le istanze e dichiarazioni presentate alle pubbliche amministrazioni per via telematica, l'art. 62 poi prevede, che le stesse (tra l'altro) possono essere (lett. *c-bis*) trasmesse "dall'istante o dal dichiarante" "*dal proprio domicilio digitale iscritto in uno degli elenchi di cui all'articolo* 6-bis*,* 6-ter *o* 6-quater ***ovvero, in assenza di un domicilio digitale iscritto,*** *da un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal Regolamento eIDAS.*

In tale ultimo caso, in assenza di un domicilio digitale iscritto, la trasmissione costituisce elezione di domicilio digitale speciale, ai sensi dell'articolo 3-bis*, comma* 4-quinquies*, per gli atti e le comunicazioni a cui è riferita l'istanza o la dichiarazione*". Emerge, dunque, uno specifico riferimento al "principio di responsabilità" scaturente dalla dichiarazione stessa (cosicché chi ha eletto il domicilio speciale è tenuto ad un certo comportamento successivo e ne risponde).

Come già più volte esposto il CAD, ai sensi dell'art. 2, comma 6, del medesimo CAD, è deputato a dettare il quadro generale del domicilio digitale (tra l'altro) salve le specifiche disposizioni dettate (tra l'altro) per il processo penale telematico.

In altre parole, se in generale, nei rapporti con la PA, la mera trasmissione costituisce "elezione di domicilio digitale (speciale, ai sensi dell'articolo 3-*bis*, comma 4-*quinquies*, per gli atti e le comunicazioni a cui è riferita l'istanza o la dichiarazione), di tale regola nel processo si trova una specifica e reiterata declinazione, nell'istituto del domicilio (telematico e speciale) eletto.

Prima di tutto, va ricordato, per simmetria con il processo civile, l'art. 16, comma 7-*bis* del citato d.l. n. 179 del 2012.

Ed infatti tale norma, che costituisce un esempio di applicazione del domicilio speciale elettivo nel processo civile è stata adeguata dal d.lgs. n. 150 del 2022, anche per il processo penale per stabilire che "*Nei procedimenti*

penali quando l'imputato o le altre parti private dichiarano domicilio presso un indirizzo di posta elettronica certificata non risultante da pubblici elenchi, le comunicazioni e a cura della cancelleria o della segreteria si effettuano ai sensi del comma 4 (7). *Nelle ipotesi di mancata consegna dei messaggi di posta elettronica certificata per cause non imputabili al destinatario, si applicano per l'imputato le disposizioni di cui all'articolo 161, comma 4, del codice di procedura penale e per le altre parti private le disposizioni di cui al comma 6 del presente decreto*".

Viene così, nel quadro di un sistema coerente che nel codice di procedura civile rinnovato valorizza il domicilio digitale generale o quello speciale elettivo, declinata anche per il settore penale una regola omogenea che, tuttavia, risente di eccezioni significative con riguardo alla prima notifica all'imputato (ferma la valorizzazione dell'indicazione di un domicilio digitale).

Ed infatti l'art. 157-*ter* (Notifiche degli atti introduttivi del giudizio all'imputato non detenuto), dispone che "1. *La notificazione all'imputato non detenuto dell'avviso di fissazione dell'udienza preliminare, della citazione in giudizio ai sensi degli articoli 450, comma 2, 456, 552 e 601, nonché del decreto penale di condanna sono effettuate al domicilio dichiarato o eletto ai sensi dell'articolo 161, comma 1. In mancanza di un domicilio dichiarato o eletto, la notificazione è eseguita nei luoghi e con le modalità di cui all'articolo 157 c.p.p.* (che regola la prima notificazione all'imputato non detenuto, privilegiando per tale prima notificazione all'imputato la consegna di copia dell'atto in forma di documento analogico alla persona, con varie declinazioni indicate nei commi successivi del medesimo 157)*, con esclusione delle modalità di cui all'articolo 148, comma 1*".

Così, se la cit. norma generale dell'art. 148 c.p.p. declina la rilevanza del domicilio digitale ai fini delle notifiche che di regola devono essere telematiche, purtuttavia fa salve le differenti discipline in relazione alla qualità soggettiva (imputato che riceve la prima notifica, imputato in diverse situazioni, querelante, persona offesa etc.) del destinatario della notifica, per individuare un regime differente (8).

---

(7) Il comma 6 del medesimo art. 16, comune al civile e al penale, è quello che stabilisce che "*6. Le notificazioni e comunicazioni ai soggetti ((diversi dall'imputato)) per i quali la legge prevede l'obbligo di munirsi di un indirizzo di posta elettronica certificata, che non hanno provveduto ad istituire o comunicare il predetto indirizzo, sono eseguite esclusivamente mediante deposito in cancelleria. Le stesse modalità si adottano nelle ipotesi di mancata consegna del messaggio di posta elettronica certificata per cause imputabili al destinatario*".

(8) Segnatamente, così recita, per aprire la strada alle diverse discipline soggettive, l'art. 148 comma quarto cit. "*in tutti i casi in cui, per espressa previsione di legge, per l'assenza o l'inidoneità di un domicilio digitale del destinatario o per la sussistenza di impedimenti tecnici, non è possibile procedere con le modalità indicate al comma 1, e non è stata effettuata la*

Segnatamente, prima di tutto, il già ricordato art. 161, c.p.p.: comma 1, in base al quale "*Il giudice, il pubblico ministero o la polizia giudiziaria, nel primo atto compiuto con l'intervento della persona sottoposta alle indagini o dell'imputato non detenuti o internati, li invitano a dichiarare uno dei luoghi indicati nell'articolo 157, comma 1,* o un indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato, ovvero a eleggere domicilio per le notificazioni dell'avviso di fissazione dell'udienza preliminare, degli atti di citazione in giudizio ai sensi degli articoli 450, comma 2, 456, 552 e 601, nonché del decreto penale di condanna. *Contestualmente la persona sottoposta alle indagini o l'imputato sono avvertiti che hanno l'obbligo di comunicare ogni mutamento del domicilio dichiarato o eletto e che in mancanza di tale comunicazione o nel caso di rifiuto di dichiarare o eleggere domicilio, nonché nel caso in cui il domicilio sia o divenga inidoneo, le notificazioni degli atti indicati verranno eseguite mediante consegna al difensore, già nominato o che è contestualmente nominato, anche d'ufficio. comma 1*-bis. *Della dichiarazione o della elezione di domicilio, ovvero del rifiuto di compierla, nonché degli avvertimenti indicati nei commi 1 e 2, è fatta menzione nel verbale*".

Un'applicazione invece della consegna in cancelleria "prospettata" in generale dall'art. 16, d.l. n. 179 del 2012 cit., comma 7-*bis*, si rinviene nelle disposizioni dell'art. 153-*bis* come riformato: art. 153-*bis* (Domicilio del querelante. Notificazioni al querelante.). — 1. *Il querelante, nella querela, dichiara o elegge domicilio per la comunicazione e la notificazione degli atti del procedimento. A tal fine, può dichiarare un indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato*. In particolare va segnalato l'ultimo comma della norma che recita: 5. *Quando la dichiarazione o l'elezione di domicilio mancano o sono insufficienti o inidonee, le notificazioni alla persona offesa che abbia proposto querela sono eseguite mediante deposito dell'atto da notificare nella segreteria del pubblico ministero procedente o nella cancelleria del giudice procedente ».*

---

notificazione con le forme previste nei commi 2 e 3, la notificazione disposta dall'autorità giudiziaria è eseguita dagli organi e con le forme stabilite nei commi seguenti e negli ulteriori articoli del presente titolo".

Ai fini delle impugnazioni, peraltro, rileva il domicilio dichiarato o eletto, anche digitale (lo dispone specificamente l'art. 157-*ter*7 comma 3, "*in caso di impugnazione proposta dall'imputato o nel suo interesse, la notificazione dell'atto di citazione a giudizio nei suoi confronti è eseguita esclusivamente presso il domicilio dichiarato o eletto ai sensi dell'articolo 581, commi 1*-ter *e 1*-quater ».

La rilevanza del domicilio digitale è poi affermata in tutte le disposizioni per le varie fasi del procedimento/processo. Così pure per le notificazioni dell'avviso di fissazione dell'udienza preliminare (articolo 165 comma 1-*bis*).

La previsione del deposito in segreteria/cancelleria, in caso di omessa dichiarazione (o sua inidoneità, si pensi alla indicazione di una casella PEC non adeguata o funzionante) è in linea con la differente qualità soggettiva del destinatario.

Il codice prevede poi, numerose applicazioni di domicilio digitale speciale elettivo, sempre collegando differenti effetti alle diverse qualità (9).

(9) l'articolo 90, comma 1-*bis*. "La persona offesa ha facoltà di dichiarare o eleggere domicilio. Ai fini della dichiarazione di domicilio la persona offesa può indicare un indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato";

l'articolo 90-*bis*: comma 1, quanto

— *a-bis*) "all'obbligo del querelante di dichiarare o eleggere domicilio per la comunicazione e la notificazione degli atti del procedimento, con l'avviso che la dichiarazione di domicilio può essere effettuata anche dichiarando un indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato";

— *a-ter*) alla facoltà del querelante, ove non abbia provveduto all'atto di presentazione della querela, di dichiarare o eleggere domicilio anche successivamente;

— *a-quater*) all'obbligo del querelante, in caso di mutamento del domicilio dichiarato o eletto, di comunicare tempestivamente e nelle forme prescritte all'autorità giudiziaria procedente la nuova domiciliazione;

— *a-quinquies*) al fatto che, ove abbia nominato un difensore, il querelante sarà domiciliato presso quest'ultimo; che, in mancanza di nomina del difensore, le notificazioni saranno eseguite al querelante presso il domicilio digitale e, nei casi di cui all'articolo 148, comma 4, presso il domicilio dichiarato o eletto; che, in caso di mancanza, insufficienza o inidoneità della dichiarazione o elezione di domicilio, le notificazioni al querelante saranno effettuate mediante deposito presso la segreteria del pubblico ministero procedente o presso la cancelleria del giudice procedente;".

II.

LA NOTIFICA TELEMATICA NELLA DISCIPLINA DEL PROCESSO PENALE E IL DOMICILIO DIGITALE

di *Roberto Patscot*

Sommario: 2.1. Introduzione. — 2.2. Il domicilio digitale nel rito penale. — 2.3. Il sistema di notificazione e i soggetti "non obbligati".

2.1. Introduzione

La novella di cui al d.lgs. 10 ottobre 2022, n. 150 pone al centro del sistema delle notifiche nel procedimento penale la modalità telematica al fine di rendere più efficiente (1) l'instaurazione del "contatto" degli atti con la sfera di conoscibilità dei soggetti ai quali le notifiche stesse sono indirizzate (2).

La notifica con modalità telematica, in realtà, aveva già avuto una prima, seppur limitata, applicazione in quanto l'art. 16, comma 4, del d.l. 18 ottobre 2012, n. 179, convertito con modificazioni in l. 17 dicembre 2012, n. 221, aveva previsto la possibilità, per le notificazioni a persona diversa dall'imputato, di effettuare le comunicazioni e le notificazioni a cura della cancelleria per via telematica all'indirizzo di posta elettronica certificata risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni, nei casi previsti dagli articoli 148, comma 2-*bis* (diposizioni dell'autorità giudiziaria per le notificazioni o gli avvisi ai difensori eseguite con mezzi tecnici idonei), art. 149 (notificazioni urgenti a mezzo del telefono e del telegrafo), art. 150 (forme particolari di notificazione disposte dal giudice) e art. 151,

(1) Per tale visione prospettica della riforma "Cartabia" si legga L. Giordano, *L'istituzione del processo penale telematico ad opera del d.lgs. 10 ottobre 2022, n. 150*, in *www.ilprocessotelematico.it*.

(2) L'intero progetto riformatore "Cartabia" in tema di notificazioni è proteso all'adozione di mezzi tecnici funzionali alla semplificazione ed in linea con la necessità di assicurare all'imputato piena consapevolezza circa le coordinate spazio-temporali del suo processo (B. Galgani in *Forme e garanzie nel prisma dell'innovazione tecnologica*, Padova, 341).

comma 2, (consegna di copia ad opera delle segreteria del pubblico ministero) del codice di procedura penale (3).

Il legislatore, ribaltando l'originaria prospettiva che vedeva l'uso delle notificazioni telematiche solo in ipotesi residuali, ha provato a spostare il "baricentro" delle notificazioni dalla modalità analogica a quella digitale riformulando l'art. 148, comma 1, c.p.p. e stabilendo, come canone generale, che, salvo che la legge disponga altrimenti, le notificazioni degli atti sono eseguite, a cura della segreteria o della cancelleria, con modalità telematiche che, nel rispetto della normativa anche regolamentare concernente la trasmissione e la ricezione dei documenti informatici, assicurano la identità del mittente e del destinatario, l'integrità del documento trasmesso, nonché la certezza, anche temporale, dell'avvenuta trasmissione e ricezione.

Tale modalità telematica, però, lungi dall'essere in concreto un modulo operativo univoco delle notificazioni, può essere utilizzata in realtà solo al ricorrere di differenti variabili fattuali e procedimentali e con diversi effetti, ciò in quanto, per la sua applicazione, vengono individuati:

1. molteplici modalità di notificazione telematica (per mezzo del domicilio digitale, del domicilio telematico e del recapito telematico, come più avanti si illustrerà)

2. differenti effetti delle modalità di notificazione telematica (si pensi ad esempio ai limitati effetti della comunicazione di cortesia al recapito telematico di cui all'art. 63-*bis*, disp. att. c.p.p.)

3. diversi presupposti fattuali che consentono la modalità di notificazione telematica (ad esempio presenza o idoneità di un domicilio digitale, comunicazione o meno di un indirizzo di posta elettronica certificata o di posta elettronica ordinaria)

4. eterogenei eventi procedimentali che consentono o meno la modalità di notificazione telematica (ad esempio non è consentita la notifica telematica all'imputato detenuto) o che modificano lo strumento telematico utilizzabile (ad esempio, la prima notifica all'imputato non detenuto è consentita al domicilio digitale, mentre per il medesimo soggetto la notifica degli atti introduttivi del giudizio è possibile al domicilio telematico se da lui tempestivamente indicato durante il "primo contatto" con il procedimento).

Si tratta, come si vede, di un quadro estremamente composito e complesso che necessita inoltre del coordinamento delle norme processuali penali con la disciplina di peculiari istituti appartenenti al generale "corpus"

(3) Si veda V. Bove, *Notifiche telematiche*, in *www.ilprocessotelematico.it*, V. Bove, *Notificazioni telematiche nel procedimento penale: questioni giuridiche e problematiche applicative*, in *Dir. pen. contemp*. 9 novembre 2015, nonché V. Bove, *Il processo penale telematico*, Milano, 2021, 32.

di norme riguardanti l'informatizzazione della pubblica amministrazione, atteso che le disposizioni del Codice dell'Amministrazioni Digitale (CAD) si applicano al processo penale "in quanto compatibili e salvo che non sia diversamente disposto dalle disposizioni in materia di processo telematico" (cfr. art. 1, comma 6, CAD).

2.2. Il domicilio digitale nel rito penale

Il perno ideale della riforma delle notifiche telematiche nel rito penale è, comunque, innegabilmente il domicilio digitale, individuato dal legislatore come strumento elettivo ed acceleratorio del procedimento di notifica.

Tra le novità più significative in materia di notificazioni vi è, infatti, il dettato di cui all'art. 148 comma 4 c.p.p. che richiama espressamente l'istituto del "domicilio digitale" stabilendo che si procede con le modalità analogiche di notifica "in tutti i casi in cui, per espressa previsione di legge, per l'assenza o l'inidoneità di un domicilio digitale del destinatario o per la sussistenza di impedimenti tecnici, non è possibile procedere" con le modalità telematiche.

È necessario, quindi, individuare il perimetro di operatività dell'istituto del domicilio digitale nel procedimento penale per verificare i casi in cui può validamente effettuarsi la notifica presso tale "spazio virtuale" (4).

In assenza di una specifica definizione di domicilio digitale del procedimento penale essa deve ricavarsi dall'art. 1, comma 1 lett. *n-ter*), del CAD che lo descrive, in generale, come un indirizzo elettronico eletto presso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento "eIDAS" (UE) 23 luglio 2014, n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, valido ai fini delle comunicazioni elettroniche aventi valore legale.

La mera elezione di un indirizzo di posta elettronica certificata non basta però per configurare l'esistenza di un domicilio digitale, infatti, perché si possa qualificare quest'ultimo come luogo "idoneo" ai fini delle notifiche nel procedimento penale (così come richiesto dall'art. 148, comma 4, c.p.p.), è necessario che la procedura di elezione soddisfi non solo l'esigenza della certezza della riferibilità al titolare dell'indirizzo elettronico, ma anche che sia affiancata da una specifica pubblicità di tale elezione con la conseguenza che

(4) Per i limiti della riferibilità dello "spazio virtuale" del domicilio digitale ad un indirizzo di posta elettronica si veda F. Nicolicchia, *Domicilio digitale e notificazioni*, in *Riforma Cartabia*, 2023, 434.

l'indirizzo eletto deve necessariamente risultare da pubblici elenchi "qualificati", come emerge dal combinato disposto degli artt. 16, comma 4, (nella sua nuova formulazione introdotta dall'art. 69 del d.lgs. 10 ottobre 2022, n. 150), 16-*ter*, d.l. 18 ottobre 2012 n. 179 convertito con modificazioni dalla l. 17 dicembre 2012, n. 221, nonché art. 6, comma 1, del CAD.

Va, in particolare, evidenziato che il novellato art. 16, comma 4, d.l. 18 ottobre 2012, n. 179 convertito con modificazioni dalla l. 17 dicembre 2012, n. 221, opera un espresso richiamo, per gli effetti dell'art. 148, comma 1, c.p.p., agli indirizzi di posta elettronica certificata risultanti da pubblici elenchi, e contribuisce così a completare esplicitamente la nozione di domicilio digitale per le notifiche nel procedimento penale stabilendo che "nei procedimenti civili e in quelli davanti al Consiglio nazionale forense in sede giurisdizionale, le comunicazioni e le notificazioni a cura della cancelleria sono effettuate esclusivamente (5) per via telematica all'indirizzo di posta elettronica certificata risultante da pubblici elenchi o comunque accessibili alle pubbliche amministrazioni, secondo la normativa, anche regolamentare, concernente la sottoscrizione, la trasmissione e la ricezione dei documenti informatici. Allo stesso modo si procede per le notificazioni da eseguire a norma dell'articolo 148, comma 1, del codice di procedura penale. La relazione di notificazione è redatta in forma automatica dai sistemi informatici in dotazione alla cancelleria".

Elementi costitutivi del domicilio digitale sono, in definitiva, la titolarità di un indirizzo elettronico eletto presso un servizio di posta elettronica certificata (o un servizio elettronico di recapito certificato qualificato) ed il suo inserimento nei registri pubblici previsti dalla legge (6). Il domicilio digitale, proprio in ragione di quest'ultima caratteristica, può distinguersi dagli affini istituti individuabili nel "domicilio telematico", o meglio nel "domicilio digitale speciale", (7) (che ricorre quando vi è una mera dichiarazione di un indirizzo di posta elettronica certificata o altro servizio elet-

(5) Già secondo la lettura prevalente, anteriore alla novella della riforma "Cartabia", della disposizione di cui all'art. 16, comma 4, d.l. 18 ottobre 2012 n. 179, convertito con modificazioni dalla l. 17 dicembre 2012, n. 221, in considerazione dell'uso dell'avverbio "esclusivamente", si riteneva che quello a mezzo PEC potesse considerarsi l'ordinario sistema legale di notificazione degli atti giudiziari nel processo penale diretti a persona diversa dall'imputato, non occorrendo alcun decreto del giudice che autorizzasse il suo impiego, si veda sul punto L. GIORDANO, *La giurisprudenza sul PPT: le linee di indirizzo della giurisprudenza di legittimità*, in *Quaderno della SSM*, n. 15.

(6) In tal senso G. SICCHIERO, *Il domicilio digitale*, in *Giurisprudenza italiana*, febbraio 2023, 293.

(7) Va in proposito rilevato che la legge 27 settembre 2021, n. 134 ha indicato, per l'esercizio della delega in materia di notificazioni, il seguente espresso criterio direttivo: "disciplinare i rapporti tra la notificazione mediante consegna al difensore e gli altri criteri

tronico di recapito certificato qualificato cfr. art. 161, comma 1, c.p.p.) e nel "recapito telematico" (8) (che consiste nell'indicazione di un indirizzo di posta elettronica anche ordinario cfr. art. 63-*bis* disp. att. c.p.p.) i quali sono svincolati da obblighi di preventivo inserimento in registri pubblici.

2.3. Il sistema di notificazione e i soggetti "non obbligati"

Il sistema di notificazione con modalità telematica presuppone, quindi, che la comunicazione raggiunga non un qualsiasi indirizzo di posta elettronica certificata nella titolarità del destinatario (9), ma il suo domicilio digitale o il diverso indirizzo di posta elettronica, preventivamente, indicato nel procedimento penale dal destinatario stesso.

Si configura perciò un meccanismo notificatorio telematico che, per la sua efficacia, nel caso del domicilio digitale prescinde dalla necessità che vi sia una volontà del destinatario dell'atto manifestata nell'ambito del procedimento penale, mentre, nel caso del domicilio telematico e del recapito telematico, postula necessariamente una manifestazione di volontà endprocedimentale del destinatario.

La volontà del destinatario, per l'efficacia della notifica telematica effettuata al domicilio digitale, può invece avere rilievo per la costituzione extraprocedimentale di quest'ultimo.

Va infatti precisato che solo alcune specifiche categorie di soggetti sono obbligate all'elezione di un domicilio digitale mentre per tutti gli altri cittadini si tratta di una mera facoltà.

In particolare, ai sensi dell'art. 3-*bis* CAD, le pubbliche amministrazioni, i gestori di servizi pubblici, le società a controllo pubblico (nei limiti di indicati dall'articolo 2, comma 2, CAD) nonché i professionisti tenuti all'iscrizione in albi ed elenchi ed i soggetti tenuti all'iscrizione nel registro delle imprese hanno l'obbligo di dotarsi di un domicilio digitale iscritto nell'elenco denominato "Indice dei domicili digitali delle pubbliche ammi-

---

stabiliti dal codice di procedura penale per le notificazioni degli atti all'imputato, in particolare con riferimento ai rapporti tra la notificazione mediante consegna al difensore e la notificazione nel caso di dichiarazione o **elezione di domicilio, anche telematico" il quale risulta essere sostanzialmente il richiamo alla possibilità di indicare un domicilio digitale speciale di cui all'art. 3-*bis*, comma 4-*quinquies*, del CAD**.

(8) Nell'esercizio della delega di cui alla legge 27 settembre 2021, n. 134 il legislatore ha ridimensionato la nozione di **recapito telematico** che, per esclusione, ricorre in tutti i casi nei quali non è richiesta necessariamente l'indicazione di un indirizzo di posta elettronica certificata.

(9) Si veda Nuove disposizioni in tema di notificazioni in relazione tematica n. 2/23 dell'Ufficio del Massimario della Corte di cassazione del 1° gennaio 2023.

nistrazioni e dei gestori di pubblici servizi articolo" (art. 6-*ter* CAD) o nell'elenco denominato "Indice nazionale dei domicili digitali delle imprese e dei professionisti" INI-PEC (art. 6-*bis* CAD) (10).

Tutti gli altri soggetti hanno, invece, la facoltà di eleggere (come anche di modificare) il proprio domicilio digitale da iscrivere nell'elenco denominato "Indice nazionale dei domicili digitali delle persone fisiche, dei professionisti e degli altri enti di diritto privato, non tenuti all'iscrizione in albi, elenchi o registri professionali o nel registro delle imprese" cd. INAD (artt. 3-*bis*, comma 1-*bis*, e 6-*quater,* comma 1, CAD).

Risulta evidente che l'esercizio di tale facoltà, manifestata fuori dal procedimento penale, si riflette, per tutti i soggetti "non obbligati", sull'efficacia delle future notifiche ricevibili nell'ambito di qualsiasi procedimento penale con una peculiarità per la posizione dei professionisti iscritti in albi ed elenchi. Per questi ultimi infatti il domicilio digitale è l'indirizzo inserito nell'elenco denominato "Indice nazionale dei domicili digitali delle imprese e dei professionisti" cd. INI-PEC (che viene inserito anche nell'I.N.A.D. quale domicilio digitale in qualità di persone fisiche), essi hanno però il diritto di eleggerne uno diverso (artt. 3-*bis*, comma 1-*bis* e 6-*quater*, comma 2, CAD). Tali soggetti appaiono perciò tenuti anche quali persone fisiche all'adozione di un domicilio digitale potendo solo esercitare una sorta di "*ius variandi*" separando la propria posizione professionale da quella personale chiedendo l'adozione di un diverso domicilio digitale in qualità di persone fisiche.

Appare chiaro che il domicilio digitale è uno strumento che, sebbene idealmente posto all'apice della gerarchia delle modalità di notificazioni, subisce una grave limitazione ad un suo generalizzato utilizzo in ragione della facoltatività dell'adozione per tutti quei soggetti che non rientrano nelle specifiche categorie, sopra descritte, di "obbligati".

In buona sostanza, colui che intenda sottrarsi alla giustizia penale potrà evitare, proprio perché non obbligato, di eleggere un domicilio digitale per farsi raggiungere dalle notifiche giudiziarie; è, pertanto, intuitiva la reale dimensione, in assenza di un'obbligatorietà generalizzata di elezione del

(10) Ai fini delle notificazioni nel processo penale è, inoltre, stato istituito, ai sensi dell'art. 16-*ter*, comma 1, d.l. 18 ottobre 2012, n. 179 convertito con modificazioni dalla l. 17 dicembre 2012, n. 221 e dell'art. 7, d.m. 21 febbraio 2011, n. 44, anche il registro generale degli indirizzi elettronici (ReGIndE), gestito dal Ministero della Giustizia, che contiene i dati identificativi nonché l'indirizzo di posta elettronica certificata dei soggetti abilitati esterni (cioè degli appartenenti ad un ente pubblico, dei professionisti iscritti in albi ed elenchi istituiti con legge, degli ausiliari del giudice non appartenenti ad un ordine di categoria o che appartengono ad ente o ordine professionale che non abbia ancora inviato l'albo al Ministero della giustizia).

domicilio digitale, dell'efficientamento ottenuto dal sistema della giustizia penale con l'introduzione di siffatta innovativa modalità di notifica.

Senza considerare che appaiono pure molto limitati i benefici che possono derivare dalla mera "speranza telematica" di una notifica digitale che potrebbe scaturire dalla ulteriore facoltà esercitabile dall'indagato o dall'imputato a seguito della novella dell'art. 161 c.p.p. a norma del quale il giudice, il pubblico ministero o la polizia giudiziaria, nel primo atto compiuto con l'intervento della persona sottoposta alle indagini o dell'imputato non detenuti o internati, li invitano anche a dichiarare o un indirizzo di posta elettronica certificata o altro servizio elettronico di recapito certificato qualificato.

Tali questioni cruciali si innestano su una riforma che pone, anche sulla spinta degli obbiettivi "prefissati" dal PNRR, grande affidamento sul nuovo paradigma telematico del processo penale che sconta purtroppo ancora il forte gap dell'evoluzione informatica del nostro paese rispetto a quella degli altri paesi tecnologicamente più avanzati.

La codificazione digitale del mondo fisico consente di scoprire un nuovo diritto (11) con strutture e paradigmi mai immaginati, tuttavia tali percorsi inesplorati passano necessariamente dalla effettiva presa di coscienza che la sfera di conoscibilità dei soggetti va individuata anche nei luoghi "virtuali" collegati agli strumenti tecnologici con i quali questi hanno un contatto ormai pressoché quotidiano (si pensi ad un futuribile sistema di notifica connesso allo smartphone nella titolarità del destinatario, magari collegato a criteri biometrici di identificazione abbinabili alla carta d'identità) e non solo ricercata nei tradizionali luoghi fisici riferibili al destinatario dell'atto.

Può dirsi in conclusione che, in una materia da sempre problematica come quella delle notificazioni nel procedimento penale (che segna con la recente riforma effettivamente progressi su molti versanti) (12), si deve compiere ancora un ulteriore coraggioso passo adeguandola alla reale dimensione della attuale sfera di conoscibilità dei soggetti, ormai sempre più immersi in un mondo di relazioni digitali supportate da tecnologie che molto possono fare per conferire ulteriore certezza ed efficienza alla comunicazione degli atti del procedimento penale.

(11) In tal senso A. Garapon, *La giustizia digitale*, Bologna, 2021.

(12) Si veda G. Colaiacovo, *Progressi e criticità del nuovo assetto delle notificazioni*, in *Giurisprudenza Italiana*, maggio 2023.

Parte VI
CONCLUSIONI

I.

LE PROSPETTIVE EUROPEE NEL FUTURO PROSSIMO

di *Stefano Nativi*

Sommario: 1.1. La cittadinanza digitale europea. — 1.1.1. Il Decennio Digitale europeo (2030). — 1.1.1.1. Il mercato unico digitale in Europa. — 1.1.2. Un approccio umano-centrico. — 1.2. Il panorama attuale. — 1.2.1. La digitalizzazione dei servizi pubblici. — 1.2.1.1. Il traguardo dell'identificazione elettronica: il Portafoglio digitale europeo. — 1.2.1.2. La posta certificata e il domicilio digitale europeo. — 1.2.2. La traiettoria italiana. — 1.2.2.1. Il rapporto 2023. — 1.2.2.2. La revisione del domicilio digitale nazionale. — 1.3. Il quadro normativo europeo sull'identità digitale. — 1.3.1. Il regolamento eIDAS (2014). — 1.3.2. La revisione di eIDAS: European ID alias eIDAS 2 (2023). — 1.3.2.1. Il portafoglio d'identità digitale unica europea (European Digital Identy Wallet). — 1.3.2.2. Usabilità e sostenibilità. — 1.3.2.3. La cibersicurezza e le misure transitorie. — 1.3.2.4. La registrazione delle parti facenti affidamento. — 1.3.2.5. Verso il domicilio digitale europeo. — 1.3.2.6. L'autenticazione dei siti Web. — 1.3.2.7. Possibili scenari applicativi. — 1.3.2.8. Entrata in vigore del regolamento e atti d'esecuzione. — 1.4. Le sfide legate al Portafoglio d'identità digitale europeo (eIDAS 2). — 1.4.1. L'innovazione tecnologica. — 1.4.1.1. Il pacchetto di strumenti (Toolbox) per un quadro d'identità digitale europea. — 1.4.1.2. Progetti pilota e ambiti applicativi. — 1.4.1.3. La certificazione di sicurezza del portafoglio d'identità digitale europeo. — 1.4.1.4. Altri strumenti a livello di Stato membro. — 1.4.1.5. La sovranità digitale europea. — 1.4.2. Sfide procedurali. — 1.4.2.1. L'efficacia giuridica a livello nazionale. — 1.4.2.2. L'adozione da parte dei privati. — 1.5. Gli scenari futuri a livello internazionale. — 1.5.1. Le iniziative delle Nazioni Unite e i nuovi standard internazionali. — 1.5.2. Le tecnologie di frontiera per l'identità digitale. — 1.5.2.1. La tecnologia blockchain. — 1.5.2.2. L'Intelligenza Artificiale. — 1.5.2.3. La biometria. — 1.6. L'identità auto-sovrana.

1.1. La cittadinanza digitale europea

Nella società odierna, tecnologicamente mediata e ricca d'informazioni, i cittadini si trovano di fronte a nuove opportunità e sfide nell'esercizio dei loro diritti e delle loro responsabilità, come pure nella partecipazione agli affari della comunità in quanto cittadini digitali. Il mondo digitale offre un ambiente ideale ai processi e alle pratiche democratiche, tra cui la diffusione e la mediazione delle informazioni online. Il dominio virtuale costituisce

un'importante piattaforma per il dialogo interculturale attraverso i social media ed è il contesto in cui i cittadini esercitano sempre più i loro diritti di partecipazione sociale, economica e politica ad ogni livello: locale, nazionale e globale. In base a queste riflessioni il Consiglio d'Europa ha introdotto il concetto di cittadinanza digitale. L'Unione europea, di conseguenza, richiede che le identità digitali siano riconosciute dai singoli Stati membri e che siano garantiti un elevato livello di sicurezza nonché il rispetto delle norme dell'Unione sulla protezione dei dati personali (i.e. il GDPR).

Il concetto di cittadinanza digitale va di pari passo con quello di cittadinanza europea, che prevede la libera circolazione e il diritto di residenza in tutta l'Unione europea. Si parla infatti di domicilio digitale europeo. Uno degli obiettivi della Commissione europea consiste nel garantire ai cittadini dell'Unione i servizi online anche in paesi europei diversi da quelli di residenza, evitando loro l'incombenza di creare nuovi account o di fornire ulteriori informazioni personali.

L'Unione Europea ha approvato una carta che sancisce i principi e i diritti digitali dei cittadini europei.

Il documento esprime i valori dell'UE e la sua visione di una trasformazione digitale sostenibile, incentrata sull'uomo. L'obiettivo è quello di garantire alle persone di godere appieno delle opportunità offerte dal Decennio Digitale europeo, entro il 2030. La dichiarazione è stata firmata dai presidenti della Commissione, del Parlamento europeo e del Consiglio, a testimonianza dell'impegno politico condiviso dell'UE e dei suoi Stati membri nel promuoverne e attuarne i principi in tutti i settori della vita digitale. I diritti e i principi digitali europei andranno ad integrare i diritti esistenti, come la protezione dei dati e la Carta dei diritti fondamentali, e forniranno una guida per l'Unione e gli Stati membri nella necessaria fase d'adattamento alla trasformazione digitale.

1.1.1. *Il Decennio Digitale europeo (2030)*

1.1.1.1. *Il mercato unico digitale in Europa*

Le tecnologie digitali, e Internet in particolare, stanno trasformando il nostro mondo. Fino ad oggi i cittadini, le imprese, la pubblica amministrazione e i governi non hanno beneficiato appieno della trasformazione digitale in corso, spesso per la presenza di ostacoli di vario tipo che hanno complicato l'utilizzo di strumenti e servizi online. Il mercato unico digitale europeo apre oggi nuove opportunità, in quanto elimina le differenze fondamentali tra il mondo virtuale e quello fisico, facilitando l'attività online tra stati europei diversi e aprendo la strada ai servizi internet paneuropei.

Il mercato unico digitale mira a garantire ai consumatori e alle imprese un migliore accesso ai beni e ai servizi online in tutta Europa, ad esempio favorendo il commercio elettronico tra gli stati e l'accesso ai contenuti online e assicurando al contempo una maggiore protezione dei consumatori. Il mercato unico digitale si propone anche di creare il contesto più idoneo alle reti e ai servizi digitali, fornendo infrastrutture e servizi ad alta velocità sicuri e affidabili, regolati da adeguate normative. Tra le principali preoccupazioni vi sono la cyber-sicurezza, la protezione dei dati, la privacy e l'equità, nonché la trasparenza delle piattaforme online.

La creazione di un mercato unico digitale effettivo ed efficace implica sfide importanti; di qui l'iniziativa politica e programmatica, lanciata dall'UE, nota come Decennio Digitale 2030. L'iniziativa persegue una visione sostenibile di società digitale, incentrata sull'uomo, da realizzare entro il prossimo decennio (i.e. il 2030), al fine di rafforzare i diritti e le capacità dei cittadini e delle imprese nel mondo virtuale.

1.1.2. *Un approccio umano-centrico*

L'attenzione all'uomo, valore fondamentale dell'UE, viene declinata nel mondo virtuale.

L'obiettivo del decennio digitale è infatti garantire che tutti gli aspetti della tecnologia e dell'innovazione digitale siano al servizio delle persone. Nessuno va lasciato indietro: tutti devono godere di libertà, protezione ed equità. Di qui l'impegno dell'Europa per allargare le competenze nell'utilizzo della tecnologia di tutti i giorni. In questo progetto la connettività raggiunge anche le persone che vivono in zone non urbane (villaggi, montagne, piccole isole e aree remote): tutti devono poter accedere alle opportunità online e condividere i vantaggi della società digitale. I principali servizi pubblici e le procedure amministrative sono offerti online per la comodità dei cittadini e delle imprese. Anche le piccole imprese utilizzano la tecnologia per prendere decisioni aziendali migliori, interagire con i propri clienti o migliorare parti delle proprie attività.

Il Decennio digitale si pone dunque come quadro completo di riferimento per tutte le azioni relative al settore digitale. Al suo interno è stata promossa la "Dichiarazione europea sui diritti e i principi digitali per il decennio digitale", proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione. La Dichiarazione sottolinea il diritto di tutti ad accedere a tecnologie, prodotti e servizi digitali sicuri, protetti e rispettosi della privacy. Ai cittadini dell'Unione va assicurata un'identità digitale sicura ed affidabile, che consenta l'accesso ad un'ampia gamma di servizi online e offline, e che sia protetta dalla criminalità informatica (incluse le violazioni dei dati e il

furto, o la manipolazione, dell'identità). La Dichiarazione afferma inoltre che ogni persona ha diritto alla protezione dei propri dati personali. Come i dati siano utilizzati e con chi siano condivisi rientra nel controllo dell'utente.

Il Decennio Digitale comprende anche un programma politico: una serie di traguardi da realizzare entro il 2023 a livello di Unione europea, i relativi obiettivi da raggiungere a livello nazionale, l'introduzione di un nuovo strumento di finanziamento per progetti multinazionali e la carta dei diritti e dei principi per i cittadini europei. Gli obiettivi del Decennio Digitale sono traguardi misurabili, che si esprimono in quattro aree fondamentali: la connettività, le competenze digitali, le imprese digitali e i servizi pubblici digitali. Per questi ultimi, in particolare, l'obiettivo a livello di stato membro è quello di raggiungere una percentuale dell'80% di cittadini in grado di utilizzare l'identità digitale nell'interazione con l'amministrazione pubblica.

1.2. Il panorama attuale

Nel settembre del 2023 la Commissione Europea, in collaborazione con gli Stati membri, ha pubblicato un rapporto sullo stato del Decennio Digitale, basato principalmente sui dati statistici ufficiali forniti dagli stati e sugli indicatori DESI (Digital Economy and Society Index), usati per monitorare le prestazioni digitali nonché i progressi dei paesi dell'Unione in termini di competitività digitale. Gli indicatori tradizionali sono stati appositamente estesi per coprire anche le nuove tecnologie connesse alla trasformazione digitale. Nei prossimi report annuali, per dotarsi di un quadro in tempo reale, il Comitato per il Decennio Digitale sta valutando di utilizzare, oltre ai dati statistici ufficiali, anche quelli ministeriali.

1.2.1. *La digitalizzazione dei servizi pubblici*

Figura 1 rappresenta, in percentuale, il tratto di strada che resta all'UE da percorrere per centrare l'obiettivo del Decennio Digitale nella virtualizzazione dei servizi pubblici digitali.

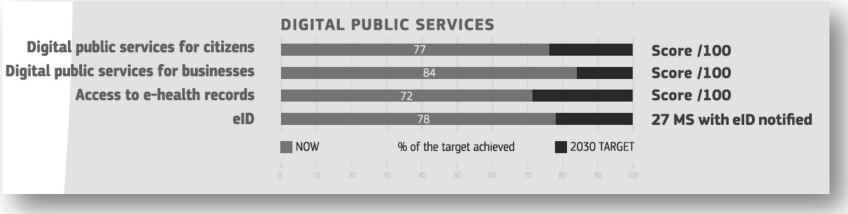


FIGURA 1. Percorso da fare (espresso in percentuale) per raggiungere, entro il 2030, il traguardo prefissato dal Decennio Digitale nel settore dei servizi pubblici digitali. La data di riferimento ("now") è rappresentata dai dati statistici ufficiali forniti dagli stati prima del settembre 2023. L'identità digitale è riferita come "eID". [fonte: Commissione Europea]

Il programma politico del Decennio Digitale prevede l'accessibilità online al 100% dei principali servizi pubblici. Altri ambiziosi traguardi sono: la possibilità per i cittadini e per le imprese dell'Unione di interagire online con le pubbliche amministrazioni, l'accesso online alle proprie cartelle cliniche elettroniche e l'accesso all'identificazione elettronica sicura (eID) per il 100% dei cittadini dell'Unione. Come evidenziato nelle conclusioni nelle conclusioni del rapporto della Commissione, molti Stati membri sono ben posizionati verso la piena digitalizzazione dei servizi pubblici e delle cartelle cliniche, nonché nella diffusione dell'identità digitale (eID) tra i loro cittadini. Sono tuttavia necessari investimenti significativi per migliorare la disponibilità e le prestazioni transfrontaliere dei servizi pubblici.

1.2.1.1. *Il traguardo dell'identificazione elettronica: il Portafoglio digitale europeo*

Il traguardo dell'identificazione elettronica definito dal Decennio Digitale potrebbe essere raggiunto grazie alla tempestiva attuazione del Portafoglio europeo d'identità digitale (*European Digital Wallet*) da parte degli Stati membri. Grazie ad esso, le persone e le imprese avranno a disposizione un servizio d'identificazione comodo, sicuro e interoperabile. Come conseguenza, meno burocrazia graverà su cittadini e imprese in tutte le loro transazioni online, sia con gli enti pubblici che con i fornitori di servizi digitali privati.

Nel rapporto sullo stato del Decennio Digitale, la Commissione raccomanda che gli Stati membri dell'Unione si preparino ad istituire e implementare il Portafoglio Europeo d'Identità Digitale, in particolare attraverso progetti pilota e mobilitando il loro ecosistema digitale. Gli stati sono inoltre invitati a notificare alla Commissione i sistemi d'identificazione conformi al regolamento sull'identità digitale (eIDAS), in particolare quelli inerenti le imprese. Infine, il Portafoglio europeo d'identità digitale andrà integrato con l'Euro digitale.

Per adattare al futuro la nostra moneta, nel giugno 2023 la Commissione europea ha proposto un quadro giuridico che disciplina gli elementi essenziali di un euro digitale, così che la Banca centrale europea possa introdurre un euro digitale ampiamente utilizzabile e disponibile. Cittadini e imprese potranno disporre di una nuova opzione di pagamento, nei negozi o nei siti

web di e-commerce, anche senza connessione a Internet e con un elevato standard di protezione dei dati. Si mira ad un euro digitale completamente interoperabile con il Portafoglio europeo d'identità digitale.

1.2.1.2. *La posta certificata e il domicilio digitale europeo*

Il regolamento eIDAS (2014) definisce gli effetti giuridici di un servizio elettronico di recapito certificato e i requisiti necessari ai servizi elettronici qualificati di recapito certificato. Nel 2022 il comitato per le firme elettroniche e le infrastrutture ("Electronic Signatures and Infrastructures committee") dell'ente di normazione europea per le telecomunicazioni (ETSI: European Telecommunications Standards Institute) ha approvato una serie di standard per facilitare la realizzazione di servizi di consegna elettronica certificata conformi ai requisiti specificati da eIDAS. In particolare, gli standard relativi ai servizi elettronici di consegna raccomandata ("Electronic Registered Delivery Services: ERDS") e quelli connessi ai servizi di posta elettronica registrata ("Registered Electronic Mail (REM) Services") aprano la porta alla posta elettronica certificata (PEC) europea. Secondo il regolamento eIDAS, un servizio di posta elettronica registrata (REM) costituisce una particolare "istanza" di un servizio elettronico di consegna raccomandata (ERDS).

L'evoluzione e l'adozione a livello europeo della PEC, la rende uno degli strumenti di punta del processo di digitalizzazione, in quanto fattore abilitante del domicilio digitale. Per PEC s'intende l'indirizzo elettronico designato presso un servizio di posta elettronica certificata e valido nelle comunicazioni elettroniche dotate di valore legale. È importante ricordare che il primo passo necessario, per la realizzazione di un sistema di PEC europeo, è il riconoscimento dell'utente titolare di un indirizzo di posta elettronica certificata. Questa operazione richiede che l'utente utilizzi uno o più strumenti e sistemi per identificare i propri dati e il proprio indirizzo email PEC. La revisione del regolamento eIDAS (2023) e l'introduzione del portafoglio d'identità digitale europeo costituiscono una risposta a questo bisogno.

1.2.2. *La traiettoria italiana*

1.2.2.1. *Il rapporto 2023*

Per quanto riguarda la situazione in Italia, nell'ambito della prima relazione sullo stato del Decennio Digitale, la Commissione europea, nel suo rapporto per paese, evidenzia che:

"L'Italia si colloca al di sotto della media UE per quanto riguarda la fornitura di servizi pubblici digitali ai cittadini (punteggio di 68 contro 77) e

alle imprese (punteggio di 75 contro 84). Nonostante i ritardi accumulati negli ultimi anni, sono stati compiuti maggiori sforzi in relazione a:

- disponibilità, efficienza e sicurezza dell'infrastruttura digitale;
- interoperabilità dei dati e delle informazioni tra le amministrazioni pubbliche;
- attuazione del principio 'una tantum';
- incremento dell'uso dell'identità digitale;
- completamento del sistema di cartelle cliniche elettroniche.

Le recenti misure adottate per garantire servizi pubblici più incentrati sull'utente e volte a migliorare l'accessibilità dei servizi pubblici digitali, incoraggeranno ulteriormente l'utilizzo dei servizi pubblici digitali da parte dei cittadini".

Nel rapporto si conclude che "L'Italia dovrebbe intensificare gli sforzi per digitalizzare i servizi pubblici. In particolare, dovrebbe accelerare l'attuazione delle misure esistenti e di quelle previste". A tale proposito, il rapporto riconosce che "il Piano di ripresa e resilienza italiano destina 48 miliardi di euro (25%) alla trasformazione digitale, di cui 42 miliardi destinati all'attuazione degli obiettivi del Decennio Digitale. L'Italia ha già realizzato diverse misure digitali".

1.2.2.2. *La revisione del domicilio digitale nazionale*

Nell'ambito del PNRR (Piano Nazionale di Ripresa e Resilienza) italiano, approvato dalla Commissione Europea nel novembre 2023, il domicilio digitale sarà rivisto e integrato con l'anagrafe nazionale dei residenti (ANPR), per consentire una corrispondenza digitale certa e sicura tra cittadini e pubbliche amministrazioni. Questa riforma è prevista entro il secondo quadrimestre del 2025.

Nel giugno 2023, in Italia, è stato attivato l'Indice Nazionale dei Domicili Digitali (INAD): i cittadini possono eleggere il proprio domicilio digitale, indicando un indirizzo PEC dove ricevere tutte le comunicazioni ufficiali della Pubblica Amministrazione. Per eleggere il proprio domicilio digitale è necessario accedere ad un portale e registrarsi al servizio utilizzando il Sistema Pubblico d'Identità Digitale (SPID), la Carta d'Identità Elettronica (CIE) o la Carta Nazionale dei Servizi (CNS). INAD nasce dalla collaborazione fra Agid (Agenzia per l'Italia Digitale), il Dipartimento per la trasformazione digitale della Presidenza del Consiglio, e Infocamere (la società delle Camere di commercio per l'innovazione digitale), che ha realizzato la piattaforma.

Grazie a INAD, tutte le comunicazioni della Pubblica Amministrazione con valore legale, come ad esempio i verbali di sanzioni amministrative,

vengono inviate direttamente nella casella di posta indicata dal cittadino, che può gestire in autonomia il proprio domicilio digitale.

1.3. Il quadro normativo europeo sull'identità digitale

Attualmente, le normative principali dell'Unione europea relative all'identità digitale sono: il regolamento eIDAS (electronic Identification, Authentication, and Trust Services), recentemente modificato per creare un Portafoglio Europeo d'Identità Digitale (European eID), e il regolamento GDPR (General Data Protection Regulation), promulgato nel maggio 2018.

1.3.1. *Il regolamento eIDAS (2014)*

Il regolamento eIDAS (atto dell'UE n. 910/2014) ha introdotto il primo quadro transfrontaliero per l'identità digitale e i servizi fiduciari. Il regolamento riguarda i regimi d'identificazione elettronica notificati alla Commissione da uno Stato membro e i prestatori di servizi fiduciari stabiliti nell'UE.

Il regolamento eIDAS è entrato pienamente in vigore dal 1° luglio 2016, mentre, a livello dell'Unione, il riconoscimento dei sistemi d'identificazione elettronica notificati è iniziato il 29 settembre 2018. Il regolamento incarica la Commissione di emanare atti delegati e di esecuzione per definire le specifiche tecniche e garantirne un'attuazione armonizzata; la sua applicazione si basa pertanto in larga misura sull'emanazione di questi atti secondari. Gli atti legislativi sono integrati dagli standard, sia europei che internazionali, promossi dalle organizzazioni ufficiali (i.e. ETSI, ITU e ISO) e da raccomandazioni e linee guida definite dalle autorità dell'UE, come l'Agenzia dell'Unione europea per la sicurezza informatica (ENISA). La base giuridica del regolamento eIDAS è rappresentata dall'articolo 114 del TFUE, che intende liberare da ostacoli il funzionamento del mercato unico, attraverso l'armonizzazione delle legislazioni degli Stati membri.

Sulla base dei risultati di una consultazione pubblica avviata nel luglio 2020, la Commissione ha valutato che il regolamento eIDAS avesse raggiunto solo parzialmente gli obiettivi fissati nel 2014. Le principali carenze evidenziate dalla consultazione sono: la struttura dell'atto, la sua limitata attuazione, l'evoluzione dell'ambiente tecnico e le mutate aspettative degli utenti. In particolare, dall'entrata in vigore della regolamentazione relativa all'identificazione elettronica, nel settembre 2018, soltanto 14 Stati membri hanno notificato almeno un regime d'identificazione elettronica (ad esempio per dimostrare l'identità online di una persona senza bisogno di password). Ne consegue che appena il 59% dei residenti dell'UE ha accesso a regimi d'identificazione elettronica affidabili e sicuri a livello transfrontaliero. Sol-

tanto 7 regimi sono interamente mobili e rispondono alle attuali aspettative degli utenti. Poiché non tutti i dispositivi tecnici che assicurano il collegamento al quadro di interoperabilità eIDAS sono pienamente operativi, l'accesso transfrontaliero è limitato; pochissimi servizi pubblici online, accessibili a livello nazionale, sono raggiungibili a livello transfrontaliero attraverso la rete eIDAS.

Nel suo discorso sullo stato dell'Unione, il 16 settembre 2020, Ursula von der Leyen, Presidente della Commissione europea, annunciava una nuova proposta della Commissione per "*un'identità elettronica europea sicura. Un'identità europea sicura, di cui ci fidiamo e che ogni cittadino può usare ovunque in Europa per fare qualsiasi cosa, dal pagamento delle tasse al noleggio di una bicicletta. Una tecnologia in cui possiamo controllare noi stessi quali dati vengono utilizzati e come*."

Nell'ottobre 2020 il Consiglio europeo ha rilevato la necessità di una revisione del quadro eIDAS, chiedendo lo sviluppo di un quadro, a livello UE, per l'identificazione elettronica pubblica sicura. Il Consiglio ha quindi invitato la Commissione a presentare, entro la metà del 2021, la proposta di una firma digitale interoperabile per il controllo della propria identità online e dei relativi dati. La firma digitale garantirebbe l'accesso ai servizi digitali pubblici, privati e transfrontalieri.

Il 3 giugno 2021 la Commissione ha adottato la proposta di Regolamento sull'identità digitale europea (European eID). La proposta modifica il regolamento eIDAS del 2014, che aveva posto le premesse per garantire un accesso sicuro ai servizi e lo svolgimento di transazioni online e transfrontaliere nell'UE, introducendo come colonna portante il portafoglio di identità digitale europea. Lo stesso giorno, la Commissione ha espresso inoltre la Raccomandazione per la realizzazione di un "Toolbox" comune dell'Unione, per un approccio coordinato verso un quadro europeo d'identità digitale.

1.3.2. *La revisione di eIDAS: European ID alias eIDAS 2 (2023)*

Nel giugno 2023 il Consiglio dell'Unione e il Parlamento europeo raggiungono un accordo sul testo della proposta di regolamento per un'identità digitale europea (eID), al fine di modificare il testo della normativa eIDAS del 2014. Il regolamento rivisto (alias eIDAS 2) costituisce un chiaro cambiamento di paradigma per l'identità digitale in Europa, con l'obiettivo di garantire a persone e imprese l'accesso universale a un'identificazione e a un'autenticazione elettronica sicura e affidabile tramite un portafoglio digitale personale su telefono cellulare.

Il regolamento stabilisce le condizioni armonizzate per l'istituzione di un quadro per i portafogli europei d'identità digitale, che devono essere forniti

dagli Stati membri. Tutti i cittadini dell'Unione e i residenti (come definiti dalle leggi nazionali) devono avere la possibilità di richiedere, selezionare, combinare, archiviare, condividere e presentare in modo sicuro i dati relativi alla propria identità. Gli utenti hanno anche il diritto di richiedere la cancellazione dei propri dati personali in modo semplice e comodo, sotto il loro esclusivo controllo, consentendone così una divulgazione selettiva.

In estrema sintesi, il regolamento realizzerà tre principi politici importanti per un'identità digitale (eID) europea:

1. la disponibilità dell'identità digitale per qualsiasi cittadino, residente o azienda dell'Unione Europea che voglia utilizzarlo;

2. l'ampia usabilità dell'identità digitale come mezzo d'identificazione, o per confermare attributi personali ai fini dell'accesso ai servizi digitali pubblici e privati in tutta l'Unione;

3. il pieno controllo, concesso agli utenti, di scegliere quali aspetti della loro identità, dei loro dati e dei loro certificati condividere con parti terze, e il diritto di tenere traccia di tale condivisione.

1.3.2.1. *Il portafoglio d'identità digitale unica europea (European Digital Identity Wallet)*

Per implementare i principi sopra introdotti, il regolamento introduce il concetto di "portafoglio europeo d'identità digitale", definito come un mezzo d'identificazione elettronica che consenta all'utente di:

- memorizzare, gestire e convalidare in modo sicuro i dati d'identità e le attestazioni elettroniche degli attributi;
- fornire i dati alle parti facenti affidamento su di essi e ad altri utenti dei Portafogli d'Identità Digitale Europei;
- firmare mediante firme elettroniche qualificate o sigillare mediante sigilli elettronici qualificati.

In quanto strumento d'identificazione elettronica rilasciato dai sistemi nazionali, il portafoglio costituirà uno strumento d'identificazione elettronica a pieno titolo. Ogni Stato membro, sotto sua responsabilità, è chiamato a fornire almeno un portafoglio elettronico, perché venga utilizzato dalle persone fisiche e giuridiche residenti nel suo territorio. Per una maggiore flessibilità e per sfruttare le tecnologie più avanzate, il regolamento consente la fornitura di un portafoglio:

a. direttamente da parte di uno Stato membro;

b. su mandato di uno Stato membro;

c. indipendentemente da uno Stato membro, ma con il riconoscimento da parte di quest'ultimo.

Nel settore privato, i fornitori più probabili di portafogli digitali saranno le banche, le telecomunicazioni e gli erogatori di servizi pubblici. Questi

ultimi soggetti ne trarranno sicuramente vantaggio nelle relazioni con i clienti.

In linea con i tre principi dell'identità digitale, i portafogli d'identità digitale europei fungeranno da "cruscotto della privacy"; grazie ad esso, gli utenti potranno controllare appieno i propri dati e richiederne la cancellazione, come previsto dal Regolamento generale sulla protezione dei dati (GDPR). La normativa prevede inoltre il diritto di utilizzare uno pseudonimo. Infine, per migliorare la fluidità degli scambi digitali, il regolamento introduce la possibilità di interazione tra portafogli. Il cruscotto dovrà garantire un maggior grado di trasparenza, privacy e controllo degli utenti sui propri dati personali. Sarà dotato di un'interfaccia facile e intuitiva, in cui appariranno tutte le parti interessate con cui l'utente condivide i dati, inclusi gli attributi e i dati condivisi.

Il portafoglio dovrà consentire agli utenti il tracciamento di tutte le transazioni eseguite, includendo almeno i seguenti dati: l'ora e la data della transazione, l'identificazione della controparte, i dati personali richiesti e i dati condivisi. Tali informazioni andrebbero conservate anche se la transazione non sia stata conclusa. Non sarà possibile negare l'autenticità delle informazioni contenute nella cronologia delle transazioni. Il cruscotto consentirà agli utenti di richiedere facilmente, ad una parte facente affidamento, la cancellazione immediata di dati personali ai sensi dell'articolo 17 del Regolamento GDPR (2016/679). In caso di richiesta illegale o inappropriata di dati personali, sarà anche semplice segnalare la parte facente affidamento all'autorità nazionale competente per la protezione dei dati, e direttamente dal Portafoglio.

1.3.2.2. *Usabilità e sostenibilità*

Il nuovo regolamento chiarisce che l'emissione, l'uso per l'autenticazione e la revoca dei portafogli sono gratuiti per le persone fisiche. Il portafoglio offrirà infine la possibilità di firma elettronica qualificata gratuita alle persone fisiche per scopi non professionali. Tali firme sono le più affidabili e hanno lo stesso valore legale di una firma autografa. Gli Stati membri potranno prevedere misure per impedire l'uso gratuito delle firme elettroniche qualificate da parte di persone fisiche per scopi professionali, garantendo però che tali misure siano giustificate e proporzionate ai rischi identificati.

Conformemente alla legislazione nazionale, gli Stati potranno istituire funzionalità aggiuntive per i propri portafogli, compresa l'interoperabilità con i mezzi nazionali d'identificazione elettronica già esistenti (ad es. lo SPID in Italia).

Al momento della sottoscrizione ad un portafoglio digitale d'identità europea (operazione denominata "on-boarding"), le persone fisiche po-

tranno firmare con firme elettroniche qualificate, gratuitamente e secondo un'impostazione predefinita, senza ulteriori procedure amministrative. Ciò consentirà agli utenti di firmare o sigillare asserzioni o attributi autoproclamati. In generale, la sottoscrizione dei cittadini e dei residenti al portafoglio dovrà essere favorita da mezzi d'identificazione elettronica dotati di un livello di garanzia 'elevato'.

I mezzi d'identificazione elettronica rilasciati al livello di garanzia 'sostanziale', andranno utilizzati solo nei casi in cui le specifiche tecniche e operative armonizzate soddisfino i requisiti stabiliti nel regolamento per il livello di garanzia 'elevato', grazie all'utilizzo di strumenti o misure supplementari. Questi ultimi dovranno essere affidabili e facili da utilizzare e si avvarranno delle procedure di "*on-boarding*" a distanza, di certificati qualificati supportati da firme qualificate, di attestazioni elettroniche qualificate di attributi o di una loro combinazione.

L'affidabilità dell'identità legale non dovrà ostacolare la possibilità, per gli utenti, di accedere ai servizi attraverso l'uso di pseudonimi, laddove non vi sia un requisito giuridico d'identità legale per l'autenticazione. Per questo motivo, i portafogli dovrebbero includere una funzionalità per generare pseudonimi, scelti e gestiti dall'utente per autenticarsi nell'accesso ai servizi online.

Infine, per promuovere l'adozione del portafoglio e incrementare l'utilizzo dell'identità digitale, gli Stati (in collaborazione con il settore privato, con i ricercatori e il mondo accademico) dovranno sviluppare programmi di formazione volti a rafforzare le competenze digitali dei loro cittadini e residenti, inclusi i più vulnerabili, come le persone con disabilità e gli anziani.

1.3.2.3. *La cibersicurezza e le misure transitorie*

Il regolamento rivisto è in linea con le politiche dell'Unione in materia di cibersicurezza ed è stato concepito per ridurre la frammentazione mediante l'imposizione di requisiti generali, in materia di cibersicurezza, ai prestatori di servizi fiduciari, già regolamentati dal regolamento eIDAS. Il portafoglio digitale è altresì coerente con altre politiche settoriali che si basano sull'utilizzo d'identità elettroniche, attestati elettronici di attributi e altri servizi fiduciari. Rientrano in tale contesto: il regolamento sullo sportello digitale unico, la normativa del settore finanziario in materia di antiriciclaggio e lotta al finanziamento del terrorismo, le iniziative per la condivisione delle credenziali relative alla previdenza sociale, il progetto di una patente di guida digitale o di documenti di viaggio digitali, e ancora iniziative volte a ridurre gli oneri amministrativi per i cittadini e per le imprese. Supportando le firme elettroniche qualificate, il portafoglio potrà anche facilitare la partecipazione politica.

La nuova versione del regolamento offre sicurezza armonizzata ai cittadini dotati d'identità digitale e anche ai fornitori di servizi online, che potranno accettare soluzioni d'identità digitale indipendentemente dal luogo in cui siano state rilasciate. Le nuove regole costituiscono una guida per gli emittenti di soluzioni europee d'identità digitale, fornendo loro un'architettura tecnica comune, un quadro di riferimento e standard comuni da sviluppare con gli Stati membri prima dell'applicazione del regolamento. I portafogli dovranno essere certificati in base a specifiche, procedure e norme di riferimento comuni adottate dalla Commissione.

Fino a quando la certificazione della conformità dei portafogli ai requisiti di cibersicurezza non sarà coperta da schemi di certificazione disponibili, come indicato nel regolamento, gli Stati membri dovranno stabilire schemi di certificazione nazionali, seguendo i requisiti armonizzati presenti nel regolamento. La certificazione della conformità ai requisiti di cibersicurezza si baserà sui relativi sistemi europei di certificazione, istituiti ai sensi del regolamento UE in materia di cibersicurezza (2019/881). I portafogli certificati saranno soggetti a valutazioni periodiche della vulnerabilità, così che eventuali punti deboli nei processi e nei servizi certificati, siano prontamente evidenziati.

I livelli di garanzia esprimono il grado di affidabilità dei mezzi d'identificazione elettronica, assicurando che la persona che rivendica una particolare identità sia effettivamente la persona a cui tale identità è assegnata. A questo proposito, il portafoglio dovrà essere emesso all'interno di un sistema d'identificazione elettronica che soddisfi il livello di sicurezza 'elevato', mentre oggi, in Europa, i sistemi pubblici d'identità digitale utilizzano, nella quasi totalità, un livello di sicurezza 'sostanziale'.

Per garantire la privacy degli utenti, i fornitori di portafogli digitali devono garantire l'inosservabilità, evitando di raccogliere dati e di visionare le transazioni degli utenti del portafoglio. In attesa di soluzioni certificate a prova di manomissione, in via transitoria, i portafogli possono fare affidamento su elementi sicuri esterni certificati per la protezione del materiale crittografico e di altri dati sensibili, o contare su soluzioni nazionali notificate con un livello di garanzia 'elevato', che dimostrino la conformità ai requisiti pertinenti del Regolamento. L'utilizzo di questa misura transitoria dovrebbe limitarsi ai casi d'uso che richiedono un livello di garanzia 'elevato', come ad esempio la sottoscrizione di un utente al portafoglio. Per l'autenticazione necessaria all'accesso ai servizi che richiedono un livello di garanzia 'sostanziale', il portafoglio non richiederà l'uso della misura transitoria.

Solo le autorità competenti degli Stati membri possono garantire un elevato livello di affidabilità nello stabilire l'identità di una persona, assicurando cioè che la persona che rivendica o afferma una determinata identità

sia effettivamente la persona che dichiara di essere. È quindi necessario che la fornitura dei portafogli d'Identità digitale europea si basi sull'identità legale dei cittadini, di altri residenti o di persone giuridiche.

In caso di uso fraudolento o illegale del portafoglio — una volta accertato da un'autorità giudiziaria nazionale — gli organi di vigilanza degli emittenti dei portafogli dovranno, su notifica, adottare le misure necessarie per garantire che la registrazione delle parti facenti affidamento nel meccanismo di autenticazione siano sospese fino a quando l'autorità di notifica non confermi che le irregolarità individuate siano state sanate.

Per la semplificazione e per la riduzione dei costi, gli Stati membri forniranno portafogli basati su standard e specifiche tecniche comuni, così da garantire un'interoperabilità senza soluzione di continuità e maggiore sicurezza informatica.

Il codice sorgente dei componenti software applicativi dei portafogli d'identità digitale europei, è concesso in licenza open-source. Gli Stati membri possono esigere che, per motivi debitamente giustificati, non vengano divulgati componenti specifici diversi da quelli installati sui dispositivi degli utenti.

1.3.2.4. *La registrazione delle parti facenti affidamento*

Ai fini della registrazione, le parti facenti affidamento sui portafogli digitali d'identità europea devono fornire le informazioni necessarie alla propria identificazione e autenticazione nei confronti degli stessi portafogli. Nel dichiarare l'uso che intendono fare dei portafogli, le parti facenti affidamento su di essi devono fornire informazioni sui dati che richiederanno e, qualora necessario, il motivo della richiesta. La registrazione delle parti aderenti dovrà facilitare le verifiche degli Stati membri riguardo alla legittimità delle attività delle parti aderenti in conformità al diritto dell'Unione. L'obbligo di registrazione non dovrà pregiudicare gli obblighi previsti da altre leggi dell'Unione o nazionali.

Le parti facenti affidamento dovranno eseguire valutazioni d'impatto sulla protezione dei dati e nel caso ne emerga un rischio elevato, dovranno consultare le autorità competenti prima del trattamento dei dati. Tali accorgimenti assicureranno il trattamento lecito dei dati personali da parte di chi si affida, in particolare quando siano in gioco dati sensibili, come quelli sanitari.

La registrazione delle parti facenti affidamento mira ad aumentare la trasparenza e la fiducia nell'uso del portafoglio europeo d'identità digitale. La registrazione dovrà essere efficace in termini di costi e proporzionata ai rischi connessi, così da attrarre i fornitori di servizi. In quest'ottica, la

registrazione dovrebbe impiegare procedure automatizzate, inclusa la gestione dei registri esistenti da parte degli Stati membri, evitando processi di pre-autorizzazione.

Il processo di registrazione dovrà consentire casi d'uso differenti, in termini di modalità di funzionamento (online/offline) o in termini di autenticazione dei dispositivi per l'interfacciamento con il portafoglio. La registrazione riguarderà esclusivamente le parti facenti affidamento che offrono servizi attraverso l'interazione digitale.

1.3.2.5. *Verso il domicilio digitale europeo*

La revisione del regolamento eIDAS riafferma l'importanza di concepire un quadro giuridico che faciliti il riconoscimento transfrontaliero tra i sistemi giuridici nazionali esistenti, in materia di servizi elettronici di recapito registrati. Tale quadro aprirà nuove opportunità di mercato ai prestatori di servizi fiduciari dell'Unione, che offriranno nuovi servizi paneuropei di recapito elettronico raccomandato. Per garantire che i dati di un servizio elettronico di recapito raccomandato qualificato siano consegnati al destinatario corretto, tale servizio elettronico dovrà garantire, con piena certezza, l'identificazione del destinatario, mentre sarà sufficiente un elevato livello di fiducia per quanto riguarda l'identificazione del mittente.

I fornitori di servizi elettronici qualificati di recapito raccomandato dovranno essere incoraggiati dagli Stati membri a rendere i loro servizi interoperabili con gli analoghi servizi elettronici forniti da altri prestatori di servizi fiduciari qualificati, al fine di trasferire facilmente i dati elettronici raccomandati tra due o più prestatori di servizi fiduciari qualificati e per promuovere pratiche eque nel mercato interno. Inoltre, in conformità con il regolamento eIDAS 2, un servizio elettronico qualificato di recapito raccomandato fornito in uno Stato membro dovrà essere riconosciuto come servizio elettronico qualificato di recapito raccomandato in tutti gli altri Stati membri.

I fornitori di servizi elettronici qualificati di recapito raccomandato possono concordare l'interoperabilità tra i loro servizi elettronici qualificati. Tale quadro d'interoperabilità dev'essere conforme ai requisiti del regolamento rivisto, e la conformità va confermata da un organismo di valutazione. La Commissione può, mediante atti di esecuzione, stabilire un elenco di norme di riferimento e, se necessario, definire specifiche e procedure per il quadro d'interoperabilità. Sia il quadro che gli strumenti d'interoperabilità costituiscono il fattore abilitante per il domicilio digitale europeo.

1.3.2.6. *L'autenticazione dei siti Web*

Per quanto riguarda i siti Web, la normativa chiarisce l'ambito di applicazione dei certificati di autenticazione qualificata (Qualified Web

Authentication Certificates: QWACs) dei siti. Questi certificati garantiscono agli utenti la possibilità di verificare chi si cela dietro un sito web, preservando al contempo le norme e gli standard di sicurezza del settore attualmente consolidati. Lo strumento QWAC era stato introdotto dal regolamento eIDAS nel 2014 (art. 38). I servizi di autenticazione dei siti web offrono agli utenti la garanzia che dietro a quei siti vi siano entità reali e legittime, favorendo così la diffusione di sicurezza e fiducia nelle transazioni commerciali online.

L'uso dei servizi di autenticazione da parte dei siti web è volontario. Tuttavia, affinché l'autenticazione dei siti possa consolidare la fiducia dell'utente e per promuovere la crescita nel mercato interno, il regolamento stabilisce obblighi minimi in materia di sicurezza e responsabilità per i relativi prestatori di servizi di autenticazione. Gli elenchi nazionali di fiducia [1] dovranno confermare lo status qualificato dei servizi di autenticazione di siti web e dei loro fornitori di servizi fiduciari, compresa la loro piena conformità ai requisiti del regolamento per quanto riguarda l'emissione di certificati qualificati. Il riconoscimento dei QWAC significa che ai fornitori di web-browser non è consentito negare l'autenticità dei certificati al solo scopo di attestare il legame tra il nome di dominio del sito e la persona fisica o giuridica a cui il certificato è rilasciato, e per confermare l'identità di tale persona. I fornitori di browser web dovranno visualizzare in modo semplice i dati d'identità certificati e gli altri attributi attestati all'utente finale, nell'ambiente del browser, affidandosi a implementazioni tecniche di loro scelta. A tal fine, i fornitori di browser web dovranno garantire il supporto e l'interoperabilità con i certificati qualificati per l'autenticazione dei siti, rilasciati in piena conformità ai requisiti del regolamento. L'obbligo di riconoscimento, interoperabilità e supporto dei QWAC non pregiudica, ai fornitori di browser web, la libertà di garantire la sicurezza del web, l'autenticazione dei domini e la crittografia del traffico web con la tecnologia e le modalità che ritengono più appropriate. Per contribuire alla sicurezza online degli utenti finali, i fornitori di browser web dovranno essere in grado di adottare, in circostanze eccezionali, misure necessarie e proporzionate in risposta a preoccupazioni fondate su violazioni della sicurezza o sulla perdita d'integrità di un certificato o di un insieme di certificati identificati. In tal caso, i fornitori di web-browser dovranno notificare, senza indebito ritardo, qualsiasi sospetto di violazione nonché le misure adottate in relazione ad un singolo certificato o ad un insieme di certificati. I destinatari della notifica

(1) In ottemperanza con il regolamento eIDAS, gli Stati membri pubblicano elenchi di fiducia di prestatori di servizi fiduciari qualificati, mentre la Commissione europea pubblica un elenco di questi elenchi di fiducia (LOTL).

saranno: l'organismo nazionale di vigilanza, la Commissione, il soggetto a cui sia stato rilasciato il certificato e il prestatore di servizi fiduciari qualificato che abbia rilasciato il certificato o l'insieme di certificati. Le autorità pubbliche degli Stati dovranno valutare la possibilità d'integrare, nei loro siti web, i certificati qualificati di autenticazione al fine di promuoverne ulteriormente l'utilizzo.

1.3.2.7. *Possibili scenari applicativi*

Il portafoglio europeo d'identità digitale mira a facilitare l'applicazione del principio "una volta sola", riducendo così gli oneri amministrativi e favorendo la mobilità transfrontaliera dei cittadini e delle imprese in tutta l'Unione e promuovendo lo sviluppo di servizi di e-government interoperabili in tutta l'Unione.

Il portafoglio consentirà ai cittadini d'identificarsi ed autenticarsi online senza dover ricorrere a fornitori commerciali, a beneficio della sicurezza e della privacy dei cittadini. Spesso infatti, le attuali soluzioni di portafoglio digitale sui telefoni cellulari annullano il controllo dei dati personali e sono scollegate da un'identità fisica verificata, il che rende più difficile contrastare le frodi e le minacce alla sicurezza informatica. Il rilascio e l'utilizzo del portafoglio elettronico è su base volontaria e rispetta i diritti di tutti i cittadini, evitando discriminazioni nei confronti di chi sceglie di non utilizzare il portafoglio digitale europeo.

Oltre ai servizi pubblici, anche le piattaforme online di grandi dimensioni designate ai sensi della legge sui servizi digitali (Digital Service Act) (es. Amazon, Booking.com o Facebook) e i servizi privati che la legge obbliga ad autenticare i propri utenti, dovranno accettare il portafoglio d'identità digitale dell'Unione Europea per accedere ai propri servizi online. Le caratteristiche e le specifiche comuni dei portafogli implementati dagli Stati membri renderanno vantaggioso, per tutti i fornitori di servizi privati, accettarli per i loro servizi, creando così nuove opportunità commerciali. Il portafoglio europeo favorirà anche la conformità dei fornitori di servizi ai diversi requisiti normativi. Oltre a memorizzare in modo sicuro la propria identità digitale, il portafoglio consentirà agli utenti di aprire conti bancari, effettuare pagamenti e conservare documenti digitali, come ad esempio la 'patente di guida mobile', una prescrizione medica, un certificato professionale o un biglietto di viaggio.

1.3.2.8. *Entrata in vigore del regolamento e atti d'esecuzione*

Una volta adottato formalmente, il nuovo regolamento per l'identità digitale europea entrerà in vigore il ventesimo giorno successivo alla sua

pubblicazione nella Gazzetta ufficiale e sarà direttamente applicabile in tutti gli Stati membri. Questi, da parte loro, dovranno fornire ai propri cittadini almeno un portafoglio d'identità digitale a distanza di 24 mesi dall'adozione degli atti d'esecuzione. Tali atti, adottati dalla Commissione, definiranno le specifiche tecniche del portafoglio e della certificazione di sicurezza. Si baseranno sulle specifiche sviluppate nell'ambito del "Toolbox" europeo per l'identità digitale (EU Digital Identity Toolbox).

In particolare, la Commissione dovrà adottare entro 6 mesi l'elenco delle norme di riferimento e, se necessario, le specifiche (es. i formati) e le procedure per il rilascio e la certificazione dei portafogli. Entro 12 mesi invece, la Commissione dovrà definire un elenco di norme di riferimento nonché, se necessario, le specifiche e le procedure prescritte per i fornitori di servizi fiduciari, sia qualificati che non. Sempre entro 12 mesi, la Commissione adotterà le linee guida a cui gli organi di vigilanza nazionale dovranno attenersi nell'esercizio dei loro compiti. Per facilitare la vigilanza e il rispetto del regolamento, gli organismi di vigilanza responsabili dei servizi fiduciari e dei portafogli dei diversi Stati membri potranno offrirsi reciproca assistenza. Gli orientamenti sugli aspetti organizzativi e sulle procedure per l'assistenza reciproca saranno emanati dalla Commissione entro 12 mesi dall'entrata in vigore del regolamento. Entro 24 mesi dall'entrata in vigore del regolamento, la Commissione valuterà se adottare un atto d'esecuzione che stabilisca un elenco di norme di riferimento, specifiche e procedure per i sigilli elettronici avanzati e per le firme elettroniche avanzate.

1.4. Le sfide legate al Portafoglio d'identità digitale europeo (eIDAS 2)

1.4.1. *L'innovazione tecnologica*

L'adozione e la piena applicazione del regolamento rivisto sarà possibile solo grazie ad alcune tecnologie abilitanti che consentiranno la sicurezza, l'interoperabilità e l'armonizzazione a livello dell'Unione europea. A tal fine sono in corso sperimentazioni tecnologiche finanziate e coordinate dalla Commissione, in stratta sinergia con gli Stati membri.

1.4.1.1. *Il pacchetto di strumenti (Toolbox) per un quadro d'identità digitale europea*

Per evitare la frammentazione e gli ostacoli tecnici dovuti a norme divergenti, e per avviare l'attuazione del futuro quadro per un'identità digitale europea, è necessaria un'efficace collaborazione tra la Commissione, gli Stati membri e il settore privato. Il traguardo comune è la messa a punto

di un pacchetto di strumenti comuni ("Toolbox"). Questo comprenderà un'architettura tecnica completa ed un quadro di riferimento: un insieme di norme e di riferimenti tecnici affiancato da una serie di orientamenti e descrizioni di buone pratiche che coprano tutti gli aspetti relativi alle funzionalità e all'interoperabilità dei portafogli europei d'identità digitale (comprese le firme elettroniche) e dei servizi fiduciari qualificati per gli attestati di attributi inclusi nel regolamento. In tale contesto, gli Stati membri dovrebbero anche raggiungere un accordo in merito ad un modello di business e ad una struttura tariffaria per i portafogli europei d'identità digitale al fine di agevolarne l'adozione, in particolare da parte delle piccole e medie imprese, in un ambito transfrontaliero. Il contenuto del Toolbox dovrà quindi svilupparsi di pari passo con i risultati di questa discussione, rispecchiandone i risultati. Il 3 giugno 2021 la Commissione adotta una raccomandazione che invita gli Stati membri a lavorare per lo sviluppo del "Toolbox", e sarà il gruppo di esperti eIDAS (eIDAS Expert Group) a fungere da interlocutore principale nell'attuazione di tale raccomandazione. Nel febbraio 2022 il gruppo di esperti pubblicherà un documento che descrive l'architettura e il quadro di riferimento dell'identità digitale europea. Questo sarà ripreso dall'ENISA nel suo report sugli standard per l'identità digitale. Lo schema fornisce una descrizione sintetica del concetto di portafoglio digitale d'identità europea. Ne vengono specificati i requisiti funzionali e non funzionali, i potenziali elementi costitutivi nonché il ruolo degli attori nell'ecosistema. A differenza del nuovo regolamento eIDAS (una volta adottato in via definitiva), lo schema resta opzionale.

Il primo Toolbox per il portafoglio d'identità digitale europea sarà quindi pubblicato dalla Commissione, in collaborazione con gli Stati membri, il 10 febbraio 2023. In linea con questo sforzo, la Commissione approva programmi pilota su larga scala, incentrati su aree ad alta priorità come le 'patenti di guida mobili', la sanità elettronica, i pagamenti e le qualifiche professionali. L'attuale versione dello sviluppo software dell'architettura di riferimento è disponibile online su un repository pubblico [2] (GitHub).

1.4.1.2. *Progetti pilota e ambiti applicativi*

La Commissione europea proporrà un prototipo di portafoglio d'identità digitale dell'Unione Europea (EUDI). Questo, finanziato nell'ambito del

[2] https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases

programma Europa Digitale (Digital Europe Programme ([3])), servirà a sperimentare e diffondere le specifiche sviluppate dagli Stati membri, in stretta collaborazione con la Commissione, e sarà sperimentato in una serie di progetti pilota su larga scala. La sperimentazione in corso si articola in quattro progetti, avviati il 1 aprile 2023, con un investimento di oltre 90 milioni di euro, di cui 46 milioni cofinanziati dalla Commissione. Alla sperimentazione partecipano oltre 250 imprese private e autorità pubbliche in 25 Stati membri, oltre che in Norvegia, Islanda e Ucraina. Vengono esaminati, in particolare, undici casi d'uso:

1. Accesso ai servizi pubblici: accesso sicuro ai servizi pubblici digitali, come la richiesta di un passaporto o di una patente di guida, il deposito delle tasse o l'accesso alle informazioni sulla sicurezza sociale.

2. Apertura di un conto bancario: Verifica dell'identità dell'utente per l'apertura di un conto bancario online, evitando l'obbligo di fornire ripetutamente dati personali.

3. Registrazione SIM: prova dell'identità ai fini dei contratti di carta SIM pre e post-pagata (registrazione e attivazione), riducendo le frodi e i costi per gli operatori di rete mobile.

4. Patente di guida mobile: sua memorizzazione e presentazione, sia nelle interazioni online che fisiche (es. consegna della patente da parte di un automobilista sul ciglio della strada).

5. Firma dei contratti: creazione di firme digitali sicure per la firma di contratti online, svincolandoci dall'onere di documenti cartacei e firme fisiche.

6. Richiesta di prescrizioni mediche: trasmissione alle farmacie dei dettagli della prescrizione e avviamento della consegna di prodotti medici.

7. Viaggi: presentazione delle informazioni contenute nei documenti di viaggio (ad es. passaporto, visto e altro), per consentire un accesso rapido e semplice durante i controlli di sicurezza e doganali in aeroporto.

8. Identità digitali organizzative: attestazione della propria legittimità in quanto rappresentanti di un'organizzazione.

9. Pagamenti: verifica dell'identità dell'utente nell'avviamento di un pagamento online.

10. Certificazione dell'istruzione: prova del possesso di credenziali educative come diplomi, lauree e certificati, che facilitano la richiesta di lavoro o di ulteriore istruzione.

11. Accesso alle prestazioni di sicurezza sociale: il portafoglio può essere utilizzato per accedere in modo sicuro alle informazioni e ai servizi di

([3]) https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en

sicurezza sociale, come le prestazioni di pensione o di invalidità. Può anche favorire la libertà di movimento, conservando documenti come la tessera europea di assicurazione malattia.

Ogni progetto pilota utilizzerà componenti dell'implementazione di riferimento sviluppata dalla Commissione europea e contribuirà a migliorarne ulteriormente la sicurezza, la facilità d'uso e l'interoperabilità. L'Italia è rappresentata in tre dei quattro consorzi di progetto e partecipa alla sperimentazione dei seguenti casi d'uso: 1, 4, 6, 8, 9.

1.4.1.3. *La certificazione di sicurezza del portafoglio d'identità digitale europeo*

In parallelo all'adozione del nuovo regolamento si stanno definendo le regole per la certificazione di sicurezza del portafoglio. In questo processo sono impegnati la Commissione, l'ENISA (European Union Agency for Cybersecurity) ([4]) ed esperti degli Stati membri. Attraverso il Cybersecurity Act (CSA), l'ENISA è stata infatti individuata come l'organizzazione più adatta ad elaborare schemi di certificazione candidati nel quadro della certificazione della cibersicurezza dell'Unione, per la sua attività nei servizi pubblici e per le sue relazioni con l'industria e con le organizzazioni di standardizzazione. I nuovi schemi di certificazione, in base a quanto stabilito nel nuovo regolamento per l'identità digitale, saranno applicati secondo le modalità già espresse nel regolamento eIDAS vigente.

1.4.1.4. *Altri strumenti a livello di Stato membro*

Gli Stati membri possono integrare, nel portafoglio digitale, diverse tecnologie per la tutela della privacy, come strumenti crittografici che consentano a una parte facente affidamento di convalidare la veridicità di una determinata dichiarazione utilizzando i dati identificativi di una persona e attestandone gli attributi, ma senza rivelarne i dati, a beneficio della privacy.

Qualora uno Stato membro abbia approvato più di un portafoglio d'identità sul proprio territorio, nell'implementazione del regolamento occorrerà agevolare il passaggio dell'utente da un portafoglio all'altro. Al fine di evitare effetti di *lock-in*, laddove sia tecnicamente fattibile, i fornitori di portafogli dovrebbero garantire l'effettiva portabilità dei dati, su richiesta degli utenti, e non dovrebbero essere autorizzati a utilizzare barriere contrattuali, economiche o tecniche che impediscano o scoraggino il passaggio effettivo tra i portafogli.

([4]) https://www.enisa.europa.eu/

Per garantire che il quadro dell'identità digitale europea sia a prova di futuro — aperto all'innovazione e allo sviluppo tecnologico — gli Stati membri sono incoraggiati a creare congiuntamente sandbox regolamentari (5) per testare soluzioni innovative in un ambiente controllato e sicuro. L'obiettivo è quello di migliorare le funzionalità, la protezione dei dati personali, la sicurezza e l'interoperabilità delle soluzioni, nonché quello di testare i futuri aggiornamenti dei riferimenti tecnici e dei requisiti legali. Tutto ciò dovrebbe favorire l'inclusione delle PMI europee, delle start-up e dei singoli innovatori e ricercatori.

Per assicurare una sufficiente diffusione dei portafogli, sarà opportuno che gli atti di esecuzione stabiliscano specifiche tecniche e operative armonizzate per l'*on-boarding* degli utenti, mediante l'uso di mezzi d'identificazione elettronica, compresi quelli rilasciati al livello di garanzia 'sostanziale'.

1.4.1.5. *La sovranità digitale europea*

Come già descritto, entro 6 e 12 mesi dalla data d'entrata in vigore del regolamento, la Commissione stabilirà, mediante atti d'esecuzione, un elenco di norme di riferimento e, se necessario, specifiche e procedure per la conformità del portafoglio e dei suoi servizi fiduciari ai requisiti della sicurezza. Queste norme e specifiche tecniche e operative faciliteranno l'accesso e l'utilizzo del portafoglio europeo d'identità digitale.

Naturalmente, il portafoglio dovrà interagire con un ecosistema di fornitori hardware e di piattaforme software, come i produttori di apparecchiature di telefonia mobile, i gestori di piattaforme di comunicazione e i servizi di reti digitali. I fornitori di questi sistemi e servizi dovranno disporre di un'interoperabilità efficace e di condizioni eque, ragionevoli e non discriminatorie per garantire l'accesso dei portafogli a specifiche caratteristiche hardware e software dei dispositivi mobili e delle reti (es. antenne per le comunicazioni in prossimità, elementi sicuri, componenti incorporati certificati, schede *microSD* e *Bluetooth Low Energy*). Questi dispositivi sono tipicamente controllati da operatori di reti mobili e da produttori di apparecchiature, che non dovranno rifiutarne l'accesso. Anche le imprese designate dalla Commissione europea come *gatekeeper* per i servizi della piattaforma di base enumerati, ai sensi del Regolamento DMA (2022/1925) (6), dovrebbero attenersi alle disposizioni specifiche in merito.

---

(5) Le sandbox regolamentari sono ambienti concreti che, fornendo un contesto strutturato per la sperimentazione, consentono di testare in un ambiente reale tecnologie, prodotti, servizi o approcci innovativi (Consiglio dell'UE).

(6) https://digital-markets-act.ec.europa.eu/index_en

1.4.2. *Sfide procedurali*

Oltre alle chiare sfide tecnologiche sopra discusse, il regolamento aggiornato sull'identità digitale dovrà affrontare sfide giuridiche e procedurali importanti, sia a livello nazionale che transfrontaliero. Per garantire il successo del portafoglio elettronico europeo, gli Stati membri saranno chiamati a sviluppare e ad estendere la loro normativa vigente in termini di servizi fiduciari e cooperazione transfrontaliera.

1.4.2.1. *L'efficacia giuridica a livello nazionale*

Il regolamento eIDAS 2 stabilisce la non contestabilità dell'efficacia giuridica di una firma elettronica, per il semplice fatto di essere in forma elettronica. Spetterà tuttavia al diritto nazionale definire l'efficacia giuridica delle firme elettroniche, ad eccezione di quanto previsto dal regolamento, secondo cui l'effetto giuridico di una firma elettronica qualificata dovrà essere equivalente a quello di una firma autografa. Nel determinare gli effetti giuridici delle firme elettroniche, gli Stati membri dovranno tenere conto del principio di proporzionalità tra il valore giuridico del documento da firmare e il livello di sicurezza e di costo richiesto da una firma elettronica. Per aumentare l'accessibilità e l'uso delle firme elettroniche, gli Stati sono incoraggiati a introdurre le firme elettroniche avanzate nelle transazioni quotidiane, per le quali offrono un livello sufficiente di sicurezza e fiducia. Per garantire la coerenza delle pratiche di certificazione in tutta l'Unione, la Commissione emanerà linee guida sulla certificazione e sulla ricertificazione dei dispositivi per la creazione di una firma elettronica qualificata e di un sigillo elettronico qualificato, specificandone validità e limitazioni temporali.

L'introduzione del portafoglio digitale europeo dovrebbe consentire l'emissione e la gestione di attributi digitali affidabili, riducendo gli oneri amministrativi nelle transazioni pubbliche e private. I cittadini e gli altri residenti potrebbero, ad esempio, dimostrare di possedere una patente di guida in corso di validità rilasciata dall'autorità di uno Stato membro. I cittadini potrebbero anche avvalersi, in un contesto transfrontaliero, delle proprie credenziali relative alla previdenza sociale o di eventuali documenti di viaggio digitali.

Il processo di notifica dei regimi d'identificazione elettronica dovrà essere semplificato e accelerato per promuovere l'accesso a soluzioni d'autenticazione e identificazione pratiche, affidabili, sicure e innovative. Lo snellimento del processo potrebbe anche incoraggiare i fornitori privati d'identità a offrire regimi d'identificazione elettronica alle autorità degli Stati, ai sensi del precedente regolamento eIDAS. La razionalizzazione delle attuali procedure di notifica e di revisione paritetica eviterà approcci eterogenei in

materia e accrescerà la fiducia tra gli Stati membri. In altre parole, i nuovi meccanismi semplificati favoriranno la cooperazione tra Stati in fatto di sicurezza e interoperabilità dei loro regimi.

Qualunque soggetto raccolga, crei e rilasci attributi attestati quali diplomi, licenze o certificati di nascita, diventerebbe un fornitore di attestati elettronici di attributi. Le parti facenti affidamento sulla certificazione utilizzerebbero gli attestati elettronici di attributi come equivalenti di quelli in formato cartaceo. Agli attestati elettronici di attributi non dovrebbero pertanto essere negati gli effetti giuridici a motivo della loro forma elettronica. A tal fine sarà opportuno stabilire requisiti generali per garantire che gli effetti giuridici degli attestati elettronici di attributi qualificati siano equivalenti a quelli degli attestati in formato cartaceo rilasciati legalmente. Tali requisiti dovrebbero soddisfare anche ulteriori indicazioni settoriali di forma, nel rispetto della normativa unionale (o nazionale).

1.4.2.2. *L'adozione da parte dei privati*

Sarà essenziale prevedere un quadro giuridico per agevolare il riconoscimento transfrontaliero tra gli ordinamenti giuridici nazionali esistenti, in materia di servizi elettronici di recapito certificato. Tale quadro potrebbe aprire, per i prestatori di servizi fiduciari dell'Unione, nuove opportunità di mercato per innovativi servizi elettronici di recapito certificato paneuropei. Adeguate normative assicurerebbero inoltre l'identificazione dei destinatari con un livello di sicurezza più elevato rispetto all'identificazione dei mittenti.

Per una maggiore attrattività e usabilità, i portafogli europei d'identità digitale devono essere accettati dai prestatori di servizi privati. Tutte le parti private facenti affidamento sulla certificazione (ad es. nei settori dei trasporti, dell'energia, dei servizi bancari e finanziari, della previdenza sociale, della sanità, dell'acqua potabile, dei servizi postali, dell'infrastruttura digitale, dell'istruzione o delle telecomunicazioni) dovrebbero accettare l'uso dei portafogli europei d'identità digitale per la prestazione dei servizi per i quali l'Unione, la nazionale o gli obblighi contrattuali impongono un'autenticazione forte dell'utente per l'identificazione online.

Qualora le piattaforme online di dimensioni "molto grandi" (come quelle definite dal regolamento sui servizi digitali: Digital Services Act) impongano agli utenti di autenticarsi per accedere ai servizi online, dovrebbero accettare per legge l'uso dei portafogli europei d'identità digitale su richiesta dell'utente, nel rispetto del principio della minimizzazione dei dati. Gli utenti non dovrebbero avere obbligo di avvalersi del portafoglio per accedere a servizi privati, ma solo qualora desiderassero usarlo.

Sarebbe opportuno elaborare codici di condotta di autoregolamentazione, a livello dell'Unione, per promuovere la disponibilità ed usabilità dei

mezzi d'identificazione elettronica, compresi i portafogli europei d'identità digitale, che rientrano nell'ambito d'applicazione del regolamento. I codici di condotta dovrebbero agevolare una più diffusa accettazione dei mezzi d'identificazione elettronica, compresi i portafogli europei d'identità digitale, da parte dei prestatori di servizi che non rientrino nella categoria delle piattaforme "molto grandi", o che si avvalgano di servizi d'identificazione elettronica di terzi per l'autenticazione degli utenti. I codici andrebbero definiti entro 12 mesi dall'adozione del regolamento. La Commissione dovrebbe valutare l'efficacia delle disposizioni atte a garantire la disponibilità e l'usabilità dei portafogli, dopo 18 mesi dalla loro introduzione e, alla luce di tale valutazione, procedere alla revisione delle disposizioni mediante atti delegati, per garantirne l'accettazione.

1.5. Gli scenari futuri a livello internazionale

Il regolamento modificato (eIDAS 2) rinforzerà la leadership europea nell'attuale contesto internazionale, che sta lavorando per un'identità legale delle persone a livello globale. L'obiettivo potrà essere raggiunto solo grazie a tecnologie emergenti, che stanno già plasmando il futuro dell'identità digitale (ad es. blockchain, biometria, identità decentralizzata).

1.5.1. *Le iniziative delle Nazioni Unite e i nuovi standard internazionali*

La spinta all'adozione diffusa dell'identità digitale sta guadagnando slancio a livello globale grazie alla crescente mobilità delle persone, che sempre più spesso accedono ad Internet attraverso dispositivi mobili. L'iniziativa ID4D (Identification for Development) delle Nazioni Unite (ONU) e della Banca Mondiale, mira a dotare tutti gli abitanti del pianeta di un'identità legale entro il 2030. L'obiettivo è quello di aiutare i paesi a realizzare il potenziale di trasformazione dei sistemi d'identificazione, compresa la registrazione civile. Questo per consentire a tutte le persone di esercitare i propri diritti, di accedere a servizi migliori e di sfruttare le nuove opportunità economiche, in linea con gli obiettivi di uno sviluppo sostenibile. Il processo risulta fondamentale in una società mondiale che si sta dirottando verso un'economia digitale e verso governi digitali. Inclusività e affidabilità dei sistemi d'identità saranno imprescindibili affinché tutti possano godere dei benefici, nella salvaguardia della privacy.

Per questo motivo, negli ultimi anni, vari paesi hanno lanciato documenti d'identità digitale, come patenti e passaporti digitali, e hanno condotto sperimentazioni sulla residenza elettronica. Anche il settore della sicurezza si è impegnato a fondo per migliorare le soluzioni di gestione e di verifica

dell'identità. Le frontiere e gli aeroporti intelligenti sono apparsi a un ritmo molto rapido, offrendo ai viaggiatori un assaggio di movimenti transfrontalieri tanto sicuri quanto rapidi, e senza soluzione di continuità. Questo grazie a più di un miliardo di passaporti elettronici in circolazione e ad una forte spinta verso la biometria, in particolare nella forma del riconoscimento facciale. Diversi gruppi di lavoro si vanno dedicando alla ricerca di nuovi standard d'identificazione che favoriscano la compatibilità e l'interoperabilità; tra questi, il nuovo gruppo di lavoro ICAO (International Civil Aviation Organization), che lavora sulle credenziali di viaggio digitali, e il gruppo di lavoro dell'ISO SC17 WG10, che lavora sugli standard di verifica per la patente di guida mobile. Quest'ultimo gruppo ha prodotto lo standard ISO/IEC 18013-5, che, concepito inizialmente per coprire le specifiche delle 'patenti di guida mobili', definisce chiaramente i protocolli di sicurezza e di comunicazione per la verifica e l'affidabilità dei documenti digitalizzati, offrendosi quindi per qualsiasi iniziativa relativa ai documenti mobili.

I portafogli digitali d'identità daranno un forte impulso ai sistemi d'identificazione digitale in tutto il mondo, introducendo applicazioni mobili sicure per archiviare versioni digitalizzate e crittografate dei documenti d'identità: siano essi un'identità, una patente di guida, la registrazione di un veicolo o credenziali sanitarie. Con eIDAS 2 l'Unione europea rinforza la sua leadership a livello globale in questo campo, garantendo i diritti digitali dei suoi cittadini.

1.5.2. *Le tecnologie di frontiera per l'identità digitale*

La nostra società vive una costante rivoluzione tecnologica, che investe inevitabilmente anche i servizi d'identità digitale. In un futuro prossimo, nel gestire le identità digitali, utilizzeremo molto probabilmente le tecnologie accennate nei prossimi paragrafi.

1.5.2.1. *La tecnologia blockchain*

La blockchain è una tecnologia di registrazione digitale che memorizza le informazioni in blocchi collegati, creando una catena di dati sicura e trasparente. Costituisce un approccio decentralizzato, che non implica entità di controllo e quindi più sicuro. Modificare i dati registrati dalla blockchain è molto difficile, il che la rende affidabile per vari tipi di transazioni. Questa tecnologia è già stata sperimentata, ad esempio, in Gran Bretagna per i pagamenti del welfare ai cittadini e in Estonia, per la residenza digitale.

In entrambi i casi ha dimostrato grande potenziale, garantendo transazioni efficienti e sicure.

1.5.2.2. *L'Intelligenza Artificiale*

L'intelligenza artificiale avrà un ruolo di primo piano nel futuro della gestione delle identità digitali. Questa tecnologia è ormai diventata parte integrante della biometria e di altre tecnologie per la verifica delle identità digitali. Naturalmente, il suo impiego ha innescato nuove sfide, come la necessità di stabilire norme per garantire che la verifica dell'identità guidata dall'intelligenza artificiale sia imparziale ed equa, che eviti discriminazioni e imprecisioni e che protegga la privacy. Inoltre, l'integrazione dell'intelligenza artificiale nei sistemi d'identità digitale richiede uno sviluppo significativo dell'infrastruttura. Ciò include algoritmi robusti, potenza di calcolo e strutture di gestione dei dati. Nel desiderio di rispondere a queste esigenze, la Commissione ha adottato una proposta di regolamento sull'intelligenza artificiale (AI Act) che ha portato ad un accordo politico preliminare nel dicembre 2023.

1.5.2.3. *La biometria*

La biometria ha inaugurato una nuova era per l'autenticazione dell'identità digitale. Nella stagione della connettività mobile, della tecnologia IoT (Internet of Things) e del cloud computing, i tradizionali metodi di accesso (es. ID utente e password) per autenticare l'identità digitale non appaiono più sufficienti a fronteggiare le nuove minacce alla cibersicurezza, e si utilizza sempre di più il riconoscimento biometrico. Il riconoscimento biometrico è un tipo di sistema informatico che identifica una persona sulla base di una o più caratteristiche fisiche o comportamentali uniche (es. le impronte digitali, il riconoscimento facciale o la scansione dell'iride) confrontandole con i dati precedentemente acquisiti e conservati nel database del sistema. La tecnologia continua a perfezionare i metodi di autenticazione biometrica, rendendoli sempre più affidabili e difficili da falsificare. Quest'evoluzione promette di migliorare la sicurezza e la facilità d'uso dei documenti d'identità digitale, sempre più parte integrante della nostra vita quotidiana.

1.6. L'identità auto-sovrana

Una tendenza rivoluzionaria dell'identità digitale è il concetto d'identità auto-sovrana (Self-Sovereign Identity: SSI). Quest'approccio offre agli individui il controllo completo della propria identità digitale, evitando la necessità di autorità centrali per la gestione dei dati personali. eIDAS 2 costituisce un passo avanti in questa direzione.

Bibliografia

- AgID, "Nasce INAD, l'Indice Nazionale dei Domicili Digitali". https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2023/06/06/nasce-inad-lindice-nazionale-domicili-digitali (accesso del 27/12/2023).
- AgID, "Regole tecniche per i servizi di recapito certificato a norma del regolamento eIDAS n. 910/2014 - Criteri di adozione standard ETSI - REMPolicy-IT Versione 1.0". https://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/22221824510O__ODocumento+finale+regole+tecniche+rem+versione+1.0+03.08.2022.pdf (accesso del 27/12/2023).
- Codeheroes, "The Future of Digital ID: Emerging Trends and Innovations in Identity Management". https://www.codeheroes.com.au/blog/digital-id-emerging-trends-and-innovations-in-identity-management#:~:text=4.,technologies%20for%20verifying%20digital%20identities. (accesso del 23/12/2023).
- Consiglio d'Europa (2020), "DEVELOPING AND PROMOTING DIGITAL CITIZENSHIP EDUCATION". Recommendation CM/Rec (2019)10 adopted by the Committee of Ministers of the Council of Europe on 21 November 2020.
- Consiglio dell'UE, "Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea. Documento del Consiglio ST9471/21. Giugno 2021.
- Consiglio dell'UE, Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity - Analysis of the final compromise text with a view to agreement. Documento del Consiglio ST15149/23. Novembre 2023.
- Commissione Europea, "Regulatory framework proposal on artificial intelligence". https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai (accesso del 23/12/2023).
- Commissione Europea, "European Digital Identity Architecture and Reference Framework - Outline". https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline (accesso del 17/12/2023).
- Commissione Europea, "COMMISSION RECOMMENDATION of 3.6.2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework". C(2021) 3968 final. file:///C:/Users/nativ/Downloads/C2021_3968_EN_ACT_part1_dNLKk3HM1tYtdlvGDYPq3Rtp6Jc_76610.pdf (accesso del 17/12/2023).
- Commissione Europea, "eIDAS Observatory". https://ec.europa.eu/futurium/en/blog/commission-runs-pilot-project-qualified-web-authentication-certificates-qwacs.html (accesso del 16/12/2023)
- Commissione Europea, "Dichiarazione europea sui diritti e i principi digitali". https://digital-strategy.ec.europa.eu/it/library/european-declaration-digital-rights-and-principles (accesso del 16/12/2023).
- Commissione Europea, "Europe's Digital Decade" https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade (accesso del 10/12/2023).
- Commissione Europea, "European Digital Rights and Principles". https://digital-strategy.ec.europa.eu/en/policies/digital-principles (accesso del 26 dicembre 2023).

- Commissione Europea, "Decennio digitale europeo: obiettivi digitali per il 2030", https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_it (accesso del 10 dicembre 2023).
- Commissione Europea, "First report on the State of the Digital Decade calls for collective action to shape the digital transition", https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4619 (accesso del 10/12/2023).
- Commissione Europea, "2023 Report on the state of the Digital Decade". https://ec.europa.eu/newsroom/dae/redirection/document/98641 (accesso del 10/12/2023).
- Commissione Europea, "2023 Report on the state of the Digital Decade: Annex Italy". https://ec.europa.eu/newsroom/dae/redirection/document/98653 (accesso del 10/12/2023).
- Commissione Europea, "Digital Economy and Society Index (DESI) 2022", https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2022 (accesso del 10/12/2023).
- Commissione Europea, "Commission welcomes final agreement on EU Digital Identity Wallet". https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5651 (accesso del 16/12/2023).
- Commissione Europea, "European Digital Identity", https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_it (accesso del 10/12/2023).
- Commissione Europea, "The Digital Europe Programme". https://digital-strategy.ec.europa.eu/en/activities/digital-programme (accesso del 16/12/2023).
- Commissione Europea, "The Digital Services Act". https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (accesso del 16/12/2023).
- Commissione Europea, "EU Digital Identity Wallet Pilot implementation". https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-implementation (accesso del 17/12/2023).
- Commissione Europea, " ANNEX to the Proposal for a COUNCIL IMPLEMENTING DECISION amending Implementing Decision (EU) (ST 10160/21; ST 10160/21 ADD 1 REV 2) of 13 July 2021 on the approval of the assessment of the recovery and resilience plan for Italy". COM(2023) 765 final.
- e-MEDINE, "EUROPEAN DIGITAL CITIZENSHIP: EVERYTHING YOU NEED TO KNOW". https://e-medine.org/european-digital-citizenship-spid-cie-pec/#:~:text=in%20the%20population.-,European%20digital%20citizenship%3A%20what%20it%20is%2C%20the%20definition,%2C%20cultural%20and%20intercultural)%C2%BB (accesso del 27/12/2023).
- EU Business, "EU negotiators reach final agreement on EU-wide digital wallet". https://www.eubusiness.com/news-eu/eu-wide-digital-wallet.81vl/ (accesso del 16/12/2023)
- ENISA, "DIGITAL IDENTITY STANDARDS". ENISA Report. Luglio 2023. file:///C:/Users/nativ/Downloads/Digital_Identity_Standards.pdf ISBN 978-92-9204-617-0, DOI 10.2824/28598.
- ETSI - Electronic Signatures and Infrastructures (ESI) TC, "Registered Electronic Mail (REM) Services; Part 4: Interoperability profiles". https://www.etsi.org/deliver/etsi_en/319500_319599/31953204/01.01.07_20/en_31953204v010107a.pdf Draft ETSI EN 319 532-4 V1.1.7 (2022-01).

- EUROSTAT, https://ec.europa.eu/eurostat/cache/infographs/ict/bloc-4.html#:~:text=The%20Digital%20Single%20Market%20opens,to%20cross%2Dborder%20online%20activity (accesso del 08/12/2023)
- Garante per la Protezione dei Dati Personali, "GDPR: il testo del regolamento" https://www.garanteprivacy.it/il-testo-del-regolamento (accesso del 11/12/2023)
- Gazzetta Ufficiale dell'Unione Europea, "REGOLAMENTO (UE) N. 910/2014 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE", https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32014R0910 (accesso del 11/12/2023).
- Gazzetta Ufficiale dell'Unione Europea, "REGOLAMENTO (UE) 2019/881 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 (« regolamento sulla cibersicurezza »). https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=PT (accesso del 17/12/2023).
- Gazzetta Ufficiale dell'Unione Europea, "REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati"). https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679 (accesso del 17/12/2023).
- Gazzetta Ufficiale dell'Unione Europea, "REGOLAMENTO (UE) 2022/1925 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali)". https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R1925 (accesso del 17/12/2023).
- ISO/IEC 18013-5:2021 "Personal identification ISO-compliant driving licence-Part 5: Mobile driving licence (mDL) application. https://www.iso.org/standard/69084.html (accesso del 23/12/2023).
- Medium, "Emerging Technologies Shaping the Future". https://medium.com/@tech_and_tea/emerging-technologies-shaping-the-future-947d8b109a56 (accesso del 28/12/2023).
- Namirial, "Riconoscimento biometrico: cos'è e a cosa serve". https://focus.namirial.it/riconoscimento-biometrico/ (accesso del 23/12/2023).
- Namirial, "PEC becomes European: what are the new standards?" https://focus.namirial.global/european-pec-certified-email/ (accesso del 27/12/2023).
- Network Digital 360, "Il wallet di identità digitale europea: i principali aspetti funzionali e operativi". https://www.agendadigitale.eu/cittadinanza-digitale/il-wallet-di-identita-digitale-europea-i-principali-aspetti-funzionali-e-operativi/ (accesso del 17/12/2023).
- Parlamento Europeo, "Revision of the eIDAS Regulation Findings on its implementation and application". https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf (accesso del 12/12/2023).
- Presidenza del Consiglio dei Ministri, "Piano Nazionale di Ripresa e Resilienza"

https://italiadomani.gov.it/content/dam/sogei-ng/documenti/PNRR%20Aggiornato.pdf (accesso del 27/12/2023)
- THALES, "Digital identity trends - 5 forces that are shaping 2023". https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/trends (accesso del 23/12/2023).
- The World Bank, "ID4D: 2022 Annual Report". https://id4d.worldbank.org/annual-report (accesso del 23/12/2023).

APPENDICE

I.
IDENTITÀ E DOMICILIO DIGITALE IN INGHILTERRA E GALLES (*)

di *James Henderson* e *Renato Nazzini*

Sommario: 1.1. Introduzione. — 1.2. Verify e One Login. — 1.3. Opinione pubblica. — 1.4. Quadro fiduciario identità e attributi digitali. — 1.5. Servizi giudiziari. — 1.6. Istanze civili. — 1.7. Altri sistemi civili. — 1.8. Sentenze e ordinanze. — 1.9. La Piattaforma Comune. — 1.10. Conclusioni.

1.1. Introduzione

I dibattiti e le pressioni legati alla precedente proposta sulle carte d'identità digitali nazionali hanno fortemente colpito i tentativi di sviluppare servizi nazionali di identità digitale nel Regno Unito.

Il Partito Laburista provò nel 2004 a introdurre un piano sulle carte d'identità ma non riuscì a far approvare la legge prima delle elezioni generali del 2005. A seguito della loro vittoria nelle elezioni, il Partito Laburista introdusse nuovamente una legge sulle carte d'identità, che fu rifiutata tre volte dalla Camera dei Lord prima di essere approvata come Legge 2006 sulle Carte d'Identità (Identity Cards Act 2006). Con questo disegno di legge, le carte d'identità non sarebbero state obbligatorie, ma dal 2008 a chiunque avesse rinnovato il passaporto sarebbe stata rilasciata una carta e i propri dati sarebbero stati inseriti in un database centrale, il Registro Nazionale delle Identità (National Identity Register). Il Registro avrebbe contenuto indirizzi attuali e passati, così come i dati biometrici [1]. A seguito delle elezioni generali del 2010, la nuova coalizione governativa tra i Conservatori e i Liberal Democratici approvò la Legge 2010 sui Documenti d'Identità (Identity Documents Act 2010) in modo da revocare la precedente legge e il database fu cancellato.

Come verrà discusso in seguito, quando si affronta il tema dell'identità digitale, il governo ha cercato ripetutamente di prendere le distanze dalla

(*) Libera traduzione, non revisionata dagli Autori.

(1) Identity Cards Act 2006, C. 15

Legge del 2006 ed evitare di creare, o di far credere di creare, un database centralizzato, carte d'identità o un piano obbligatorio sull'identità digitale.

Probabilmente come conseguenza, l'approccio del Regno Unito alle identità digitali è stato in qualche modo frammentato. Anche i servizi governativi sono quasi interamente federati. Gli utenti creano account per ogni servizio specifico in modo separato, ognuno con i propri standard per la verifica dell'identità. Nessuna identità digitale creata può essere, per impostazione predefinita, trasferita o utilizzata per altri servizi. Nel 2023 il governo ha riferito la presenza di più di 190 percorsi di iscrizione e 44 account separati (2).

1.2. Verify e One Login

Si è tentato di affrontare gli approcci disconnessi alle identità digitali con il piano di garanzia dell'identità GOV.UK Verify ("Verify"), il quale è stato in funzione da maggio 2016 ad aprile 2023. Questo piano, al contrario del Registro Nazionale delle Identità proposto dalla Legge 2006 sulle Carte d'Identità, permetteva agli utenti di verificare la propria identità tramite diversi "provider di identità" di terze parti, i quali erano stati approvati dal governo per effettuare controlli sulle identità con un livello di sicurezza standard. Per impostazione predefinita, non era presente un'archiviazione centralizzata dei dati e i servizi in questione raccoglievano una quantità minima necessaria sulle informazioni dell'utente.

Nel 2020, al suo apice, Verify era utilizzato per 22 servizi. Tuttavia, Verify non è riuscito a raggiungere in modo sistematico gli obiettivi. È partito 4 anni dopo il previsto, ha avuto costantemente un'adesione minore di quella attesa, e nel 2021 aveva raggiunto un tasso di successo di verifica solo del 50% (3).

Dal 2021, il Servizio Digitale Governativo (Government Digital Service) ("GDS"), sotto l'Ufficio di Gabinetto (Cabinet Office), si è adoperato per creare un sostituto chiamato GOV.UK One Login ("One Login"), un piano condiviso di identità digitale per accedere ai servizi online governativi

(2) Cabinet Office e Government Digital Service, *Cabinet Office launches consultation on departmental data sharing* (2023) disponibile sul sito <https://www.gov.uk/government/news/cabinet-office-launches-consultation-on-departmental-data-sharing>

(3) Government Digital Service, 'GOV.UK Dashboard' (2021) <https://webarchive.nationalarchives.gov.uk/ukgwa/20210315085419mp_/https://www.gov.uk/performance/govuk-verify> consultato 2023.

centrali (4). È stato concepito per essere l'unico accesso a qualsiasi servizio governativo, e per permettere agli utenti di creare un'identità digitale che possa essere verificata e riutilizzata in sicurezza per tutti i servizi governativi. Verify era destinato a essere chiuso nel 2021, ma la chiusura è stata posticipata per concedere più tempo allo sviluppo di One Login (5).

Al contrario dei suoi predecessori, One Login si basa prevalentemente su verifiche in-house, nonostante ad agosto 2023 il sistema abbia avviato un controllo dell'identità dal vivo presso gli uffici postali per coloro non disposti o non in grado di usare il sistema di verifica dell'identità dall'app o dal browser (6). Ancora una volta, tuttavia, non era presente un archivio centrale dei dati come il Registro Nazionale delle Identità; i dati archiviati sono segmentati e conservati solamente per un periodo di tempo limitato (7).

A partire da giugno 2023, One Login viene utilizzato per otto servizi governativi, tra cui l'Agenzia per gli Standard dei Conducenti e dei Veicoli (Driver and Vehicle Standards Agency), la Conservatoria dei Registri Immobiliari (HM Land Registry) e il Dipartimento Entrate e Dogane (HM Revenue and Customs). Tuttavia, il sistema è attualmente volontario, perciò i dipartimenti governativi che gestiscono i servizi possono decidere quando e addirittura se iscriversi, quindi è poco chiaro quale sarà la portata finale del sistema, anche se il GDS spera che possa essere ampliato per includere i servizi governativi locali (8). Il piano d'azione pubblicato fornisce pochi dettagli o informazioni utili (9).

1.3. Opinione pubblica

Tra il 4 gennaio 2023 e il 1° marzo 2023, il governo ha effettuato una campagna di raccolta pareri sulla bozza delle Norme Governative Digitali

---

(4) Government Digital Service, *GOV.UK One Login: June 2023 update* (2023), disponibile sul sito https://gds.blog.gov.uk/2023/06/24/gov-uk-one-login-june-2023-update/.

(5) Hansard HC vol. 693 col. 7WS-8WS (27 aprile 2021).

(6) Government Digital Service, *The new in-person identity check for GOV.UK One Login* (2023) disponibile sul sito https://gds.blog.gov.uk/2023/08/30/the-new-in-person-identity-check-for-gov-uk-one-login/.

(7) Mark Say, 'GDS promotes the prospects for GOV.UK One Login' *Uk Authority News* https://www.ukauthority.com/articles/gds-promotes-the-prospects-for-govuk-one-login/.

(8) Government Digital Service, *One Login for Government: December 2021 update* (2021) disponibile sul sito https://gds.blog.gov.uk/2021/12/01/one-login-for-government-december-2021-update/.

(9) Government Digital Service, 'GOV.UK One Login Roadmap' (2023) <https://www.sign-in.service.gov.uk/about/roadmap> consultato.

2023 (Divulgazione Informazioni) (Servizi Verifica Identità) (10). Le norme proposte sono state progettate come supporto all'avvio di One Login, abilitando i controlli sulle identità a fronte di una più ampia gamma di dati fidati già a disposizione degli enti pubblici e permettendo agli utenti di riutilizzare, una volta verificata, l'identità One Login in modo più agevole.

Il potere di Fornitura di Servizi Pubblici (Public Service Delivery) ("PSD") (Capitolo 1 della Sezione 5 della Legge 2017 sull'Economia Digitale (Digital Economy Act 2017) consente a determinate autorità pubbliche di condividere informazioni personali per gli obiettivi stabiliti nelle norme. Per esercitare il potere PSD, il governo deve definire obiettivi specifici per i quali i dati possono essere condivisi e nominare le determinate autorità pubbliche a cui si applicano questi obiettivi. La bozza delle norme propone la creazione di un nuovo obiettivo per gli enti pubblici, specificato nella Sezione 4 della Legge, per consentire la condivisione dei dati atti a verificare l'identità digitale. Inoltre, propone l'aggiunta di 4 nuovi enti pubblici alla Sezione 4, permettendo loro di effettuare la condivisione di dati per verificare le identità e per gli obiettivi di fornitura di servizi pubblici (11).

Le risposte ricevute sono state estremamente negative. La maggioranza ha espresso preoccupazioni sulla privacy e la sicurezza dei dati e pensa che questi siano più importanti di eventuali benefici. Una parte considerevole degli utenti ha espresso preoccupazioni su questioni più ampie, piuttosto che sulle domande specifiche sulle norme per la condivisione dei dati (12).

Il Governo ha ipotizzato che molte persone erano "fortemente condizionate dalle opinioni contrarie all'attivazione dell'identità digitale obbligatoria dei cittadini e alla condivisione dei dati per supportarla in linea di principio", evidenziando come il 75% delle email ricevute avesse utilizzato uno dei pochi modelli disponibili. In particolar modo, erano presenti anche timori riguardo al fatto che il piano avrebbe portato all'introduzione delle carte nazionali d'identità o identità digitali obbligatorie. In risposta a quest'apprensione, il Governo ha dichiarato di aver capito che non ha il supporto dei cittadini riguardo alle carte d'identità nel Regno Unito e ha affermato che non esistono piani per introdurre identità digitali obbligatorie. Il Governo ha inoltre evidenziato il fatto che sia stato chiesto agli enti

(10) Cabinet Office, *Government response to the consultation on draft legislation to support identity verification* (2023).

(11) Cabinet Office e Government Digital Service, *Cabinet Office launches consultation on departmental data sharing 8.*

(12) Cabinet Office, *Government response to the consultation on draft legislation to support identity verification*, pp. 12-13.

pubblici di minimizzare la quantità di dati personali condivisi, garantendo che si trattasse del minimo necessario per un dato servizio (13).

Sono state espresse anche preoccupazioni più ampie riguardo al fatto che i servizi di verifica dell'identità potessero portare a un sistema di credito sociale, alla rimozione della moneta fisica oppure a una maggiore sorveglianza governativa. Nel complesso, fino al 20% delle risposte era fuori tema, a seconda delle domande (14). Il Governo, in risposta, ha pubblicato una pagina con le FAQ per confutare tali fraintendimenti (15).

In totale sono stati ricevuti 66233 pareri; tuttavia, non si trattava di un sondaggio scientifico che cercava di valutare l'opinione pubblica in generale. Sussisterebbe una distorsione di selezione, secondo il quale le persone più contrarie al piano sarebbero le più propense a commentarlo.

Nonostante ciò, questa campagna di indagine è riuscita a mostrare, perlomeno, la presenza di una significativa minoranza di persone che nutre pareri estremamente negativi riguardo al piano identità digitale e le relative potenziali implicazioni.

1.4. Quadro fiduciario identità e attributi digitali

Separatamente, nel 2020, il Governo si è adoperato per sviluppare un nuovo quadro giuridico per le identità digitali (16). Nel 2021 ha quindi pubblicato i documenti politici per un Quadro fiduciario identità e attributi digitali del Regno Unito (Digital Identities and Attributes Trust Framework) ("DIATF"), con la versione più recente pubblicata a gennaio 2023 (17).

Con questo sistema, il Governo intende creare un piano di identità digitale distribuito e decentralizzato. Il DIATF crea un processo di standard,

---

(13) Cabinet Office, Central Digital & Data Office and Government Digital Service, 'Additional information: GOV.UK One Login' (2023) <https://www.gov.uk/government/consultations/draft-legislation-to-help-more-people-prove-their-identity-online/outcome/additional-information-govuk-one-login> consultato 2023.

(14) Cabinet Office, *Government response to the consultation on draft legislation to support identity verification*, p. 13.

(15) Cabinet Office, Central Digital & Data Office and Government Digital Service, 'FAQs on government digital identity consultation response' (2023) <https://www.gov.uk/government/news/faqs-on-government-digital-identity-consultation-response> consultato 2023.

(16) Cabinet Office e Department for Digital Culture Media & Sport, 'Digital Identity: Call for Evidence Response' (2020) <https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response> consultato 2023.

(17) Department for Science Innovation and Technology, Department for Digital Culture Media & Sport and Julia Lopez, 'UK digital identity and attributes trust framework - beta version' (2023) <https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version> consultato 2023.

orientamento e certificazione per provider di servizi di identità privati ("IDSP"). Per diventare provider certificati, un IDSP deve, tra le altre cose, seguire gli standard sulla sicurezza definiti nella Guida alle buone pratiche 45 (Good Practice Guide 45) su come verificare l'identità di qualcuno e osservare gli standard sulla sicurezza e protezione dei dati. Esiste un piano dati volontario con l'obiettivo di rendere i servizi interoperabili tra loro. Attualmente, la concessione di licenze governative non è considerata attuabile, quindi la certificazione sarà eseguita da enti certificatori indipendenti.

Il quadro sarà supervisionato da un organo di governo. Al momento è gestito dal Dipartimento per la Cultura, i Media e lo Sport (Department for Culture, Media and Sports) ("DCMS"). È stato affermato che si tratta di un provvedimento provvisorio, ma la struttura istituzionale finale non è ancora stata decisa. È stato pianificato che le legislazioni future permetteranno agli organi di governo di rilasciare marchi di fiducia per le organizzazioni certificate, ma attualmente il DCMS ha semplicemente un elenco interno.

Il DIATF è principalmente destinato al settore privato, ma è previsto che le organizzazioni del settore pubblico potranno lavorare con l'organo di governo per aggiungere il quadro di certificazione. Sono già iniziati i test per il diritto al lavoro, il diritto all'affitto e i controlli del casellario giudiziale.

Il quadro entrerà ufficialmente in vigore con la Proposta di Legge Protezione Dati e Informazioni Digitali (n. 2), che creerà una base legale per il DIATF e consentirà agli IDSP certificati di ottenere dati personali su un utente dai dipartimenti governativi.

È possibile che One Login con il tempo venga integrato nel quadro, sia essendo in grado di agire come un IDSP sia accettando identità digitali verificate esternamente, ma a tal fine non c'è stato nessun annuncio, al di là di una dichiarazione dell'Ufficio di Gabinetto che One Login "si impegna ad aderire ai principi chiave" del DIATF (18) e che "sta collaborando con il DCMS per garantire che le proposte politiche e legislative siano coerenti" (19).

Tuttavia, al momento, il Governo britannico sembra stia perseguendo due piani paralleli di identità digitale, gestiti da dipartimenti governativi differenti: uno cerca di introdurre un quadro distribuito e decentralizzato che eviti lo spettro di un piano nazionale carta d'identità o identità digitale

(18) Cabinet Office, Central Digital & Data Office e Government Digital Service, 'Additional information: GOV.UK One Login'.

(19) Cabinet Office, Central Digital & Data Office e Government Digital Service, 'Consultation on draft legislation to support identity verification' (2023) <https://www.gov.uk/government/consultations/draft-legislation-to-help-more-people-prove-their-identity-online/consultation-on-draft-legislation-to-support-identity-verification> consultato 2023.

rilasciata da un governo, mentre l'altro cerca di creare un unico sistema di identità digitale consolidato che possa essere utilizzato su tutti i servizi pubblici.

1.5. Servizi giudiziari

I servizi giudiziari stanno tentando un proprio processo di digitalizzazione, la maggior parte del quale fa parte dell'ambizioso programma di riforma del Servizio Corti e Tribunali (HM Courts and Tribunal Service) ("HMCTS"), in funzione dal 2016 con l'obiettivo di modernizzare e digitalizzare il sistema giudiziario. Il portafoglio dei programmi è composto da 44 progetti su cinque aree di lavoro, che riguardano i reati, il civile, la famiglia, i tribunali e le proprietà dei tribunali (20).

Tuttavia, i progressi sono stati alquanto irregolari, con ritardi, sforamenti del budget e nuove versioni. Il completamento del programma era previsto per il 2020, ma attualmente lo si prevede per il 2024. Inoltre, nella fretta di rispettare le scadenze, molti servizi non funzionano con l'efficienza prevista.

Inizialmente erano presenti piani per una singola piattaforma comune per richieste civili, familiari e giudiziarie, simile alla piattaforma comune per la criminalità, ma tale proposta è stata respinta dal Governo nel 2017. Perciò, la digitalizzazione di questi servizi ha preso la forma di iniziative individuali per ogni giurisdizione esistente.

L'obiettivo più importante, per la maggior parte delle cause civili, familiari e giudiziarie, è che l'intero processo si svolga online. Sir Geoffrey Vos, il Manutentore dei Documenti e delle Note della Cancelleria d'Inghilterra e Galles (Master of the Rolls and the Head of Civil Justice in England and Wales), in un importante discorso al King's College London, ha delineato un sistema a tappe nel quale gli eventuali querelanti sarebbero in grado in ricevere consulenze pre-azione online, essere indirizzati a portali online di risoluzione alternativa delle controversie e, se questo non dovesse bastare, a processi giudiziari online. L'ambizione è che si tratti di sistemi integrati, con gli stessi dati trasmessi tra ciascuno di essi (21).

Tale processo sarà supervisionato dal Comitato Regolamenti Procedure Online (Online Procedure Rule Committee), creato a giugno 2023 e attualmente presieduto da Sir Geoffrey. Tale Comitato ha la supervisione statutaria

(20) National Audit Office, *Progress on the courts and tribunals reform programme* (HC 1130, 2023) seconda appendice.

(21) Vedi Geoffrey Vos, 'Speech on the 150th Anniversary of the Technology and Construction Court' (2023) <https://www.judiciary.uk/speech-by-the-master-of-the-rolls-justice-in-the-digital-age/> consultato 2023.

dei processi di risoluzione delle controversie creato dal programma di riforma e portali e processi digitali di pre-azione (22).

Una complicanza è rappresentata dal fatto che molti dei portali che questo quadro spera di includere non sono creati o mantenuti dal HMCTS: ad esempio, il portale Ufficiale Richieste Risarcimento (Official Injury Claim) per le richieste di risarcimento per colpo di frusta, realizzato dall'Ufficio Assicurativo Auto (Motor Insurers Bureau), oppure la moltitudine di siti per i diversi difensori civici (ombudsman). Potrebbero esistere fino a 100 portali di questo tipo, ma non c'è un totale ufficiale. Si spera che il Comitato Regolamenti Procedure Online sia in grado di definire un'archiviazione coerente dei dati e interfaccia API (23), ma non sono state ancora avanzate proposte concrete né è chiaro se il sistema verrà progettato per essere compatibile con One Login o con il Quadro DIATF.

Molte delle disposizioni per i tribunali civili sono state attivate tramite indicazioni pratiche. Mentre i cambiamenti al Codice di procedura civile (Civil Procedure Rules) ("CPR") richiedono uno strumento statutario (24), le indicazioni pratiche possono essere modificate in modo relativamente semplice. Tuttavia, le indicazioni pratiche possono essere semplicemente emesse dal Manutentore dei Documenti (Master of the Rolls), con l'approvazione del Lord Cancelliere (Lord Chancellor) (25). In particolare, il CPR Parte 51 permette alle indicazioni pratiche di prevalere sul CPR per determinati periodi o per determinati tribunali come parte di piani pilota (26). Questo ha permesso un avvio graduale e flessibile. I sistemi possono essere introdotti nei singoli tribunali su base volontaria, e poi estesi agli altri tribunali, oppure resi obbligatori con relativa facilità.

1.6. Istanze civili

I tribunali civili si stanno spostando verso un sistema "digitale di default" di presentazione delle istanze per corti e tribunali. Si tratta di uno dei pochi cambiamenti che precede l'attuale programma di riforma. Il Report Jackson 2010 raccomanda, tra le altre cose, la presentazione elettronica delle

(22) Judicial Review and Courts Act 2022, s. 22-24.

(23) Vedi Geoffrey Vos, 'Speech to the Chartered Instituted of Arbitrators: Roebuck Lecture 2022' (2022) <https://www.judiciary.uk/speech-by-the-master-of-the-rolls-ciarb-roebuck-lecture/> consultato 2023.

(24) Civil Procedure Act 1997, s. 4(3).

(25) Civil Procedure Act 1997, s. 5. 'The Lord Chief Justice has nominated the Master of the Rolls to make practice directions for the civil courts under Constitutional Reform Act 2005', sch. 2 pt. 1.

(26) CPR 51.2.

dichiarazioni di causa e di altri documenti procedurali e la conservazione elettronica dei documenti che sono a disposizione delle parti, del tribunale e della magistratura.

Il 16 novembre 2015, è stata introdotta l'implementazione della presentazione elettronica delle istanze presso le Corti Reali di Giustizia (Royal Courts of Justice) al Rolls Building, a Londra, come Piano Pilota Lavoro Elettronico (Electronic Working Pilot Scheme) sotto le Indicazioni pratiche 510 (Practice Direction 510), usando il Sistema CE-File (archiviazione elettronica tribunali). Nonostante continui a essere etichettato come "pilota", e precedentemente definito come una soluzione provvisoria, il piano è stato ampliato ed esteso diverse volte e attualmente non vi è nessuna indicazione sulla sua interruzione.

A oggi, il sistema può essere utilizzato per le richieste di risarcimento della Parte 7, Parte 8, Parte 20 e per le domande di pre-azione presso le giurisdizioni del Rolls Building (il quale include la Divisione Cancelleria Corte Suprema (Chancery Division of the High Court), il Tribunale Commerciale (Commercial Court), il Tribunale per la Tecnologia e l'Edilizia (Technology and Construction Court), il Tribunale Circuito Commerciale (Circuit Commercial Court) e il Tribunale dell'Ammiragliato (Admiralty Court)), i Tribunali delle Imprese e Proprietà Registri Distrettuali (Business and Property Courts District Registries), l'Ufficio Centrale e Registri Distrettuali della Divisione Corte Reale (Central Office and District Registries of the King's Bench Division), nonché per i procedimenti di valutazione dettagliata e le richieste di risarcimento della Parte 8 presso l'Ufficio costi (Costs Office) e per le domande di autorizzazione per appelli e impugnazioni presso la Corte d'Appello (Court of Appeal) (Sezione Civile).

La presentazione elettronica delle istanze sta diventando sempre di più un obbligo se le parti sono rappresentate giuridicamente. Dal 30 aprile 2019 è diventato obbligatorio per tutti i Tribunali delle imprese e proprietà. Per la Divisione Corte Reale è diventato obbligatorio a luglio 2019, mentre per i Registri Distrettuali di Birmingham, Bristol, Cardiff, Leeds, Liverpool, Manchester e Newcastle a ottobre 2021. Per l'Ufficio Costi Tribunali Ultima Istanza (Senior Courts Cost Office) è diventato obbligatorio da ottobre 2019 e per la Corte d'Appello da febbraio 2022. È prevista l'introduzione della presentazione elettronica delle istanze per l'Ufficio Tribunale Amministrativo (Administrative Court Office), e da agosto 2023 è stato introdotto un nuovo sistema gestione casi come parte del Sistema CE-File, sebbene la presentazione elettronica delle istanze non sia ancora possibile.

1.7. Altri sistemi civili

Attualmente il HMCTS utilizza il sistema "account MyHMCTS", avviato all'inizio del 2020, come parte del programma di riforma del 2016.

Questo sistema non è stato ancora integrato in One Login. A questo punto non è chiaro se lo sarà, in quanto l'integrazione con One Login è interamente volontaria.

I singoli non possono accedere al sistema per conto proprio, a differenza delle organizzazioni che devono prima registrarsi per un account MyHMCTS, che richiede il numero di Pagamento tramite account ("PBA") dell'organizzazione, il numero di riferimento DX (se rilevante), e l'identificativo dell'Autorità Regolamentazione Avvocati (Solicitors Regulation Authority) ("SRA") dell'organizzazione o una registrazione professionale equivalente, e il nome e l'email della persona che sarà nominata "amministratore account" MyHMCTS. L'amministratore sarà quindi responsabile di creare gli account per i singoli utenti.

MyHMCTS è attualmente utilizzato per richieste di risarcimento per danni civili, risarcimenti monetari, procedimenti per divorzio, repliche del tribunale del lavoro, diritto di famiglia, rimedi finanziari, richieste di immigrazione e asilo, e successioni. La speranza è che la parte amministrativa di questi progressi possa essere svolta interamente online, integrata da udienze in remoto o di persona. Diversi di questi servizi si sono rivelati avere abbastanza successo, con l'80% di tutte le richieste di omologazione ricevute online e il 94% di valutazioni positive da parte degli utenti (27) e oltre 445000 richieste online per risarcimento monetario con il 95% di valutazioni positive (28).

Proprio come il Sistema CE-File, l'uso del sistema sta diventando sempre più un obbligo per i clienti professionali. Da giugno 2020, è diventato obbligatorio per le richieste di immigrazione e asilo (29). Dal 24 agosto 2020, il sistema è diventato obbligatorio per provvedimenti di consenso per rimedi finanziari (30). Dal 2 novembre 2020, è diventato obbligatorio per tutte le concessioni di richieste omologazioni (31). Infine dal 4 aprile 2022, quasi tutti i danni civili richiesti dalle parti professionalmente rappresentate devono essere emessi online utilizzando il portale per i risarcimenti danni su MyHMCTS e dal 15 settembre è diventato obbligatorio anche per le repliche (32).

Al di là di questo, il servizio legale nelle cause civili viene ancora svolto di default in presenza. Tuttavia, sotto l'Indicazione pratica 6A, le parti

(27) HM Courts & Tribunal Service, *Fact sheet: Probate online* (2023).

(28) HM Courts & Tribunal Service, *Fact sheet: Online Civil Money Claims* (2023).

(29) Michael Clements, *Presidental Practice Statement No 2 or 2020: Arrangements During the COVID-19 Pandemic* (2020).

(30) 36T PD.

(31) The Non-Contentious Probate (Amendment) Rules 2020 SI 2020 n. 1059.

(32) 51ZB PD.

possono indicare per iscritto la volontà ad accettare notifiche per via elettronica, come fax oppure email. La sola aggiunta di un numero di fax sarà considerata un'indicazione scritta sufficiente, ma per gli indirizzi email inclusi sarà necessario fornire una conferma esplicita. Nella causa *Barton v Wright Hassall LLP* (33), un querelante ha provato a notificare una richiesta di risarcimento agli avvocati del convenuto tramite email quando quest'ultimo non aveva dichiarato di essere disposto ad accettare la notifica tramite tale mezzo. Il tribunale si rifiutò di rimediare a questo errore, constatando che il ricorrente non aveva adottato misure ragionevoli per notificare il modulo di richiesta risarcimento in conformità con la norma. Questa causa ha anche evidenziato come le disposizioni specifiche relative alle notifiche via email siano state progettate per assicurare agli avvocati la possibilità di organizzarsi per controllare e gestire le email (a quel tempo una modalità di servizio innovativa).

Tuttavia, poiché l'emissione e la presentazione delle richieste di risarcimento sono diventate gradualmente obbligatorie per tutti i procedimenti civili, i tribunali si sono chiesti se queste norme continuassero ad avere uno scopo utile (34).

Se vengono forniti più indirizzi email, il documento è ritenuto notificato se inviato a uno qualsiasi dei due indirizzi email indicati. Tutti gli indirizzi email forniti sono specifici per un dato procedimento, piuttosto che avere un'email apposita legata a una persona particolare per tutta la corrispondenza giuridica, e non solo quella ufficiale.

In base alla Regola 6.15, i tribunali hanno poteri discrezionali per consentire la notifica tramite mezzi alternativi, qualora la notifica fisica oppure la notifica elettronica standard non sia fattibile. Si tratta di una misura estremamente ampia. Nella causa *Gray v Hurley* (35), il tribunale ha concesso un ordine di notifica al convenuto tramite un messaggio WhatsApp.

1.8. Sentenze e ordinanze

Durante la pandemia da Covid-19, i tribunali hanno emesso la maggior parte delle sentenze con riserva da remoto. Tale procedura ha funzionato così bene che in alcuni tribunali è stata mantenuta. A dicembre 2021, il Manutentore dei Documenti (Master of the Rolls) ha fornito indicazioni pratiche alla Sezione civile della Corte d'Appello che, salvo diversamente indicato, le sentenze con riserva saranno emesse a distanza con comunica-

(33) [2018] UKSC 12.
(34) [2018] UKSC 12, par. 29.
(35) [2019] EWHC 1636 (QB).

zione via email al BAILII (British and Irish Legal Information Institute — Ente Britannico e Irlandese di Informazione Giuridica) e agli Archivi Nazionali (The National Archives). Allo stesso modo, da ottobre 2022, le sentenze della Cancelleria (Chancery Division) sono inviate sia via email che agli Archivi Nazionali. Fino ad aprile 2022, venivano inviate anche al BAILII.

Diversamente, mentre le bozze delle sentenze sono spesso messe a disposizione degli avvocati per via elettronica prima della loro pubblicazione, la sentenza stessa viene ancora emessa in tribunale. Tuttavia, se non vi sono richieste da presentare in seguito alla sentenza, quest'ultima può essere emessa da un giudice in solitaria ([36]). Le notifiche delle sentenze possono avvenire elettronicamente, come indicato dalle regole menzionate precedentemente.

I creditori che cercano di far rispettare una sentenza per risarcimento danni hanno attualmente un compito potenzialmente arduo se il debitore non collabora con il processo. L'onere pesa totalmente sul creditore per aver dato inizio al processo, e non vi è un sistema formale per chiedere informazioni a terze parti, come dipartimenti governativi o banche. Esistono disposizioni legislative che lo agevolerebbero, ai sensi degli articoli 95-102 della Legge 2007 sui Tribunali, le Corti e l'Applicazione della Legge (Tribunals, Courts and Enforcement Act 2007), ma non è chiaro se queste disposizioni entreranno mai in vigore.

1.9. La Piattaforma Comune

A differenza del Sistema CE-File, generalmente ben accolto, l'avvio della Piattaforma Comune (Common Platform) utilizzata nei tribunali penali è stato penalizzato da difficoltà e ritardi. Inizialmente concepita nel 2013, la Piattaforma Comune è stata progettata per digitalizzare i processi giudiziari e sostituire i sistemi esistenti di gestione delle cause utilizzati dall'HMCTS e dalla Procura della Corona (Crown Prosecution Service) ("CPS").

Precedentemente a questo, i tribunali della Corona utilizzavano la piattaforma del Sistema Digitale Cause Tribunale Corona (Crown Court Digital Case System) ("CCDCS"), che permetteva agli utenti di vedere e stampare i documenti giudiziari, come gli atti di accusa, le dichiarazioni dei testimoni, le prove, le istanze e il materiale non utilizzato che era stato caricato. Allo stato attuale, il CCDCS è ancora in uso per i materiali processuale nei tribunali della Corona, mentre la Piattaforma Comune è al momento utilizzata per l'amministrazione dei casi.

([36]) PD 40E 5.1.

La registrazione per entrambi i servizi richiede un indirizzo email sicuro Criminal Justice Secure eMail (Email sicura per la giustizia penale) ("CJSM"). Il servizio email CJSM è disponibile per un'ampia gamma di organizzazioni e individui coinvolti nel sistema giuridico penale, tra cui la polizia, il Servizio sanitario nazionale (National Health Service) ("NHS") e le carceri. Tutte le domande devono essere sostenute dalla polizia, dal governo centrale oppure dal NHS (37).

La Piattaforma Comune doveva essere attiva entro marzo 2018. Questo si è rivelato più difficile del previsto, e nel 2021, si è deciso che costruire un singolo sistema fosse poco pratico, e che invece si sarebbe realizzato solamente un sistema giudiziario che potesse essere collegato con i sistemi esistenti del CPS. A gennaio 2023, l'interfaccia non ha ancora finito di essere testata (38). Attualmente, l'HMCTS prevede la consegna completa della piattaforma entro marzo 2025 (39).

L'avvio è stato ulteriormente prorogato dalla pandemia di Covid-19 e da una sospensione tra agosto 2021 e marzo 2022 per risolvere le principali problematiche relative a prestazione, stabilità e velocità. Anche dopo l'interruzione, i problemi non sono stati del tutto risolti e tra marzo e ottobre 2023, l'HMCTS ha registrato 231 incidenti critici che hanno interessato gli utenti (40). Membri della Società forense (Law Society) hanno notato diversi gravi problemi, tra cui cause sparite dal sistema, difficoltà ad accedere ai documenti della causa, indicazioni non visualizzate sul sistema, errori tecnici e ritardi dovuti a giudici, consulenti legali e personale non in grado di accedere al sistema (41). I tribunali sono stati costretti ad accontentarsi, tornando al vecchio sistema o addirittura ai documenti cartacei.

Il programma è stato nuovamente sospeso a settembre 2022 dopo che l'HMCTS ha rilevato che il sistema non aveva notificato le agenzie partner delle azioni necessarie in circa 3000 casi (1%). Ulteriori indagini hanno constatato che il mancato invio delle comunicazioni poteva aver influenzato gli esiti giudiziari in 357 cause. Per esempio, in 35 cause ai singoli non è stato fornito il braccialetto elettronico che avrebbero dovuto avere (42). Da ottobre

(37) Criminal Justice Secure eMail, 'About CJSM' (2023) <https://cjsm.justice.gov.uk/why/index.html> consultato 2023.

(38) National Audit Office, *Progress on the courts and tribunals reform programme 32.*

(39) House of Commons Committee of Public Accounts, *Progress on the courts and tribunals reform programme* (HC 1002, 2023) 4.

(40) National Audit Office, *Progress on the courts and tribunals reform programme 32.*

(41) House of Commons Committee of Public Accounts, *Progress on the courts and tribunals reform programme, CPR0003, The Law Society Submission, 30 March 2023, par. 47.*

(42) National Audit Office, *Progress on the courts and tribunals reform programme, 32-33.*

2022, vi sono stati molteplici casi di sciopero da parte di consulenti legali e collaboratori giudiziari in più di 60 corti di giustizia per protestare contro la Piattaforma Comune (43).

Nel 2022, l'Associazione degli Avvocati (Bar Council), l'organo di rappresentanza degli avvocati in Inghilterra e Galles, ha riportato che la Piattaforma Comune era "ampiamente percepita come un fallimento. Gli utenti dei tribunali hanno avuto difficoltà ad accedere al sistema, vi sono perplessità sul design della piattaforma, e i partecipanti non erano sicuri del fatto che il progetto fosse ancora in corso, perché ritenevano ci fosse poca informazione o adesione" (44).

Nonostante ciò, lo sviluppo ha continuato e da agosto 2023 è in uso in tutti i tribunali penali (45), sebbene molte delle funzioni basilari non saranno ultimate prima di marzo 2024, con il lancio completo l'anno successivo.

1.10. Conclusioni

In Inghilterra e Galles sono presenti diversi programmi per quanto riguarda le identità digitali e una riforma digitale, ma al momento è poco chiaro se, quando e anche come daranno i loro frutti. Non vi è un sistema centralizzato e unificato, nonostante ci siano aspirazioni per crearne uno, o perlomeno creare un sistema progettato per essere interoperabile. Tuttavia, i problemi prolungati correlati al lancio della Piattaforma Comune, che aveva l'obiettivo di creare un sistema unico unificato per le attività procedurali, e al GOV.UK Verify, il quale aspirava a creare un quadro comune per collegare i sistemi esistenti ma disconnessi, sono di avvertimento. È rilevante che il piano d'azione per l'adozione di One Login sia notevolmente limitato. Sembra certo che la digitalizzazione dei servizi giudiziari sia il futuro, e vi sono alcuni singoli sistemi che sembrano funzionare bene. Il Sistema CE-File è stato accettato in modo positivo come sistema digitale di archiviazione, ma saranno necessari altri sistemi per una più ampia gestione delle cause online. I tribunali si sono impegnati per favorire una giustizia digitale dove possibile, e questo è stato notevolmente propiziato dalla flessibilità delle indicazioni pratiche, come quelle sulle udienze e l'emissione di sentenze da remoto, ma sono risultate essere in qualche modo delle soluzioni ad hoc. Un ostacolo

(43) House of Commons Committee of Public Accounts, *Progress on the courts and tribunals reform programme, CPR0003, The Law Society Submission, 30 March 2023, par. 51.*

(44) The Bar Council, *Access Denied: The state of the justice system in England and Wales in 2022* (2022) 10.

(45) HM Courts & Tribunal Service, *Every criminal court now connected to single data system for the first time* (2023).

significativo sarà provare a coordinare e unificare questi sistemi, ma proposte concrete in tal senso non hanno ancora preso forma. Finora, i tribunali civili sono riusciti a evitare i problemi della Piattaforma Comune, ma l'integrazione potrebbe rivelarsi lo stesso problematica.

Vi è una tensione di fondo tra l'opinione pubblica e le politiche di governo. Da una parte, vi è il desiderio di evitare qualsiasi tipo di sistema nazionale unico sulle identità digitali o qualsiasi sorta di sistema centralizzato di archiviazione dati alla "grande fratello", ma dall'altra parte vi è un desiderio di coordinazione e condivisione dati, in modo che le persone non debbano accedere e gestire più servizi completamente disconnessi tra loro. Sfortunatamente, le proposte per risolvere questa dicotomia sono poche. Fino ad allora, i sistemi informali e frammentari saranno dominanti.

II.

I PRINCIPI GUIDA DEL PROCESSO DI DIGITALIZZAZIONE DELLA PRATICA PROCESSUALE (*)

di *Samir Merabet*

Sommario: 2.1. La tecnologia digitale è la risposta alla crisi del sistema giudiziario? — 2.2. Giustizia 1.5. — 2.3. Manifestazioni della digitalizzazione in Francia. — 2.3.1. Strumenti per la digitalizzazione delle procedure. — 2.3.2. I rischi della digitalizzazione delle procedure — 2.4. Protezione dai pericoli della digitalizzazione delle procedure in Francia. — 2.4.1. I rischi del principio di neutralità tecnologica. — 2.4.1.1. *De lege lata*, efficacia del diritto a un processo equo. — 2.4.1.2. *De lege ferenda*, la consacrazione del principio guida del processo digitale.

2.1. La tecnologia digitale è la risposta alla crisi del sistema giudiziario?

Intelligenza artificiale, open data (1), videoconferenze, sistemi di supporto alle decisioni, blockchain... le innovazioni tecniche in grado di rinnovare la pratica processuale sono numerose e possono suscitare entusiasmo, anche se l'istituzione giudiziaria sta vivendo delle difficoltà, se non addirittura una "crisi" (2). A suo tempo, l'informatica ha facilitato notevolmente l'organizzazione dei procedimenti sia civili che penali. Il Professor Catala aveva teorizzato fin dall'inizio tutti i vantaggi che il diritto in generale e la pratica processuale in particolare avrebbero potuto trarre dall'informatica (3). I nuovi strumenti digitali dovrebbero essere a loro volta fonte di progresso. I vantaggi potenziali sono numerosi. La tecnologia digitale potrebbe consentire di automatizzare alcuni compiti, risparmiando così tempo,

---

(*) Libera traduzione, non revisionata dall'Autore.

(1) L. Cadiet (a cura di), *L'open data des décisions de justice*, 29 nov. 2017, disponibile su *www.justice.gouv.fr.*

(2) L. Cadiet e E. Jeuland, *Droit judiciaire privé*, LexisNexis, 10e ed., 2017, n. 32: "In realtà, la crisi del sistema giudiziario non è solo materiale: il sistema giudiziario è insufficientemente attrezzato, il suo bilancio è inadeguato e le sue risorse non sono aumentate in proporzione alle richieste delle parti in causa. La crisi del sistema giudiziario è anche morale, o politica, o ideologica, che dir si voglia".

(3) P. Catala, *Le droit à l'épreuve du numérique, Juris ex Machina*, PUF, 1998.

o di facilitare l'accesso ai tribunali per le parti in causa. Questa digitalizzazione delle procedure è attualmente in corso in Francia.

2.2. Giustizia 1.5

L'istituzione giudiziaria non ha motivo di essere immune dalla crescente digitalizzazione della società. Alcuni strumenti digitali sono ormai relativamente vecchi e si potrebbe quindi pensare che siano pienamente integrati nell'organizzazione dei tribunali francesi in generale, e nelle questioni procedurali in particolare. Eppure, la rivoluzione digitale nella giustizia francese è ancora lontana. La crisi sanitaria e il primo lockdown del 17 marzo 2020 hanno rivelato tutta la portata dei limiti dell'infrastruttura digitale del sistema giudiziario (4). Da un punto di vista molto pragmatico, la maggior parte dei magistrati e dei cancellieri non erano dotati di computer portatili professionali. La Corte dei conti ha espresso forti critiche sulla continuità che il servizio giudiziario pubblico è stata in grado di offrire in questo periodo (5). Questo dimostra quanta strada ci sia ancora da fare per completare il processo di digitalizzazione. Tuttavia, le autorità pubbliche hanno recentemente compreso l'importanza della posta in gioco. Nel 2017, il Ministero della Giustizia francese ha adottato un piano di trasformazione digitale (PTD) per il periodo 2018-2022. Lo stanziamento di un budget di 530 milioni di euro era destinato a modernizzare l'istituzione giudiziaria e, in particolare, a consentire una migliore dematerializzazione delle procedure. Sebbene l'approccio sembrasse ambizioso, i risultati attesi non sembrano essere stati raggiunti. La Corte dei conti ha rilevato che questi investimenti sono serviti in realtà solo a recuperare l'arretrato accumulato negli anni precedenti. In questa fase, quindi, la Francia non è un modello da seguire per quanto riguarda la digitalizzazione del sistema giudiziario. Tuttavia, il numero di procedure digitalizzate sta gradualmente aumentando.

2.3. Manifestazioni della digitalizzazione delle procedure in Francia

2.3.1. *Strumenti per la digitalizzazione delle procedure*

a) Digitalizzazione delle procedure nel diritto francese. Il diritto francese si sta gradualmente digitalizzando. Ad esempio, l'articolo 800-1 del

(4) A. Coignac, *Les tribunaux judiciaires à l'épreuve de la crise sanitaire* (Tribunali messi alla prova dalla crisi sanitaria), JCP G 2020, n. 20-21, 624.

(5) Corte dei conti, *Le plan de continuité d'activité des juridictions judiciaires pendant la crise sanitaire liée à l'épidémie de covid 19, mai 2021* (Il piano di continuità operativa per i tribunali giudiziari durante la crisi sanitaria legata all'epidemia di Covid 19, maggio 2021), disponibile su *www.coursdescomptes.fr.*

Codice di procedura penale francese prevede che tutti gli atti processuali, "siano essi atti di indagine, atti istruttori, decisioni giudiziarie o qualsiasi altro atto processuale, possano essere redatti o convertiti in formato digitale". Alla luce di ciò, il recente decreto del 23 giugno 2020 autorizza, ai sensi dell'articolo R. 249-9 del Codice di procedura penale francese, la creazione di un "fascicolo penale digitale", al fine di "facilitare e migliorare il trattamento dei fascicoli penali da parte dei magistrati, dei cancellieri e delle persone autorizzate ad assistere le parti in causa" (6). Anche la procedura civile è in fase di digitalizzazione.

b) Rinvio a giudizio. Il diritto francese ha optato per la digitalizzazione di alcuni atti di rinvio a giudizio. In alcuni casi, le norme procedurali consentono sia la notifica digitale degli atti che quella tradizionale, per posta o depositati presso la cancelleria del tribunale. È il caso, ad esempio, della procedura semplificata di recupero crediti. Quando il debito non supera i 5.000 euro, il creditore può avviare la sua azione interamente online, attraverso la "piattaforma per le controversie di modesta entità". Una volta completata la procedura e se il debitore si rifiuta di adempiere, il creditore può portare il caso in tribunale per ottenere un mandato di esecuzione. In altri casi, la tecnologia digitale è diventata l'unico modo per portare un caso in tribunale, pena l'inammissibilità. È il caso, in particolare, dei procedimenti di appello, che devono essere tutti svolti per via telematica, pena l'inammissibilità dell'appello, il che comporta non poche difficoltà quando gli strumenti messi a disposizione a questo scopo presentano limiti tecnici dovuti al modo in cui sono stati concepiti.

c) Comunicazione di documenti e atti. Uno dei principali vantaggi della tecnologia digitale è la dematerializzazione degli scambi, che consente un notevole risparmio di tempo e risorse. La comunicazione elettronica in ambito giuridico offre quindi prospettive di notevole interesse. Ciò è tanto più importante quando una delle parti ha sede all'estero o addirittura oltreoceano. Il quadro di riferimento per tale innovazione deve tuttavia essere attentamente valutato nella misura in cui tale comunicazione ha importanti conseguenze sull'esecutività degli atti e sul principio del contraddittorio. A questo proposito, un decreto del 3 maggio 2019 contribuisce alla digitalizzazione della procedura in questione (7).

d) Firma degli atti. La dematerializzazione delle procedure rende arcaiche alcune pratiche. È il caso, ad esempio, della stampa di una decisione

(6) A. Chavent-Leclère, *Le dossier pénal numérique*, Procédures, 2020, n. 10, nota 15.

(7) Decreto n. 2019-402 del 3 maggio 2019 su diverse misure relative alla comunicazione elettronica in materia civile e alla notificazione di atti all'estero, C. Bléry, T. Douville e J.-P. Teboul, *Nouveau décret de procédure civile: présentation générale* (Nuovo decreto di procedura civile: presentazione generale), Dalloz actualité, 24 maggio 2019.

giudiziaria, che deve essere firmata da un magistrato prima di essere nuovamente digitalizzata. Per evitare queste noiose operazioni, da qualche anno il diritto francese ha autorizzato la firma elettronica degli atti giudiziari. Un primo testo aveva avviato questa pratica in ambito commerciale, per le sentenze dei tribunali di commercio (8). Il processo è stato successivamente esteso alle sentenze civili con un decreto del 20 novembre 2020 (9). Il testo prevede procedure tecniche specifiche per garantire l'integrità di queste firme. Così, "la firma elettronica contiene l'identificazione del firmatario, un token temporale che garantisce l'integrità del documento e la data della firma, e un certificato di firma elettronica qualificata e valida rilasciato dal Ministero della Giustizia".

e) Un bilancio contrastante. Questa breve presentazione mostra che la digitalizzazione delle procedure viene attuata gradualmente, per fasi. I casi presi in considerazione sembrano indicare innovazioni adottate una tantum da parte del Ministero della Giustizia, in assenza di un vero e proprio approccio di ampio respiro volto a ripensare la procedura nel suo complesso per adattarla alle sfide della tecnologia digitale. Inoltre, allo stesso tempo, sono state individuate una serie di carenze significative. Alcuni esempi dimostrano quanto la tecnologia non sia sempre all'altezza delle ambizioni dell'amministrazione giudiziaria e, più in generale, dei professionisti del diritto. Negli ultimi anni, la piattaforma e-barreau ha accelerato la digitalizzazione delle procedure. Tuttavia, ci sono ancora pratiche che presto sembreranno obsolete. Ad esempio, anche se alcune procedure sono completamente dematerializzate, alcuni tribunali continuano a richiedere l'invio di memorie in formato cartaceo, con l'onere per le parti di fornire buste affrancate da restituire al termine della procedura. Gli strumenti attuali presentano anche altri limiti. Ad esempio, la piattaforma e-barreau consente lo scambio di documenti tramite RPVA (Rete Privata Virtuale dell'Avvocato), ma con un limite massimo di 10 MB, rendendo necessario l'utilizzo di altri mezzi, come la posta elettronica. Anche la procedura di ricorso è compromessa dalle limitazioni degli strumenti digitali. Ad esempio, lo spazio a disposizione per inserire la dichiarazione di appello online è di soli 4080 caratteri. Se a volte questo limite può essere più che sufficiente, in altri casi crea delle difficoltà. Date le gravi conseguenze del mancato deposito di una

(8) Ordinanza del 9 aprile 2019 relativa alla firma elettronica delle decisioni prese dai tribunali commerciali; Y. Broussole, *Les principales dispositions de l'arrêté du 9 avril 2019 relatif à la signature électronique des décisions rendues par les tribunaux de commerce* (Le principali disposizioni dell'ordinanza del 9 aprile 2019 sulla firma elettronica delle decisioni emesse dai tribunali commerciali), LPA 20 sett. 2019, n. 147, p. 12.

(9) Ordinanza del 20 novembre 2020 sulla firma elettronica delle decisioni giudiziarie in materia civile.

dichiarazione di appello, gli avvocati sono costretti a cercare metodi alternativi, come la redazione della dichiarazione di appello su carta e la successiva allegazione del documento alla dichiarazione online, con le incertezze procedurali che accompagnano tale manovra. Lungi dal facilitare la procedura, i limiti degli strumenti digitali utilizzati possono renderla più difficile. In questo caso, la forma vincola la sostanza.

2.3.2. *I rischi della digitalizzazione delle procedure*

Si potrebbe criticare la lentezza con cui la tecnologia digitale si sta diffondendo nei tribunali francesi. D'altro canto, questa osservazione potrebbe essere interpretata più positivamente come una dimostrazione di una certa saggezza, per non precipitare sviluppi i cui pericoli sono attualmente difficili da percepire. È più probabile che il ritardo sia dovuto più che altro a una mancanza di risorse e di lungimiranza, ma forse questa situazione è preferibile, in modo da prepararsi ai rischi posti dalla digitalizzazione delle procedure.

a) Dai vantaggi agli svantaggi. Se riusciamo a vedere i vantaggi di questi sistemi, possiamo anche intuirne i possibili svantaggi. Tanto per cominciare, c'è il fenomeno dell'*illectronisme*, neologismo francese che sta ad indicare il cosiddetto analfabetismo digitale. Questo termine si riferisce alle persone che hanno difficoltà o impossibilità a utilizzare gli strumenti digitali, situazione che riguarda quasi il 15% della popolazione francese. Per queste persone, l'eventuale obbligo di utilizzare strumenti digitali per avviare un procedimento giudiziario può comportare l'impossibilità di accedere alla giustizia. È auspicabile che, a lungo termine, il rinnovamento generazionale porti a una riduzione di questo fenomeno. Anche se ciò dovesse accadere, non vorrebbe dire tutte le difficoltà sarebbero risolte. Le preoccupazioni sono legittime e sono state espresse dalla CEPEJ.

b) Formalismo digitale e accesso alla giustizia. Per quanto sofisticati siano i dispositivi digitali che utilizziamo, non siamo mai al sicuro da errori o bug. Tutti noi lo sperimentiamo regolarmente con i dispositivi che utilizziamo nella vita quotidiana. Ovviamente, lo stesso vale per i dispositivi digitali utilizzati a fini processuali. Tuttavia, in questo caso le conseguenze sono più gravi. Un eventuale errore o malfunzionamento potrebbe mettere in discussione l'azione stessa di una parte in causa. In definitiva, l'accesso alla giustizia potrebbe essere compromesso. Lungi dall'agevolare le azioni procedurali delle parti in causa, la tecnologia digitale potrebbe costituire una nuova trappola in grado di vanificarne le richieste, unicamente a causa di difetti procedurali. Queste situazioni non sono casi da manuale. Dalla giurisprudenza francese si possono trarre diversi esempi. Il più significativo riguarda senza dubbio la procedura di appello.

c) Il caso della dichiarazione di appello. Ogni volta che una procedura è dematerializzata, c'è il rischio che un'azione fallisca a causa di un problema informatico. A questo proposito, le difficoltà incontrate nel diritto francese per quanto riguarda la dichiarazione di appello sono particolarmente rivelatrici. In materia civile, il diritto francese prevede che le dichiarazioni di appello siano presentate alla Corte di Appello per via telematica, pena l'inammissibilità, rilevabile anche d'ufficio, ai sensi dell'articolo 930-1 del Codice di procedura civile francese. La procedura dematerializzata è quindi essenziale per l'ammissibilità dell'appello. Questa digitalizzazione ha comportato delle difficoltà, dovute sia alle norme procedurali che ai vincoli tecnici. In primo luogo, il diritto francese subordina l'effetto devolutivo dell'impugnazione al rispetto di alcuni requisiti formali: la dichiarazione di appello deve specificare i capi della sentenza impugnata e la Corte di Appello è competente solo per questi capi. In secondo luogo, la piattaforma utilizzata per depositare la dichiarazione di appello presenta dei limiti tecnici. La dichiarazione di appello deve essere presentata attraverso la Rete Virtuale Privata della Giustizia (RPVJ), una piattaforma per il compimento di atti processuali. Lo spazio a disposizione per inserire la dichiarazione di appello su questa piattaforma è di soli 4.080 caratteri. A volte questo spazio è sufficiente, ma non lo è in tutti i casi. Gli avvocati hanno quindi preso l'abitudine di allegare alla dichiarazione d'appello un documento che riporta in dettaglio i capi della sentenza impugnati. Secondo la prassi, alcuni avvocati utilizzavano questo metodo di allegazione anche quando il limite di caratteri non era stato raggiunto. I vincoli tecnici legati allo strumento digitale utilizzato hanno portato alla nascita di nuove pratiche che, formalmente, consentivano ancora alla Corte di Appello di essere debitamente informata. Tuttavia, è sorto un dibattito sulla natura dell'allegato a questa dichiarazione d'appello, che non rispettava il formalismo elettronico previsto dai testi. La Corte di Cassazione ha adottato un approccio molto formale, ritenendo che, a meno che non ci fosse un problema tecnico, i capi di sentenza contenuti nell'appendice non fossero sottoposti alla Corte di Appello (10). Pertanto, solo se la dichiarazione di appello supera il numero di caratteri autorizzato è possibile introdurre validamente un'appendice, a condizione che vi si faccia esplicito riferimento. Le conseguenze di questa decisione sono state tanto più dannose in quanto la soluzione è stata immediatamente applicabile, anche ai procedimenti in corso, rischiando così di privare le parti in causa dei loro

(10) Cass. Civ. 2e, 13 genn. 2022, n. 20-17.516, Dalloz actualité, 20 genn. 2022, oss. R. Laffly; D. 2022. 325, nota M. Barba; ibid. 625, oss. N. Fricero; AJ fam. 2022. 63, oss. F. Eudier e D. d'Ambra; *Rev. prat. rec.* 2022. 9, cron. D. Cholet, O. Cousin, M. Draillard, E. Jullien, F. Kieffer, O. Salati e C. Simon.

mezzi di impugnazione, a meno che non regolarizzassero la dichiarazione di appello irregolare. Tutto ciò dimostra quanto la digitalizzazione della pratica processuale, lungi dall'agevolarla, possa portare a un eccessivo formalismo. In questo caso, il problema era principalmente legato a un servizio arbitrariamente limitato a 4.080 caratteri. Pertanto, il modo in cui lo strumento digitale è stato concepito, indipendentemente dalle norme procedurali applicabili, rischia di privare le parti in causa del diritto di ricorso. È stata prevista una riforma per porre fine a questo formalismo. Un decreto del 25 febbraio 2022 (11) ha modificato l'articolo 901 del Codice di procedura civile francese, accompagnato da un decreto della stessa data che modifica il decreto del 20 maggio 2022 (12), con l'obiettivo di rendere validi i ricorsi presentati tramite un'appendice allegata alla dichiarazione di appello. La soluzione non era probabilmente sufficientemente chiara, in quanto le Corti d'appello continuavano a ritenere che un'appendice fosse ammissibile solo in presenza di un impedimento tecnico (13). Pertanto, se i capi di sentenza impugnati erano di lunghezza inferiore a 4.080 caratteri, dovevano comparire direttamente sul modulo elettronico della piattaforma, pena l'inammissibilità. Per porre fine all'incertezza, la Corte di Cassazione ha emesso un parere che consente di ammettere i ricorsi presentati in questo modo (14). È sorprendente che una situazione del genere abbia dato luogo a diverse sentenze della Corte di Cassazione e a una riforma dei testi applicabili. Soprattutto, c'è da temere che lo stesso approccio porti troppo spesso a digitalizzare la procedura rendendola più complessa, mentre l'obiettivo iniziale era proprio quello di semplificarla.

2.4. Protezione dai pericoli della digitalizzazione delle procedure in Francia

2.4.1. *I rischi del principio di neutralità tecnologica*

Numerose branche del diritto si confrontano oggi con la tecnologia digitale, provocando talvolta profondi sconvolgimenti giuridici. Non c'è dubbio che l'evoluzione del diritto non sia più in grado di tenere il passo con

(11) Decreto n. 2022-245 del 25 febbraio 2022 che promuove il ricorso alla mediazione, attua la legge sulla fiducia nel sistema giudiziario e modifica diverse disposizioni.

(12) Ordinanza del 20 maggio 2020 sulla comunicazione elettronica in materia civile dinanzi alle corti d'appello.

(13) Corte di Appello di Rennes, 14 marzo 2022.

(14) Cass. Civ. 2e, parere, 8 lug. 2022, n. 22-70.005, Dalloz actualité, 30 agosto 2022, oss. R. Laffly; D. 2022. 1498, nota M. Barba; Gaz. Pal. 13 sett. 2022, p. 17, nota M. Bencimon; ibid. 25 ott. 2022, nota C. Bléry; JCP 2022. 1345, oss. L. Veyre.

le innovazioni digitali. Di conseguenza, le nuove tecniche vengono spesso applicate in assenza di norme specificamente concepite per la loro applicazione. In questi casi, ovviamente, non c'è un vuoto giuridico, in quanto si applica un gran numero di norme preesistenti. A volte, l'assenza di norme specifiche non è dovuta a un ritardo del legislatore, ma a una vera e propria scelta di politica legislativa. La creazione di nuove norme rende la legge più complessa e talvolta è preferibile affidarsi esclusivamente a un principio di neutralità tecnologica, in base al quale la legge si applica indipendentemente dalla natura delle tecniche utilizzate. Applicato alle norme procedurali, ciò porta, ad esempio, a considerare equivalenti i documenti cartacei o elettronici e a duplicare semplicemente le norme procedurali preesistenti in forma digitale. Questo metodo ha il pregio della semplicità e talvolta è giustificato. D'altro canto, vi sono altre situazioni in cui l'assenza di norme specifiche non affronta i rischi che emergono dal diritto positivo e che richiederebbero la definizione di un principio appropriato. La digitalizzazione della pratica processuale non fa eccezione. Se a volte le norme di diritto sostanziale consentono di prevenire i rischi derivanti dalla digitalizzazione delle procedure (A), altre situazioni richiedono la definizione di nuovi principi (B).

2.4.1.1. De lege lata*, efficacia del diritto a un processo equo*

a) Il diritto di accesso alla giustizia. La digitalizzazione della pratica processuale può servire a migliorare l'accesso alla giustizia. La dematerializzazione può offrire un certo numero di strumenti in grado di avvicinare le parti in causa all'amministrazione giudiziaria, soprattutto quando le parti sono geograficamente lontane dai tribunali. D'altro canto, la tecnologia digitale può produrre l'effetto opposto. La complessità di una procedura digitalizzata e i possibili bug possono impedire il successo di un'azione legale, a causa del formalismo informatico. In alcuni casi, questi vincoli digitali possono privare le parti in causa del loro diritto al ricorso. In tali circostanze, il diritto di accesso alla giustizia, uno degli elementi alla base del diritto a un processo equo, potrebbe contribuire a proteggere le parti dalle conseguenze dannose della digitalizzazione delle procedure. È proprio questo il punto di vista che la Corte europea dei diritti dell'uomo sembra adottare nella sentenza Xavier Lucas/Francia del 9 giugno 2022 (15). Il caso riguardava un ricorso per l'annullamento di un lodo arbitrale. In linea di principio, il

(15) CEDU, 9 giugno 2022, Xavier Lucas c/France, n. 15567/20, D. 2022. 2330, oss. Clay; ibid. 2023. 571, oss. Fricero; AJ fam. 2022. 353, oss. Eudier; Dalloz IP/IT 2022. 352, oss. Nalbant; JCP 2022. 785, oss. Milano; ibid. 1345, oss. Mayer; Gaz. Pal. 25 ott. 2022, p. 56, nota Plissonnier.

ricorso dovrebbe essere presentato per via telematica ai sensi degli articoli 1495 e 930-1 comma 1 del Codice di procedura civile francese. Tuttavia, la piattaforma e-barreau prevista a tale scopo non consentiva di scegliere l'opzione di presentare un "ricorso per l'annullamento di un lodo arbitrale". Il ricorrente non ha quindi rispettato la procedura informatica e ha presentato il suo ricorso in modo tradizionale, sostenendo che vi era una "causa estranea" che lo esentava dalle formalità elettroniche. Il problema era indubbiamente dovuto a un errore umano: nella configurazione della piattaforma non era stata presa in considerazione la possibilità di presentare un ricorso per l'annullamento di un lodo arbitrale, per cui al ricorrente non era stata proposta alcuna voce corrispondente. Tuttavia, la Corte di Cassazione ha respinto l'ammissibilità del ricorso, dimostrando un approccio particolarmente rigoroso (16) che è stato criticato dai giudici della Corte di Strasburgo. La Corte europea si è pronunciata contro il ragionamento dei giudici francesi, ritenendo che "facendo prevalere il principio dell'obbligo di comunicazione per via telematica per adire la Corte di Appello, senza tener conto degli ostacoli pratici incontrati dal ricorrente nell'adempiere a tale obbligo, la Corte di Cassazione ha dato prova di un formalismo che la garanzia della certezza del diritto e della corretta amministrazione della giustizia non richiedeva e che deve pertanto essere considerato eccessivo" (17). Questo ragionamento non mette in discussione la legittimità della formalità elettronica, ma ne stigmatizza solo gli eccessi, soprattutto quando le circostanze del caso dimostrano che un ricorrente diligente non potrebbe ragionevolmente soddisfare tali requisiti. È auspicabile che lo stesso ragionamento si applichi ogniqualvolta la digitalizzazione di una procedura comporti restrizioni ai diritti delle parti in causa.

b) I diritti della difesa. La digitalizzazione delle procedure può essere accompagnata dalla dematerializzazione della pratica processuale. Questa dematerializzazione è completa per alcuni procedimenti, come le ingiunzioni di pagamento per le controversie di modesta entità, e solo parziale per altri procedimenti, ad esempio quando una delle parti non è fisicamente presente all'udienza ma solo tramite videoconferenza. In entrambi i casi, non è in gioco tanto la digitalizzazione del procedimento quanto l'udienza stessa. Ciò comporta inevitabilmente delle difficoltà in termini di contraddittorio. L'assenza delle parti all'udienza potrebbe influire sullo svolgimento del proce-

(16) Cass. 26 sett. 2019, n. 18-14.708 P: D. att. 2 ott. 2019, nota Bléry; ibid. 29 ott. 2019, oss. Jourdan-Marques; D. 2019. 1891; ibid. 2435, oss. Clay; JCP 2019. 1185, nota Weiller; ibid. 1349, nota Ortscheidt: JCP E 2019. 1554, nota Casson; Gaz. Pal. 19 nov. 2019, p. 25, nota Bensaude.

(17) CEDU, 9 giugno 2022, Xavier Lucas c/France, prec. §57.

dimento. Tuttavia, tale approccio è stato previsto in Francia durante la crisi del Covid. La crisi sanitaria ha suscitato notevoli criticità per lo svolgimento delle udienze. In particolare, le parti contagiate dal virus o suscettibili di esserlo non potevano partecipare, con il rischio che i casi venissero sistematicamente archiviati. Per ovviare a questo problema, l'articolo 2 dell'ordinanza del 18 novembre 2020 intendeva imporre alle parti l'uso della videoconferenza in tutti i procedimenti davanti ai tribunali penali. Se l'idea di garantire la continuità del servizio pubblico di giustizia durante questo periodo era lodevole, il metodo utilizzato era discutibile e ha provocato forti reazioni da parte di accademici, magistrati e avvocati. Una disposizione simile adottata durante il primo periodo della pandemia era già stata censurata dal Consiglio costituzionale francese in una decisione del 4 giugno 2021. Il Consiglio aveva stabilito che l'obbligo di utilizzare la videoconferenza senza il consenso delle parti dinanzi ai tribunali penali violava i diritti fondamentali. In particolare, nella sua decisione il Consiglio costituzionale aveva fatto riferimento all'articolo 16 della Dichiarazione dei diritti dell'uomo e del cittadino del 1789, che recita: "*Ogni società in cui la garanzia dei diritti non è assicurata, né la separazione dei poteri stabilita, non ha una costituzione*" e da cui derivano i diritti di difesa. Applicando questo principio al testo in questione, il Consiglio ha dedotto che "da tutto quanto precede risulta che, tenuto conto dell'importanza della garanzia che può essere annessa alla presentazione fisica dell'interessato davanti al giudice penale e delle condizioni di utilizzo di questo mezzo di telecomunicazione, queste disposizioni violano i diritti della difesa in un modo che non potrebbe essere giustificato dal particolare contesto sanitario derivante dall'epidemia di Covid-19 durante il periodo della loro applicazione. Senza bisogno di esaminare gli altri reclami, devono quindi essere dichiarate contrarie alla Costituzione" (18). Il Consiglio di Stato si è pronunciato nello stesso modo, utilizzando una base diversa, quella del diritto a un processo equo ai sensi dell'articolo 6§1 della Convenzione europea dei diritti dell'uomo. Ha quindi stabilito che le disposizioni dell'articolo 2 dell'ordinanza del 18 novembre 2020 consentono al giudice di richiedere l'uso di mezzi audiovisivi di telecomunicazione dinanzi a tutti i tribunali penali. Non subordinano l'esercizio di questa facoltà ad alcuna condizione o criterio giuridico. Considerata l'importanza della garanzia legata alla comparizione fisica dell'imputato davanti al giudice penale, queste disposizioni violano il diritto a un processo equo garantito dall'articolo 6 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, e non possono essere

(18) Consiglio costituzionale francese, 4 giugno 2021, DC n. 2021-911/919 QPC, § 10.

giustificate dal contesto della lotta contro l'epidemia di Covid-19 (19). Queste due decisioni sono istruttive in quanto non escludono l'uso di dispositivi di videoconferenza in modo generale e assoluto. In primo luogo, è chiaro che si tratta delle garanzie associate ai procedimenti penali, per cui nulla sembra vietare misure equivalenti per i procedimenti civili. È comprensibile che la natura unica del procedimento penale, e in particolare l'importanza del principio della personalizzazione della pena, spieghi perché l'assenza della presenza fisica delle parti all'udienza possa avere un'influenza decisiva sull'esito della controversia. Gli stessi problemi non si applicano ai procedimenti civili. D'altra parte, alcune controversie sono anche di natura personale, il che potrebbe giustificare lo stesso principio di divieto, in particolare per i procedimenti relativi al diritto di famiglia o allo status personale. In secondo luogo, i divieti qui menzionati sono in parte giustificati dall'assenza di un quadro di riferimento per il potere del giudice di imporre alle parti l'uso della videoconferenza, suggerendo così che un potere non discrezionale e strettamente controllato potrebbe essere compatibile con i diritti della difesa. Non è troppo difficile pensare che la videoconferenza non presenti sistematicamente grandi pericoli. D'altra parte, se del caso, potrebbe non essere sufficiente il semplice utilizzo della videoconferenza, senza alcun altro adattamento delle norme procedurali.

2.4.1.2. De lege ferenda*, la consacrazione del principio guida del processo digitale*

a) Principi guida del processo 2.0. Il Codice di procedura civile francese si apre con un capitolo dedicato ai "principi guida del contenzioso". In ventiquattro articoli, il Codice elenca le regole fondamentali che guidano l'intero processo civile e le norme procedurali che vi si applicano. Si tratta di principi quali la natura pubblica del procedimento (art. 22 CPC), la riparazione dell'onere della prova (art. 9) e il principio del contraddittorio (art. 14). Questi principi fungono da bussola per l'applicazione di tutte le norme procedurali. L'individuazione dei rischi specifici delle procedure digitali potrebbe giustificare l'introduzione di nuovi principi volti a fornire un quadro di riferimento per la digitalizzazione del contenzioso (20).

b) Principio di sussidiarietà. La digitalizzazione delle procedure legali presenta diverse virtù. In particolare, può essere utilizzata per migliorare

(19) CE, 4 agosto 2021, n. 447916.

(20) S. Merabet, *Hommage posthume à l'abandon de DataJust: des principes directeurs de la justice numérique* (Omaggio postumo all'abbandono di DataJust: principi guida per la giustizia digitale), in *Revue Pratique de la prospective et de l'innovation*, 2022-1, 4.

l'accessibilità e la velocità. In questo senso, dovrebbe essere accolta con entusiasmo. Tuttavia, questa osservazione non è assoluta e non può essere applicata uniformemente a tutte le controversie. Ci sono aree in cui l'uso dei processi digitali potrebbe, al contrario, risultare dannoso per la qualità della giustizia. Gli esempi sopra riportati dimostrano che esiste un rischio significativo che il processo di digitalizzazione vada a scapito delle parti in causa. Non c'è dubbio che non tutte le controversie si prestano allo stesso modo alla digitalizzazione, che quindi dovrebbe essere presa in considerazione solo quando serve a migliorare la giustizia. La diffusione degli strumenti digitali dovrebbe quindi essere regolata dal principio di sussidiarietà. Questo principio di sussidiarietà permetterebbe di evitare diverse insidie. In primo luogo, richiederebbe una politica globale e concertata sulle future applicazioni di questi sistemi, evitando di sprecare risorse nello sviluppo di progetti che non verranno portati a termine o che saranno inefficaci. In secondo luogo, eviterebbe la potenziale corsa a capofitto che il progresso tecnico spesso produce. Ad esempio, una volta che uno strumento è stato utilizzato, soprattutto quando fa risparmiare una notevole quantità di tempo, c'è un rischio considerevole che le persone non rinuncino a usarlo, anche se sono stati riscontrati malfunzionamenti. In definitiva, il principio di sussidiarietà consentirebbe una riflessione più generale sulla giustizia digitale e sulla concertazione preventiva, coinvolgendo le diverse parti coinvolte in questo o quel tipo di controversia, per valutare collettivamente gli usi più virtuosi di questi strumenti.

c) Principio di accessibilità. Il diritto in generale, e la pratica processuale in particolare, sono complessi e tecnici. Questa tecnicità è insita nella disciplina. È proprio per mitigare questa complessità che sono stati concepiti gli ufficiali giudiziari e che la rappresentanza da parte di un avvocato è resa obbligatoria in molti procedimenti. Si tratta quindi di una difficoltà ineludibile che fa parte del campo giuridico stesso. D'altra parte, la natura tecnica del diritto non deve essere aggravata dalla natura tecnica dell'informatica, dovuta alla digitalizzazione delle norme procedurali. Per questo motivo è importante garantire che, ogni volta che le norme procedurali fanno uso di strumenti digitali, un principio di accessibilità ne regoli la progettazione e l'attuazione. Questo principio di accessibilità può essere garantito con diversi mezzi, a beneficio sia degli operatori del diritto che delle parti in causa.

In primo luogo, la formazione dei professionisti del diritto svolge un ruolo dcisivo. La procedura digitale è attuabile solo se tutte le parti coinvolte ne conoscono il funzionamento. In caso contrario, c'è il rischio che l'esito di una controversia non dipenda più solo dallo Stato di diritto, ma dalla sua applicazione digitale. La tecnologia informatica potrebbe in quel caso prevalere sulla tecnologia giuridica. Potremmo quindi preoccuparci dell'emer-

gere di un ordinamento digitale che prevalga sull'ordinamento giuridico. Ciò avverrebbe, ad esempio, se le richieste di una parte fossero accolte non perché un giudice ne è convinto, ma perché la parte ha una maggiore padronanza dell'informatica.

In secondo luogo, l'accessibilità richiede anche un supporto per le parti in causa. La formazione professionale sugli strumenti digitali può essere sufficiente a garantire l'accesso alla giustizia quando la rappresentanza legale è obbligatoria. Lo stesso non si può dire per altre procedure. Dato che una parte significativa della popolazione è affetta da analfabetismo digitale, i sistemi di giustizia digitale non possono essere diffusi su larga scala senza preoccuparsi della loro capacità di utilizzo. In nessun caso l'accesso alla giustizia dovrebbe essere impedito o reso più difficile dalle tecnologie informatiche. La tecnologia digitale può avvicinare la giustizia ad alcune persone, ma allo stesso tempo può escluderne altre. In pratica, ciò significa che ogni procedura digitale deve essere accessibile in un altro modo, con mezzi più tradizionali. Questo è già il caso in Francia per le procedure che rientrano nell'e-barreau, ma che possono essere accessibile in altri modi per i soggetti non rappresentati che non hanno accesso alla piattaforma. In ultima analisi, tuttavia, la coabitazione sistematica di procedure tradizionali e digitali potrebbe dare luogo a difficoltà organizzative. Si potrebbero forse prevedere alternative per garantire il servizio pubblico della giustizia, come ad esempio sportelli locali in cui le parti in causa potrebbero essere accompagnate per espletare le formalità necessarie. In ogni caso, è certo che la digitalizzazione del sistema giudiziario dovrà essere sistematicamente accompagnata da misure volte a garantire un accesso effettivo alla giustizia.

d) Principio di umanità. Sin dalla Rivoluzione industriale, si teme che l'uomo venga sostituito dalla macchina. La rivoluzione digitale sta rinnovando questa antica minaccia. Dagli strumenti più semplici come le videoconferenze e l'informatica a quelli più sofisticati come i sistemi di intelligenza artificiale, c'è il rischio che il progresso della tecnologia digitale sia accompagnato da un declino delle persone coinvolte nel sistema giudiziario, siano esse avvocati, magistrati o cancellieri. La cronica mancanza di risorse nel sistema giudiziario e il conseguente allungamento dei termini processuali potrebbero portare a questo risultato. La CEPEJ è preoccupata per questo e ritiene che "l'utilizzo di strumenti e servizi digitali nei sistemi giudiziari è finalizzato a migliorare l'efficienza e la qualità della giustizia, ma non deve mai cercare di sostituire la figura del giudice. Il giudice deve rimanere al centro del procedimento". Gli stessi professionisti del diritto esprimono questa preoccupazione. Il 23 novembre 2021, quasi 3.000 magistrati francesi hanno pubblicato un articolo nel quale esprimevano la loro preoccupazione per le conseguenze della mancanza di risorse nel sistema giudiziario. L'arti-

colo conteneva una conclusione preoccupante: "Il nostro sistema giudiziario soffre di questa logica di razionalizzazione che disumanizza e tende a trasformare i magistrati in esecutori statistici, laddove, più che altrove, dovrebbe essere una questione soprattutto di umanità" (L'appel des 3000, Le Monde, 23 novembre 2021). Per scongiurare questi pericoli, è necessario garantire che in ogni fase della procedura, anche nel caso di procedure digitalizzate, le parti abbiano accesso a un interlocutore umano, per assicurarne il corretto svolgimento. L'obiettivo sarebbe quello di evitare, ad esempio, che un ricorso sia dichiarato inammissibile semplicemente a causa di un problema con un modulo informatico.

III.

IDENTITÀ DIGITALE E COMUNICAZIONE ELETTRONICA NELLA PROCEDURA CIVILE TEDESCA (*)

di *Jonathan Hager* e *Wolfgang Hau*

3.1. Introduzione

Il sistema giudiziario civile è un pilastro importante del sistema giudiziario di qualsiasi ordinamento giuridico e svolge un ruolo cruciale nella risoluzione delle controversie tra privati, aziende ed enti statali. In questo contesto, la Germania, in quanto maggiore economia europea, è al centro dell'attenzione internazionale. Fortunatamente, la struttura, l'efficienza e l'equità della procedura civile tedesca sono relativamente buone (1). Purtroppo, un quadro diverso emerge quando si considera la digitalizzazione dei procedimenti civili. Secondo uno studio del 2022, la Germania è in ritardo di diversi anni rispetto alla media internazionale (2). Le ragioni principali addotte sono la mancanza del personale necessario per la digitalizzazione e un atteggiamento avverso alla tecnologia da parte dei decisori (3). Tuttavia,

(*) Libera traduzione, non revisionata dagli Autori.

(1) Ad esempio, la Germania si colloca al quarto posto in un confronto tra 140 Paesi secondo il *WJP Rule of Law Index* 2022, disponibile all'indirizzo <https://worldjusticeproject.org/rule-of-law-index/global/2022/Germany/Civil%20Justice/> (tutti i siti web citati sono stati consultati l'ultima volta il 22 agosto 2023).

(2) Studio del Boston Consulting Group, della Bucerius Law School e di Legal Tech Germany: "Il futuro della giustizia digitale", 2022, pag. 9.

(3) Ibidem.

l'ulteriore sviluppo della procedura civile attraverso le possibilità digitali è discusso e perseguito anche in questo Paese da tutte le parti della scienza giuridica. Il legislatore ha da tempo l'intenzione di digitalizzare e nell'attuale legislatura ha messo all'ordine del giorno l'aumento dell'efficienza dei procedimenti civili attraverso la digitalizzazione (4). Così, nel corso degli ultimi anni, alcuni meccanismi sono stati introdotti nel nostro Codice di procedura civile, come l'obbligo attivo di trasmettere gli atti processuali per via elettronica per alcune parti ai sensi dell'articolo 130d del Codice di procedura civile (5) o l'imminente obbligo per i tribunali di tenere un fascicolo elettronico ai sensi dell'articolo 298a (1) frase 1 del Codice di procedura civile. D'altra parte, permangono ostacoli enormi, come i disaccordi all'interno del governo in materia di finanziamenti (6).

Questo articolo è dedicato allo stato attuale della digitalizzazione dei procedimenti civili tedeschi. La presentazione segue il corso del procedimento civile, dalla presentazione della domanda di risarcimento all'esecuzione della sentenza. Particolare attenzione è dedicata all'identificazione dei mittenti e alle opzioni di accesso digitale.

3.2. Inizio del procedimento civile

3.2.1. *Ricezione della richiesta da parte del tribunale*

Ai sensi della sezione 253 (1) del Codice di procedura civile, i procedimenti civili diventano generalmente pendenti nel momento in cui la richiesta di risarcimento viene depositata presso il tribunale. La dichiarazione di credito può — e in alcuni casi deve — essere depositata presso il tribunale come documento elettronico ai sensi delle sezioni 130a, 169 (4) ZPO.

3.2.1.1. *Modulo elettronico*

Ai sensi dell'articolo 130a (3) frase 1 del Codice di procedura civile, esistono due modi per presentare un documento elettronico: o viene fornito con una firma elettronica qualificata della persona responsabile (variante 1, a questo scopo *a*) oppure semplicemente firmato e inviato con un "mezzo di

(4) Accordo di coalizione dell'attuale governo, disponibile su <https://www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf>, p. 84.

(5) Codice di procedura civile tedesco, legge del 5 dicembre 2005 (Gazzetta ufficiale federale I 3202), modificato da ultimo dall'articolo 19 della legge del 22 febbraio 2023 (Gazzetta ufficiale federale 2023 I 1), di seguito "ZPO".

(6) Si veda la 93a Conferenza dei Ministri della Giustizia del 10 novembre 2022 (decisione sul punto I.16).

trasmissione sicuro" (variante 2, inoltre *b*). Se nessuno di questi due requisiti è soddisfatto quando la dichiarazione di credito viene inviata elettronicamente, ad esempio se la dichiarazione di credito viene inviata come allegato a un semplice messaggio di posta elettronica, la forma procedurale non è rispettata; l'azione non è quindi correttamente depositata e non è proceduralmente valida.

a) *Firma elettronica qualificata*

La firma elettronica qualificata ai sensi della sezione 130a (3) frase 1 var. 1 ZPO è una firma elettronica avanzata (cfr. art. 3 n. 11 in combinato disposto con l'art. 26 del Regolamento eIDAS (7)) creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per le firme elettroniche (art. 3 n. 12 del Regolamento eIDAS). In Germania, ciò è garantito da speciali componenti software e hardware: La chiave della firma è memorizzata su una chip card precedentemente richiesta, che viene letta con l'aiuto di un lettore di carte dopo aver inserito un PIN. È possibile che questa procedura venga semplificata in futuro da una firma remota, in base alla quale l'utente ottiene l'accesso con un software speciale da un cosiddetto prestatore di servizi fiduciari; il dispositivo di creazione della firma rimane quindi presso questo prestatore e l'utente deve solo effettuare il login tramite un'applicazione o un'applicazione web (cfr. anche il considerando 52 del Regolamento eIDAS) (8).

Il documento può essere fornito con la firma come un altro file ("*staccato*") o la firma può essere inclusa nel documento e inviata come un unico file ("*inline*") (9). Ai sensi della sezione 4 (2) dell'ERVV (10), anche se vengono inviati più documenti (ad esempio, un'azione associata a una domanda di provvedimenti cautelari), ogni documento deve essere firmato

(7) Regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU 2014 L 257/73), di seguito "Regolamento eIDAS".

(8) Riehm, in: Fest/Gomille (eds.), *Festschrift für Johannes Hager zum 70. Geburtstag*, 2021, 71, 78.

(9) Herberger, in: Riehm/Dörr (a cura di), *Digitalizzazione e procedura civile*, 2023, 293, par. 13.

(10) Ordinanza sulle condizioni quadro tecniche per le transazioni giuridiche elettroniche e sulla casella di posta elettronica speciale delle autorità pubbliche, nella versione pubblicata il 24 novembre 2017 (Gazzetta ufficiale federale I 3803), modificata da ultimo dall'articolo 6 della legge sull'ampliamento delle transazioni giuridiche elettroniche con i tribunali e sulla modifica di altre disposizioni del 5 ottobre 2021 (Gazzetta ufficiale federale I 4607), di seguito "ERVV".

singolarmente; non è quindi ammessa una firma per un cosiddetto contenitore di più documenti (11).

Il vantaggio della firma qualificata rispetto alla firma semplice o avanzata è che il documento non deve necessariamente essere trasmesso tramite un canale di trasmissione sicuro ai sensi della sezione 130a (4) ZPO. Ai sensi della sezione 130a (2) frase 2 ZPO in combinato disposto con la sezione 4 (1) ERVV, il documento può anche essere inviato alla casella di posta elettronica giudiziaria e amministrativa (12). Questa casella di posta elettronica, in uso già da diversi anni, è concepita in modo diverso tra i tribunali dei singoli Länder, poiché l'amministrazione della giustizia è di competenza dei Länder nel quadro del sistema federale tedesco. Nella maggior parte dei Länder, ci si collega a una piattaforma fornita dal tribunale e vi si carica il documento in questione. Ciò che le caselle di posta elettronica hanno in comune, tuttavia, è che i messaggi sono criptati end-to-end e, mantenendo il cosiddetto standard OSCI (13), l'intercettazione o la manipolazione è quasi impossibile.

Le opzioni di trasmissione di cui alla sezione 130a ZPO sono esaustive. Ne consegue che i documenti elettronici, anche se sono stati firmati in modo qualificato, non possono essere inviati come semplice e-mail o consegnati al tribunale su un supporto di file (14).

b) *Documenti semplicemente firmati*

Se un documento semplicemente firmato ai sensi della sezione 130a (3) frase 1 var. 2 ZPO deve essere inviato al tribunale, ciò deve necessariamente avvenire con un mezzo di trasmissione sicuro ai sensi della sezione 130a (4) ZPO. La "sicurezza" in questo caso non si riferisce alla sicurezza informatica, ma al requisito di poter trarre una conclusione affidabile sull'identità del mittente (15). Nella pratica, tuttavia, agli avvocati viene regolarmente sconsigliata la trasmissione di documenti elettronici semplicemente firmati, perché in questo modo i documenti non sono ugualmente protetti da successive manipolazioni (16).

Ai sensi dell'art. 3 n. 10 del Regolamento eIDAS, le firme semplici sono dati allegati in formato elettronico che il firmatario utilizza per firmare. È sufficiente che il firmatario aggiunga il proprio nome per iscritto. Non è

(11) BGH, 5 maggio 2019 - VII ZB 570/18, NJW 2019, 2230.

(12) Vedere <http://www.egvp.de>.

(13) "Standard Online Services Computer Interface", in questo caso il contenuto del messaggio è separato dai dati utente richiesti durante la trasmissione; Müller, *E-Justice - Praxishandbuch*, 6ª ed., 2021, 37.

(14) BeckOK ZPO/von *Stelle*, 49a edizione 2023, § 130a, n. marginale 13.

(15) Müller, E-*Justice - Praxishandbuch*, pag. 28.

(16) Ibidem.

richiesta la firma autografa (scannerizzata o su touchpad). Il mezzo di trasmissione praticamente più importante è costituito da speciali caselle di posta elettronica utilizzate dai mittenti, diverse a seconda della natura del contendente. Per creare una casella di posta elettronica di questo tipo, l'identità dell'utente deve essere confermata separatamente. In pratica, l'utente riceve una carta con chip con la quale deve effettuare il login tramite un lettore di carte e un PIN prima di ogni utilizzo. In pratica, la più importante è la casella di posta elettronica speciale dell'avvocato ("beA", Sezione 31a (6) BRAO [17]). Anche le autorità pubbliche e le persone giuridiche di diritto pubblico dispongono di una casella postale di questo tipo [18]. I notai e i consulenti fiscali possono utilizzare una casella postale corrispondente [19] e anche le persone fisiche e giuridiche di diritto privato possono istituire una casella postale speciale a partire dal 1° gennaio 2022 (sezione 130 (4) n. 4 ZPO, sezioni 10 e seguenti ERVV).

La praticabilità di questo approccio è fortemente messa in dubbio, soprattutto per le persone fisiche, perché la procedura di identificazione e configurazione è relativamente complessa. Tuttavia, chiunque abbia attivato la funzione online della propria carta d'identità può effettuare l'identificazione senza una chip card o un lettore di carte separato. Tuttavia, ciò è reso più difficile dal fatto che il software corrispondente deve essere acquistato da fornitori terzi ed è a pagamento. I costi partono da circa 20 euro al mese, per cui per le singole persone interessate non vale la pena di creare un account per i procedimenti legali. I cittadini possono anche utilizzare un account esistente per comunicare elettronicamente con l'amministrazione per le comunicazioni giudiziarie. Ma anche in questo caso, l'identità dell'utente deve essere prima verificata da un'autorità pubblica, per cui l'utilizzabilità per i cittadini non è ancora garantita senza ostacoli logistici. Per le aziende, si può prendere in considerazione anche un sigillo elettronico qualificato, art. 38 del Regolamento eIDAS.

Per completezza, va menzionato anche l'invio tramite un account di posta elettronica speciale ai sensi della sezione 130a (4) frase 1 n. 1 ZPO, per il cui utilizzo il mittente deve confermare separatamente la propria identità ("De-Mail"). Tuttavia, questa opzione non viene quasi più utilizzata nella pratica; il principale fornitore del servizio, Telekom, ha già disattivato il servizio entro il 31 agosto 2022.

---

[17] Legge federale sugli avvocati, legge del 1° agosto 1959 (Gazzetta ufficiale federale I 565), modificata da ultimo dalla legge del 10 marzo 2023 (Gazzetta ufficiale federale I 64).

[18] Casella di posta elettronica speciale delle autorità pubbliche ("beBPo").

[19] Casella di posta elettronica speciale per notai o consulenti fiscali ("beN" o "BStBK").

c) *Redazione della dichiarazione di sinistro*

Ai sensi della sezione 2 (1) frase 1 dell'ERVV, la dichiarazione di sinistro deve essere generalmente trasmessa in formato PDF, eccezionalmente in formato TIFF per la rappresentazione senza perdita di immagini. Ne consegue che la dichiarazione di sinistro può contenere solo file di testo e immagini. Non è possibile incorporare file audio o video in una memoria o negli allegati; questi devono essere inviati separatamente. Le prove, se in formato digitale di testo o di immagine, possono essere allegate alla memoria. In pratica, spesso viene consegnata al tribunale una chiavetta USB contenente le prove in forma di file. Le prove fisiche, in particolare i documenti originali, devono ancora essere presentate al tribunale in forma analogica. Una scansione non ha praticamente alcun valore probatorio (si veda il punto C.III.3.a). C.III.3.a)).

3.2.1.2. *Servizio attivo di utilizzo*

In sintesi, un documento elettronico, anche se semplicemente firmato, può essere inviato al tribunale attraverso un canale di trasmissione sicuro, quindi in pratica utilizzando apposite caselle di posta elettronica. Se il documento è dotato di firma elettronica qualificata, in alternativa può essere inviato alla casella di posta elettronica del tribunale tramite una piattaforma. La possibilità di utilizzare anche i mezzi di trasmissione tradizionali (classicamente la trasmissione di un documento firmato per posta, fax o messaggeria) dipende dalla natura delle parti coinvolte.

a) *Persone fisiche*

Le persone fisiche possono intentare una causa presso i tribunali locali senza l'aiuto di un avvocato. Questi tribunali sono competenti — in forma molto semplificata — per le controversie di valore inferiore a 5.000 euro e per tutti i reclami derivanti da contratti di locazione residenziale (§ 23 GVG ([20])). Se una persona fisica desidera presentare una causa, può utilizzare mezzi di trasmissione elettronici, ma non è obbligata a farlo; può anche presentare la causa oralmente a verbale presso l'ufficio del tribunale. Tuttavia, ciò richiede la presenza fisica del giudice, per cui non si può ancora parlare di deposito digitale di una causa in questo modo. Una procedura legislativa che prevede un emendamento alla sezione 129a del Codice di procedura civile (ZPO) dovrebbe ora apportare un miglioramento: In futuro

([20]) Legge sulla costituzione dei tribunali, nella versione promulgata il 9 maggio 1975 (Gazzetta ufficiale federale I 1077), modificata da ultimo dalla legge del 19 dicembre 2022 (Gazzetta ufficiale federale I 2606), di seguito "GVG".

dovrebbe essere possibile depositare un'azione legale anche oralmente, tramite video, presso la cancelleria del tribunale (21).

b) *Persone giuridiche di diritto privato*

Lo stesso vale per le persone fisiche e per le persone giuridiche di diritto privato, che possono adire il tribunale distrettuale con gli stessi mezzi attraverso un rappresentante.

c) *Avvocati*

Presso i tribunali civili di grado superiore, i tribunali regionali, una causa deve essere presentata da un avvocato per essere efficace (sezione 78 (1) frase 1 ZPO). Ai sensi della sezione 71 (1) GVG, i tribunali sono generalmente competenti per tutte le controversie civili con un importo superiore a 5.000 euro.

Ai sensi della sezione 130d frase 1 del Codice di procedura civile (ZPO), a partire dal 1° gennaio 2022 gli avvocati non hanno a disposizione mezzi alternativi per trasmettere le istanze, gli allegati e tutte le altre memorie preparatorie. Per essere ammissibili in tribunale, le memorie devono essere trasmesse per via elettronica (22). Tuttavia, la legge prevede alcune eccezioni a questo obbligo di utilizzo attivo, in particolare ai sensi della sezione 130d frase 2 dello ZPO, se la trasmissione non è possibile per motivi tecnici, indipendentemente dal fatto che provengano dalla sfera del tribunale, dal fornitore di software o dal mittente (23). Un'altra eccezione è prevista per i documenti di dimensioni particolari ai sensi della sezione 3 ERVV in combinato disposto con la sezione 5 (1) n. 3 ERVV. È possibile trasmettere un massimo di 1.000 file e 200 megabyte (24). Questo limite è stato continuamente aumentato nel corso degli anni ed è probabile che venga ulteriormente innalzato in futuro. Un punto debole della casella postale, tuttavia, è ancora l'interfaccia macchinosa e la mancanza di compatibilità con i software più comuni degli studi legali (25). Non è possibile inviare una memoria direttamente dal programma di gestione dei dati di uno studio legale.

d) *Persone giuridiche di diritto pubblico e autorità pubbliche*

Tutte le autorità pubbliche e le persone giuridiche di diritto pubblico sono soggette allo stesso obbligo di utilizzo della professione legale, sezione

---

(21) Progetto di legge del Governo federale per promuovere l'uso della tecnologia della videoconferenza nei tribunali civili e specializzati, disponibile all'indirizzo <https://dserver.bundestag.de/brd/2023/0228-23.pdf>, di seguito "Progetto di legge".

(22) BGH, 24 novembre 2022 - IX ZB 11/22, NJW 2023, 525, par. 7.

(23) BT-Drucksache 17/12634, 27.

(24) Secondo avviso relativo all'articolo 5 dell'ordinanza sulle transazioni legali elettroniche del 10 febbraio 2022.

(25) Müller, *E-Justice - Praxishandbuch*, 17 e segg.

130d frase 1 ZPO. Sono ugualmente obbligati a creare e utilizzare una speciale casella di posta elettronica delle autorità pubbliche.

e) *Notai, consulenti fiscali e ufficiali giudiziari*

Sebbene queste parti debbano istituire e mantenere una casella postale speciale (cioè sono soggette all'obbligo passivo di utilizzarla), possono continuare a inviare le memorie al tribunale con i mezzi tradizionali (sezione 173 (2) frase 1 n. 1 var. 2-4 ZPO).

3.2.2. *Inoltro del ricorso da parte del tribunale al convenuto*

Se l'azione è stata validamente depositata presso il tribunale, quest'ultimo deve notificare formalmente l'azione al convenuto. Le modalità di notifica sono disciplinate dai §§ 173 e segg. ZPO.

3.2.2.1. *Nessun obbligo di consegna elettronica*

Ai sensi dell'articolo 173 (1) del Codice di procedura civile, dal 1° gennaio 2023 la notificazione elettronica è disciplinata in cima alle norme sulle forme di notificazione. Ciò non comporta ancora l'obbligo per i tribunali di notificare gli atti per via elettronica. Altre forme di notificazione - come le possibili forme di notificazione postale di documenti fisici di cui ai §§ 175 e segg. ZPO — possono continuare a essere utilizzate nell'ambito della discrezionalità del tribunale (26). D'altro canto, il cancelliere sceglierà la forma di notificazione elettronica come forma più semplice, sicura ed economica, a condizione che esista un mezzo di trasmissione sicuro da parte del destinatario.

3.2.2.2. *Cassetta postale digitale delle parti del procedimento e obbligo di utilizzo passivo*

Ai sensi dell'articolo 173 (1) del Codice di procedura civile, un prerequisito per la notifica di un documento elettronico è che il destinatario abbia stabilito un mezzo di trasmissione sicuro in modo che la sua identità sia chiaramente garantita al momento della notifica. Pertanto, la notifica alla casella di posta elettronica delle parti non è possibile, anche se è stata utilizzata una firma elettronica qualificata (27). La necessità di creare un mezzo di trasmissione sicuro dipende anche dalla natura della parte del destinatario.

---

(26) BT-Drucksache 19/28399, 34 f.

(27) Schultzky, MDR 2022, 201, 204 par. 18.

a) *Avvocati, autorità, notai, consulenti fiscali, ufficiali giudiziari e altri professionisti del contenzioso*

L'obbligo di utilizzo attivo degli avvocati, delle autorità pubbliche e delle persone giuridiche di diritto pubblico (28) si riflette in un obbligo di utilizzo passivo (sezione 173 (2) frase 1 n. 1 var. 1, n. 2 ZPO). Tuttavia, anche i notai, gli ufficiali giudiziari e i consulenti fiscali devono aprire un canale di trasmissione per la notifica di documenti elettronici (sezione 173 (2) frase 1 n. 1 var. 2-4 ZPO).

Per i soggetti di cui all'articolo 173, paragrafo 2, del Codice di procedura civile, l'avviso di ricevimento elettronico dimostra che l'atto è stato effettivamente ricevuto dal destinatario. L'avviso di ricevimento elettronico va oltre l'avviso di ricevimento automatico, perché il suo contenuto non solo conferma la ricezione nella casella di posta elettronica, ma anche quella di persona da parte del destinatario. Questo è importante perché la prova della notifica di un atto non può essere fornita in altro modo (sezione 175(4) ZPO) (29). L'avviso di ricevimento è una reliquia del diritto tedesco risalente all'epoca dei documenti fisici, che oggi sembra impraticabile e fuori sistema nel contesto dello scambio elettronico di documenti (30). In pratica, tuttavia, il software delle caselle postali speciali è in grado di riconoscere e rispondere automaticamente alla richiesta di ricevuta. Tuttavia, poiché questo metodo richiede una speciale impostazione del software, molte voci suggeriscono che un avviso di ricevimento automatico dovrebbe essere sufficiente *de lege ferenda* (31).

b) *Persone fisiche e giuridiche di diritto privato*

La legge considera le persone fisiche e giuridiche di diritto privato come parti processuali regolarmente meno professionali. Pertanto, un atto può essere notificato loro per via elettronica solo se hanno acconsentito alla notifica elettronica. Pertanto, devono agire in prima persona. Ai sensi della sezione 173 (4) frase 2 dello ZPO, il consenso si considera dato se hanno precedentemente presentato un documento per via elettronica al tribunale, ossia se hanno praticamente creato una casella postale speciale e hanno inviato una memoria attraverso di essa. In questo caso, la legge non prevede la prova della notifica tramite ricevuta di ritorno. L'atto si considera invece notificato per finzione (cioè a prescindere dall'effettiva notifica) il terzo

(28) Cfr. sopra al punto B.I.2.c), *d*).

(29) Gli avvocati sono inoltre tenuti a restituire i documenti ai sensi del § 14 del Codice deontologico degli avvocati.

(30) Herberger, in: Riehm/Dörr (a cura di), *Digitalisation and Civil Procedure*, 290, par. 7.

(31) Stürner, ZZP 2022, 369, 377; Bernhardt, jM 2022, 90, 91.

giorno successivo alla data di ricezione indicata nell'avviso di ricevimento automatico. Se non c'è il consenso o la rappresentanza legale della persona, resta in vigore il metodo tradizionale di notifica ai sensi dei §§ 174 e seguenti. ZPO, si applicano le modalità di notifica tradizionali.

3.3. Ulteriore corso del procedimento civile

3.3.1. *Gestione dei file*

Quando il ricorso viene ricevuto, non solo viene notificato al convenuto, ma il tribunale apre anche un fascicolo. Attualmente, ciò può essere fatto elettronicamente ai sensi della sezione 298a, paragrafo 1, frase 1 del Codice di procedura civile; dal 1° gennaio 2026, ciò sarà addirittura obbligatorio. Sebbene anche la struttura del fascicolo elettronico sia di competenza dei Länder, questi ultimi si sono riuniti in due gruppi e hanno sviluppato due sistemi compatibili tra loro. La struttura del fascicolo elettronico corrisponde in linea di principio a quella di un fascicolo fisico: i documenti ricevuti sono archiviati cronologicamente e dotati di un proprio numero di pagina. Se un documento viene presentato fisicamente, deve essere scansionato e aggiunto al fascicolo (sezione 298a (2) ZPO). Tuttavia, le prove possono entrare a far parte del fascicolo elettronico solo in misura limitata. Ciò dipende dalla forma della prova ([32]). Nel caso dei documenti, ciò vale solo se si tratta di semplici file di testo o di immagini senza alcuna pretesa di originalità. Per i documenti originali vale un altro discorso: Questi non possono essere digitalizzati in sostituzione e sono quindi conservati fisicamente presso il tribunale ([33]). Per quanto riguarda i file audio o video che fanno parte della prova, lo stato attuale del file elettronico non è ancora pronto per includerli nel file stesso. In pratica, viene spesso creato un segnaposto in formato PDF che contiene un link al file conservato altrove ([34]). Le prove fisiche a scopo di ispezione vengono archiviate in modo analogo presso il tribunale e il file viene fornito con i relativi riferimenti.

3.3.2. *Audizione orale*

Per quanto riguarda la digitalizzazione dei procedimenti orali, in particolare attraverso le video udienze, tali udienze sono teoricamente possibili

([32]) Vedi sotto C.III.

([33]) JANSEN/SCHLICHT, in: RIEHM/DÖRR (a cura di), *Digitalisation and Civil Procedure*, 308, par. 9.

([34]) Ibidem.

dal 1° gennaio 2002 ai sensi dell'articolo 128a del Codice di procedura civile. Tuttavia, è solo dopo la pandemia di Covid 19 che si è fatto un uso significativo di questa possibilità. Le video udienze sono aumentate notevolmente negli ultimi anni, raggiungendo talvolta percentuali superiori al 50% (35). La decisione di tenere o meno un'udienza video è a discrezione del tribunale; le parti non hanno il diritto di farlo. Un'attuale proposta di legge intende spostare questa discrezionalità in modo significativo verso l'organizzazione di un'udienza video (36). Secondo la legge attuale, il tribunale deve essere presente in aula. Il principio della pubblicità è preservato dal fatto che l'udienza può essere seguita in aula attraverso gli schermi. Lo ZPO non prevede ancora un'udienza orale completamente digitale, ma è ora previsto (37). La trasmissione dell'udienza all'edificio giudiziario deve essere mantenuta.

La registrazione audio o video dell'udienza è vietata ai sensi della sezione 128 (3) frase 1 dello ZPO, anche con il consenso delle parti. L'opinione prevalente è inoltre contraria a una videoregistrazione separata delle singole udienze, anche con il consenso esplicito del testimone (38). Al contrario, l'attuale proposta di legge propone almeno una videoregistrazione preliminare dell'udienza ai fini della redazione del verbale (39). I procedimenti in cui almeno una parte si trova all'estero sono ancora considerati problematici (40). Secondo l'opinione prevalente in Germania, un'udienza video sarebbe in contrasto con il principio di sovranità del diritto internazionale, in quanto il potere dello Stato verrebbe di fatto esercitato in territorio straniero (41). Si può controbattere che, finché la partecipazione all'udienza è volontaria, non si può parlare di coercizione da parte dello Stato (42). Anche l'invio di memorie in preparazione del procedimento orale può essere effettuato da territori stranieri. Poiché le memorie scritte preparano già la maggior parte della decisione, soprattutto nei procedimenti civili più estesi, ci si chiede

(35) Irskens, in: Riehm/Dörr (eds.), *Digitalisierung und Zivilverfahren*, 429, n. 2 marginale.

(36) Bill, <https://dserver.bundestag.de/brd/2023/0228-23.pdf>.

(37) Ibidem.

(38) Mantz/Spoenle, MDR 2020, 637, 639 par. 14; Irskens, in: Riehm/Dörr (eds.), *Digitalisierung und Zivilverfahren*, 437, par. 30; Schultzky, NJW 2003, 313, 314. Dissenso Zöller/Greger, ZPO, 34ª ed. 2022, sezione 128a ZPO, par. 9.

(39) Bill, <https://dserver.bundestag.de/brd/2023/0228-23.pdf>.

(40) A questo proposito, *Voß*, in: Reuß/Windau (a cura di), *Göttinger Kolloquien zur Digitalisierung des Zivilverfahrensrechts*, vol. 1, 2022, p. 43.

(41) BGH, 5 novembre 1999 -1 StR 286-99, NJW 1999, 3788, 3789 (sul procedimento penale); *Musielak/Voit/Stadler*, ZPO, 20a ed. 2023, § 128a, n. marginale 8; *Zöller/Greger*, § 128a, n. marginale 10, ciascuno con ulteriori prove.

(42) Stürner, ZZP 2022, 369, 392.

perché le dichiarazioni nel procedimento orale debbano avere un carattere coercitivo al di là di questo.

3.3.3. *Assunzione di prove*

3.3.3.1. *Audizione di testimoni*

In linea di principio, l'esame dei testimoni, dei periti e delle parti può avvenire in video ed essere trasmesso in aula (artt. 284, comma 2, 128a, comma 2, ZPO). A differenza della partecipazione delle parti e dei loro rappresentanti al procedimento orale, l'audizione per l'assunzione di prove è possibile solo su richiesta di una parte. Il tribunale non è vincolato dalla richiesta e decide a sua discrezione. Contrariamente alla tendenza delle udienze orali alle udienze video, le trasmissioni video delle udienze sono ancora un'eccezione. In particolare, la valutazione della credibilità delle dichiarazioni dei testimoni via video è considerata significativamente più difficile (43), che a sua volta può essere evitata nei casi critici con un uso responsabile della discrezionalità da parte della magistratura (44). In futuro, dovrebbe essere possibile ordinare un esame video senza una domanda; tuttavia, le parti interessate dovrebbero avere il diritto di opporsi (45).

3.3.3.2. *Ispezione visiva*

La presentazione di prove in forma digitale originale rientra senza ulteriori indugi nelle norme sulla prova visiva, ossia nei §§ 371 ZPO e seguenti. Se la prova ha una forma fisica, non è ancora disciplinato dalla legge se la prova possa essere presentata mediante rappresentazione digitale sulla base dei §§ 284 S. 2, 128a par. 2 del Codice di Procedura Civile. 2, 128a comma 2 del Codice di Procedura Civile, sia possibile la rappresentazione digitale. Ciò è già affermato *de lege lata* da un'opinione diffusa (46), e l'attuale disegno di legge prevede un chiarimento esplicito (47). Tuttavia, resta il fatto che deve essere possibile fornire prove anche in forma digitale. Poiché l'impressione visiva, nonostante il termine tedesco sia fuorviante, può riferirsi a tutte le percezioni sensoriali, la prova digitale non può essere considerata se riguarda gli aptici, gli odori o i sapori. Se si parte dal presupposto che i file

(43) *Glunz*, Effetti psicologici nell'uso giudiziario della tecnologia video, 2012.

(44) Cfr. BT-Drucksache 17/12418, pag. 14.

(45) Progetto di legge, https://dserver.bundestag.de/brd/2023/0228-23.pdf.

(46) Zöller/Greger § 128a, n. marginale 7; Schultzky, NJW 2003, 313, 314. Dissenso Musielak/Voit/Stadler, § 128a, n. marginale 5.

(47) Bill, <https://dserver.bundestag.de/brd/2023/0228-23.pdf>.

di immagini e suoni sono ammissibili come prova visiva (o lo saranno presto grazie alla prevista modifica della legge), le parti hanno sostanzialmente tutte le opzioni a disposizione. Pertanto, se le registrazioni di immagini o suoni puri non sono sufficienti, possono anche offrire mezzi di prova moderni come rappresentazioni VR o simulazioni 3D. In sostanza, il file deve essere funzionalmente equivalente all'immagine analogica. Il tribunale decide a sua discrezione se questo è il caso e quindi se la prova deve essere fornita in formato digitale o analogico (48).

3.3.3.3. *Documenti*

a) *Documenti fisici*

Di norma, la prova dei documenti fisici deve essere fornita presentando il documento originale ai sensi della sezione 420 del Codice di procedura civile. Le parti con l'obbligo attivo di utilizzare la comunicazione legale elettronica (49) devono inoltre inviare una copia digitale al tribunale ai sensi delle sezioni 130d, 131 ZPO. La presentazione di un documento originale fisico ha il vantaggio che, ai sensi della sezione 416 del Codice di procedura civile, costituisce una prova completa, a prescindere dalla convinzione del tribunale, che le dichiarazioni in esso contenute provengono dai presunti emittenti, ossia che è "autentico".

È possibile presentare una scansione di un documento, ma il file è solo un oggetto di ispezione. Ciò significa che può essere presa in considerazione nella valutazione delle prove, ma la prova della sua autenticità non è stabilita. A causa del pericolo di manipolazione dei documenti scannerizzati, ad essi non viene riconosciuto l'ampio valore probatorio del § 416 ZPO (50). Molte voci criticano il fatto che solo i documenti originali possano essere una prova adeguata della loro autenticità: A causa dell'archiviazione elettronica dei documenti in molte famiglie e aziende, il rischio di perdere le prove è relativamente alto. La certezza del diritto sarebbe quindi utile nella gestione della documentazione, che nella pratica avviene già spesso in modo puramente digitale, se il valore probatorio dei documenti scansionati fosse rafforzato *de lege ferenda* (51).

I documenti pubblici in forma digitalizzata hanno un valore probatorio notevolmente superiore. Indipendentemente dalla convinzione del tribunale, l'originale costituisce una prova completa, ai sensi dell'articolo 415 del

(48) Irskens, in: Riehm/Dörr (eds.), Digitalisierung und Zivilverfahren, p. 440, par. 37.
(49) Cfr. sopra al punto B.I.2.c), *d*).
(50) Irskens, in: Riehm/Dörr (eds.), *Digitalisierung und Zivilverfahren*, 441, par. 39.
(51) Irskens, in: Riehm/Dörr (a cura di), *Digitalisierung und Zivilverfahren*, 453, n. marginale 71 con ulteriori riferimenti.

Codice di procedura civile, che la dichiarazione, comprese le circostanze che la accompagnano, come l'ora e il luogo dell'esecuzione, l'autorità e la persona che registra la dichiarazione, è stata fatta in modo corretto e completo con il contenuto indicato nel documento (52). Se un documento viene scansionato da un'autorità pubblica, il valore probatorio della scansione è correlato a quello dell'originale ai sensi della sezione 371b ZPO; anche in questo caso si presume l'autenticità della scansione (sezione 437 ZPO).

b) *Documenti elettronici*

Secondo l'interpretazione tedesca, i documenti elettronici sono sempre prove prima facie e sviluppano effetti probatori speciali solo attraverso disposizioni speciali. Anche i mezzi di prova speciali menzionati nel Regolamento eIDAS, come la lettera raccomandata elettronica qualificata, non sono documenti secondo l'interpretazione dello ZPO. Le corrispondenti regole di presunzione, come l'articolo 43(2) del Regolamento eIDAS, si applicano invece direttamente ai sensi dell'articolo 288 del TFUE.

Semplici documenti elettronici come e-mail, cronologie di chat o dati di sorveglianza sono soggetti alla libera valutazione delle prove come oggetti di ispezione ai sensi della sezione 286 (1) ZPO. Se la controparte contesta l'autenticità del documento, la parte che ha l'onere della prova deve dimostrarlo, ad esempio presentando un protocollo di trasmissione o consegnando lo smartphone contenente una cronologia di chat a un esperto. Lo stesso vale per i file con firma elettronica avanzata ai sensi dell'art. 3 n. 11 e dell'art. 26 del Regolamento eIDAS. Tuttavia, può avere un maggiore potere persuasivo nel contesto della valutazione delle prove.

Se è disponibile un documento elettronico con firma elettronica qualificata ai sensi dell'art. 3 n. 12 del Regolamento eIDAS, si applica di conseguenza la regola della prova inconfutabile di cui alla sezione 416 ZPO (53) (sezione 371a (1) ZPO), a condizione che la firma faccia riferimento alle dichiarazioni corrispondenti. I documenti elettronici pubblici sviluppano l'effetto probatorio sul loro contenuto anche senza una firma elettronica qualificata (sezione 371a (3) frase 1 in combinazione con la sezione 415 ZPO). Se tale firma è anche allegata al documento, costituisce inoltre una prova completa della sua autenticità ai sensi della sezione 371a (3) frase 2 in combinato disposto con la sezione 437 ZPO. Se il documento elettronico proviene da un'autorità straniera, il valore probatorio del suo contenuto è lo stesso. Tuttavia, anche nel caso di una firma elettronica qualificata, l'autenticità non è presunta perché per tali documenti non esiste un riferimento

(52) BeckOK *ZPO*/Krafka, 49ª edizione 2023, § 415, n. marginale 19.

(53) Vedi sopra al punto C.III.3.a).

corrispondente nei §§ 371 e segg. ZPO alla sezione 416 ZPO per tali documenti (54).

3.4. Sentenza ed esecuzione

Nell'ambito della gestione elettronica dei fascicoli, la sentenza può essere emessa anche in forma elettronica (sezione 130b ZPO). Tuttavia, ai sensi delle sezioni 724 (1) e 725 ZPO, per l'esecuzione è ancora necessaria una copia esecutiva della sentenza, che può essere rilasciata solo in forma cartacea (sezione 317 (2) frase 1, (3) ZPO). Lo stesso vale per l'istanza di esecuzione e per la dichiarazione di credito: Il deposito digitale è obbligatorio anche a livello di esecuzione per gli avvocati, le autorità pubbliche e le persone giuridiche di diritto pubblico (sezione 753 (5) in combinato disposto con la sezione 130d ZPO).

Se il tribunale è l'organo competente per l'esecuzione (come nel caso dell'esecuzione di crediti pecuniari), la domanda può essere aggiunta al fascicolo elettronico senza ulteriori indugi. Se, invece, è un ufficiale giudiziario a eseguire l'ordinanza (come nel caso del pignoramento di beni mobili), l'applicazione digitale porta ancora pochi progressi: sebbene gli ufficiali giudiziari debbano aprire un canale di trasmissione sicuro per il servizio elettronico ai sensi della sezione 173 (2) frase 1 n. 1 ZPO, allo stesso tempo devono continuare a conservare i loro fascicoli in forma cartacea *de lege lata*; la sezione 298a ZPO non si applica a loro. Ciò può portare alla scansione e alla trasmissione digitale di un documento stampato da parte dell'avvocato e alla successiva stampa da parte dell'ufficiale giudiziario. Per evitare che ciò accada in futuro, è necessaria l'introduzione di un registro dei titoli di proprietà elettronico puramente digitale, per poter rinunciare in futuro alle copie esecutive analogiche (55). Oggi, l'ufficiale giudiziario prepara già la dichiarazione dei beni del debitore in forma digitale ai sensi della sezione 802f, paragrafo 5 del Codice di procedura civile e la trasmette elettronicamente al tribunale, che la amministra digitalmente (sezioni 802f, paragrafo 6, 802k, paragrafo 1, frase 1 del Codice di procedura civile). Inoltre, gli ufficiali giudiziari possono visualizzare le informazioni su Internet per decidere se è necessario ottenerle nuovamente. Se un oggetto deve essere

(54) Kienzle, NJW 2019, 1712, 1714.

(55) Nel 2021, il gruppo di lavoro "Modernizzazione della procedura civile" ha pubblicato un documento di discussione a nome dei tribunali superiori e della Corte Suprema Federale che ha ricevuto molta attenzione in Germania, accessibile all'indirizzo <www.justiz.bayern.de/media/images/behoerden-und-gerichte/oberlandesgerichte/nuernberg/diskussionspapier_ag_modernisierung.pdf>, pag. 106 e segg.

messo all'asta, ciò può essere fatto su una piattaforma internet ai sensi della sezione 814 (2) n. 2 ZPO.

3.5. Conclusione

In sintesi, si può affermare che la digitalizzazione dei procedimenti civili in Germania ha fatto progressi significativi. Già dal 1° gennaio 2018, quasi tutti i tribunali (56) possono essere aditi in modo giuridicamente vincolante per via elettronica, e l'ulteriore elaborazione digitale dei documenti sarà garantita al più tardi quando entrerà in vigore l'obbligo di deposito elettronico dal 1° gennaio 2026.

Tuttavia, vi è ancora bisogno di una riforma sotto diversi aspetti. In particolare, sarebbe auspicabile una comunicazione semplificata con l'autorità giudiziaria per far valere i diritti delle persone fisiche e giuridiche che non entrano regolarmente in contatto con i tribunali. A tal fine, si propone di aprire la casella di posta elettronica del tribunale per i documenti elettronici semplicemente firmati (57). Per l'esecuzione delle controversie di minore entità, sembra ipotizzabile anche un procedimento accelerato completamente digitale (58), o un portale della giustizia dei tribunali civili concepito in modo uniforme in tutta la Germania (59). Per aumentare l'efficienza dei procedimenti legali, si chiede la creazione di una piattaforma di scambio elettronico di messaggi e documenti nei procedimenti giudiziari (60). Il divieto di video udienze con parti che partecipano dall'estero è particolarmente problematico nel contesto del processo. Inoltre, lo scarso valore probatorio dei documenti scansionati ha un impatto negativo sulla pratica della conservazione digitale dei documenti nelle aziende e da parte dei privati.

Alla luce del progressivo sviluppo degli ultimi anni, questo contributo rappresenta una semplice istantanea di un processo di riforma in corso. Spetta ancora alla comunità giuridica, al legislatore e alle altre parti interessate risolvere i problemi esistenti e adattare la procedura civile alla realtà digitale del settore privato, bilanciando le nuove possibilità con gli interessi dei contendenti e i principi dello Stato di diritto.

---

(56) Esiste ancora un'eccezione per quanto riguarda le Corti costituzionali federali e di alcuni Länder.

(57) Documento di discussione, pag. 29 e.

(58) Documento di discussione, pag. 76 e segg.

(59) Documento di discussione, pag. 10 e seguenti.

(60) Documento di discussione, pag. 26 e.

ISBN 978-88-28-84248-4

024216280