Dati biometrici, firma grafometrica e contratti elettronici. Quali implicazioni per la Cyber Security

di **MARIA ROSARIA LENTI**

Abstract

The purpose of this contribution is to analyze the evolution of the subscription arrangements for the conclusion of the contractual instrument, from electronic signatures to graphometric signatures and biometric data, highlighting the advantages and criticalities of these innovations under the security profile and the prevention and protection measures developed by the Guarantor Authority.

1. Introduzione. La dinamicità della moderna realtà economica e l'avvento della tecnologia hanno rivelato l'esigenza di una rivisitazione delle tradizionali modalità di conclusione dei contratti.

Si è, così, profilata l'ipotesi di abbandonare il supporto cartaceo e di avvalersi dei mezzi informatici, più conformi alla frequenza e alla rapidità degli scambi.

La trasfusione dei moderni standard tecnologici nel settore negoziale ha, però, richiesto un adeguamento delle norme, che già disciplinavano le fasi della formazione, la forma e la prova dei contratti, alle connotazioni degli strumenti elettronici e la creazione di una nuova regolamentazione, che precisasse gli effetti e le modalità di redazione dei negozi telematici.

Dunque il legislatore, nel tentativo di (in)seguire le nuove tecnologie e di trasporle nel diritto, si è trovato ad affrontare un ventaglio di problematiche nuove e del tutto inaspettate, in termini di furto d'identità e di protezione dei dati, e a fare i conti con il complesso funzionamento del mondo digitale,

inesplorato e imprevedibile per il giurista, privo di conoscenze tecniche in merito.

Il presente contributo ha l'obiettivo di analizzare l'evoluzione delle modalità di sottoscrizione dei contratti, dalla firma elettronica alla firma grafometrica e all'utilizzo dei dati biometrici, mettendo in risalto i vantaggi e le criticità di tali novità sotto il profilo della sicurezza e vagliando le misure di prevenzione e di protezione elaborate dall'Autorità Garante per la Protezione dei Dati Personali.

2. Dalla firma olografa alla firma digitale. Nell'ambito del settore documentale, la sottoscrizione autografa di un atto pubblico o di una scrittura privata rappresenta l'ultimo momento della più tradizionale forma di manifestazione di volontà negoziale.

La firma consente di assolvere a tre funzioni. Essa, difatti, vale ad individuare l'autore della sottoscrizione, che, quindi, si assume la responsabilità di quanto dichiarato[1], e ad ingenerare una presunzione *iuris tantum* di accettazione da parte del sottoscrittore del contenuto negoziale.
Per di più ad essa va riconosciuta una valenza probatoria.

Quando il contratto è redatto nella forma dell'atto pubblico, la sottoscrizione suggella l'intervenuto accordo in un atto che ha una forza probatoria privilegiata: soltanto mediante una querela di falso è possibile contestare la provenienza delle volontà negoziali delle parti e l'attestazione del pubblico ufficiale che tali dichiarazioni sono state rese in sua presenza (art. 2700 c.c.).

Se, invece, la sottoscrizione autografa chiude una scrittura privata, quest'ultima fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi ha sottoscritto, soltanto se la firma è autenticata o se la parte contro cui è prodotta la scrittura riconosce la propria sottoscrizione (art. 2702 c.c.).

1 Cass. civ., 2 febbraio 2006, n. 2332, in *Mass. Giur. It.*, 2006; Cass. civ., 16 agosto 2004, n. 15949, in *Mass. Giur. It.*, 2004; Cass. civ., 14 febbraio 2013, n. 3730, in *CED Cassazione*, 2013.

In seguito alla rivoluzione digitale il legislatore ha ritenuto opportuno elaborare una nuova forma di documento, che potesse prescindere dal supporto cartaceo, ma strutturato in modo tale da rispondere ai requisiti di validità formale e di efficacia probatoria e all'esigenza di imputazione dell'atto tradizionale.

I primi interventi hanno riguardato il settore pubblicistico.

L'art. 15 della L. 7 agosto 1990 n. 241 ha previsto l'obbligo per le pubbliche amministrazioni di concludere accordi per la disciplina dello svolgimento di attività di interesse comune, da sottoscrivere, a pena di nullità, con firma digitale, firma elettronica avanzata o altra firma elettronica qualificata. Successivamente l'art. 11 del d.lgs. 12 aprile 2006 n. 163, in tema di affidamento dei lavori pubblici ha prescritto, a pena di nullità, la stipula del contratto con modalità elettroniche; previsione poi ribadita dal d.lgs. 18 aprile 2016 n. 50 in materia di aggiudicazione dei contratti di concessione, appalti pubblici e contratti pubblici relativi a lavori, servizi e forniture[2].

Occorreva affermare questa tendenza, favorevole al modello digitale, anche in campo privatistico.

I vantaggi della stipulazione di un contratto mediante strutture telematiche erano visibili ad occhio nudo.

Innanzitutto il formato digitale accorciava i tempi e i costi non solo di redazione e sottoscrizione, ma anche di trasmissione[3] dell'atto, di registrazione e di pubblicità, riduceva gli spazi e gli oneri di conservazione, e, infine, consentiva una circolazione del documento medesimo con maggiore facilità e immediatezza.

2 Oltre ai comuni vantaggi derivanti dall'utilizzo delle strutture informatiche, il legislatore ha promosso l'impiego di tali supporti per una maggiore trasparenza dell'operato della Pubblica Amministrazione.

3 La scrittura privata non richiede la contestualità dei soggetti sottoscriventi, ma proposta e accettazione possono essere predisposti in momenti e luoghi diversi. In tal caso, il vantaggio apportato dalla fruizione di strutture informatiche, in termini di riduzione dei tempi e dei costi, è ancora più tangibile.

Nel panorama giuridico ha fatto, quindi, ingresso il documento informatico[4], quale rappresentazione informatica di atti, dati e fatti giuridicamente rilevanti[5], su cui può essere apposta una firma elettronica semplice, una firma elettronica qualificata o una firma digitale[6].

Ma quale valore attribuire ad un documento così composto?
E' plausibile affermare che la firma elettronica, in tutte le sue tipologie, permetta di assolvere le tre funzioni, innanzi descritte in materia di firma autografa, vale a dire quella indicativa (dell'autore), dichiarativa (dell'accettazione del contenuto dell'atto) e probatoria?

La firma elettronica, definita dall'art. 1 del D. Lgs. 82/2005 (Codice dell'Amministrazione Digitale, di seguito CAD) come l'insieme dei dati in forma elettronica, allegati o connessi tramite un'associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica, costituisce una forma debole di firma, in quanto non si avvale di meccanismi di autenticazione del firmatario o idonei ad assicurare l'integrità del documento. Dunque essa è liberamente valutabile in giudizio.

La funzione indicativa e quella dichiarativa sono, invece, assolte dalla firma elettronica avanzata, la quale è composta da un insieme di dati in forma elettronica, creati con mezzi sui quali il firmatario conserva un controllo esclusivo e i quali garantiscono l'identificazione e la connessione univoca tra firmatario e documento informatico.

Per quanto attiene, invece, all'aspetto probatorio, la soluzione a tale quesito non poteva non tener conto di un dato immediatamente tangibile di diversità tra firma autografa e firma digitale.

La prima è indissolubilmente legata alla persona del sottoscrittore: se la parte deve apporre la sottoscrizione di propria pugno, deve necessariamente partecipare all'atto, in quanto nessun altro può intervenire per firmare con il suo

4 Il documento informatico risponde alla nozione di documento come mezzo materiale di rappresentazione di atti o fatti, in cui la materialità consiste nella fisicità degli impulsi elettronici impressi sui supporti.
5 E' questa la definizione dell'art. 1 del D.P.R. del 28 dicembre 2000 n 445.
6 La firma digitale costituisce una tipologia della firma elettronica qualificata.

nome e cognome. D'altronde sarebbe facilmente rilevabile la divergenza tra la firma autentica e la firma falsificata.

Diversamente l'apposizione della firma digitale, che è composta da una sequenza alfanumerica crittografica di byte, potrebbe sfuggire alla diretta partecipazione del titolare della stessa. Difatti l'attività di digitazione di dati informatici potrebbe anche essere compiuta da un terzo, senza che vi sia un segno evidente di tale sostituzione, e anche all'insaputa del titolare della firma digitale medesima.

Pertanto il pericolo di un'abusiva apposizione della firma digitale e la inidoneità della firma digitale a provare, in maniera assoluta ed inconfutabile, che il sottoscrivente sia il reale titolare, hanno condotto il legislatore, a riconoscere l'efficacia di mera scrittura privata, ai sensi dell'art. 2702 c.c., al documento sottoscritto con firma avanzata, qualificata o digitale, formato nel rispetto delle regole tecniche che garantiscono l'identificabilità dell'autore, l'integrità e l'immodificabilità del documento (art. 21, secondo comma del CAD)[7]. L'art. 21 succitato ha, quindi, previsto che l'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.

Il conferimento al documento informatico del solo effetto della scrittura privata consente al titolare di rifiutare la paternità del documento, dando prova del "furto" di identità digitale, o di sottrazione dei codici identificativi, nonostante le misure di sicurezza adottate ai sensi dell'art. 32 del CAD.

In realtà, il rinvio dell'art. 21 del CAD all'art. 2702 c.c. appare improprio in quanto quest'ultimo articolo riserva al titolare la possibilità di disconoscimento della firma olografa, mentre la firma digitale non pone un problema di autenticità in senso stretto e di formale titolarità. Difatti, la connessione della firma digitale al titolare del dispositivo di firma è certa ed inequivocabile, per cui non è possibile un disconoscimento, ma, in tale ipotesi, emerge un problema di

7 Originariamente, l'art. 6 del D. Lgs. 23 febbraio 2002 n. 10 aveva attribuito al documento sottoscritto con la firma digitale o con altro tipo di firma elettronica avanzata valenza di piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritto, vale a dire il valore probatorio di un atto pubblico o di una scrittura privata autenticata.

abusiva appropriazione, data la prospettazione dei pericoli di furto dell'identità digitale e di utilizzo indebito dei dispositivi di firma.

Il legislatore ha, quindi, posto sullo stesso piano due situazioni in realtà intrinsecamente differenti, allo scopo, però, di tutelare, in senso lato, la reale riconducibilità del documento al titolare della firma. Egli ha attribuito ad un soggetto la possibilità di disconoscere la firma recante il suo nome e cognome, apposta su una scrittura privata cartacea, così come ha riconosciuto il potere al titolare di una firma digitale di dimostrare di non aver personalmente apposto e non aver autorizzato nessuno ad apporre la sua firma, escludendo così la paternità del documento medesimo.

Si vengono a delineare le medesime dinamiche esistenti nel mondo analogico.

Sotto il profilo probatorio, il documento informatico corredato da firma digitale, al pari della scrittura privata, rappresenta una fattispecie del tutto contestabile e compromettibile.

Salve le ipotesi di querela di falso, la non ripudiabilità del documento informatico può essere conseguita solo con l'autenticazione della firma digitale medesima o con la redazione dell'atto pubblico informatico.

Difatti, ai sensi dell'art. 25 del CAD, l'autentica delle firme digitali da parte del pubblico ufficiale, oltre a garantire la legittimità del contenuto dell'atto, scagiona ogni ipotesi di illegittima sottrazione del dispositivo di firma, certificando la provenienza della firma medesima da parte dell'effettivo titolare, ed elimina la possibilità di future contestazioni relative alla vigenza dei certificati di firma al momento della sottoscrizione[8], assicurando la validità del certificato di firma nel momento dell'apposizione della firma digitale.

Sia nell'autenticazione delle firme, sia nella redazione di un atto pubblico informatico, il pubblico ufficiale dovrà utilizzare un sistema informatico che renda visibile e verificabile la generazione delle firma digitali sul documento medesimo, dovrà predisporre un documento non falsificabile e statico e che

8 La conseguenza è rilevante dato che l'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso, equivale a mancata sottoscrizione.

consenta di rilevare e registrare ciò che può essere stato aggiunto dopo le sottoscrizioni[9], garantendo così la non modificabilità del documento e la tutela della volontà delle parti.

3. Dalla firma digitale alla firma grafo metrica e all'utilizzo dei dati biometrici. La sottoscrizione di un contratto con firma digitale presenta, però, degli inconvenienti.

In primo luogo, è necessario che ogni parte del contratto abbia acquistato il dispositivo di firma, sostenendo i relativi costi, da un'autorità di certificazione abilitata al rilascio e che essa sia ancora valida. L'acquisizione comporta, inoltre, per il titolare, l'adempimento di oneri di custodia relativamente al dispositivo di firma e il pin di accesso. La realtà è che la firma digitale è diffusa in ambito professionale e aziendale, ma è ancora avvertita da molti come uno strumento non indispensabile e di complessa fruibilità.

In secondo luogo la sottoscrizione di un contratto con firma digitale richiede l' interoperabilità tra i vari sistemi di firma digitale. Spesso, però, il sistema operativo utilizzato non adopera lo stesso linguaggio dei software connessi alle varie firme digitali, non riconoscendo detti sistemi di firma e impedendo, così, il perfezionamento del contratto.

In terzo luogo, la mancata percezione da parte dei titolari della firma digitale come propria sottoscrizione ha indotto gli stessi, più o meno consapevolmente, a concedere a terzi l'utilizzo della smart card e del relativo codice, determinando la crescita dei casi di utilizzazione indebita.

Tali criticità hanno costituito il terreno fertile per la nascita e la diffusione della firma grafometrica.

La firma grafometrica consiste nella trasposizione della propria sottoscrizione olografa su un dispositivo elettronico (tablet). Essa può valere non solo a riprodurre la firma del sottoscrivente come se il tablet fosse un foglio di carta, ma anche a rivelare ulteriori connotati relativi alla persona che

9 Tale obiettivo viene conseguito mediante l' implementazione del pdf/a, parte dello standard ISO 32000.

sottoscrive. I dispositivi, infatti, sono in grado di acquisire un insieme di altri dati biometrici di natura identificativa, rientranti nella categoria delle caratteristiche biometriche comportamentali[10], vale a dire la velocità di tracciamento, l'accelerazione, la pressione, le inclinazioni, i salti in volo.

I dati biometrici[11] consentono in modo univoco di individuare il titolare, evidenziando la connessione necessaria e universale tra corpo e identità.

Per tali ragioni, originariamente, la firma grafometrica era stata introdotta per accompagnare la firma digitale, al fine di aumentarne il livello di sicurezza; in un secondo momento, essa è stata considerata come autonomo strumento di identificazione o di sottoscrizione.

La firma grafometrica si mostra come un mezzo più vantaggioso, in termini di comodità e immediatezza, rispetto alla firma digitale.

Essa consente con più facilità di concludere un contratto con strumenti digitali, perché non richiede la titolarità di alcun dispositivo di firma, non può comportare problemi di comunicazione tra i sistemi informatici e non può dar luogo a fenomeni di utilizzo dei dispositivi di firma da parte di terzi.

Inoltre la stretta affinità con la firma autografa favorisce la diffusione di tale modalità di conclusione di contratti.

Per rintracciare il valore probatorio della firma grafometrica è necessario individuare la sua natura giuridica.

---

10 Nella biometria è possibile distinguere due categorie: la biometria fisica, basata sulla estrazione di dati da caratteristiche anatomiche del soggetto, quali l'iride, l'impronta digitale, le caratteristiche del volto, e la biometria comportamentale, basata su elementi attinenti al comportamento di uno specifico soggetto, quali l'emissione della voce e l'apposizione di una firma: *Linee guida in materia di riconoscimento biometrico e firma grafometrica*, Allegato A al Provvedimento del Garante del 12 novembre 2014.

11 I dati biometrici sono definiti dal Regolamento 2016/679 del Parlamento europeo e del Consiglio come «dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o ne confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici». Tra questi si ricorda l'impronta digitale, la topografia della mano o il riconoscimento dell'iride. L'utilizzo dei dati biometrici è oggi molto diffuso non solo per la sottoscrizione di documenti informatici, ma anche per l'accertamento dell'identità personale, per il controllo di accessi a locali o aree, per l'attivazione di dispositivi elettronici. La questione ha suscitato anche l'interesse del *Working Party Article 29*, un organismo consultivo e indipendente di rilevanza comunitaria, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione.

Senza dubbio, essa costituisce una tipologia di firma elettronica, quale insieme dei dati in forma elettronica, allegati oppure connessi ad altri dati elettronici.

La firma *de qua* ha, tuttavia, la possibilità di potenziare il suo valore giuridico e l'effetto probatorio, qualificandosi come firma elettronica avanzata. In tal caso sarà determinante che le modalità di generazione, apposizione e verifica delle firme rispettino i requisiti soggettivi ed oggettivi richiesti per le firme avanzate. Alla base dell'acquisizione della firma biometrica vi dovrà essere un processo che garantisca l'identificazione univoca del firmatario e l'integrità del documento, anche nella fase di conservazione.

Vi è quindi una differenza, sotto il profilo probatorio, tra la firma grafometrica quale mero tratto grafico apposto su un tablet, senza che vi sia alcuna registrazione di dati biometrici, e la firma grafometrica su dispositivo che ne conserva ed elabora i dati, e ne garantisce la riconducibilità al titolare.

Nel primo caso, essa sarà liberamente valutabile in giudizio; nel secondo caso, essa farà piena prova, fino a querela di falso, della provenienza della dichiarazione, salvo il disconoscimento.

In ogni caso, in entrambe le ipotesi, l'accertamento della veridicità della sottoscrizione sarà più simile a quello compiuto in caso di firma autografa. Difatti il recupero del segno grafico comporterà anche il ritorno alle tradizionali metodologie di verifica dell'autenticità della firma e il perito potrà inoltre usufruire delle ulteriori informazioni fornite dai dati biometrici scaturenti direttamente dalla firma biometrica.

4. Le minacce cyber derivanti dall'uso della firma grafometrica. L'utilizzo della firma grafometrica e dei dati biometrici pone degli evidenti pericoli di tutela della riservatezza dei dati personali.

Non a caso l'art. 31 del Codice in materia di protezione dei dati personali dispone che detti dati, oggetto di trattamento, devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in

modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Purtroppo l'acquisizione non consentita di dati biometrici non è mai fine a se stessa, ma strumentale al compimento di ulteriori illeciti. Tra questi, appaiono significativi il trattamento illecito di detti dati per fini discriminatori o di controllo sociale, il furto d'identità digitale, la falsificazione della firma biometrica.

4.1 Il trattamento illecito dei dati biometrici. I dati biometrici sono degli identificatori universali, legati univocamente ad un determinato soggetto. Alcuni di essi denotano lo stato di salute, l'etnia di appartenenza, le caratteristiche fisiche di un utente.

La raccolta di detti dati potrebbe avvenire per realizzare degli scopi non dichiarati e illegittimi. Difatti, in assenza di misure preventive e di controllo, nulla impedisce ad istituzioni e privati di acquisire i dati biometrici e di combinarli con altri dati sensibili, ricavati da banche dati differenti, al fine di tracciare un profilo completo del soggetto di riferimento.

La conoscenza degli elementi fisici e comportamentali rappresenterebbe un'arma pericolosa nelle mani dei titolari del trattamento, i quali potrebbero attuare politiche di discriminazione o di controllo e condizionamento indiretto. A livello macroscopico, sarebbe possibile seguire gli spostamenti degli utenti in via generalizzata, compromettendone la privacy.

Paradossalmente, la biometria perderebbe la sua funzione di risorsa per la sicurezza semplificata e si tradurrebbe in una forma di controllo da parte di terzi.

4.2 Il furto d'identità digitale. Il termine di identità comprende due accezioni: una che attiene intimamente al soggetto e l'altra connessa all'appartenenza dell'individuo alla collettività.

Si fa riferimento, quindi, sia alla qualità del soggetto che, in termini oggettivi, consente la sua individuazione, sia alla proiezione sociale della sua personalità[12].

Se l'identità personale ha tale doppia valenza, è chiaro che anche l'interesse sotteso alla sua tutela non può che essere doppio. Il legislatore, difatti, intende garantire non solo il diritto del soggetto titolare di essere riconosciuto, ma anche l'interesse dei terzi alla corretta identificazione dei consociati[13]. Si vuole salvaguardare la persona e la pubblica fede, la quale può essere violata da inganni relativi alla vera essenza della persona e delle sue azioni.

Ma se per diritto all' identità si intende l'interesse del soggetto ad essere rappresentato nella vita di relazione con i suoi connotati, a non veder alterato il proprio patrimonio intellettuale, religioso, ideologico, a non veder disconosciuta la paternità delle proprie azioni o a non vedersi attribuita la titolarità di azioni altrui, allora non può non essere ricompresa, nella nozione di identità personale, anche quella digitale, quale manifestazione del soggetto nelle attività informatiche e nel web.

Anche l'identità digitale presenta un doppio volto: essa può manifestarsi nella rappresentazione sul web di un soggetto e può ridursi all'insieme dei codici elettronici che consentono l'identificazione del soggetto nei sistemi informatici, in virtù di una correlazione tra tali cifre e l'utente[14]. I codici elettronici

12 La giurisprudenza ha ricondotto il diritto all'identità nella categoria dei diritti fondamentali, come tutelati dall'art. 2 della Costituzione, espressione del libero e integrale svolgimento della persona umana: Cass. civ., 22 giugno 1985, n. 3769, in *CED Cassazione;* Cass. civ., 7 febbraio 1996, n. 978, in *Foro it.*, 1996, c. 1253.

13 In realtà la nozione di identità personale si è, nel tempo, riempita di significato. Originariamente il bene tutelato era quello della individualità, ai fini di una corretta identificazione del soggetto quale autore di una determinata prestazione o attività: la tutela dei diritti soggettivi, protetti legislativamente dalle *property rules* (cfr. art. 7 c.c. e art. 10 c.c.; in Germania par. 12 BGB), era rimessa all'intervento autonomo dei singoli. Successivamente, acquisisce rilevanza la dimensione sociale della personalità e la sua esplicazione nei rapporti con i terzi. L'ordinamento si attribuisce un ruolo di controllo, per assicurare il rispetto dell'identità di ciascun soggetto.

14 La rilevanza dell'identificazione digitale è evidente anche in ambito europeo. Il recente Regolamento EIDAS (*Electronic, Identification, Authentication, Signature)* promuove un mercato unico digitale, mediante la creazione di un quadro giuridico uniforme per le firme elettroniche, i documenti elettronici e i servizi relativi ai certificati di autenticazione dei siti web, pur lasciando ogni Paese libero di creare il proprio sistema di identificazione elettronica. L'Agenda Digitale del

possono consistere in parole chiave (password), componenti biologiche (impronta digitale o vocale, riconoscimento del volto, iride) o elettroniche connesse a dispositivi (smart card, tessere magnetiche).

Il furto di identità digitale si configura, quindi, come l'appropriazione da parte di soggetti non legittimati degli elementi che consentono sul web il riconoscimento del soggetto, nonché dei suoi codici elettronici e delle sue caratteristiche biometriche.

Differenti possono essere le modalità attraverso cui si realizza il furto d'identità: si possono captare informazioni personali mediante l'*hackeraggio* dei sistemi telematici, attraverso condotte fraudolenti (*phishing*), quali l'invio di e-mail da fittizi istituti bancari, o mediante estrapolazione di dati da documenti smarriti.

Anche in tali casi, il danno è cagionato non solo al titolare dei dati, che perde il suo profilo in rete e in maniera definitiva, in quanto i dati denotano l'utente in maniera esclusiva, ma anche alla collettività, che non ha più alcuno strumento per individuare tale soggetto e il suo operato.

La tutela dell'identità digitale è sancita dall'art. 494 c.p. che sanziona con la reclusione fino ad un anno la condotta di chi, al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome, stato, qualità cui la legge attribuisce un effetto giuridico.

La Suprema Corte ha specificato che il reato di sostituzione di persona ai sensi dell'art. 494 c.p. può essere compiuto in rete, mediante l'indebito utilizzo degli account personali[15].

E' evidente che l'oggetto del furto può essere rappresentato da qualsiasi connotazione identificativa, non solo da password e codici utenti, ma anche dall'insieme dei dati biometrici e degli elementi sottesi alla firma grafometrica.

Governo Italiano ha, invece, introdotto lo SPID, vale a dire un sistema che consentirà di realizzare la propria identità digitale, mediante una corrispondenza biunivoca tra soggetto e dati personali, i quali potranno essere utilizzati per accedere automaticamente ad altre piattaforme web.

15 Cass. pen., 14 dicembre 2007, n. 46674, in *Dir. Internet,* 2008, 3, 249; Cass. pen., 3 aprile 2012, n. 12479, in *CED Cassazione*, 2012.

Le conseguenze dannose si moltiplicano quando il furto d'identità digitale diviene funzionale al compimento di altri reati, generalmente contro il patrimonio, o costituisce una forma di aggravante di altri illeciti penali[16].

E' il caso del reato di frode informatica, che può essere "accompagnato", ai sensi dell'art. 640 *ter* c.p., dal furto o dall'indebito utilizzo dell'identità digitale, integrando la fattispecie del concorso formale tra reati.

Il *phishing*, ad esempio, costituisce una tipologia di frode informatica e si realizza mediante la sottrazione dei dati elettronici e biometrici, correlati, ad esempio, ai servizi di *home banking*, da parte degli autori dell'illecito, i quali, in un secondo momento, li utilizzano per realizzare spostamenti di denaro e accrediti non autorizzati. Si può realizzare una frode informatica anche mediante l'intercettazione dei flussi dei dati della vittima e il reindirizzamento automatico su siti web fraudolenti, simili a quelli da lei abitualmente consultati per effettuare acquisti *on line*.

Ricorre il concorso di reati anche tra il delitto di cui all'art. 494 c.p. e l'illecito di cui all'art. 615 *ter* c.p., consistente nell'accesso abusivo in un sistema informatico protetto da misure di sicurezza.

4.3 La falsificazione della firma biometrica. L'utilizzo di dispositivi che raccolgono i dati biometrici dovrebbe avvenire in modo tale da escludere che dal modello acquisito si possa ricavare il campione biometrico.

Il processo di raccolta dei dati dovrebbe, infatti, essere unico e irreversibile.

Il rischio di una registrazione e successiva elaborazione dei dati è che si dia luogo ad una riproduzione non autorizzata dei dati biometrici, utilizzabili al di fuori del contesto nel quale sono stati legittimamente raccolti.

Oltre al rischio della riproduzione, vi è anche quello della falsificazione biometrica, vale a dire della creazione di caratteristiche biometriche artificiali a

16 Non meno diffuse sono le fattispecie aventi ad oggetto condotte prodromiche alla sostituzione di persona con furto d'identità: si fa riferimento alla diffusione di programmi informatici (virus) aventi come scopo quello di alterare il sistema informatico, ad esempio acquisendo le credenziali di accesso, di cui all'art. 615 *quinquies* c.p.

partire da elementi biometrici esistenti. Se dalla manipolazione delle caratteristiche biometriche registrate è possibile ottenere nuove identità digitali, è evidente il pericolo del compimento di truffe e scambi d'identità.

5 Le misure preventive. Di fronte alle minacce di furto d'identità e di trattamento illecito dei dati biometrici, si è ravvisata la necessità della predisposizione di una regolamentazione per l'adozione di misure di protezione e di un apparato cautelare.

L'Autorità Garante per la Protezione dei Dati Personali ha emanato delle linee guida in materia di riconoscimento biometrico e firma grafometrica, in allegato al Provvedimento del 12 novembre 2014, in cui ha tracciato un quadro uniforme di riferimento per l'adozione di strumenti tecnologici nel rispetto dei principi di legittimità stabiliti dal Codice e degli standard di sicurezza.

Al fine di impedire che il trattamento dei dati biometrici possa tradursi in una ingerenza eccessiva ed ingiustificata, l'Autorità ha prescritto il rispetto dei criteri di liceità, necessità, finalità e proporzionalità.

La liceità del trattamento da parte di operatori privati implica il preventivo consenso informato dell'interessato, sempre revocabile e libero da qualsiasi condizionamento, manifestato in forma libera ed espressa[17]. Ai sensi dell'art. 13 del Codice, l'informativa deve specificare le finalità perseguite, le modalità di trattamento e i tempi di conservazione dei dati, la natura obbligatoria o facoltativa del conferimento dei dati e la possibilità di avvalersi di procedure alternative, i soggetti ai quali i dati personali possono essere comunicati.
Se il dispositivo è nella esclusiva disponibilità dell'interessato, l'informativa deve riguardare anche la custodia e gli adempimenti conseguenti al suo smarrimento, alla sottrazione e al malfunzionamento.

La necessità del trattamento comporta che la finalità indicata non è conseguibile in via anonima, ma richiede inevitabilmente l'identificazione

17 Il consenso non è richiesto nei casi in cui il Garante non lo ritenga opportuno, in virtù della prevalenza dell'interesse del titolare del trattamento, con apposito provvedimento.

dell'interessato. L'utilizzazione dei dati personali biometrici è quindi imprescindibile.

Il trattamento dei dati biometrici è, inoltre, ammesso solo per le finalità comunicate: non è possibile estrarre dati ulteriori rispetto a quelli necessari per conseguire gli scopi menzionati, né utilizzare i dati registrati lecitamente per operazioni di trattamento incompatibili con quelle consentite.

La raccolta dei dati biometrici è incentrata sul principio di minimizzazione, per cui non è consentita l'acquisizione di dati non pertinenti e ulteriori rispetto a quelli essenziali per le finalità da perseguire.

In secondo luogo, l'Autorità ha imposto una serie di adempimenti giuridici prima dell'inizio del trattamento. Difatti essa richiede al titolare del trattamento dei dati biometrici[18] un'apposita notifica al Garante e, per il trattamento di dati diversi da quelli sensibili e giudiziari, che può cagionare la lesione dei diritti e delle libertà fondamentali, la presentazione di un'apposita richiesta di verifica preliminare, con indicazione dell'analisi dei rischi e le modalità con cui intende garantire il rispetto delle misure di carattere generale, degli adempimenti giuridici e delle misure di sicurezza. Il Garante può prescrivere misure e accorgimenti specifici per consentire il corretto utilizzo dei dati.

L'Autorità ha, però, individuato delle tipologie di trattamento meno rischiose, in relazione alla tipologia dei dati trattati, alle finalità perseguite e le misure di sicurezza adottabili, per le quali ha escluso la necessità della verifica preventiva, imponendo, tuttavia, anche per tali trattamenti, l'adozione di tutti gli accorgimenti essenziali per garantirne la sicurezza, il rispetto dei presupposti di legittimità imposti dal Codice e l'obbligo di notifica al Garante e di informativa all'utente.

In tale categoria di trattamenti esenti, è presente quello relativo all'apposizione della firma grafometrica.

Il Provvedimento in tema di biometria dell'Autorità Garante del 12 novembre 2014 esclude la necessità della verifica preliminare per l'utilizzo di

18 Ai sensi dell'art. 37 del Codice in materia di protezione dei dati personali, sono escluse determinate categorie di soggetti in ragione dell'attività svolta.

sistemi di firma grafometrica, ma solo se essi posseggono i connotati del meccanismo della firma elettronica avanzata.

Il sistema di firma grafometrica deve, cioè, apportare le medesime garanzie della firma elettronica avanzata, vale a dire deve assicurare l'autenticità e l'integrità dei documenti e tutelare i dati dai rischi di furto e tentativi di frode.

A tal fine, sarà necessario, preliminarmente, identificare il firmatario, utilizzare dispositivi che non conservino i dati biometrici raccolti, ma siano programmati in modo tale che essi vengano cancellati automaticamente una volta completata la sottoscrizione, pur garantendo la memorizzazione degli stessi all'interno dei documenti informatici, e sarà essenziale prevedere sistemi alternativi di sottoscrizione non basati sulla disposizione di dati biometrici.

Anche la redazione degli atti pubblici e le autentiche delle scritture private con firma grafometrica è ormai ammessa, in seguito al Provvedimento dell'Autorità Garante del 25 novembre 2015. Il sistema predisposto dai pubblici ufficiali, come verificato dall'Autorità, permette che i dati biometrici relativi alla sottoscrizione (posizione, pressione, inclinazione, velocità) vengano, unitamente al tratto grafico della firma, acquisiti dal documento informatico, per poi essere completamente cancellati dai dispositivi. Anche in tali ipotesi, configurandosi un trattamento di dati sensibili, non si potrà prescindere dall'informazione preventiva ai sottoscriventi, dalla presenza di sistemi alternativi di sottoscrizione e dal consenso al trattamento dei dati.

6. Note conclusive. Il passaggio dalla firma elettronica alla firma grafometrica mette in evidenza come il processo di dematerializzazione del corpo sia stato posto a servizio della conclusione dei negozi giuridici.

I dati biometrici hanno una forte capacità distintiva, ma il legame corpo-informazione pone delle implicazioni rilevanti per la *cybersecurity*. I rischi di frode informatica, di furto d'identità nonché di trattamento illecito dei dati sono già stati analizzati dall'Autorità Garante per la Protezione dei Dati Personali. Tuttavia, in una realtà complessa come quella digitale, le fattispecie criminose e

le relative modalità di attuazione possono assumere sempre nuovi contorni. Ecco perché appare opportuno che i fenomeni connessi all'uso dei dati elettronici e biometrici siano costantemente sotto osservazione, in modo tale da elaborare tempestivamente, qualora fosse opportuno, una linea difensiva e da prevenire la reiterazione degli illeciti, predisponendo adeguate misure di prevenzione.

Riferimenti bibliografici

G. BAVETTA, voce *Identità (diritto alla)*, in *Enc. dir.,* vol. XIX, Giuffrè Editore, Milano, 1970.
C. M. BIANCA, *Diritto civile*, *Il contratto*, Giuffrè Editore, Milano, 2000.
F. CAJANI, *La tutela penale dell'identità digitale alla luce delle novità introdotte dal d.l. 14 agosto 2013 n. 93*, in *Cass. pen*., 3, 2014.
B. CARPINO, voce *Scrittura privata*, in *Enc. dir.*, vol. XLI, Giuffrè Editore, Milano, 1989.
P. CIPOLLA, *Social network, furto d'identità e reati contro il patrimonio*, in *Giur. merito*, 12, 2012.
R. CLARIZIA, *Informatica e conclusione del contratto*, Giuffrè Editore, Milano, 1985.
F. COCUCCIO, *Il diritto all'identità personale e l'identità "digitale"*, in *Dir. famiglia*, 3, 2016.
CONSIGLIO NAZIONALE DEL NOTARIATO, Studio n. 3- 2006 /IG, *Codice dell'amministrazione digitale, firme elettroniche e attività notarile*, (est. M. Nastri), in *Studi e Materiali*, 2006.
L. CUOMO, *Profili giuridici del trattamento biometrico dei dati,* in *Riv. it. med. leg.*, 1, 2014.
F. DELL'AVERSANA, *Documento e firme elettroniche: dal digitale alla grafometria*, Notartel, Roma, 2016.
G. FALCO, voce *Identità personale*, in *Nuovo Dig. it.*, vol. VI, Utet, Torino, 1938.
R. GENGHINI, *Atti pubblici in forma digitale*, in L. GENGHINI, *La forma degli atti notarili*, Cedam, Padova, 2010.
A. GENTILI, *I documenti informatici: validità ed efficacia probatoria*, in *Dir. internet*, 2006, 3.
G. GIACOBBE, *L'identità personale tra dottrina e giurisprudenza. Diritto sostanziale e strumenti di tutela*, in AA.VV., *La lesione dell'identità personale e il danno non patrimoniale*, Giuffrè Editore, Milano, 1985.
G. RESTA, *Identità personale e identità digitale*, in *Dir. informatica*, 3, 2007.
B. SANTACROCE, *Dalla firma digitale alla firma biometrica: quadro giuridico di riferimento per l'applicazione dei nuovi dispositivi di firma,* in P. RIDOLFI (a cura di), *Il nuovo CAD. Commenti e prospettive. Atti del Convegno dell'8 luglio 2011. Roma, Accademia dei Lincei*, Fondazione Siav Academy, Rubano, 2011.
A. TORRENTE - P. SCHLESINGER, *Manuale di diritto privato*, Giuffrè Editore, Torino, 2015