ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

3 MAGGIO 2023

Ambiti di interesse per la regolazione delle economie dei dati nel rapporto tra diritto e tecnologia

di Agostino Sola
Dottorando di ricerca in *Law & Business*
Università Luiss Guido Carli

Ambiti di interesse per la regolazione delle economie dei dati nel rapporto tra diritto e tecnologia*

di Agostino Sola
Dottorando di ricerca in *Law & Business*
Università Luiss Guido Carli

Abstract [It]: L'articolo osserva le principali conseguenze giuridiche derivanti dall'acquisita centralità economica dei dati e delle moderne tecniche di sfruttamento. In particolare, si prendono come riferimento le tradizionali discipline della *privacy*, della tutela dei consumatori e della concorrenza osservandone le evoluzioni e proponendone un'analisi tramite lo studio della normativa e della giurisprudenza. L'utilizzo con finalità economiche dei dati si connota per la crescente interdisciplinarietà e complementarietà degli interessi coinvolti che determina importanti mutamenti dell'azione amministrativa con finalità di regolazione tanto con riferimento alle competenze già esistenti (nel senso della necessità di un loro coordinamento) quanto con riferimento all'emersione di nuove autorità di tutela. Quest'ultimo profilo sarà oggetto di approfondimento specifico con riferimento all'evoluzione della disciplina della *cybersicurezza*.

Title: Areas of interest for the regulation of data economies in the relationship between law and technology
Abstract [En]: The article observes the main legal consequences arising from the economic centrality acquired by data and the modern exploitation techniques. Traditional disciplines of privacy, consumer protection and competition are taken as reference by observing their evolutions and proposing an analysis through the study of legislation and case law. The use with economic purposes of data is connoted by the growing interdisciplinary and complementary nature of the interests involved, which determines important changes in administrative action with regulatory purposes both with reference to already existing competencies (in the sense of the need for their coordination) and with reference to the emergence of new protection authorities. The latter profile will be the subject of specific in-depth study with reference to the evolution of the cybersecurity discipline.

Parole chiave: economie dei dati; diritto e tecnologia; competenze amministrative; privacy; antitrust; cybersicurezza; tutela del consumatore
Keywords: data economics; law and technology; administrative competences; privacy; antitrust; cybersecurity; consumer protection

* Articolo sottoposto a referaggio.

1. Introduzione: diritto e tecnologia nella centralità dei dati

Il progresso tecnologico delle società, qui da intendersi in senso lato, è sempre stato influenzato dalla scienza e dalla tecnica e, con esse, dalla minore o maggiore disponibilità di dati. L'evoluzione tecnologica offre sempre nuovi dati e sempre nuove capacità di elaborazione: senza adeguata tecnologia, infatti, l'acquisizione di grandi quantità di dati – inintelligibili alla conoscenza umana - rimarrebbe fine a se stessa e priva di qualsiasi utilità pratica e, quindi, di rilevanza economica.

In questo contesto il ruolo delle amministrazioni pubbliche nella regolazione delle economie dei dati muta e deve essere correttamente contestualizzato nel più ampio rapporto tra tecnologia e diritto.

L'evoluzione tecnologica, grazie al progresso della tecnica,[1] ha da sempre interessato anche il diritto, intrecciandosi in un profondo legame che li rende assolutamente permeabili alle novità, l'uno dell'altro.[2]

Il diritto, non soltanto amministrativo, sta risentendo profondamente della trasformazione in essere della società contemporanea derivante dallo sviluppo dell'informatica e dell'intelligenza artificiale.

Da una parte, infatti, la tecnologia influenza la quotidianità dei rapporti giuridici[3],e, per quanto d'interesse, è anche la pubblica amministrazione ad utilizzare l'evoluzione tecnologica per il perseguimento dei propri fini. Nel contesto di riferimento, infatti, la tecnologia interagisce con il diritto offrendogli strumenti innovativi per il perseguimento delle proprie finalità[4] ed anche la pubblica amministrazione sta subendo l'influenza di questi nuovi modelli decisionali basati sui dati poiché ne percepisce l'utilità per il perseguimento degli interessi pubblici tramite la possibile individuazione di inediti modelli di efficienza

[1] La nozione di tecnologia è, d'altronde, molto ampia. La tecnologia, infatti, ha ad oggetto lo sviluppo e l'applicazione di strumenti tecnici - ossia di quanto è applicabile alla soluzione di problemi pratici, all'ottimizzazione di procedure, all'adozione di decisioni, alla scelta di strategie finalizzate a dati obiettivi – sulla base di conoscenze scientifiche, matematiche e informatiche. Enciclopedia Treccani.it, voce "Tecnologia". È chiaro, dunque, che la concezione del termine varia a seconda del periodo storico di riferimento: è intuitivo comprendere che ciò che secoli fa costituiva un'importante applicazione tecnologica potrebbe non rivestire tale carattere in un'epoca successiva.

[2] Il diritto è, infatti, una scienza sociale e, come tale, risente delle grandi direttrici di cambiamento della società. Il diritto mantiene una funzione ordinatrice anche riguardo ai mutamenti tecnologici e scientifici della società. Si pensi alla crescente sensibilità maturata in ambito ecologico che ha portato ad un ripensamento del diritto ambientale, ad esempio, ovvero all'impatto avuto dall'espansione dell'industria ferroviaria.

[3] Le rivoluzioni scientifiche e tecnologiche contribuiscono a modificare i paradigmi sociali e, quindi, giuridici: portano a trasformazioni anche radicali della società umana e, conseguentemente, del contesto normativo di riferimento. Si pensi, ad esempio, alle questioni di bioetica che il progresso scientifico ha sollevato. In tema di rapporto tra diritto e nuovi sviluppi tecnologici e scientifici, tanto in termini generali quanto con riferimento a specifici fenomeni, si veda A. SANTOSUOSSO, M. TOMASI, *Diritto, scienza e nuove tecnologie*, Wolters Kluwer, 2021.

[4] Si sta facendo riferimento alla previsione dell'adozione di misure di rispetto delle disposizioni di tutela della privacy *by default* e *by design* sin dalle fasi di progettazione delle attività che coinvolgono il trattamento di dati personali. Si tratta dell'incorporazione di specifici principi e norme nella tecnica al fine di conformare l'utilizzo dei sistemi tecnologici al rispetto delle disposizioni normative applicabili.

In tema, F. ROMEO, *Dalla Giuritecnica di Vittorio Frosini alla* Privacy by Design*,* in *Informatica e diritto,* 2/2016, p. 9-23 richiamata da F. FAINI, *op. ult. cit., p. 17*. In realtà, occorre osservare che l'adozione di misure di rispetto delle disposizioni normative, applicabili già nella fase di progettazione delle attività (tanto umane quanto tecnologiche), è presente anche nelle disposizioni in tema di *cybersicurezza*.

dell'azione pubblica basata sui dati, ciò con riferimento alla digitalizzazione dei processi decisionali pubblici ovvero nell'offerta di nuovi servizi pubblici.[5]

Ma non soltanto. Il progresso tecnologico, con l'emersione di fenomeni inediti, conduce ad un adattamento delle regole per disciplinare le nuove possibilità offerte dall'evoluzione tecnologica[6] e per governare realtà economiche, sociali e politiche, plasmate dal cambiamento tecnico-scientifico.[7]

In tale contesto, ad esempio, l'azione amministrativa si confronta con posizioni soggettive e fenomeni inediti, manifestazioni della *data driven innovation*: il sorgere di nuovi interessi e nuove dinamiche impone una regolamentazione delle situazioni create dal progresso, tanto mediante la riformulazione e il ripensamento degli istituti giuridici già esistenti quanto attraverso la creazione di nuove forme di tutela. E su questi profili ci si intende soffermare.

Si osserva ora, nel descritto contesto, l'impatto che le economie dei dati e, in generale, l'evoluzione tecnologica ha avuto sui principali interessi pubblici coinvolti: dalla modifica del concetto di *privacy* sino all'emersione di nuovi interessi quale quello relativo alla *cybersicurezza*.

2. Cenni sull'evoluzione della nozione di *privacy* tra diritto e tecnologia

Tra i profili di maggior interesse relativi alla istanze di regolazione conseguenti alla valorizzazione economica dei dati, pare meritevole di considerazione la riflessione che si va sviluppando in relazione all'evoluzione del concetto stesso di *privacy*.[8] Si tratta, infatti, di un cambiamento giuridico dettato, inevitabilmente, dallo sviluppo tecnologico.[9] In questo contesto, la categoria giuridica della *privacy* si è andata modificando in risposta alla necessità di adeguamento del diritto alle istanze di tutela avanzate in

[5] Sul tema si sta concentrando l'attenzione della dottrina, cui si rimanda per una trattazione più ampia ed esaustiva. In particolare, sul tema dell'applicazione delle tecnologie informatiche all'attività amministrativa, R. CAVALLO PERIN, D.U. GALETTA (a cura di) *Il diritto dell'amministrazione pubblica digitale*, Giappichelli, 2020; con riferimento all'utilizzo dei *big data* nei processi decisionali pubblici si richiama F. COSTANTINO, *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei big data,* in *Diritto Pubblico,* 1/2019, p. 43; M. TRESCA, *Big data, Open data e algoritmi: i dati del servizio della pubblica amministrazione [Lo "Stato digitale"]*, in *Riv. Trim. Dir. Pubbl.,* 2/2021, p. 545; ma sia consentito anche il richiamo ad A. SOLA, *Utilizzo di big data nelle decisioni pubbliche tra innovazione e tutela della privacy*, in *Medialaws,* 3/2020.

[6] In tema F. FAINI, *Diritto e tecnologia. Il diritto dell'informatica,* in F. FAINI – S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche,* Giappichelli, 2021.

[7] Così ricorda M. MAGGIOLINO, *I big data e il diritto antitrust,* Egea, 2018, p. 5. L'obiettivo del legislatore, alla prova dell'innovazione, è quello di ridurre il "*gap between technological develpomentes and public policy*" (OECD, *Going Digital: shaping policy, improving lives*, 2019, p. 18.

[8] In tema, *ex multis,* F. PIZZETTI, *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Giappichelli, 2021; R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, Giuffrè, 2003; R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario alla Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy): scritti in memoria di Stefano Rodotà*, Giuffrè - Francis Lefebvre, 2019.

[9] In tema di deve ricordare la Convenzione di Strasburgo n. 108/1981, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*, considerata uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato dei dati personali, nonché il primo strumento normativo in materia di tutela dei dati sul quale si sono fondati i successivi interventi, normativi e giurisprudenziali, in relazione agli effetti delle evoluzioni tecnologiche sulla protezione dei dati personali. In questi termini, G. FORMICI, *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali*, Giappichelli, 2021, p. 40-41.

conseguenza dell'utilizzazione con finalità economiche dei dati personali. Evoluzione impensabile prima dell'avvento delle tecnologie dell'informazione e della comunicazione per come oggi note.

Nel precedente capitolo si sono descritti i principali modelli economici basati sui dati che coinvolgendo dati personali, possono sollevare questioni afferenti alla *privacy*. Ad esempio, la raccolta di dati personali, complice lo sviluppo delle possibilità di estrazione, sta diventando sempre più completa ed accurata, riducendo lo spazio privato dell'individuo.[10] Del pari, le acquisite capacità di archiviazione cristallizzano nel tempo le informazioni acquisite. Le analisi algoritmiche sviluppate sono in grado poi di estrarre sempre nuova conoscenza e portare a un impatto discriminatorio reale sugli individui.[11]

E così, allora, il termine *privacy* viene utilizzato nella duplice accezione di diritto al rispetto della vita privata e diritto alla protezione dei dati personali. Vi è stata una evoluzione della teorizzazione del diritto alla protezione dei dati personali in uno con lo sviluppo delle tecnologie dell'informazione e della comunicazione dalle quali è derivata la diffusa circolazione di dati e informazioni, anche di carattere personale, nonché i conseguenti pericoli per i diritti e le libertà individuali.[12]

In questo contesto, si deve muovere dalla considerazione della *privacy* quale diritto fondamentale riconducibile ai diritti di libertà dell'individuo, secondo l'espresso riconoscimento in tal senso effettuato dalla Carta dei Diritti Fondamentali dell'Unione Europea.[13]

La prima teorizzazione della privacy, nell'accezione di riservatezza, intesa come "*right to be let alone*"[14], ha trovato esplicita tutela nel diritto primario dell'art. 7 della Carta dei Diritti Fondamentali dell'Unione Europea[15] e si è ampliata sino ad essere definita quale diritto al controllo sull'utilizzo e sulla circolazione dei propri dati personali tramite l'articolo 8 (*"Protezione dei dati di carattere personale"*)[16].

---

[10] Un numero crescente di entità, come i rivenditori online, i fornitori di servizi Internet (ISP), i sistemi operativi, i browser, i social media e i motori di ricerca, i fornitori di servizi finanziari (banche, società di carte di credito, ecc.) e gli operatori di telefonia mobile sono in grado di raccogliere grandi quantità di dati. Tale raccolta di dati può essere limitata a un contesto o a una transazione specifica, ma solitamente copre un'ampia gamma di attività economiche e sociali.

[11] La pubblicità comportamentale che si basa sul tracciamento online dei consumatori e sulla raccolta e l'analisi delle relative informazioni personali, al fine di fornire loro una pubblicità adeguata alle loro esigenze e ai loro interessi.

[12] In tema, S. RODOTÀ, *Tecnologia e diritti,* Il Mulino, Bologna, 1995.

[13] Anche in alcune carte costituzionali si trova un esplicito riferimento alla riservatezza anche intesa come controllo sull'utilizzo e sulla circolazione dei propri dati personali: G.C. FERONI, *I dati personali come oggetto di un diritto fondamentale* in P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Giappichelli, 2022, p. 65.

[14] È ritenuta la prima definizione della privacy, espressione DI S. WARREN, L. BRANDEIS, *The right to privacy*, Harvard Law Review, 5/1890. La definizione di privacy, ad oggi, ha impegnato e continua ad impegnare giuristi di tutto il mondo come osserva D.J. SOLOVE, *Conceptualizing Privacy*, *California Law Review*, 90/2002, p. 1088. Già nel 1890, S. WARREN, L. BRANDEIS, *id.*, osservavano come non si potesse dubitare dell'esistenza del diritto individuale ad una "*full protection in person and in property*" il cui contenuto doveva essere indagato "*from time to time to define a new the exact nature and extent of such protection*".

[15] Come noto, alla Carta dei Diritti Fondamentali dell'Unione Europea, cd. Carta di Nizza, è attribuito il medesimo valore giuridico dei Trattati per effetto dell'art. 6 del Trattato di Lisbona. Formalmente, dunque, la Carta ha rango di diritto primario, se non addirittura "*costituzionale*", superiore al trattato, nella misura in cui essa esprime dei principi fondamentali dell'Unione o di alcuni principi generali di diritto.

[16] E' quella che viene definita una nuova dimensione del diritto alla riservatezza mediante la quale viene riconosciuto al singolo "*non il semplice diritto di essere lasciato in pace, ma quello di controllare l'esattezza dei dati che lui stesso ha esternato e, se del caso,*

Sulla scia di tale declinazione si è giunti alla separazione delle due accezioni della *privacy,*[17] se non già alla rappresentazione di due distinti diritti.[18]

Si è registrata, dunque, un'evoluzione del diritto alla riservatezza, inteso come oggetto di tutela prima statica e negativa[19] e poi dinamica e positiva[20], propria dell'adeguamento della dimensione tecnologica del diritto dell'individuo alla riservatezza dei dati personali quale manifestazione del più ampio diritto all'intangibilità della sfera privata.[21]

anche di correggerli, potendo da ultimo avere un interesse qualificato a cancellare quanto di sé aveva un tempo reso pubblico", così G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto Pubblico*, 1/2019, p. 91.

[17] Nel senso che si evidenzia una distinzione terminologia tra le due accezioni, sintomo del fatto che il diritto alla protezione dei dati personali non verrebbe più ad essere ricompreso nella *privacy* ma nella *data protection*, termine ritenuto più specifico: M. GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço Juridico,* 1/2013, p. 152.

[18] Come osserva l'Avvocato Generale Sharpston nelle cause riunite C 92/09 e C 93/09 nelle proprie conclusioni del 18 giugno 2010 (ECLI:EU:C:2010:353) al punto 71. L'evoluzione normativa avrebbe portato alla creazione di "*due diritti distinti: uno classico (tutela della vita privata ai sensi dell'art. 8 della CEDU) e un diritto più moderno (le disposizioni della Convenzione n. 108 relative alla tutela dei dati)*". Analoghi diritti vengono riconosciuti dalla Carta dei Diritti Fondamentali dell'Unione Europea agli artt. 7 e 8.

[19] In questi termini, G. FORMICI, *La disciplina della data retention tra esigenze securitarie e tutela dei diritti fondamentali*, Giappichelli, 2021, p.36 facendo riferimento all'art. 7 ("*Rispetto della vita privata e della vita familiare"*) Carta dei Diritti Fondamentali dell'Unione Europea.

L'accezione negativa della tutela della *privacy* va intesa quale divieto di ingerenza da parte delle autorità pubbliche. Si tratta di un'elaborazione conseguente alla formulazione dell'art. 12 UDHR -Dichiarazione universale dei diritti dell'uomo che ritroviamo anche nell'art. 8 CEDU. In questi termini, F. ROSSI DAL POZZO, *Il mercato unico digitale europeo e il regolamento UE sulla privacy*, in R. CAVALLO – PERIN, D.U. GALETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Giappichelli, 2020, p. 49.

[20] Il carattere positivo della *privacy,* invece, lo si apprezza in relazione al riconoscimento del diritto del singolo alla formazione di una propria sfera privata in cui sviluppare la propria identità personale. Sfera personale che, nella società dell'informazione, è composta anche dalle informazioni disponibili, sulle quali deve essere esercitato un potere di controllo da parte dell'interessato. La prima applicazione pratica di questa "*information privacy"* si rinviene nella citata Convenzione di Strasburgo n. 108/1981, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*. In questi termini, F. ROSSI DAL POZZO, *Il mercato unico digitale europeo e il regolamento UE sulla privacy*, in R. CAVALLO – PERIN, D.U. GALETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Giappichelli, 2020, p. 50-51.

[21] Al punto che la tutela dei dati personali diviene di fondamentale importanza affinché una persona possa godere del proprio diritto al rispetto della vita privata come osservato dalla Corte EDU nella sentenza 4 dicembre 2008, S & Marper/Regno Unito [GC], nn. 30562/04 e 30566/04 (punto 103).

Come in effetti è anche riportato nel considerando 10 DIR. 95/46/CE, la protezione dei dati personali tutela diritti e libertà fondamentali dell'individuo, in particolare del diritto alla vita privata. Nei dati personali, infatti, si identifica e si riconosce l'individualità della persona ma, nonostante ciò, non sono i dati personali in quanto tali a rappresentare l'oggetto del diritto fondamentale dell'individuo ma la loro protezione.

In tal senso, allora, la disciplina di tutela della *privacy* riguarda "*innanzitutto la protezione delle persone fisiche non i dati in sé e per sé considerati; in altri termini, non è tutelato il dato in sé e per sé, ma in via mediata il dato come rappresentazione della persona*", vera e propria "*specificazione del diritto generale della personalità… classificabile come un diritto fondamentale*" (G. ALPA, *La "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR,* Cedam, 2019, p. 11 e ss.).

Tuttavia, osserva sempre l'A., il diritto fondamentale che deriva dalla tutela della *privacy* risulta essere "*condizionato e bilanciato: diverso, quindi, dai diritti costituzionalmente garantiti dagli artt. 2 e 3 della nostra Costituzione, e diverso dai diritti della personalità così come costruiti nel corso di più di un secolo, come diritti assoluti, inalienabili, indisponibili.*".

Il carattere dinamico della tutela e l'interesse pubblico alla circolazione dei dati personali si manifestano altresì nell'istituzione di una specifica autorità indipendente cui affidare poteri di controllo e di intervento in materia.[22]

L'evoluzione della *privacy* ha così adeguato la sfera privata oggetto di tutela al contesto tecnologico di riferimento, facendovi rientrare anche le informazioni che circolano tramite dati. Il rispetto della vita privata ha come corollario il rispetto dei dati personali[23]: in particolar modo, come anticipato, separa il più ampio diritto alla riservatezza distinguendo tra la "*protezione dei dati personali*", la cui portata assiologica è ben definita dall'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea, e la "*privacy*", intesa come riservatezza, tutelata ai sensi dell'art. 7.

In termini generali, come accennato, l'evoluzione della concezione della privacy, qui brevemente descritta, è paradigmatica in quanto ha portato al riconoscimento di un valore economico, diretto o indiretto, da attribuire alla circolazione dei dati personali,[24] aprendo alla loro patrimonializzazione nei modelli economici *data driven*. Questa prima tesi ci è utile per introdurre il concetto dell'utilizzo economico dei dati personali e per osservare l'impatto della tecnologia sulle categorie ordinamentali del giudizio.

2.a. Il dato personale nelle economie basate sui dati: la disciplina generale del GDPR (Regolamento (UE) 2016/679)

Si è così rilevato come il diritto alla protezione dei dati personali abbia una sua natura dinamica. Tale peculiarità deve essere osservata nel più ampio contesto dell'attuale evoluzione tecnologica delle economie basate sui dati.

L'attuale contesto socioeconomico di riferimento può essere considerato quale diretto corollario della tesi per la quale la possibilità di utilizzo (*recte,* trattamento) dei dati personali è insita nel riconoscimento

[22] Interessante anche l'osservazione in V. RICCIUTO, *Circolazione e scambio dei dati personali. Il problema della regolazione del nuovo fenomeno patrimoniale*, in *Rivista di diritto dell'impresa*, 2/2021, p. 261 laddove individua "*tre momenti del rapporto tra autorità pubbliche e privati nella regolamentazione del trattamento dei dati*". In particolare, di interesse pare il secondo momento nel quale, per effetto della diffusione degli "*elaboratori elettronici e dell'informatica nei rapporti comuni*" viene demandata all'autorità la funzione di tutela e garanzia dei singoli. Nel terzo momento, invece, acquisita consapevolezza circa l'utilizzo con finalità economiche dei dati, il ruolo dell'autorità incoraggia lo scambio e la circolazione dei dati personali svolgendo ulteriori funzioni di "*regolazione del mercato e di promozione della libera circolazione dei dati*".

[23] In tema si segnala la sentenza Corte EDU, *Leander c. Svezia,* 26 marzo 1987, n. 9248/81, §48, nella quale per la prima volta, pur rapidamente, la protezione dei dati personali viene ricondotta nell'ambito di applicazione del diritto al rispetto della vita privata. Ma in generale, nella giurisprudenza della Corte EDU si è andato affermando il riconoscimento delle informazioni e dei dati come elemento afferente alla vita privata.

[24] Si potrebbe osservare, allora, come non sia il diritto in sé ad avere un prezzo quanto piuttosto il bene su cui detto diritto viene esercitato. Lo stesso potrebbe dirsi per la privacy, dove la tutela si rivolge direttamente alla sfera individuale tramite i dati che lo rappresentano. Rilevano in tal senso gli studi, nazionali ed internazionali, relativi ad un'analisi di una concezione proprietaria della privacy, si veda in tal senso N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, 2019. Si consideri anche come, ad oggi, dati non sono tutelati a priori ma solamente nella misura in cui in essi si riconosce l'individualità della persona: oggetto di tutela è sempre il diritto fondamentale della persona.

del diritto di tutela e controllo riconosciuto al singolo. Non c'è controllo sulla circolazione dei propri dati personali senza circolazione. E se i dati personali, oltre a poter circolare liberamente, possono essere trattati e raccolti è evidente (o, meglio, non è possibile escluderlo *a priori*) che detta utilizzazione possa avvenire per fini commerciali.[25] È in questo senso che, allora, si può parlare di una tutela dinamica di protezione e controllo dei dati nella loro circolazione e nei loro utilizzi.[26]

Tale approccio è condiviso a livello europeo e si rinviene anche nel Regolamento UE 2016/679 laddove, al considerando 4 e seguenti, riconosce una "*funzione sociale*" alla circolazione dei dati personali ed il necessario contemperamento tra la *data protection* ed altri diritti fondamentali. Lo stesso legislatore europeo, dunque, riconosce ed ammette il carattere proteiforme della tutela dei dati personali nel momento in cui impone di bilanciare gli utilizzi dei dati personali con le eventuali ulteriori esigenze garantite da altrettanti diritti fondamentali.[27] In effetti, come è stato più volte osservato, la tutela dei dati personali non viene a costituire una prerogativa assoluta ma va considerata e bilanciata alla luce della sua funzione sociale, economica e di pubblica sicurezza.

Si riconosce, dunque, un valore patrimoniale ai dati personali e, con esso, la loro mercificazione,[28] secondo quello che viene a determinare il passaggio «*da una dimensione "morale" e di tutela di un diritto fondamentale ad*

[25] In termini generali, sul tema si rinvia a N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR,* CEDAM, Milano, 2019; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di) *I dati personali nel diritto europeo*, Giappichelli, 2019. Si viene a parlare altresì di un vero e proprio *diritto* del titolare a trattare i dati personali: F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Padova, Cedam, 2018.

[26] S. RODOTÀ, *Il mondo nella rete. Quali diritti quali vincoli*, Roma-Bari, 2014, p. 31-32. Prescindendo dal carattere economico dell'utilizzo dei dati personali, ad esempio, si può ricordare l'annosa questione relativa alla trasparenza nel settore pubblico in rapporto alla tutela dei dati personali. Conflitto che si acuisce specialmente nel mondo digitale come ricorda la Corte Costituzionale, sent. n. 20/2019 osservando come "[i] *diritti alla riservatezza e alla trasparenza si fronteggiano soprattutto nel nuovo scenario digitale: un ambito nel quale, da un lato, i diritti personali possono essere posti in pericolo dalla indiscriminata circolazione delle informazioni, e, dall'altro, proprio la più ampia circolazione dei dati può meglio consentire a ciascuno di informarsi e comunicare."*

[27] Nonostante ciò, però, salvando l'impostazione più garantista della tutela dei dati personali, la Commissione Europea osserva chiaramente come non si possa far riferimento ad alcuna mercificazione della *privacy* nei rapporti interstatuali. Il riferimento è alla COM(2017) 7 "*Scambio e protezione dei dati personali in un mondo globalizzato*" dove espressamente si prevede che "[l]*a privacy non è una merce di scambio. Internet e la digitalizzazione dei beni e dei servizi ha trasformato l'economia globale: il trasferimento transfrontaliero di dati, compresi i dati personali, è parte dell'operatività quotidiana delle imprese europee di tutte le dimensioni e in tutti i settori. Poiché gli scambi commerciali utilizzano sempre più i flussi di dati personali, la riservatezza e la sicurezza di tali dati è diventata un fattore essenziale della fiducia dei consumator*i." La stessa Comunicazione richiama la COM(2015) 497 final del 14.10.2015, p. 8, secondo cui "[l]*e norme in materia di trattamento dei dati personali non formano oggetto dei negoziati né sono interessate dagli accordi commerciali*".

[28] Evoluzione contestata dal Garante europeo della protezione dei dati con la *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content* resa sulla proposta della direttiva UE 2019/770. Il Garante ritiene tale evoluzione pericolosa poiché aprirebbe alla possibilità di considerare i diritti fondamentali come "mera merce". In realtà, "…*che il carattere pervasivo delle logiche di mercato abbia coinvolto anche interessi protetti da diritti personali non è una novità…"* osserva R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2/2020, p. 763.

Nonostante ciò, come si dirà, la Direttiva UE 2019/770 - in uno con il riconosce il valore economico dei dati come oggetto di scambio per la fruizione di servizi digitali, di fatto riconoscendo e tipizzando l'intervenuta commercializzazione dei dati personali.

una "negoziale" e di commercializzazione dei dati»[29]. In questa direzione, il modello regolamentare europeo, con apprezzabile lungimiranza, prende atto del mutamento tecnologico e sociale intervenuto sotto la vigenza della precedente normazione[30] ed anticipa la possibilità che i dati diventino bene giuridico economicamente valutabile. In tal senso, ad esempio, si può leggere il considerando 6, laddove si afferma che "*la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali"* con particolare riferimento alla "*tecnologica attuale consente tanto alle imprese tanto alle autorità pubbliche di utilizzare i dati personali, come mai in precedenza, nello svolgimento delle loro attività*". La circolazione dei dati, nell'architettura del regolamento, diventa un fenomeno necessario ed inevitabile, purché nel rispetto dei limiti della dignità umana.[31]

Il modello europeo priva del carattere di assolutezza il diritto alla protezione dei dati di carattere personale ma ne riconosce il carattere relativo e ne ammette possibili bilanciamenti in virtù *"della sua funzione sociale"* (considerando 4). La cornice normativa, dunque, mantiene una forte impronta liberale che ammette un bilanciamento tra la protezione dei dati personali e la libertà d'impresa. È stato già osservato – anche sotto altri profili non inerenti esclusivamente ai dati personali - come l'importanza dei dati sia tale che un'eventuale restrizione alla loro circolazione potrebbe pregiudicare lo sviluppo economico: i dati, infatti, sono ormai pacificamente riconosciuti quale fonte di innovazione e crescita economica e di benessere sociale, come ampiamente già osservato.

La disciplina generale del GDPR regola, in parte, lo sfruttamento con finalità economiche dei dati tramite algoritmi, in particolare dagli artt. 22 e seguenti. Si tratta di una cornice normativa non specifica che prevede vaste eccezioni tali da non offrire una disciplina esaustiva del fenomeno.[32] In tal senso, infatti, l'articolo 22 introduce il diritto a che l'interessato non venga sottoposto – e, quindi il relativo diritto ad opporsi - ad un trattamento automatizzato dei propri dati- compresa la profilazione[33]- che produca effetti

---

In tema, in termini più ampi sulla mercificazione del dato personale nell'attuale contesto economico si rimanda a M. MURSIA, C.A. TROVATO, *The commodification of our digital identity: limits on monetizing personal data in the European context,* in *MediaLaws,* 2/2021, p. 165 ss.

[29] Così G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Il diritto dell'informazione e dell'informatica*, 3/2020, p. 636.

[30] Direttiva 95/46/CE, adottata il 24 ottobre 1995 con lo specifico scopo di armonizzare le norme in materia di protezione dei dati personali per garantire un "flusso libero" (free flow of data) dei dati e promuovere un elevato livello di tutela dei diritti fondamentali dei cittadini.

[31] In questi termini, R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2/2020, p. 765.

[32] A. BOIX PALOP, *Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones*, in *Teoría y Método. Revista de Derecho Público*, n. 1/2020, p. 28, osserva che tale disposizione consente a qualsiasi previsione normativa che autorizzi processi decisionali automatizzati di derogare alla disciplina in materia di protezione dei dati personali, senza la preventiva necessità di ottenere il consenso degli interessati, ad esempio. D.U. GALETTA, J. G. CORVALÀN, *Intelligenza Artificiale per una Pubblica Amministrazione 4.0? Potenzialità, rischi e sfide della rivoluzione tecnologica in atto*, in *federalismi.it*, n. 3/2019

[33] Sono trattamenti largamente diffusi nelle economie data driven. Le "*Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679*" (WP251) evidenziano i rapporti tra la profilazione e le

giuridici[34] che lo riguardano o che incida allo stesso modo significativamente sulla sua persona.[35] In tema, tuttavia, è necessario osservare come l'applicazione concreta di tale diritto incontri due ordini di limitazioni. Da un lato, infatti, lo stesso art. 22 ammette la possibilità di ricorrere a decisioni automatizzate qualora basata sul consenso esplicito dell'interessato ovvero qualora necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento – ipotesi tipica dei rapporti privatistici nei sistemi economici *data driven* – previa individuazione delle misure adeguate alla tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

2.b. Acquisizione e sfruttamento dei dati personali: la tutela (anche) consumeristica delle Direttive (UE) 2019/770 e 2019/771

Si è ormai radicata la duplice accezione dei dati personali: da una parte, rappresentano la manifestazione di valori afferenti alla sfera della personalità, dell'uguaglianza e della dignità dell'uomo e, dall'altra, rappresentano ormai un *asset* patrimoniale suscettibile di sfruttamento economico.

decisioni automatizzate: da una parte, infatti, le decisioni automatizzate possono essere prese ricorrendo o meno alla profilazione, la quale a sua volta può essere svolta senza che vengano prese decisioni automatizzate. Tuttavia, la profilazione e il processo decisionale automatizzato non sono necessariamente attività separate. Qualcosa che inizia come un semplice processo decisionale automatizzato potrebbe diventare un processo basato sulla profilazione, a seconda delle modalità di utilizzo dei dati.

[34] Il Regolamento non definisce i concetti di "*giuridico*" o "*in modo analogo significativi*". Sul tema, però, nuovamente occorre fare riferimento alle citate linee guida WP251 secondo cui un "effetto giuridico" possa riferirsi a tutte quelle decisioni, basate unicamente su un trattamento automatico, che incidano sui diritti giuridici di una persona, quali la libertà di associarsi ad altre persone, di votare nel contesto di un'elezione o di intraprendere azioni legali ovvero che possano sullo status giuridico di una persona o sui suoi diritti ai sensi di un contratto. Quanto agli "*effetti analoghi*", invece, si deve ritenere che il Regolamento faccia riferimento all'impatto significativo delle decisioni automatizzate che, pur non coinvolgendo diritti umani, colpiscano significativamente altri interessi: le linee guida riportano, a titolo esemplificativo, decisioni che negano a una persona un'opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio.

[35] Si veda anche il considerando 71, in base al quale "*l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona*". Disposizioni analoghe erano già contenute all'art. 15 della dir. 95/46/CE, recepito dall'art. 14 del d.lgs. 196/2003.

Nelle economie digitali osserviamo come dati e metadati[36] siano prodotti – più o meno volontariamente[37] – dagli utenti quale controprestazione del servizio offerto, spesso gratuitamente.[38]

Tutto ciò è dovuto all'interesse economico per l'acquisizione di dati, anche di carattere personale, all'interno delle descritte economie dei dati per la realizzazione dell'attività d'impresa.[39] Le peculiarità risiede altresì nella circostanza per la quale i dati estratti da *software* e algoritmi per la fruizione dei servizi digitali risultano poi diversi dai dati personali immessi dall'utente.

Sulla scia di queste considerazioni, pur a fronte di iniziali difficoltà,[40] con la Direttiva (UE) 2019/770 il legislatore europeo ha inteso disciplinare, anche sotto il profilo consumeristico, l'erogazione di contenuti e servizi digitali[41] a fronte della cessione di dati personali - da intendersi più correttamente come consenso al trattamento – senza però qualificare ciò come controprestazione contrattuale, anche se di natura non pecuniaria.[42] In un rapporto di reciproca integrazione si segnala la Direttiva (UE) 2019/771 avente ad oggetto i contratti di vendita di beni con elementi digitali, quali quei beni che incorporano o che sono interconnessi con un contenuto digitale o un servizio digitale in modo tale che la mancanza di detto contenuto digitale o servizio digitale impedirebbe lo svolgimento delle funzioni dei beni.[43]

---

[36] In via di prima approssimazione, si possono definire i metadati come "dati sui dati". Si tratta in realtà di "dati di attività", registrati nel corso di un'azione principale. Da una telefonata, ad esempio, possono essere estratti dati riguardanti la data e l'ora, la durata, il numero del mittente e quello del destinatario, le localizzazioni e via dicendo.

[37] Il riferimento è alla cessione di dati personali attiva e passiva tramite i *cookies*. Sul punto, A. DE FRANCESCHI, *Il "pagamento" mediante dati personali* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di) *I dati personali nel diritto europeo*, 2019, p. 1384.

[38] Così facendo, dunque, gli utenti, pagando il servizio offerto mediante i loro dati, sarebbero, in ottica imprenditoriale, "*carefree billionaires"* senza alcun limite alla capacità di spesa dei propri dati. In questi termini, V. ZENO-ZENCOVICH, *Do "Data Markets" Exist?* in *MediaLaws,* 1/2019, p. 9.

[39] Ad esempio, secondo quanto emerso dall' Osservatorio sulle piattaforme online pubblicato dall'Autorità per le Garanzie nelle Comunicazioni, nel 2018 Google ha ottenuto ricavi pubblicitari per utente a livello mondiale di 37 €, conseguiti grazie ai dati conferiti per l'utilizzo dei loro servizi gratuiti. Seguono Facebook (21 €) e Instagram (11 €).

[40] La gratuità dell'offerta di servizi digitali ha determinato una grande difficoltà di riconoscere un effettivo valore economico dei dati personali. Si è poi riconosciuto che dietro a tale gratuità, solo apparente, si nascondeva un'operazione economica molto elementare: lo sfruttamento con finalità economiche dei dati raccolti dagli utenti, come osserva V. ZENO-ZENCOVICH, *Do "Data Markets" Exist?* in *MediaLaws,* 1/2019, p. 28-29.

[41] Nella definizione di contenuti e servizi digitali rientrano, per espressa indicazione a carattere esemplificativo, "*programmi informatici, applicazioni, file video, file audio, file musicali, giochi digitali, libri elettronici o altre pubblicazioni elettroniche, nonché i servizi digitali che consentono la creazione, la trasformazione o l'archiviazione dei dati in formato digitale, nonchè l'accesso a questi ultimi, fra cui i software come servizio quali la condivisione audio e video e altri tipi di file hosting, la videoscrittura o i giochi offerti nell'ambiente di cloud computing e nei media sociali*" (considerando 19).

[42] La versione originaria del Regolamento, infatti, indicava i dati personali come "*controprestazione non pecuniaria"*, osserva G. SCIANCALEPORE, *I dati come oggetto del contratto tra la Direttiva sui contenuti digitali e il GDPR* in P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Giappichelli, 2022, p. 121, richiamando anche R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2/2020, p. 769, nella misura in cui riporta sul punto le preoccupazioni espresse dal Garante europeo della protezione dei dati.
Nonostante ciò, la direttiva estende ai servizi erogati a fronte della cessione di dati personali "*alcune garanzie consumeristiche essenziali"*. In questi termini, P. STANZIONE, *Introduzione,* in P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Giappichelli, 2022, p. 5-6.

[43] La Direttiva (UE) 2019/770 al considerando 21 – da cui è ripresa la definizione dell'art. 2– propone tre esempi di beni con elementi digitali: *smart TV*, *smartphone*, *smartwatch*. Si tratta di casi in cui il prodotto fisico (televisore, telefonino, orologio) diventa il veicolo per accedere a contenuti o servizi digitali, anche tramite applicazioni e software preinstallati

In ogni caso, per espressa previsione, è fatta salva l'applicazione della disciplina di protezione dei dati personali per lo specifico trattamento eseguito dal titolare.

La Direttiva (UE) 2019/770 trova applicazione in tutti quei casi in cui viene fornito un contenuto digitale o un servizio digitale al consumatore, il quale si impegna a fornire i propri dati personali all'operatore economico secondo un rapporto sinallagmatico di natura contrattuale. Sono esclusi quei casi in cui la fornitura di dati personali risulta necessaria per l'adempimento della prestazione.

Al contratto così stipulato, dunque, si applica la disciplina speciale prevista dalla direttiva in materia di conformità del contenuto digitale o del servizio digitale; di responsabilità contrattuale dell'operatore economico; di regime probatorio; di rimedi, diritti e obblighi per il consumatore e correlati obblighi dell'operatore economico in caso di difetto di conformità; di modifiche contrattuali.

La Direttiva (UE) 2019/771 trova applicazione in relazione ai contratti di vendita tra un consumatore e un venditore, anche aventi ad oggetto beni con elementi digitali, e prevede una disciplina speciale ulteriormente differenziata rispetto alla Direttiva (UE) 2019/770.

Le vicende del trattamento dei dati personali non risultino soggette solamente alla disciplina di tutela della persona propria del GDPR possono essere oggetto di diversi plessi normativi, anche con applicazione congiunta. Quando il trattamento dei dati personali si collochi nel contesto di una vicenda di consumo e, dunque, di un fenomeno di mercato interviene la regolazione del diritto contrattuale generale e speciale, del diritto dei consumatori e del diritto della concorrenza. In questo senso, infatti, il Regolamento (UE) 2016/679 individua una disciplina orizzontale di carattere generale sull'attività di trattamento e sulla circolazione dei dati personali, indipendentemente dal settore di riferimento, con l'indicazione di una specifica autorità di regolazione e controllo. Le specifiche disposizioni di carattere contrattuale che disciplinano l'operazione avente ad oggetto l'attività di trattamento e la circolazione dei dati personali sono, a loro volta, oggetto di ulteriori strumenti normativi (come si sono osservate le Direttive (UE) 2019/770 e 2019/771) sulla cui applicazione sono chiamate a vigilare altre e distinte autorità pubbliche.

2.c. La mercificazione del dato personale al vaglio delle autorità giurisdizionali: il caso italiano sulle pratiche commerciali scorrette in attesa dell'intervento della Corte di Giustizia

In questo contesto normativo di riferimento, si iniziano a registrare primi interventi di natura giurisdizionale conseguenti alla patrimonializzazione del dato personale e, per essa, i primi approcci negoziali alla protezione dei dati personali. In particolare, sono state censurate pratiche commerciali

digitale. In tutti questi casi trova applicazione la Direttiva (UE) 2019/771. Diversamente, per continuare l'esempio, le applicazioni scaricate da un app store su uno smartphone rappresentano l'oggetto di un contratto di fornitura distinto dal contratto di vendita dello *smartphone* stesso e non troverà applicazione la Direttiva (UE) 2019/771 bensì la Direttiva (UE) 2019/770.

scorrette aventi ad oggetto l'acquisizione, con finalità economiche, di dati personali degli utenti da parte di una nota piattaforma di social network.[44]

La sanzione irrogata dall'AGCM è stata sottoposta al vaglio giurisdizionale del TAR e del Consiglio di Stato, trovando parziale conferma.[45]

L'aspetto di maggiore interesse attiene al fatto che le condotte sanzionate ai sensi della disciplina consumeristica avessero ad oggetto la raccolta, lo scambio con terzi e l'utilizzo, con finalità commerciali, dei dati personali degli utenti, attività relative al trattamento ed alla circolazione dei dati personali. Come visto, però, oggetto di disciplina e tutela da parte del Regolamento (UE) 2016/679 non sono i dati personali in quanto tali bensì i diritti fondamentali dei soggetti cui si riferiscono e che, in quanto tali, rimangono insuscettibili di valutazione economica. Astrattamente, le vicende relative al trattamento dei dati personali (che non sono considerati come beni patrimoniali) non potrebbero essere destinatarie delle disposizioni di tutela del consumatore, funzionali alla tutela della libertà negoziale nei rapporti di natura contrattuale tra operatori economici e consumatori. Il mutamento di paradigma si è avuto grazie al riconoscimento della rilevanza patrimoniale della cessione di dati personali nella fruizione dei servizi digitali così da consentire l'applicazione delle disposizioni di tutela del consumatore e poterne individuare una lesione. Le sentenze richiamate rimarcano ed affermano, per la prima volta in sede giurisdizionale, l'avvenuta patrimonializzazione dei dati personali sulla scorta del passaggio dal concetto di *privacy* come riservatezza al controllo sui proprio dati, già evidenziato. Corollario di ciò è la possibilità di regolazione dell'utilizzo con finalità economiche dei dati anche tramite le forme di tutela del consumatore: più correttamente, non si è esclusa a priori la possibilità di intervento di distinte autorità, ciascuna secondo la propria competenza, qualora siano coinvolti dati personali.[46] E così, allora, si deve ritenere che le disposizioni sul trattamento dei dati personali non escludono che il trattamento in sé considerato possa non essere conforme ad altri disposizioni, come evidenziato nel caso di specie con riferimento alla tutela

[44] L'accesso alla piattaforma veniva indicato come "*gratuito*". L'AGCM, nella propria ricostruzione, condivisa anche dal giudice amministrativo, ha ritenuto che, nonostante non vi fosse alcuna controprestazione in denaro, i dati personali degli utenti venivano ceduti per la loro utilizzazione commerciale con finalità economiche, principalmente derivanti dallo sfruttamento pubblicitario, da parte della piattaforma. La rilevanza patrimoniale di tale cessione di dati personali non può condurre alla definizione del servizio come "gratuito" che, al contrario, determina una pratica commerciale scorretta nei confronti degli utenti che, in quanto tale, deve essere sanzionata.

[45] Si fa riferimento alle sentenze di primo grado (TAR Lazio, sede di Roma, Sez. I, 10 gennaio 2020, n. 260 – 261) e del Consiglio di Stato (Consiglio di Stato, Sez. VI, 29 marzo 2021, n. 2630-2631). La sanzione irrogata è stata confermata solo parzialmente in relazione alla pratica commerciale ingannevole realizzata per non aver adeguatamente informato gli utenti dell'attività di raccolta ed utilizzo, per finalità economiche, dei propri dati personali. È stata, invece, annullata la sanzione nella parte in cui contestava una pratica commerciale aggressiva per l'indebito condizionamento degli utenti a consentire la raccolta e l'utilizzo, anche da parte di terzi, dei propri dati personali. In tema, A. DAVOLA, R. PARDOLESI, *Protezione dei dati personali, tutela della concorrenza e del consumatore (alle prese con i 'dark pattern'): parallele convergenti?* In *Foro Italiano,* III, p. 325 in commento a Consiglio di Stato, Sez. VI, 29 marzo 2021, n. 2631.

[46] In tema, M. MIDIRI, *Proteggere I dati personali con le tutele del consumatore,* in *Giornale di diritto amministrativo,* n. 5/2021, p. 609 ss., P. TANDA, *I nuovi orizzonti della nozione di "privacy" e la patrimonializzazione dei dati personali da parte dei "social network"*, in *Diritto e processo amministrativo,* n. 3/2020, p. 731.

consumeristica. In questo senso, ad esempio, nella vicenda richiamata, il Consiglio di Stato, facendo propria la decisione di primo grado, ha osservato come non vi sia incompatibilità o antinomia tra la normativa per la protezione dei dati personali e quella sulla protezione del consumatore. Le due tutele risultano complementari l'una all'altra, ciascuna imponendo obblighi informativi specifici, funzionali alla protezione dei dati personali e del loro trattamento ovvero alla consapevolezza delle scelte economiche del consumatore.

L'interdipendenza delle competenze amministrative si è osservata in un'altra ipotesi paradigmatica nella quale la violazione del diritto alla protezione dei dati personali è stata indicata come sintomo di violazione del diritto della concorrenza. In particolare, il riferimento è alla censura mossa dall'autorità tedesca per la concorrenza (*Bundeskartellamt*) verso Facebook per abuso di posizione dominante fondato sul deteriore trattamento dei dati personali riservato agli utenti in violazione della normativa di protezione.[47] La questione sta ora interessando anche la Corte di Giustizia dell'Unione Europea a seguito del rinvio pregiudiziale svolto dall'Oberlandesgericht Düsseldorf (Tribunale superiore del Land, Düsseldorf, Germania) in relazione alla competenza di un'autorità nazionale garante della concorrenza, quale il Bundeskartellamt, ad esaminare, in via principale o incidentale, i comportamenti di un'impresa alla luce di talune disposizioni del regolamento (UE) 2016/679.[48]

2.d. Breve analisi empirica sulla quantificazione del valore dei dati personali

I dati, come visto, non hanno un valore intrinseco che dipende dalle informazioni che, in un determinato contesto, possono essere estrapolate. Non sfuggono a tale logica economica neppure i dati personali i quali, anzi, hanno un valore apprezzabile in termini monetari. Tale valore, tuttavia, non è univoco in quanto, come già detto, dipende dal contesto del loro utilizzo e la stessa valutazione monetaria di uno stesso insieme di dati può divergere in modo significativo tra gli operatori del mercato.[49]

[47] M. MIDIRI, *Le piattaforme e il potere dei dati (Facebook non passa il Reno),* in *Il diritto dell'informazione e dell'informatica,* 1/2021, p. 122 – 124; M. MIDIRI, *Proteggere I dati personali con le tutele del consumatore,* in *Giornale di diritto amministrativo,* n. 5/2021, p. 610-611 richiama in nota la dottrina che maggiormente si è occupata di questi temi. La prospettiva antitrust è, invece, analizzata da A. DAVOLA, *"I vestiti nuovi dell'imperatore". Il contenzioso tra il bundeskartellamt tedesco e Facebook in tema di abuso di posizione dominante alla luce del progressivo snaturarsi del diritto antitrust*, in *Diritto di internet,* 1/2021.

[48] Si vedano le conclusioni dell'Avvocato Generale, Athanasios Rantos, presentate il 20 settembre 2022, nella causa C-252/21 (ECLI:EU:C:2022:704).

[49] In questo senso, ad esempio, in OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, 2015, Paris, p. 197, è stato dimostrato che negli Stati Uniti gli individui sarebbero disposti a rivelare i loro numeri di previdenza sociale per una media di 240 dollari, lo stesso insieme di dati può essere acquistato per meno di 10 dollari da broker di dati.

Non esiste, infatti, una metodologia comunemente accettata per stimare il valore dei dati personali. In questo senso, si possono registrare due possibili approcci basati sulle valutazioni di mercato[50] ovvero sulla percezione individuale del valore dei dati personali e della privacy.[51]

Nelle economie dei dati, specialmente nei settori nei quali i dati forniti rappresentano la controprestazione per i servizi offerti, è stata evidenziata la presenza di un fortissimo squilibrio informativo tra l'imprenditore e l'utente – inconsapevole del reale valore di mercato delle informazioni su di sé che fornisce. Ciò si deve, in larga parte, alla difficoltà, per il soggetto cui i dati si riferiscono, di individuarne il valore da attribuire.

A tal riguardo, vale la pena di riportare un esperimento di economia comportamentale svolto in relazione all'osservazione della valutazione degli utenti circa le proprie informazioni personali.[52] Lo studio proposto rivela che il valore attribuito alle informazioni personali cresce non appena si ha consapevolezza che altri sono interessati per scopi commerciali alle informazioni fornite (*asset consciousness*), inducendo così ad uno sviluppo della "psicologia della proprietà" (*psychology of ownership*) che porta ad apprezzare maggiormente le informazioni personali (*pay to sold)*. All'opposto, se i dati personali devono essere valutati in termini economici per essere conservati o protetti (*pay to protect*), alle informazioni personali viene attribuito un valore economico inferiore, se non nullo.[53]

Al netto di quanto rappresentato, si manifesta il rischio che la quantificazione del valore dei dati forniti dall'utente, spesso, potrebbe essere superiore a quello del servizio o del contenuto digitale fornito.[54] In

[50] Questa metodologia si basa sui valori osservati o ricavati dall'incontro tra domanda ed offerta nei mercati dei dati. Tale valore risulta, comunque, influenzato dalla redditività dei dati e dalla loro influenza in termini finanziari sull'impresa che li utilizza (ossia, tra i tanti, i ricavi medi per utente), i prezzi praticati sui mercati dei dati , il costo conseguente ad un *data breach* e i prezzi dei dati nei mercati illegali. In questi termini, OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, n. 220/2013, OECD Publishing, Paris, p. 19.

[51] L'attribuzione di valore ai dati personali basata sulla valutazione degli individui si fonda, ad esempio, sui risultati di sondaggi ed esperimenti economici, nonché sulla disponibilità degli utenti a pagare per proteggere i propri dati. In questi termini, OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD Digital Economy Papers, n. 220/2013, OECD Publishing, Paris, p. 19.

[52] S. SPIEKERMANN, J. KORUNOVSKA, C. BAUER, *Psychology of Ownership and Asset Defense: Why People Value Their Personal Information Beyond Privacy*, 2012, DOI: 10.2139/ssrn.2148886. L'esperimento cui fanno riferimento è basato su un sondaggio online dove 1059 utenti di Facebook hanno rivelato quanto sarebbero disposti a pagare per mantenere le proprie informazioni personali.

[53] Dal richiamato esperimento riportato, è emerso che, alla domanda su quanto gli utenti intervistati sarebbero disposti a pagare per salvare il loro profilo Facebook dall'eliminazione, il 48% ha affermato che non avrebbe pagato; con una media di valore tra 0 e 2€ per il "salvataggio" del proprio profilo.
L'esempio riportato, pur inerente all'ambito dell'economia comportamentale della privacy, ci dimostra l'incoerenza di molti utenti che, svalutando i propri dati, o non prestando particolare attenzione alla loro diffusione, esprimono poi gravi preoccupazioni per la privacy, secondo quello che viene definito il fenomeno della *privacy paradox*.

[54] Osserva A. DE FRANCESCHI, *Il "pagamento" mediante dati personali* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di) *I dati personali nel diritto europeo,* 2019, p. 1384, come "*gli individui sottostimano il valore dei propri dati personali"* e, dunque, tendano ad accettare, "*senza una preventiva adeguata riflessione"* una controprestazione (la fornitura di beni e servizi) di *"valore marginale",* sicuramente inferiore e quello dei dati ceduti.

altre parole, il fornitore del servizio potrebbe trarre vantaggio dall'inconsapevolezza degli utenti. E così, dunque, l'importanza della corretta quantificazione del valore dei dati forniti dall'utente si apprezza anche in relazione agli inevitabili impatti sulle scelte commerciali di imprese e consumatori, in applicazione anche delle rispettive tutele che, come visto, risultano sempre più interdipendenti.

3. Profili concorrenziali dell'economia basata sui dati

L'acclarato riconoscimento del valore economico dei dati, anche personali, presenta – come in parte accennato - interessanti risvolti anche in ambito concorrenziale. Ad oggi, ad esempio, la quantità di dati posseduta (e le diverse possibilità di accesso a questi) può incidere direttamente sulla qualità dei servizi offerti, interessando la concorrenza.[55] Ancora, l'accumulo di dati posseduti da un'impresa potrebbe suscitare preoccupazioni di ordine economico dovute alla concentrazione del potere di mercato e nella preclusione dello sviluppo di imprese concorrenti dovuto all'impossibilità, e, comunque, la difficoltà ad accedere ai dati.[56]

Ma, ancora, nelle economie basate sui dati la concorrenza tra imprese si potrebbe fondare sui livelli di tutela dei dati personali quale elemento qualitativo del servizio offerto[57] e portando, così, a fenomeni in cui viene richiesto il pagamento di un prezzo positivo agli utenti al fine di evitare la raccolta di dati personali a fini pubblicitari.[58]

---

[55] Occorre prestare attenzione a ritenere che la maggior quantità di dati posseduta da un soggetto economico si traduca "…*automaticamente prima in un vantaggio informativo fondato e poi in un vantaggio competitivo da far valere in un qualsiasi mercato…*". Va, infatti, verificata caso per caso la relazione tra possesso dei dati e vantaggi concorrenziali. Così M. MAGGIOLINO, *I big data e il diritto antitrust*, Egea, Milano, 2018, p. 22.

[56] Si tratta della teoria dell'*essential facilities* secondo cui i dati, quale fattore di produzione, sarebbero un input insostituibile. Ancora, il possesso di grandi quantità di dati in capo alle imprese già presenti sul mercato determinerebbe una barriera all'ingresso per potenziali *competitors*. Su questi temi, A. PRETA, L. ZOBOLI, *Profili regolatori e concorrenziali in tema di accesso e condivisione dei dati,* in *Analisi Giuridica dell'Economia,* 1/2019; V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten Legal Perspectives on the 'Big Data Revolution'*, in *Concorrenza e Mercato*, 23/2016; G. COLANGELO, *Big data, piattaforme digitali e antitrust*, in *Concorrenza e Mercato*, 23/2016; G. COLANGELO – M. MAGGIOLINO, *Big data, data protection and antitrust in the wake of the "bundeskartellamt" case against Facebook* in *Riv. It. Antitrust,* 1,9/2017; I. GRAEF, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, International Competition Law Series, Vol. 68/2016, Kluwer, Law International.

[57] E a darne atto è la stessa Commissione nel caso *Facebook/Whatsapp* laddove, con riferimento al cd. *multi-homing*, ossia l'utilizzo di più fornitori del medesimo servizio, osserva come gli utenti valorizzino *privacy* e sicurezza e, specie tra le *app* di messaggistica istantanea, ciò ha portato all'introduzione di app che affrontano specificamente tali questioni.
La stessa Apple sta aumentando la sua attenzione per la privacy degli utenti delle app, costringendo gli sviluppatori a essere più trasparenti sulla raccolta dei dati e avvertendo che potrebbero essere rimossi se non rispettano una nuova misura anti-tracking.

[58] Si tratta del modello "*pay-for-privacy*" (PFP) con cui si prevede il pagamento da parte dei consumatori di una quota aggiuntiva per evitare che i loro dati vengano raccolti ed estratti a fini pubblicitari Come osservato in M. MURSIA, C.A. TROVATO, *The commodification of our digital identity: limits on monetizing personal data in the European context,* in *MediaLaws,* 2/2021, p. 166 citando S. ELVY, *Paying for privacy and the personal data economy*, in Columbia Law Rev., 117(6), 2017, p. 1369 ss, secondo la quale questi modelli renderebbero la privacy un prodotto commerciabile, non accessibile a tutti con conseguenti disuguaglianze e discriminazioni.
Nel report "*Predicts 2023: AI, Social Toxicity and Disappearing Customers Forge the Future of Marketing*" già entro quest'anno ben l'85% dei consumatori che hanno un reddito familiare superiore a 120.000 dollari annui e che devono accedere a

Nel contesto delle disposizioni di tutela della concorrenza, dunque, i dati rappresentano un fattore determinante nell'individuazione delle condotte abusive. Ed anzi l'applicazione delle regole proprie del diritto *antitrust* ha ricoperto un ruolo centrale nella regolazione dei fenomeni dell'economia basata sui dati, non senza qualche difficoltà. Le prime risposte ordinamentali, infatti, sono state di tipo pro-competitivo. A fronte del riconoscimento di condotte illecite di natura anticompetitiva, mediante l'applicazione dei concetti giuridici indeterminati propri del antitrust,[59] si richiama l'accennata tendenza delle autorità nazionali di tutela della concorrenza ad enfatizzare elementi propri della disciplina di tutela dei dati personali per l'individuazione delle condotte abusive. Al contrario, le autorità giudiziarie hanno mostrato maggior cautela nell'applicazione di queste ultime disposizioni per finalità concorrenziali, mantenendo salda la separazione tra competenze.[60] Si tratta di una tendenza che, ove confermata, potrebbe comportare l'applicazione del diritto della concorrenza oltre i propri confini, ipotesi non sempre condivisa in dottrina "*...per quanto possa apparire giusto o opportuno...*"[61], specialmente quando si richiede un intervento antitrust volto a colmare potenziali vuoti normativi a tutela di altri e distinti interessi.

Come visto, tuttavia, alla luce delle conclusioni rassegnate innanzi alla Corte di Giustizia dell'Unione Europea,[62] l'Avvocato Generale ha proposto un'interpretazione della normativa di riferimento tale da consentire ad un'autorità garante della concorrenza, nell'ambito dei propri poteri, di esaminare, in via incidentale, la conformità delle condotte esaminate con le norme a tutela dei dati personali, se del caso anche consultando l'autorità preposta.

vari servizi online, pagheranno per dispositivi elettronici, software e piani di abbonamento che consentono loro di evitare completamente la pubblicità personalizzata, beneficiando così di una maggiore privacy.

[59] Si intendono qui le condotte anticompetitive ricondotte all'interno degli schemi attuativi tipici del diritto antitrust posti direttamente a protezione del funzionamento del mercato. Tali condotte vanno tenute distinte da quelle nelle quali rilevino altresì altri interessi meritevoli di tutela, come quelli di natura consumeristica o di protezione dei dati personali. Ciò si deve alla questione della "*plurioffensività dei comportamenti lesivi delle disposizioni antitrust*": in tema, M. MAGGIOLINO, *I big data e il diritto antitrust,* Egea, Milano, 2018, p. 109 ss.. Si veda ID., *passim*, per una ricostruzione delle condotte rilevanti realizzate mediante l'utilizzo di big data: dalla loro formazione alla determinazione del potere di mercato fino alla determinazione dei loro utilizzi anticompetitivi.

[60] È questa anche l'impostazione seguita dalla Commissione europea nel caso dell'acquisizione Facebook/Whatsapp laddove si è esclusa dall'ambito di applicazione del diritto antitrust qualsiasi eventuale preoccupazione relativa alla privacy derivante dalla maggior concentrazione di dati, ritenendo che rientrasse nell'ambito delle norme europee sulla protezione dei dati. Affermazione di cui non sembrerebbe convinta neanche la Commissione quando, tre anni dopo, di fronte al mutamento della privacy policy dei servizi offerti da Whatsapp e Facebook, irroga una sanzione per omessa comunicazione di informazioni rilevanti impattanti sulla sfera della *privacy*.

[61] In questi termini, M. MAGGIOLINO, *I big data e il diritto antitrust,* Egea, Milano, 2018, pp. 155 e ss. Da questa ipotesi, tuttavia, deve essere distinta, nel senso della sua legittimità, quella in cui si riscontrino condotte a carattere plurioffensivo che, in quanto tale, risulti in violazione di distinte disposizioni di tutela, come nel caso Facebook, già citato, sanzionato del *Bundeskartellamt* tedesco nel quale condizioni di iniquità nel trattamento dei dati personali sono state assunte quale specifico parametro di valutazione della violazione dell'art. 102 TFUE.

[62] Si vedano le conclusioni dell'Avvocato Generale, Athanasios Rantos, presentate il 20 settembre 2022, nella causa C-252/21 (ECLI:EU:C:2022:704).

3.a. I dati quali parametro di valutazione delle condotte lesive della concorrenza nell'esperienza europea

Titolare delle funzioni di tutela della concorrenza in ambito europeo, la Commissione ha fronteggiato, nel corso degli ultimi anni, condotte peculiari delle economie basate sui dati.

Ad esempio, nel 2017, infatti, la Commissione europea ha sanzionato Google per aver abusato della propria posizione dominante nel mercato dei motori di ricerca a vantaggio del proprio servizio di comparazione degli acquisti (c.d. *Google Shopping*), a danno di concorrenti e consumatori. In questo caso, i dati hanno svolto un ruolo fondamentale nell'individuazione dell'abuso poiché l'illecito anticoncorrenziale si veniva a caratterizzare per una distorsione del traffico di dati, elemento fondamentale di comparazione e competizione nelle economie dei dati.[63] Garantire un costante approvvigionamento di dati, infatti, al netto degli effetti di rete diretti ed indiretti derivanti dalle interazioni all'interno della piattaforma,[64] consente di generare ricavi che possono essere utilizzati per investire nel migliorare la qualità dei servizi offerti mediante gli schemi della *data driven innovation*[65]. Nel caso in commento venne accertato come Google desse maggior visibilità e risalto al proprio servizio di comparazione degli acquisti, ponendolo al primo posto (o comunque tra i primi posti) tra i risultati del proprio motore di ricerca.

Di analogo tenore anticoncorrenziale sono state ritenute quelle condotte volte (pur con diversa metodologia) a garantire una stabile, duratura e costante acquisizione di dati degli utenti per il loro sfruttamento con finalità economiche.[66]

---

[63] Come osservato dalla Commissione nel caso richiamato (§7.2.2 CASE AT.39740 Google Search (Shopping)).

[64] Si pensi, ad esempio, sempre in tema di servizi di acquisti comparativi come un elevato numero di interazioni sulla piattaforma (derivante da un sostenuto traffico di dati verso la stessa) migliori la capacità di convincere (utenti, commercianti, *advertisers*) ad utilizzare il servizio e a fornire ulteriori dati (attrattività del servizio), anche consentendo di ottenere recensioni degli utenti più originali.

[65] Facendo ricorso ad algoritmi di *machine learning,* ad esempio, si possono indicare suggerimenti di acquisto e ricerca maggiormente aderenti alle preferenze degli utenti, con evidenti ripercussioni in termini di acquisti effettuati.

[66] La prima ipotesi è offerta dal caso Google Android 2018 (Caso AT.40099 con decisione della Commissione del 18 luglio 2018). La condotta abusiva è stata indicata nell'abbinamento della propria applicazione per la ricerca generica (*Google Search*) al proprio portale di vendita di applicazioni per Android (*Google Play Store*). Così facendo, il prodotto principale (*Google Play Store*) non poteva essere ottenuto senza il prodotto abbinato (*Google Search*), limitando la concorrenza e garantendo tanto un vantaggio competitivo significativo che i fornitori concorrenti di servizi di ricerca generica non possono compensare quanto il mantenimento e al rafforzamento della posizione dominante di Google in ciascun mercato nazionale dei servizi di ricerca generica.

Ulteriori ipotesi potrebbe indicarsi nel caso Google Search (AdSense) 2019 (Caso AT.4041: l'indagine condotta è stata avviata nel quadro più ampio del caso Google Search (Caso AT.39740). In tale fattispecie è stato osservato come Google sfruttasse la propria posizione dominante sul mercato imponendo una serie di clausole restrittive nei contratti con siti web di terzi, impedendo ai propri concorrenti di inserire su tali siti pubblicità collegate alle ricerche. Nella fornitura dei propri servizi di intermediazione pubblicitaria, infatti, Google aveva prima imposto un obbligo di fornitura esclusiva, che impediva ai concorrenti (principalmente, Microsoft e Yahoo) di inserire annunci pubblicitari collegati alle ricerche sui siti web più significativi dal punto di vista commerciale ed ha poi introdotto una cosiddetta strategia di "*esclusiva non rigida*" volta a riservare gli spazi migliori per i propri annunci collegati alla ricerca e a controllare le prestazioni degli annunci dei concorrenti.

L'attenzione verso i profili concorrenziali connessi alla centralità dei dati e delle tecnologie di elaborazione di questi è tale da assurgere a nuovo parametro della valutazione di compatibilità delle fusioni e delle concentrazioni societarie. Anche l'accumulo di dati su vasta scala (o di tecnologie per il loro sfruttamento) mediante acquisizioni potrebbe portare effetti negativi sulla concorrenza, tanto in termini di minore competitività sui mercati quanto in termini di minore innovazione. Nelle economie basate sui dati, infatti, si osserva l'incremento di operazioni di fusione e concentrazione dettate esclusivamente dall'interesse all'acquisizione di determinati *asset* di dati o di tecnologie particolari con l'effetto che si registra una riduzione della pressione concorrenziale nei mercati con il consolidamento della posizione dominante dei grandi operatori economici già presenti. Il fenomeno prende il nome di *killing acquisitions* ed è rivolto principalmente ai concorrenti potenziali, principalmente *starts-up* dall'elevato potenziale innovativo[67], mascherandosi dietro l'apparente una "*giustificazione di efficienza dinamica*"[68].

Ad esempio, tra le recenti operazioni societarie mosse dall'acquisizione di dati si segnala il caso Facebook/Whatsapp (2014). Inizialmente la fusione non era stata impedita dalla Commissione che aveva ritenuto che il settore delle applicazioni di comunicazione digitale fosse caratterizzato dall'ingresso frequente di nuovi operatori sul mercato e brevi cicli di innovazione e che, dunque, grandi quote di mercato avrebbero potuto, comunque, rivelarsi effimere. Nonostante ciò, successivamente, nel 2017, venne individuata una violazione degli obblighi procedurali del regolamento sulle concentrazioni poiché venne omessa la possibilità (pur nota al momento dell'operazione societaria) di abbinare i dati degli utenti del servizio di messagistica istantanea (Whatsapp) a quelli del *social network*.[69] Le informazioni inesatte o

[67] Nei mercati caratterizzati da una forte innovazione tecnologica, le imprese dominanti – per mantenere e consolidare la propria posizione – possono alternativamente investire direttamente in innovazione, procurandosi la tecnologia avanzata, ovvero evitare che altre imprese ottengano tali tecnologie. Se la prima ipotesi non solleva questioni antitrust, la seconda può rappresentare un illecito anticoncorrenziale. Sul punto, M. MIDIRI, *Privacy e antitrust: una risposta ordinamentale ai Tech Giant,* Federalismi.it, 14/2020, p. 213, nota 17, laddove riporta H. HOVENKAMP, *Antitrust and the Movement of Technology*, 19 *George Mason Law Rev.*, 2012, 1119, ed i richiami contenuti. Il fenomeno è stato osservato anche nel rapporto presentato dell'House Commitee on the Judiciary sulla concorrenza nei mercati digitali (*"Investigation of competition in digital markets"*) dove si riconoscono le acquisizioni societarie quale elemento del potere di mercato degli operatori economici digitali, specialmente nei casi in cui siano volte a neutralizzare una minaccia competitiva. Da ciò deriva la forte necessità di rafforzare il controllo antitrust nelle acquisizioni. Basti pensare che, in America delle quasi 100 acquisizioni di Facebook, la Federal Trade Commission si è impegnata in un'indagine approfondita su una sola acquisizione: l'acquisto di Instagram da parte di Facebook nel 2012. In calce al rapporto citato sono indicate tutte le acquisizioni societarie poste in essere da Facebook, Google, Amazon, Apple sin dalla loro fondazione.
Il tema è ampiamente trattato in dottrina. Tra i primi contributi si segnala M. MAGGIOLINO, *I big data e il diritto antitrust,* Egea, Milano, 2018, pp. 206-212.

[68] Come osserva M. MIDIRI, *Le piattaforme e il potere dei dati (Facebook non passa il Reno),* in *Il diritto dell'informazione e dell'informatica,* 1/2021, p. 114.

[69] E ciò nonostante la Commissione avesse già manifestato la propria preoccupazione relativamente alla possibilità di abbinare automaticamente gli account tramite collegamento del numero di telefonia mobile all'account social, pur rimanendo poi indifferente alle questioni relative alla tutela dei dati personali, ritenendosi priva di competenza, anche qualora derivanti da operazioni societarie rilevanti ai sensi della disciplina antitrust.
In risposta alle preoccupazioni della Commissione, è interessante osservare come Facebook, tuttavia, affermava che – alla luce della tecnologia in suo possesso – era impossibile abbinare automaticamente gli account ma che tale

fuorvianti rilasciate, ha precisato la Commissione, non avrebbero comunque inciso sulla decisione di autorizzare l'operazione.[70]

In altri casi di fusioni societarie, invece, la Commissione, maturando maggior consapevolezza sul ruolo primario dei dati, ha imposto una specifica disciplina di *data separation.*[71]

4. L'introduzione di specifiche discipline di *cybersicurezza*

La centralità dei dati, unitamente all'utilizzo di risorse tecnologiche, sta sollevando inedite questioni ordinamentali in risposta alle quali si iniziano ad osservare, come si vedrà anche a livello europeo, primi esempi di politiche di regolamentazione *ex ante* sulla loro circolazione ed utilizzo.

Un aspetto di indubbia novità relativo alla risposta degli Stati è offerto dalla crescente attenzione per i profili inerenti alla *cybersicurezza*, la cui vulnerabilità è stata resa evidente con la diffusione della digitalizzazione che ha portato all'emersione di nuovi ed imprevisti profili di rischio.

La *cybersicurezza*, infatti, viene invocata al fine di garantire l'affidabilità e la sicurezza di quelle attività[72], pubbliche e private, aventi carattere economico ovvero sociale, che vengono svolte mediante utilizzo di

abbinamento rimaneva possibile solo se effettuato manualmente dagli utenti o, comunque, previa rielaborazione dei codici delle app. In realtà, emerse successivamente, la società era già in possesso di tecnologie che consentivano l'abbinamento degli utenti tra le varie piattaforme, non tanto per integrazione orizzontale (scambio di messaggi tra l'una e l'altra) quanto piuttosto per altre finalità (commerciali).

[70] In dottrina è stata approfondita la questione se l'esito della decisione di autorizzare l'operazione avrebbe potuto essere diverso, specialmente sotto il profilo dell'*online advertising*, e viene risolta in senso positivo in V. BAGNOLI, *Questions that Have Arisen since the EU Decision on the Whatsapp Acquisition by Facebook*, Market and Competition Law Review, 3/2019. In particolare, nella ricostruzione della Commissione, viene osservato come, nonostante i servizi di *social network* e le *app* di comunicazione, pur separati, presentino alcune sovrapposizioni nelle funzionalità offerte (scambio, condivisione e pubblicazione di contenuti multimediali), non vi siano elementi tali da ritenere l'operazione conclusa in contrasto con il diritto europeo. L'elemento nuovo derivante dalla possibilità di aggregazione e abbinamento dei dati degli utenti, potrebbe sollevare preoccupazioni in tema di *online advertising*. Ma, sul punto, la Commissione ebbe a osservare come – indipendentemente dall'utilizzo dei dati degli utenti per finalità commerciali (la pubblicità mirata sui social network) – vi sarebbe comunque una quantità di dati degli utenti in Internet, utile per scopi pubblicitari e non sono sotto il controllo esclusivo di Facebook, tale da non generare dubbi circa la compatibilità dell'operazione con il mercato interno. In realtà, stando alla *privacy policy* di Whatsapp, gli unici dati personali di cui è in possesso son solamente i nomi e i numeri di telefono, dati ampiamente diffusi. La questione sarebbe ben diversa laddove ad essere raccolti a fini commerciali fossero i dati derivanti dal contenuto delle *chat*.

[71] Si tratta del caso Google/Fitbit (2020) con cui la Commissione, approvata definitivamente l'acquisizione da 2,1 miliardi di dollari di Fitbit da parte di Google, ha posto alcune condizioni relative alla concorrenza ma anche concernenti la protezione dei dati sanitari degli utenti. Tra queste vi sarebbe quella di non utilizzare i dati sanitari per fini di *advertising* e di memorizzarli in ambienti separati rispetto agli altri dati. L'obiettivo è evidentemente quello di evitare che i dati già in possesso di Google (frutto delle interazioni con e nella piattaforma e delle potenti e sconosciute elaborazioni algoritmiche) siano ulteriormente aumentati con dati di natura biologica e sanitaria. La durata degli impegni presi è stata fissata in dieci anni, salva la possibilità di proroga fino a un massimo di ulteriori dieci anni. A salvaguardia dell'effettiva attuazione degli impegni è prevista la nomina di un trustee chiamato ad operare in piena indipendenza e con ampi poteri ispettivi (tra cui l'accesso ai registri, al personale, alle strutture o alle informazioni tecniche di Google).

[72] Come osservato da A. TINA, *Cybersicurezza: integrità dei processi e dei dati*, in M. CIAN, C. SANDEI, *Diritto del Fintech*, 2020, p. 103, i rischi per le imprese, legati ad un *cyber attack,* possono essere così enucleati: *privacy liability* (1); *network security liability* (violazione rete aziendale) (2); *media liability* (violazione copyright) (3); interruzione di attività – malfunzionamenti (4); *data asset loss* (5); *cyber extortion* (6); *cyber crime* (7).

tecnologie digitali e, in generale, nello "spazio cibernetico"[73]. Come visto, nelle economie dei dati l'erogazione di beni e servizi è sempre più mediata da piattaforme e servizi digitali. Reti e sistemi informativi non coinvolgono solamente le economie dei dati ma sono essenziali per il funzionamento anche di molte imprese dell'economia tradizionale che fondano le proprie strategie di mercato proprio sull'accesso ai servizi offerti dalle piattaforme digitali.

Da tale interdipendenza deriva la necessità di garantire – tramite idonee misure di *cybersicurezza* - la sicurezza, la continuità e l'affidabilità delle reti e dei sistemi informativi attraverso cui vengono offerti tali servizi.

In termini più generali, come già osservato a livello globale,[74] si sta assistendo alla comparsa di nuove minacce alla sicurezza che, in quanto tali, richiedono risposte inedite in grado di salvaguardare la spinta innovativa delle economie basate sui dati.

Tra i profili di rischio legati alla *cybersicurezza* si devono tenere in considerazione anche i sistemi aggregati di conservazione di dati, necessari per le attuali tecnologie algoritmiche, in relazione ai quali troverà applicazione la disciplina europea di protezione dei dati personali, potendosi evidenziare sul punto un'ulteriore ipotesi di interdipendenza tra sistemi normativi di tutela.[75]

La necessità di una adeguata risposta alle nuove minacce derivanti dalla diffusione delle tecnologie digitali ha determinato una rinnovata sensibilità per gli aspetti propri della *cybersicurezza* tanto in relazione al corretto funzionamento dei sistemi informativi quanto in relazione al possibile coinvolgimento di dati personali.

L'erogazione di beni e servizi mediante l'utilizzo di infrastrutture digitali ha manifestato il bisogno che queste siano rese affidabili e sicure a vantaggio tanto degli utenti dei servizi digitali quanto degli operatori coinvolti. L'aumento delle infrastrutture digitali e la crescente accessibilità a strumenti informatici e digitali sono indicati quali fattori che hanno condotto, nell'ultimo decennio, a sempre più frequenti attacchi cibernetici, dovuti anche alla scarsità (in termini qualitativi e quantitativi) dei mezzi di difesa.[76]

---

[73] In via di prima approssimazione potremmo definire l'oggetto della disciplina relativa alla *cybersicurezza* come quello "spazio cibernetico" formato dalle infrastrutture informatiche, *hardware* e *software,* interconnesse tra loro e attraverso le quali circolano dati e nelle quali si relazionano utenti. In particolare, nello spazio cibernetico si ricomprende internet, le reti di comunicazioni, i sistemi di elaborazione dati e i dispositivi attraverso cui si accede alla rete.
Ad oggi, la *cybersicurezza* viene definita dalla legislazione europea (Reg. UE 2019/881, articolo 2, punto 1) quale "*l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*".

[74] Rapporto OECD, *Data-Driven Innovation. Big Data for Growth and Well-Being,* 2015, p. 40.

[75] Con particolare riferimento alla Sezione II del Reg. UE 2016/679 (GDPR) in tema di misure di sicurezza da adottare qualora siano coinvolti dati personali. E ciò indipendentemente dalla conservazione dei dati per finalità pubblicistiche (*public data retention*), anche a carattere securitario.

[76] In particolare, per una visione d'insieme si deve osservare la "Relazione sulla politica dell'informazione per la sicurezza" relativa all'anno 2021. In particolare, viene osservata una tendenza in crescita delle attività ostili per la sicurezza cibernetica: nel corso del 2021, ad esempio, maggiormente colpite sono le infrastrutture informatiche della Pubblica Amministrazione (69%, in diminuzione di 14 punti percentuali rispetto al 2020), perlopiù Amministrazioni

La creazione e il mantenimento di uno spazio digitale capace di offrire adeguate garanzie di sicurezza, infatti, rappresenta una condizione necessaria per fruire pienamente delle possibilità, in parte ancora inesplorate, offerte dal progresso tecnologico. Viceversa, le garanzie di sicurezza consentono altresì di evitare l'esposizione a rischi sistemici rovinosi per lo Stato, ad oggi ancora il principale obiettivo degli attacchi cibernetici.

In termini più generali, dunque, in ragione del crescente utilizzo delle tecnologie informatiche, la *cybersicurezza* non è più solo limitata a settori strategici per la sicurezza nazionale (difesa militare, infrastrutture essenziali, telecomunicazioni) ma coinvolge l'intero mercato e trova un'applicazione generalizzata anche ad attività economiche e sociali svolte mediante sistemi informatici. Tratto distintivo della *cybersicurezza* è quello di riuscire, attraverso la tutela del proprio interesse primario, a rappresentare anche distinti ed ulteriori interessi di carattere pubblicistico. In altri termini, la *cybersicurezza* rappresenta uno strumento di tutela eterogenea e di applicazione interdisciplinare. In particolare, ad esempio, la *cybersicurezza,* nel garantire l'inviolabilità delle reti, tutela altresì i dati digitali che in queste sono conservati. Dati digitali che, spesso, hanno carattere personale e per i quali si rende necessaria una particolare tutela che tenga altresì in considerazione la specifica normativa sui dati personali. La disciplina di sicurezza delle reti non esclude l'applicazione delle regole poste a protezione dei dati personali che prevedono l'adozione di "*misure tecniche e organizzative adeguate*"[77] tali da evitarne trattamenti non autorizzati, e, quindi, illeciti. La portata degli obblighi previsti dalla disciplina della protezione dei dati personali, è stato già osservato,[78] è in larga parta sovrapponibile alla disciplina sulla *cybersicurezza*: senza pretesa di esaustività, si consideri che entrambe le discipline prevedono misure di sicurezza "*adeguate*" alla gestione del rischio e tra queste rientra, ormai, anche la gestione del rischio *cyber*.

Ad oggi, la rinnovata consapevolezza della pericolosità del fenomeno ha oggi portato il legislatore nazionale ed europeo ad ideare una strategia normativa al fine di assicurare *ex ante* la tenuta cibernetica

Centrali dello Stato (56%, valore in aumento rispetto all'anno precedente) e infrastrutture IT riferibili a enti locali e strutture sanitarie (pari a circa il 30%). In ambito privato, sono stati interessati prevalentemente i settori energetico (24%), dei trasporti (18%) e delle telecomunicazioni (12%).

[77] Così prevede l'art. 5, Reg. 679/2016/UE, in tema di principi applicabili al trattamento dei dati personali, da leggere unitamente all'art. 24 sulla responsabilità del titolare del trattamento dei dati personali.

[78] In particolare, M. GIORDANO, I. OLDANI, M. SIMBULA, *Principi di sicurezza applicabili ai cloud computing services: GDPR, Direttiva NIS e PSD2 a confronto*, in *Ciberspazio e diritto*, 1/2020, p. 123; A. TINA, *op. ult. cit.,* p. 99 e, sulla complementarità delle due discipline, M. VIGGIANO, *Cybersecurity and Data Protection in European Union Policies and Rules: The NIS Directive anche the GDPR Synergy*, in G. DE MINICO, O. POLLICINO (a cura di) *Virtual freedoms terrorism and the law,* Giappichelli, 2020, p. 63-78. Ancora, sul rapporto tra *privacy* e *cybersicurezza* è interessante richiamare la guida dell'autorità inglese per la protezione dei dati personali. Lo stesso considerando 63 della "*direttiva NIS*" 2016/1148/UE osserva la possibile compromissione di dati personali a seguito di evento con un impatto sulla sicurezza della rete e dei sistemi informativi ragion per cui, poi, nel corpo della Direttiva si delinea, una rete di collaborazione e scambio di informazioni tra autorità e si prevedono "*ove opportuno e conformemente al diritto nazionale*" (art. 8) consultazioni e collaborazioni tra le autorità competenti e le autorità per la protezione dei dati nazionali. Ad oggi, tale direttiva è stata sostituita per effetto dell'entrata in vigore della Dir. 2022/2555 "*relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)*".

dei sistemi digitali così da limitare le possibilità di attacco, diversamente dalle prime disposizioni in materia che, complice l'assoluta novità del fenomeno, si concentravano su una "*difesa, per ora, di tipo prevalentemente - anche se non esclusivamente - reattivo*"[79].

5. Conclusioni

Le economie dei dati, per come brevemente descritte, si manifestano per una certa *complessità*, di cui se ne percepisce l'essenza. Si tratta di fenomeni economici che richiedono modalità di sfruttamento diversificate dei dati per le quali necessitano di approvvigionamenti costanti e che si sviluppano grazie ad elaborazioni tecniche sempre nuove. Le economie dei dati corrono lungo infrastrutture di comunicazione elettronica di rilevanza globale. Le economie dei dati hanno determinato la diffusione delle economie digitali e, con esse, nuove relazioni economiche e nuove modalità di manifestazione di diritti costituzionalmente garantiti veicolate dai dati.

E così, dunque, l'utilizzo dei dati con finalità economiche rappresenta altresì un fenomeno sociale complesso. Su tale complessità *sociale* interviene lo Stato, riconoscendo nuovi spazi e nuove modalità di intervento, estese ad ampi e diversi ambiti dell'ordinamento giuridico[80]. In risposta a tale fenomeno complesso, dunque, la risposta amministrativa risulta, ad oggi, altrettanto complessa, sicuramente complicata ma non per questo del tutto caotica.

Si è visto in precedenza come lo sfruttamento dei dati personali con finalità economiche sia suscettibile di essere regolato dalle disposizioni di tutela dei dati personali, dalle disposizioni di tutela del consumatore, dalle disposizioni a tutela della concorrenza, dalle singole disposizioni specifiche del settore economico interessato e, sempre più spesso, anche dalle disposizioni sulla *cybersicurezza*.

Ma i fenomeni complessi possono essere oggetto di approcci diversi e così le economie dei dati, guidate dalle tecnologie sviluppatesi nel corso degli ultimi anni, presentano nuove sfide, anche regolatorie, che non sono limitate al solo diritto: i paradigmi socio-economici ormai in via di consolidazione hanno stravolto i precedenti modelli sociali, economici, politici, culturali e finanche mentali[81].[82]

Il compito cui sono chiamati gli interpreti e gli studiosi del diritto è ora quello di verificare se, nelle ipotesi dei fenomeni complessi, l'attività di regolazione, tanto *ex ante* quanto *ex post*, possa essere applicabile nelle

[79] Presidenza del Consiglio dei ministri, "*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*", 2014, p. 11

[80] Ad esempio, il potere economico raggiunto dalle piattaforme digitali interessa anche i mercati finanziari tanto con riferimento alla profittabilità degli investimenti in esse quanto con riferimento all'espansione nell'erogazione di servizi finanziari ad opera delle stesse. In termini, A. CANEPA, *I mercanti dell'era digitali*, Giappichelli, Torino, 2020, p. 132.

[81] La scienza medica, infatti, si sta concentrando altresì sugli effetti psicologici dell'utilizzo di internet e, in particolare, sul conseguente calo del livello di attenzione registrato.

[82] Come rileva S. PIETROPAOLI, *Scienza giuridica e tecnologie informatiche: la complessità di un rapporto ineludibile*, in F. FAINI – S. PIETROPAOLI (a cura di), *Scienza giuridica e tecnologie informatiche*, Giappichelli, 2021, p. 4.

forme tradizionali ovvero se, per le loro peculiarità, tale attività richieda un adattamento dei diversi elementi del modello procedimentale.