

VALENTINA BARELA

ACCEZIONE AGGREGATA DEL DATO: SHUFFLE DEGLI INTERESSI IN GIOCO E NECESSITÀ DI UN APPROCCIO INTERDISCIPLINARE A PRESIDIO DEL DIRITTO DI AUTODETERMINAZIONE DELLA PERSONA

SOMMARIO: 1. Le mutate dinamiche relazionali nella nuova età tecnologica. Il diritto alla riservatezza quale primo tangibile emblema dell'evoluzione della valenza del dato. — 2. Accezione aggregata del dato. Valore patrimoniale e polifunzionalità dei big data. — 3. Centralità degli strumenti informatici in un sistema competitivo di big data. Incidenza sulle valutazioni concorrenziali e rischio di abuso di posizioni dominanti. — 4. Validità e limiti del consenso nel GDPR a fronte del valore competitivo dei big data. — 5. Riflessioni conclusive.

1. LE MUTATE DINAMICHE RELAZIONALI NELLA NUOVA ETÀ TECNOLOGICA. IL DIRITTO ALLA RISERVATEZZA QUALE PRIMO TANGIBILE EMBLEMA DELL'EVOLUZIONE DELLA VALENZA DEL DATO.

Negli ultimi venti anni si è assistito ad un enorme sviluppo tecnologico ¹, ove il flusso vorticoso di dati e informazioni ha rivoluzionato le dinamiche delle interrelazioni tra le persone coinvolgendo la sfera privata e pubblica dell'individuo, interferendo con la sistematica giuridica nonché con le fisionomie dei diritti anche di recente definizione. Si pensi al diritto alla riservatezza, del quale si è assistito ad una metamorfosi, per cui “da guscio protettivo della persona” è divenuto “patrimonio informativo circolante, come denominatore comune di tutte le realtà

¹ Sul rapporto dell'uomo con la tecnologia che ha mutato la “dimensione del nostro vivere” [...] “delineando una diversa antropologia” si veda l'apertura dei lavori di Pasquale Stanzone, Presidente dell'Au-

torità garante della protezione dei dati personali, al Convegno, *Privacy e neurodiritti. La persona al tempo delle neuroscienze*, 28 gennaio 2021, consultabile in www.garanteprivacy.it

industriali, commerciali, culturali, pubbliche e private e come riferimento costante in tutti i campi di attività”².

Nella società tecnologica, il diritto alla *privacy* si è evoluto, assumendo caratteristiche completamente nuove, tanto che si è reso necessario il ricorso ad un nuovo schema ricostruttivo di questo diritto. Si è passati dalla dimensione “passiva” del diritto alla riservatezza, inteso — secondo la teorizzazione dei due giuristi statunitensi, Samuel D. Warren e Louis D. Brandes — come “diritto ad essere lasciati soli” (“*The Right to be let alone*”) ³, ossia diritto individuale di libertà da esercitare e tutelare a fronte di intrusioni nella propria sfera privata, ad una forma attiva di partecipazione informativa e dunque al “diritto a disporre dei propri dati”. Di qui, nel tempo, il diritto alla *privacy* ha visto riconoscersi non solo una tutela statica, “negativa”, ossia volta ad escludere le interferenze altrui, di stampo angloamericano (appunto incentrata su una dimensione individualistica radicata sulla proprietà privata) ma anche una tutela dinamica, espressione di una autodeterminazione informativa *in primis* e decisionale poi, quale diritto a controllare le informazioni inerenti la propria persona e la propria vita, intesa come privata, lavorativa e sociale ⁴.

La trasformazione della *privacy*, piuttosto rappresentativa di quanto rivoluzionario sia stato l’avvento di Internet e del computer, ha determinato nuove esigenze di tutela della riservatezza dei dati personali ⁵, come, ad esempio, impedire che notizie

² Così, G. SANTANIELLO, *Tipologia delle innovazioni tecnologiche e protezione dei dati personali*, in AA.VV., *Innovazioni tecnologiche e privacy. Sviluppo economico e progresso civile* Sezione I - Protezione dei dati e sviluppo tecnologico, a cura di G. Rasi, 2004, in www.grantepriacy.it

³ Cfr. S.D. WARREN, L.D. BRANDEIS, *The Right to Privacy*, in 4 *Harv. L. Rev.* 193 (1890). Si legga A. STIANO “Il diritto alla *privacy* alla prova della sorveglianza di massa e dell’intelligenze sharing: la prospettiva della Corte Europea dei Diritti dell’Uomo”, in *Riv. di Dir. Intern.*, fasc. 2, 1 giugno 2020, p. 511 e ss., in cui si rileva come “la concezione così individuata era funzionale a garantire la protezione dei sentimenti e delle emozioni, come estensione del diritto alla proprietà privata, contro la crescente invadenza della carta stampata. In particolare, le caratteristiche che la stampa andava gradualmente assumendo, proiettava com’era verso un’ottica commerciale, facevano presagire i rischi crescenti di ingerenza nello spazio relativo alla vita privata e domestica dell’individuo”. Alla nozione personalistica del diritto alla *privacy*

per cui la diffusione non volontaria di informazioni personali o la diffusione di false informazioni rappresentavano una forma di violazione della *privacy*, si è contrapposta quella dominicale, riconducibile al concetto di proprietà intellettuale. Si veda G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 214 e ss. Nel nostro ordinamento, le prime analisi del diritto ad essere lasciati sono prevalentemente lette in F. Carnelutti, *Il diritto ad una vita privata*, in *Riv. trim. dir. pub.*, 1955, p. 3.

⁴ Sul punto si v. M.G. STANZIONE, *Consenso e trattamento dei dati personali nella dimensione europea*, in AA.VV., *I “poteri privati” delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, p. 79; G. CERRINA FERRONI, *I dati personali come oggetto di un diritto fondamentale*, in *ult. op. cit.*, p. 71.

⁵ Secondo una prima definizione sono “dati personali” tutte le informazioni che identificano o rendono identificabile una persona fisica e che possono fornire dettagli sulle sue caratteristiche, le sue abitudini, stile di vita, relazioni personali, stato di salute, situazione economica, ecc. All’in-

riguardanti la sfera intima della persona possano essere divulgate e conosciute da terzi, con il rischio di procurare forme di discriminazione. Ruolo centrale è stato poi assunto dalle nuove e febbrili forme di comunicazione e strumenti di informazione, si pensi ai blog, ai social network ⁶, alle riviste online, alla messaggistica istantanea che hanno posto ad alto rischio il rispetto della dignità. Questa nuova era digitale ha sopraffatto l'uomo, potenziando le strumentalità dei più forti e "strutturati" finanziariamente, ma mortificando le capacità di controllo del singolo individuo, dando origine a turbolenti fenomeni, nuovi diritti e diverse esigenze; si pensi alle fake news, al diritto all'oblio ⁷ o alla necessità, da ultimo, di identificare i cc.dd. *gatekeepers*, ossia coloro che gestiscono la diffusione di specifiche notizie, che detengono pertanto il grande potenziale di garantire o minacciare in modo drammatico la democrazia del pensiero. Al fine di arginare i danni conseguenti ad un controllo fazioso delle notizie, il recente Regolamento *Digital Market Act*, adottato dal Parlamento europeo e dal Consiglio il 14 settembre 2022 ha inteso disciplinare il ruolo, all'interno dei mercati digitali, di coloro che, appunto, si occupano di gestire piattaforme e servizi strategici che collegano in via diretta consumatori e aziende, per costruire un ambiente di-

terno di questa categoria generale, si possono distinguere: dati identificativi, che sono quelli che permettono l'identificazione diretta, come i dati anagrafici (ad es., il nome e cognome), le immagini, ecc.; i dati sensibili che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale; i dati giudiziari che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (a titolo esemplificativo, i provvedimenti penali di condanna definitiva, la liberazione condizionale, il divieto ad obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato. Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni elettroniche (via telefono o internet) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

Sulle ambiguità ed insidie che si celano dietro questa espressione si v. ZENO-ZENCOVICH - G. GIANNONE CODICILIONE, *The Legal perspectives on the "Big data Revo-*

lutions", in *Concorrenza e mercato*, n. 2, 2016, p. 35; R.S. HEIMES, *Privacy and Innovation: Information as Property and the Impact on Data Subject*, in *New Eng. L. Rev.*, 49, 2015, p. 649; P.M. SCHARTZ, *Property and Personal Data*, in *Harv. L. Rev.*, 117, 2004, p. 2056.

⁶ Si v. S. SICA - G. GIANNONE CODICILIONE, *I social network sites e il "labirinto" delle responsabilità*, in *Giur. mer.*, n. 12, 2012, p. 2714 e ss.

⁷ Cfr. art. 17 del Regolamento generale sulla protezione dei dati. Sull'argomento si v. V. D'ANTONIO, *Oblio cancellazione dei dati nel diritto europeo*, in S. SICA - V. D'ANTONIO - G.M. RICCIO, *La nuova disciplina europea della privacy*, Padova, 2016, p. 197; G. RESTA, V. ZENO-ZENCOVICH, *Il diritto all'oblio dopo la sentenza Google Spain*, Roma, 2015, *passim*; T.E. FROSINI, *Google e il diritto all'oblio preso sul serio*, in *Il diritto dell'informazione e dell'informatica*, n. 4-5, 2014, p. 563 e ss.; M.C. PERCHINUNNO, *Identità personale, identità digitale e diritto di cronaca*, in *Contratto e impresa*, n. 4, 2020, p. 1442 e ss. Per una disamina comparatistica si v. AA.VV., *The Right To Be Forgotten. A Comparative Study of the Emergent Right's Evolution and Application in Europe, the Americas, and Asia*, a cura di F. Werro, Springer-Verlog, 2020, *passim*.

gitale più leale e stimolare l'innovazione del settore proteggendo i consumatori ⁸.

L'inadeguatezza dell'originale approccio al tema della riservatezza (secondo lo schema della proprietà privata, "my home my castle") è pertanto conseguente alla registrazione nella rete delle moltissime attività digitali compiute dagli utenti del *web* — spesso inesperti e inconsapevoli delle "tracce" dai medesimi lasciate con le proprie azioni nel mondo digitale — che sollevano la necessità di un adeguamento dell'impianto normativo sul tema. Ciò soprattutto in ragione del fatto che l'utente del *web*, ad oggi, è sì fruitore, ma anche produttore di contenuti informativi mediante la condivisione di documenti di vario genere (come ad esempio, fotografie, filmati, raccolte di testi), la realizzazione di siti in cui sviluppare il proprio diario pubblico o la partecipazione ai *social network*.

Inoltre, dalla diffusione di una grande quantità di dati, anche personali, nel mondo digitale e dalla correlata possibilità di utilizzazione della stessa da parte di soggetti privati, ma anche pubblici, per le più diverse finalità, è derivata pertanto la necessità di affiancare alla tutela della *privacy* intesa in senso tradizionale (come diritto al rispetto della propria sfera personale), una tutela che va oltre la sfera della vita privata e delle relazioni sociali, garantendo il controllo sulla circolazione dei propri dati personali, divenuto indispensabile.

Difatti, il Regolamento UE n. 2016/679 ⁹, noto come GDPR, ha avuto primariamente proprio lo scopo di perseguire un equilibrio tra la protezione dei diritti personali e l'innovazione nella società dell'algoritmo e permettere lo sviluppo del Mercato Unico Digitale (*Digital Single Market*) Europeo, senza addentrarsi tuttavia nelle dinamiche sinallagmatiche del contratto, né quelle volte al riconoscimento ed inquadramento del *new property right* delle "in-

⁸ Il Digital Market Act (DMA) è entrato in vigore il 1° novembre 2022 e diventerà applicabile il 2 maggio 2023. Entro due mesi da tale data, le imprese che forniscono servizi di piattaforma di base dovranno notificare alla Commissione se soddisfano le soglie quantitative e fornire tutte le informazioni pertinenti. La Commissione disporrà quindi di 45 giorni lavorativi per adottare una decisione che designi un *gatekeeper* specifico. Costui disporrà di un massimo di sei mesi dopo la decisione della Commissione per garantire il rispetto degli obblighi e dei divieti stabiliti nel DMA. I documenti pubblicati dal Parlamento europeo e dal Consiglio forniscono una buona

panoramica delle cose da fare e da non fare che i guardiani dovranno rispettare.

⁹ Per effetto dell'entrata in vigore del Regolamento Generale sulla protezione dei dati, viene ad essere abrogata la Direttiva CE n. 46/1995. Questa Direttiva, emanata il 24 ottobre 1995, in materia di tutela delle persone fisiche, con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, si è dimostrata — per la sua semplicità di impianto, uno strumento idoneo a consentire ai nuovi Paesi, nel corso degli anni entrati a far parte dell'Unione Europea, di adempiere all'obbligo di dotarsi di legislazioni di protezione dati con essa coerenti.

formazioni digitali”¹⁰. Ad ogni modo al Regolamento europeo, rispetto all’impostazione del codice della privacy, si deve dare il merito di aver spostato l’attenzione sul controllo dei dati, proprio perché ne fosse riconosciuta la libera circolazione, con conseguente rafforzamento dei diritti dell’interessato, il quale deve sapere se i suoi dati sono usati e come vengono usati, al fine di tutelare sé stesso¹¹.

Il valore economico e la forza competitiva del dato sono però divenuti esponenziali soprattutto nella composizione aggregata del dato, ossia quando esso è considerato in associazione con altri dati¹². La disponibilità di una grande quantità di dati, in tal caso, può incidere in modo determinante sulla crescita economica dell’attività autorizzata ad utilizzarli e questo fattore coinvolge interessi pubblici ed economici, come la competitività, particolarmente vigilata soprattutto oltreoceano¹³. L’Europa, ad ogni modo, rimane un terreno maggiormente sensibile alla tutela dei

¹⁰ Sul punto si v. V. FALCE, *Big data e diritti esclusivi: Liasons dangereux tra innovazione e mercato*, in AA.VV., *Informazione e big data tra innovazione e concorrenza*, a cura di V. Falce, G. Ghidini e G. Olivieri, Milano, 2018, pp. 114-115. Sulla inadeguatezza della nozione materiale di proprietà dei paesi di *civil law* e sulla maggiore adattabilità della nozione anglosassone di *property* si v. S. SICA - V. D’ANTONIO, *La commodification dei dati personali nella data driven economy*, cit., p. 133 e ss. G. ALPA, *La proprietà dei dati personali, in Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 27.

¹¹ Non è un caso che nel Considerando 9 del Regolamento n. 679/2016, con tono critico sia espressamente affermato che “sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell’applicazione della protezione dei dati personali nel territorio dell’Unione, né eliminato l’incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La presenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all’interno dell’Unione. Tali differenze possono pertanto costituire un freno all’esercizio delle attività economiche su scala dell’Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell’Unione

[...]”. Si v. F. PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo sulla Privacy*, Torino, 2016, passim; M.G. STANZIONE, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. e dir. priv.*, fasc. 4, 2016, p. 1249 e ss.

¹² Cfr. L. CALIFANO - C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati nel Regolamento UE 2016/679*, Napoli, 2017, passim; V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, n. 2, 2018, p. 32.

¹³ E. MACCIO, D. MULA, *Big data e strumenti negoziali*, in AA.VV., *Informazione e big data tra innovazione e concorrenza*, cit., p. 149 e ss. Invero, un tema molto complesso negli US è il rapporto tra interesse pubblico, interesse nazionale ed il diritto e la libertà degli utenti di conoscere e disporre dei propri dati personali. Al riguardo, ed in particolare in merito al trasferimento dei dati all’estero, fuori UE, si v. V. D’ANTONIO, *I “ponti” per il trasferimento di dati Eu-USA: dai Safe Harbour Privacy Principles al Privacy Shield*, in *Scritti in onore di Mario G. Losano, Dalla filosofia del diritto alla comparazione giuridica*, a cura di A. Somma, Torino, 2021, p. 31; S. SICA-V. D’ANTONIO, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in AA.VV., *La protezione transnazionale dei dati personali*, a cura di G. Resta e V. Zeno-Zencovich, Roma, 2016, p. 137 e ss.; M. MACCIOLINO, *I big data tra Stati Uniti e Unione Europea*, in AA.VV., *Informa-*

diritti della persona e quindi alla tutela del dato personale, intesa anche nel suo significato originale. D'altronde, come è ben noto, la disciplina introdotta con il Regolamento si è andata ad aggiungere a quelle già presenti nel panorama europeo e a livello nazionale in cui erano già riconosciuti i due distinti diritti fondamentali oggetto di ulteriore normazione: il diritto alla *privacy*¹⁴, e la protezione dei dati personali. Si ricorda che il primo era stato codificato per la prima volta nella Convenzione Europea dei Diritti dell'Uomo (CEDU), con la previsione dell'art. 8, par. 1, in base al quale "ognuno ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza"¹⁵, e protetto anche da Convenzioni internazionali (la Convenzione americana sui diritti dell'uomo, il cui art. 11 rispecchia sostanzialmente il dettato dell'art. 8 della CEDU), mentre il secondo aveva trovato riconoscimento nell'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea (CFRUE) e nell'art.

mazione e big data tra innovazione e concorrenza, a cura di V. Falce, G. Ghidini e G. Olivieri, Milano, 2017, p. 265 e ss.; G. GIANNONE CODICILIONE, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in *Il Diritto dell'informazione e dell'informatica*, fasc. 4-5, 2015, p. 286 e ss. V. D'ANTONIO, *Il trasferimento dei dati all'estero*, sub artt. 42-45, in S. Sica, P. Stanzone, *Nuova disciplina della privacy*, Bologna, 2005, p. 155 e ss.

¹⁴ In Italia, uno dei primi interventi legislativi in materia di protezione dei dati è riconducibile alla L. n. 675/1996, concernente la tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Trattasi della legge di recepimento italiana della Direttiva n. 95/46/CE ed introdotta per rispettare gli Accordi di Schengen, entrata in vigore nel maggio 1997 e poi abrogata dal D.Lgs. 30 giugno 2003 n. 196, meglio noto come Codice in materia di dati personali. L'entrata in vigore del Codice, avvenuta il 1° gennaio 2004, ha rappresentato la conclusione del processo di recepimento delle Direttive europee in materia (la n. 95/46/CE e la n. 2002/58/CE), riunendo in un unico testo una regolamentazione che si era, nel tempo, stratificata a seguito di numerosi interventi modificativi e integrativi.

¹⁵ È opportuno riferire che diverse Convenzioni internazionali sui diritti umani riconoscono la privacy quale diritto fondamentale della persona. Il Consiglio dei diritti umani delle Nazioni Unite si è più volte espresso nel senso che "gli stessi diritti che le persone hanno offline devono essere tutelati anche online". L'art. 8, paragrafo 1,

della Convenzione Europea dei diritti dell'uomo (CEDU) chiarisce che "ognuno ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza", mentre l'art. 8, paragrafo 2, elenca le legittime interferenze con tale diritto, prevedendo che "non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisce una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui". Nell'Unione Europea, il diritto alla vita privata e alla protezione dei dati è sancito anche dall'art. 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea (CFRUE), e dall'art. 16, paragrafo 1, del Trattato sul Funzionamento dell'Unione Europea (TFUE), in base ai quali "ognuno ha diritto alla protezione dei dati personali". L'art. 8 del CFRUE elenca i principi che devono essere rispettati in relazione al trattamento dei dati personali, attuati dalla Direttiva n. 95/46/CE, successivamente abrogata dal Regolamento UE n. 2016/679 (GDPR). Si segnala, poi, che la *privacy* e la protezione dei dati sono disciplinate anche da accordi coinvolgenti Stati non europei. Tra gli stessi, viene in rilievo la Convenzione americana sui diritti dell'uomo adottata nel 1969, il cui art. 11 rispecchia l'art. 8 della CEDU e riconosce che "nessuno può essere oggetto di interferenza arbitraria o abusiva con la sua vita privata, la sua famiglia, la sua casa o sua corrispondenza, o di illeciti attacchi al suo

16, comma 1, del Trattato sul Funzionamento dell'Unione Europea (T.F.U.E.), alla cui stregua "ognuno ha diritto alla protezione dei dati personali che lo riguardano".

2. ACCEZIONE AGGREGATA DEL DATO. VALORE PATRIMONIALE E POLIFUNZIONALITÀ DEI BIG DATA.

L'insieme crescente delle informazioni generate da sorgenti eterogenee, quali *log*, *e-mail*, *social media* e *database* tradizionali, divulgate attraverso le piattaforme digitali, è diventato evidentemente oggetto di interesse per le imprese operanti nell'odierna economia sempre più *data driven*¹⁶, e l'accesso ai dati degli utenti del *web* ha rappresentato (e tuttora rappresenta) per le stesse una grande opportunità, in quanto, attraverso la conoscenza delle informazioni sulle preferenze e sui bisogni dei consumatori ricavate dalla memorizzazione delle stesse sui siti *Internet* dai medesimi visitati, è possibile offrire servizi sempre nuovi, qualitativamente migliori, personalizzati rispetto alle esigenze dei singoli consumatori e a prezzi più accessibili rispetto a quelli praticati sui mercati tradizionali.

La digitalizzazione ha coinvolto, pertanto, non solo le persone e le loro vite private, ma anche l'economia, tanto che si è parlato di una "quarta rivoluzione industriale", di cui caratteristiche principali sono proprio i dati e la velocità. L'innovazione tecnologica, che ha contribuito allo sviluppo di un mondo virtuale caratterizzato sempre più da globalità e multidimensionalità, ha fatto emergere anche un nuovo ruolo e un nuovo valore del "dato", in ragione del fatto che lo stesso non è più isolato, ma parte integrante di raccolte digitali, dinamiche e interattive. L'incremento costante e l'enorme varietà dei dati trasmessi e scambiati sulle *attention platforms* (quali i motori di ricerca e i *social networks*) e sulle *matching platforms* (ossia piazze di scambi virtuali) ha dato origine all'ecosistema dei "*Big Data*", i cui tratti caratteristici sono rappresentati, come noto, dalle quattro "V": *Volume*, *Velocità*, *Varietà* e *Veridicità*, cui nel tempo se n'è aggiunta una

onore o alla sua reputazione". Si ricorda, infine, che alla Convenzione 108 adottata dal Consiglio d'Europa nel 1981 — primo accordo internazionale vincolante sulla protezione dei dati e unico in materia di sicurezza e sorveglianza nazionale — possono aderire anche i non membri del Consiglio d'Europa. I Paesi extraeuropei hanno infatti firmato la Convenzione e adottato le linee guida sulla tutela dei diritti individuali contro il trattamento automatizzato dei dati personali. Anche a livello nazionale sono adottati testi normativi in tema di *privacy* e

di protezione dei dati, nella generalità dei casi basati su principi comuni, come quelli della limitazione della raccolta, della qualità dei dati, della specificazione delle finalità, della limitazione dell'uso, delle garanzie di sicurezza, dell'apertura, della partecipazione individuale e della responsabilità. Ciò è dovuto principalmente al fatto che le normative nazionali sono state fortemente influenzate dai principi sanciti dalle linee guida dell'OCSE.

¹⁶ Si v. S. SICA-V. D'ANTONIO, *La com-modification dei dati personali nella data driven society*, cit., p. 130 e ss.

quinta, quella di *Valore*, tradottasi, poi, nelle dinamiche competitive in termini di “*potere di mercato*”¹⁷.

La massiccia quantità di dati e di informazioni divulgate attraverso le piattaforme digitali in favore delle imprese per ottenere beni o servizi, o per condividere con altri utenti foto, messaggi attraverso i *social networks*, è diventata oggi la nuova energia dell'economia, posto che la sua conoscenza consente di orientare le offerte e di comprendere l'andamento dei mercati e il sentimento dei consumatori¹⁸.

Nell'attuale economia digitale, avere accesso a queste grandi raccolte di dati e saperne estrarre valore e conoscenza, attraverso le tecnologie di *analytics*¹⁹, è diventato la vera chiave competitiva per le grandi aziende e le piccole medie imprese.

Grazie all'utilizzo di tecniche di analisi altamente sofisticate,

¹⁷ Gli studiosi sono concordi nell'affermare che i *Big Data* costituiscono degli aggregati di dati di notevoli dimensioni, che si espandono continuamente e velocemente. Da qui l'individuazione dei loro tratti caratteristici che li distinguono dalle banche dati tradizionali, rappresentati dal Volume, dalla Velocità, dalla Varietà e Veridicità, oltre che dal Valore. Esaminando singolarmente, si può affermare che per “Volume” deve intendersi la quantità dei dati (strutturati o non strutturati) generati ogni secondo. Tali dati sono generati da sorgenti eterogenee, quali: log, e-mail, social media e database tradizionali; per “Varietà” deve intendersi la diversa tipologia di dati che vengono generati, accumulati e utilizzati; per “Velocità” deve intendersi la velocità con cui i nuovi dati vengono generati. A tal proposito, viene in rilievo non solo la rapidità nella generazione dei dati, ma anche la necessità che questi dati/informazioni arrivino in un sistema *real-time*, al fine di effettuare un'analisi degli stessi; per “Veridicità”, deve intendersi la misura dell'affidabilità dei dati; per “Valore” deve intendersi il risultato del processo di analisi del dato, ossia la conoscenza che si ottiene quando vengono utilizzate le informazioni acquisite e che permettono alle imprese nei processi aziendali di migliorare le *performance*, di prendere decisioni più informate, tempestive e consapevoli proprio grazie al vasto mondo dei *Big Data*. Si legga, *ex pluribus*, M. GAL - D.L. RUBINFELD, *Access Barriers to Big Data*, 2016 disponibile su <http://arizonalawreview.org/pdf/59-2/59arizbre339.pdf>; ancora, sul tema, S. HOFFMANN (2016), *Electronic Health Records and Medical Big Data*, Cambridge University Press, 111; R. WALKER (2015), *What is Big Data?*, Oxford University Press Scholarship

Online; S.G. HOFMANN (2016), *Regulation of Cloud Service under US and EU Antitrust Competition and Privacy Laws*, Peter Lang Academic Research, Frankfurt am Main, p. 35 e ss.; cfr. sul punto anche M.E. STUCKE, A. GRUNIS (2016), *Big Data and Competition Policy*, Oxford University Press, p. 16 e ss.

¹⁸ Questa è espressione è alquanto rappresentativa del valore aggiunto offerto dai dati. Si legga A. D'ADDA e C. FORTUNATI “I dati sono il nuovo petrolio delle compagnie di assicurazioni”, *Il Sole 24 ore*, 4 dicembre 2019.

¹⁹ Con riguardo alle varie tipologie di tecniche di analisi dei dati più sofisticate, è necessario menzionare i *data mining*, ovvero l'insieme di tecniche e metodologie che hanno per oggetto l'estrazione di un'informazione a partire da grandi quantità di dati (e l'utilizzo scientifico, industriale o operativo di questa informazione). Molto utile è, altresì, l'analisi predittiva, che cerca di prevedere il comportamento dei clienti, i guasti delle attrezzature, delle strumentazioni ed apparecchiature aziendali oltre che di altri eventi futuri, che possono minare profondamente le sorti delle aziende. La *machine learnig* che rappresenta una tecnica di intelligenza artificiale che utilizza algoritmi automatizzati per “sfogliare” i *set* di dati in modo estremamente rapido. Il *machine learnig* è stato adottato in una vasta gamma di settori per supportare diversi obiettivi aziendali, tra cui il calcolo del valore del ciclo di vita del cliente, la determinazione dei prezzi dinamici, la manutenzione predittiva, la classificazione delle immagini. La creazione del modello di calcolo del valore del ciclo di vita del cliente si è rivelata di fondamentale importanza per le aziende di e-commerce, ma è applicabile anche in molti altri settori,

dette “*big data analytics*”, su grandi volumi di dati (strutturati, semi — strutturati e non strutturati), gli stessi vengono trasformati in informazioni utili e funzionali per l’ottimizzazione della presa di decisioni, comportanti, ad esempio, modifiche ai processi interni all’organizzazione dell’impresa in tutte le sue funzioni aziendali (*marketing*, vendite, acquisiti, logistica, HR, ecc.), o modifiche alla struttura stessa dei mercati (si pensi alle iniziative di *Google* nel mondo dei viaggi o in quello del *digital marketing*, sfruttando la conoscenza degli utenti del *web*).

Tuttavia, se è innegabile l’incremento dell’efficienza e delle opportunità profittevoli per le imprese conseguenti all’utilizzo di nuovi e performanti strumenti di analisi dei dati — potendo le stesse, attraverso la raccolta e l’analisi di dettagliate informazioni sui consumatori, sviluppare un sistema di *digital marketing* personalizzato, grazie alla conoscenza della cronologia delle attività dell’utente del *web* e delle sue preferenze — altrettanto innegabili sono i nuovi rischi creati dall’utilizzo dei *dataset* e dai mercati digitali sotto i profili della protezione dei dati personali, del pluralismo informativo e della concorrenza ²⁰.

La capacità di analisi e di valorizzazione ed elaborazione dei dati, da parte dei grandi operatori digitali attivi su scala globale, ha dato origine a nuove forme di sfruttamento economico del dato e della sua valorizzazione ai fini della profilazione algoritmica legata a diversi scopi commerciali, generando nuove concentrazioni di potere; da ciò l’emergere di nuove problematiche giuridiche connesse al tema della “commercializzazione” o “patrimonializzazione” dei dati personali, ossia della possibilità di attribuire al dato un valore economico, di scambio, equiparabile a quello della moneta.

Nell’attuale mercato digitale, il dato, solo originariamente considerato estrinsecazione dell’identità e della personalità dei soggetti cui inerisce, ha acquisito un valore patrimoniale non solo però per gli operatori economici che possono compiere attività di profilazione sottesa ad offerta più vincente ma anche per i consumatori/utenti del *web* che sono di fatto obbligati ad offrire i propri dati personali per accedere ai servizi digitali, solo in apparenza gratuiti ²¹. Si è parlato della c.d. “trappola del dono”, intendendosi con tale espressione il fatto che l’utente del *web*

in quanto con lo stesso si valutano enormi quantità di dati di clienti, per determinare quelli che effettuano più acquisti, i più fidelizzati o una combinazione di questi due tipi di clienti. Dette informazioni consentono, dunque, alle aziende di concentrarsi sulle strategie di *marketing* per incoraggiare i clienti ad interagire con il loro *brand*.

²⁰ Si cfr. R.M. VISCONTI, *Valutazione dei Big data e impatto su innovazione e digital branding*, in *Il Dir. Ind.*, n. 1, 2016, p. 46 e ss.

²¹ Sul tema del dato quale forma di “moneta di scambio” cfr. A. De FRANCESCO, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, p. 67 e ss.; F. BRAVO, *Lo “scambio dei dati personali”*

viene tratto in inganno dall'offerta di un servizio solo in apparenza gratuito, in realtà "remunerato" con la cessione, più o meno consapevole, dei propri dati personali ²². Viene, dunque, a configurarsi una situazione in cui i servizi digitali vengono offerti a "prezzo zero", contro il consenso dell'utente al trattamento dei propri dati personali per scopi spesso non necessari alla fornitura dei servizi stessi, con la conseguenza che il numero di dati acquisiti è superiore a quello strettamente necessario e questo *surplus* di dati viene a rappresentare una forma di remunerazione del servizio del titolare da parte dell'interessato. Parimenti, nel caso dell'attività di marketing, affiancata al trattamento principale dei dati, la cessione dei dati personali può essere considerata controprestazione non monetaria del trattamento principale solo apparentemente gratuito ²³.

È evidente come questa nuova dimensione del dato — non più solo estrinsecazione dell'identità e della personalità degli individui cui inerisce, ma anche risorsa suscettibile di sfruttamento economico, in quanto capace di diventare controprestazione a fronte dell'offerta di beni o servizi digitali secondo gli schemi sinallagmatici — abbia reso necessario assicurare al diritto alla *privacy* una tutela aggiuntiva, estesa anche alle attività riguardanti il trattamento dei dati personali; ciò anche in ragione del

nei contratti di fornitura dei servizi digitali e il consenso dell'interessato tra autorizzazione e contratto, in *Contr. e Impresa*, 2019, p. 34 e ss.; V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inf.*, 2018, p. 709; F. CACCIA, *La libertà ed espressione del consenso, in I dati personali*, a cura di V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, 2020, p. 249 ss.; A. STAZI, F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparativistica*, in questa *Rivista*, fasc. 2, 1 aprile 2019, p. 442 e ss.

²² Cfr. T.E. FROSINI, *Libertà, Egalité Internet*, seconda ed., Napoli, 2019, p. 19 e ss. S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e diritto privato*, 2016, p. 513 e ss.

²³ L'allerta dei Garanti sul punto è abbastanza risalente. Il Garante per la protezione dei dati personali, in numerosi provvedimenti, tra cui il prov. 4-7-2013 n. 330, reperibile sul sito www.garanteprivacy.it, doc. web n. 2542348, ha ribadito che è necessario che l'interessato sia previamente informato che la prestazione del consenso a fini ulteriori non condiziona l'accesso al

servizio; parimenti, l'AGCM abituata a valutare l'offerta di servizi gratuiti subordinati a messaggi promozionali, ha rilevato che la circostanza con la quale l'operatore subordini la prestazione di un servizio espressamente qualificato come "gratuito" alla possibilità di inviare messaggi pubblicitari all'utente non può considerarsi indifferente ai fini della valutazione della convenienza dell'offerta e può integrare una pratica commerciale scorretta laddove suscettibile di indurre in errore il consumatore. Si confrontino sul punto i provvedimenti del 20 dicembre 2001 nn. 10270, 10276, 10277, 10278 e 10279. È di tutta evidenza come l'illegittima raccolta dei dati presenti in una piattaforma o la loro cattiva gestione da parte del professionista possa integrare una possibile violazione dei principi in materia di corretto trattamento dei dati personali (materia di interesse del Garante per la protezione dei dati personali), ma al contempo costituire anche oggetto di indagine da parte dell'AGCM, chiamata a verificare se la richiesta dei dati sia avvenuta secondo modalità tali da condizionare la libertà di scelta del consumatore, interessato solo all'ottenimento del premio relativo ad una campagna promozionale, obbligandolo anche a partecipare al programma di fidelizzazione della clientela.

fatto che all'utente/consumatore è sostanzialmente precluso conoscere, sin dal momento della raccolta dei propri dati, il futuro ed eventuale impatto che un nuovo trattamento applicato al materiale informativo acquisito potrebbe avere su di lui.

Questa lettura del fenomeno, la realistica presa di coscienza del valore commerciale dei dati personali, tanto da considerarli assimilabili ai beni in senso giuridico e, dunque, possibile oggetto di disposizione mediante lo strumento contrattuale, viene evidenziata non solo dall'Autorità Garante della Concorrenza e del Mercato, ma anche dalla Giurisprudenza nazionale, trovatisi a vagliare di recente la legittimità dei provvedimenti adottati dalla predetta Autorità per pratiche commerciali scorrette poste in essere da importanti operatori commerciali ²⁴.

Ed è proprio l'acquisita consapevolezza del valore economico dei dati informativi, delle numerose finalità di utilizzo delle raccolte massive dei dati e dell'estensione ormai globale della filiera legata ai dati stessi, che ha indotto il Legislatore Europeo a cristallizzare questo punto con la Direttiva n. 771/2019 relativa a determinati aspetti di fornitura di contenuto digitale e di servizi

²⁴ Si legga la sentenza del TAR Lazio, Roma, n. 261 del 10 gennaio 2020, in www.giustizia-amministrativa.it, con cui è stata definita la vicenda giudiziaria che ha visto contrapposti l'Autorità Garante della Concorrenza e del Mercato e Facebook Inc. in relazione a presunte pratiche commerciali scorrette da quest'ultima poste in essere in violazione degli artt. 20, 21, 22, 24 e 25 del Codice del Consumo (D.lgs. 6 settembre 2005 n. 206). Con detta pronuncia, il Giudice Amministrativo ha sanzionato la pratica posta in essere da Facebook Inc. in violazione degli artt. 21 e 22 del Codice del Consumo, per aver indotto irragionevolmente gli utenti/consumatori a registrarsi sulla piattaforma senza averli adeguatamente e tempestivamente informati del fatto che avrebbe trattato i loro dati per finalità commerciali o per monetizzarli, enfatizzando la sola gratuità del servizio. In detta sentenza si è affermato che "A fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili forme di protezione, quali il diritto di revoca del consenso, di accesso, di rettifica, oblio, sussiste pure un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati". Da tale premessa il Giudice Amministrativo trae la conclusione che "il fenomeno della "patrimonializzazione" del dato

personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un "social network", ritenendo non condivisibili le argomentazioni difensive di Facebook secondo le quali l'unica tutela del dato personale sarebbe rinvenibile nella sua accezione di diritto fondamentale dell'individuo. Detto approccio è stato ritenuto non condivisibile dal Giudice investito della controversia, proprio perché — si legge nella citata pronuncia — "sconta una visione parziale delle potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un "asset" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto". Il TAR del Lazio afferma, dunque, il principio in base al quale: "in termini generali, il valore economico dei dati dell'utente impone al professionista di comunicare al consumatore che le informazioni ricavabili da tali dati saranno usate per finalità commerciali che vanno al di là della utilizzazione del social network: in assenza di adeguate informazioni, ovvero nel caso di affermazioni fuorvianti, la pratica posta in essere può

digitali, attuata in Italia con D.lgs. 4 novembre 2021 n. 173, per cui, ai sensi del nuovo articolo 135-*octies*, il professionista può fornire un contenuto o un servizio digitale al consumatore a fronte del pagamento di un prezzo oppure della comunicazione dei dati personali del consumatore stesso. Si registra, inoltre, in tal senso anche l'orientamento del Consiglio di Stato, che con decisione del 29 marzo 2021, n. 2631 ha dichiarato l'illiceità delle dichiarazioni di gratuità del contratto da parte del gestore di un social network spianando la strada per la piena legittimazione della scelta del soggetto di consentire il trattamento dei propri dati personali anche come esercizio della libertà economica ²⁵, contemplata dall'art. 135-*octies* del Codice del Consumo.

3. CENTRALITÀ DEGLI STRUMENTI INFORMATICI IN UN SISTEMA COMPETITIVO DI BIG DATA. INCIDENZA SULLE VALUTAZIONI CONCORRENZIALI E RISCHIO DI ABUSO DI POSIZIONI DOMINANTI.

Non può negarsi che il fenomeno dei *data* e del valore dei dati in ragione del loro assemblamento comporti l'adozione di strumenti informatici che tra l'altro sono sempre in evoluzione; d'altronde, la stessa aggregazione opera a flusso continuo, in modo automatico, determinando una crescente progressione geometrica dell'informazione. La massimizzazione della utilità del dato è possibile proprio dalla correlazione con altri dati, la cui modalità è variabile e diversamente efficace, a seconda della finalità a cui è sotteso l'utilizzo, che andrà ad ogni modo ad incidere sulle caratteristiche del servizio. L'accessibilità a tali dati ha modificato in modo radicale le modalità con le quali vengono offerti ed erogati i servizi.

L'acquisizione del dato può essere compiuta dal singolo operatore, ovvero attraverso terzi che offrono il proprio servizio di assemblamento e catalogazione, i big data provider, ossia infrastrutture di dati, con cui vengono instaurati specifici rapporti contrattuali, attraverso contratti di somministrazione di servizi, che sigillano il rapporto tra il big data provider e il big data supplier. Questo strumento contrattuale non è tuttavia in grado di garantire la tutela delle aspettative del big data supplier, posto che il valore dei big data non è intrinseco, ma è strettamente

quindi qualificarsi ingannevole". La citata sentenza si spinge oltre il riconoscimento della valenza negoziale del dato personale, affermando, tra l'altro, l'assenza di incompatibilità tra le norme a tutela del consumatore e quelle a tutela del dato personale, ponendosi le stesse "in termini di completezza, imponendo, in relazione ai rispettivi fini di tutela, obblighi informativi

specifici, in un caso funzionali alla protezione del dato personale, inteso quale diritto fondamentale della personalità, e nell'altro alla corretta informazione da fornire al consumatore al fine di fargli assumere una scelta economica consapevole".

²⁵ Si veda Cons. Stato, 29 marzo 2021 n. 2631, in *Diritto della famiglia e delle persone*, n. 3, I, 2021, p. 963.

correlato non solo alla quantità dei dati ma anche alla combinazione delle informazioni archiviate, che determina l'effettivo valore economico, variabile a seconda dell'attività che deve essere svolta attraverso quei dati, e quindi a seconda del destinatario di tali dati. D'altronde le "informazioni", non sono tutelabili in quanto tali ma solo nella misura in cui rappresentano "valore economicamente utile". Analogamente, sotto il profilo soggettivo in sede contrattuale, ciò che acquista centralità non è oggi il tema della titolarità del singolo, bensì quello dell'accessibilità al dato o ai dati, così come l'assenza di una *net neutrality* e quindi la necessità di garantire una simmetria tra la disponibilità dei dati del comune utente e quella degli operatori dei big data, in modo da superare quella disparità che sembra riproporre le disparità tra consumatore professionista.

Acquisito il loro peculiare valore nella misura in cui sono assemblati in un determinato modo, attraverso sistemi quali gli algoritmi, si deve constatare che i *data* attribuiscono dei diritti che non sono comunque propriamente dominicali ²⁶, giacché preminenza è assunta dall'utilizzo che terzi possono fare degli stessi, e della effettività o meno del diritto del titolare di ordinare la cancellazione dei dati forniti. I dati, invero, in ragione della loro ampia usufruibilità, del valore economico e delle incidenze sulla competitività del mercato, nonché dell'impatto sociale che generano, possono anche essere beni collettivi, nella misura in cui essi rappresentano arricchimento, condivisione, strumento di soddisfazione dei bisogni collettivi ²⁷. Difatti, la interoperatività e l'interconnessione dei servizi collettivi, rafforzata laddove si tratti di servizi pubblici, è obiettivo odierno europeo nell'ambito di un disegno di un mercato e sistema europeo che sia in grado di offrire a tutti gli utenti accesso ai servizi offerti dai diversi operatori ²⁸. Il software che elabora un dataset, ossia un certo insieme di dati, è riconosciuto e regolato dal diritto d'autore, ma il funzionamento, la gestione e la responsabilità sono gestiti dall'autonomia privata. Tuttavia, il funzionamento del software, che opera attraverso uno specifico codice, elaborato attraverso criteri predefiniti, individuato da programmatori, richiede un aggiornamento continuo che formalmente trova tutela attraverso il diritto d'autore (art. 45 Codice della Proprietà intellettuale), ma sostanzialmente la velocità della definizione dei nuovi processi non consente di offrire concreta tutela ²⁹.

²⁶ V. ZENO-ZENCOVICH, *La "datasfera". Regole giuridiche per il mondo digitale parallelo*, in *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Torino, 2018, p. 102.

²⁷ Cfr. S. RODOTÀ, *Vivere la democrazia*, Bari, 2018 (ed), p. 111.

²⁸ O. POLLICINO, *Accesso, interconnessione ed interoperabilità: le novità apportate dal pacchetto Telecom ne confermano il ruolo chiave nel nuovo assetto regolatore del settore delle comunicazioni elettroniche*, in questa *Rivista*, f. 4-5, 2012, p. 743 ss.

²⁹ Sul punto si v. L. C. UBERTAZZI,

La ricerca di soluzioni attraverso le categorie giuridiche strettamente civilistiche non sembra però soddisfare le esigenze di tutela della persona e questo perché la tematica del trattamento dei dati e della tutela della *privacy*, oltre ad aver subito un mutamento legato ai nuovi interessi e alle dinamiche comunicative delle persone, nonché alle attività poste in essere dagli stessi utenti, deve anche confrontarsi con le questioni inerenti il mercato e la concorrenza, che ineludibilmente sono alimentate dal valore economico oramai riconosciuto ai dati ³⁰.

Si deve incentivare la convergenza dell'efficacia operativa delle norme di settore, nonché e maggiormente delle Autorità garanti investite nei vari ambiti di tutela. A tal fine nel 2017 l'Autorità per le garanzie delle comunicazioni, l'Autorità garante per la concorrenza e il mercato e il Garante per la protezione dei dati personali hanno avviato congiuntamente una *Indagine conoscitiva sui Big Data* volta ad approfondire gli effetti del fenomeno dei big data nel panorama economico sociale e i suoi effetti nei tradizionali inquadramenti giuridici. Da subito l'Indagine ha palesato come la raccolta e soprattutto l'utilizzo dei dati personali vengono in rilievo sotto il profilo *antitrust* "nella misura in cui i dati si configurano come "beni economici" idonei a generare un profitto per le imprese". La cooperazione delle tre autorità garanti mostra la portata delle problematiche ma soprattutto la necessità di operare attraverso una costante collaborazione per evitare incongruità di interventi.

Inoltre, le autorità di concorrenza sono consapevoli del fatto che l'attività di profilazione — resa possibile dall'acquisizione massiva dei dati — portata ai suoi estremi, "può agevolare comportamenti abusivi idonei a ridurre la contendibilità degli ecosistemi delle principali piattaforme, rendendo persistente il loro potere di mercato, e che la diffusione di algoritmi di prezzo, anch'essa agevolata dalla disponibilità di grandi quantitativi di dati, può facilitare la stabilità di cartelli e la creazione di contesti di mercato favorevoli ad equilibri collusivi" ³¹.

È evidente, dunque, come l'utilizzo dei *Big Data* venga ad interessare ambiti di competenza e comportamenti di diversa natura, la cui soluzione richiede l'impiego sinergico degli strumenti a tutela della *privacy*, del consumatore e della concorrenza

Banche dati e privacy, in *Rivista di diritto industriale*, 2002, p. 631; P. DE FILIPPI, L. MAUREL, *The paradoxes of open data and how to get rid of it? Analysing the interplay between open data and sui-generis rights on databases*, (2015), in 23 *Int. J. Law of the Privacy Directive*.

³⁰ Si v. A.F. FONDRIESCHI, *A Fragile Right: The Value of Civil Law Categories and New Forms of Protection in Algorith-*

mic Data Processing under the GDPR, in *Osservatorio di diritto civile e commerciale*, n. 2, 2019, p. 435.

³¹ Così le *Linee guida* di cooperazione sul tema dei *Big Data* e le raccomandazioni di *policy* del luglio 2019 concertate tra l'Autorità Garante della Concorrenza e del Mercato, del Garante per la protezione dei dati personali e dell'Autorità per le Garanzie nelle Comunicazioni.

e la cooperazione tra il Carante dei dati personali e dell'Autorità *Antitrust*. I modelli di *business* fondati sui *Big Data* (caratterizzati dall'elevato livello di concentrazione e dalla presenza di operatori che detengono posizioni dominanti; si pensi a tal proposito ai mercati dei motori di ricerca, dei *social network*, dei *marketplace*, ecc.), assumono spesso la struttura di mercato c.d. *a due o più versanti*, che si caratterizza per la presenza di due o più gruppi di utenti e di effetti di rete diretti e/o indiretti e di un'unica piattaforma, gestita da un operatore che ha proprio il compito di creare un collegamento tra i due gruppi indipendenti di utilizzatori, al fine di facilitare le transazioni e minimizzare i costi. Si tratta, ad esempio, di piattaforme *online* che danno luogo a mercati a più versanti c.d. di attenzione (come i motori di ricerca *online* o i *social network*) o di scambio (ad esempio, i *marketplace* del commercio elettronico)³².

Esistono, poi, altri fattori in grado di incidere significativamente sul processo competitivo come la presenza di c.d. *switching costs*, ovvero di limitazioni tecniche e/o economiche impeditive per gli utilizzatori della possibilità di cambiare fornitore. Ciò può avvenire, ad esempio, per assenza di interoperabilità tra sistemi di operatori concorrenti, generando fenomeni di c.d. *lock-in*, o per la scarsa propensione degli utenti a cambiare fornitore a causa dell'esistenza di significativi effetti di rete.

Nei mercati a due versanti, pertanto, l'accesso ad una grande quantità di dati può alimentare le esternalità di rete e costituire un significativo vantaggio competitivo, in quanto, per un potenziale nuovo entrante, potrebbe risultare difficile acquisire la quantità e la tipologia dei dati necessari per fornire un servizio adeguato ai propri clienti, nonché sviluppare la capacità necessaria per analizzarli. Non si dimentichi che l'attività di raccolta e di elaborazione dei dati richiede importanti investimenti che non tutti gli operatori economici sono in grado di sostenere, per cui spesso si preferisce accedere a piattaforme realizzate da terzi,

³² A titolo esemplificativo, si pensi agli innumerevoli siti di viaggio, nei quali, da una parte, vi sono i viaggiatori (gli utenti) e dall'altro le compagnie aeree o le strutture alberghiere (le imprese). Si pensi ancora ai mercati relativi ai sistemi operativi. Questi ultimi forniscono un'interfaccia tra dispositivi *hardware* (come *computer*, telefoni cellulari, *console* per videogiochi) da un lato e applicazioni *software* (come videogiochi, elaboratori di testi), dall'altro. In tale contesto, come ben evidenziato nell'*Indagine conoscitiva* sui *Big Data*, gli effetti di rete assumono particolare rilievo, in quanto "nelle c.d. piattaforme di attenzione, ad esempio, chi ha più utenti dispone di più

dati per migliorare il proprio servizio, attirando a sua volta ancora più utenti e determinando così effetti di rete indiretti, che si traducono in barriere all'uscita per gli utenti e in un più difficile ingresso per nuovi operatori. Più dati consentono inoltre una maggiore capacità di generare valore nei confronti degli inserzionisti pubblicitari, aumentando i ricavi che potranno a loro volta essere investiti nella qualità del servizio, dando luogo a effetti di rete indiretti. Tali effetti di rete possono progressivamente portare l'intero mercato a determinarsi a favore di una determinata piattaforma (c.d. *market tipping*), consolidandone la posizione".

mediante licenze d'uso, o comunque realizzare infrastrutture e piattaforme condivise ³³.

Inoltre, è chiaro che laddove i *Big Data* vengano assimilati a risorse ritenute essenziali per la realizzazione di un determinato prodotto o servizio, detta circostanza potrebbe creare una condizione di privilegio per l'impresa detentrica di quei dati e permettere a quest'ultima di godere di un vantaggio competitivo, rafforzando la propria posizione di mercato, creando anche barriere all'entrata, laddove sia precluso ai nuovi entranti di accedere alla medesima categoria di dati in termini di volume e varietà ³⁴.

Lo sfruttamento abusivo della posizione di dominanza acquisita nel mercato dagli operatori titolari di grandi *dataset* costituisce la maggiore preoccupazione per il diritto *antitrust* derivante dalla *digital economy* e a detto tema è strettamente legato quello delle barriere all'ingresso, e alla possibilità di considerare i dati come *essential facility*, cui ben si potrebbero collegare le condotte consistenti in pratiche escludenti e nel rifiuto di licenza ³⁵.

Possibili abusi di posizione dominante sono stati talvolta ricollegati anche alle pratiche dei prezzi personalizzati ³⁶. Tuttavia, le

³³ Si cfr. E. MACCIO - D. MULA, *Big Data e strumenti negoziali*, in AA.VV., *In-formazione e big data tra innovazione e concorrenza*, cit., p. 150 e ss. i quali osservano come l'acquisizione dei dati sfruttando sistemi e tecnologie dei terzi avvenga secondo specifici rapporti contrattuali, che vedono, interagire il soggetto titolare dell'infrastruttura informatica in grado di acquisire, archiviare ed elaborare grandi quantità di dati (detto *big data provider*), sotto forma di servizio, e un soggetto che intende acquisire i dati prodotti dagli utenti della propria attività (detto *big data supplier*). Il servizio di acquisizione, archiviazione e gestione dei dati preesiste all'attività del *big data supplier*, circostanza che insieme alla prestazione tipica del contratto, potrebbe suggerire di aderire alla qualificazione del rapporto instaurato tra *big data provider* e *big data supplier* come contratto di somministrazione di servizi. Oltre a detti soggetti, si registra poi, la presenza di operatori economici, detti *big data client*, interessati ad utilizzare le informazioni acquisite sul comportamento economico e sociale degli utenti.

³⁴ Al fine di comprendere se e in che misura i *Big Data* costituiscano concretamente una barriera all'entrata per la fornitura di un particolare servizio, è necessario affrontare la questione in riferimento ai singoli mercati e tenere presenti almeno tre aspetti: a) la rilevanza dei *Big Data* per la fornitura del bene/servizio alla luce di tutte

le caratteristiche del mercato in questione; b) la natura, la qualità e la quantità alla luce di dati necessari per poter competere efficacemente; c) la numerosità/varietà di fonti (sia *online* che *offline*) utilizzabili per generare la conoscenza rilevante per offrire i servizi in maniera competitiva. Tuttavia, la dottrina ha osservato come la caratteristica dei dati, comune a molti beni immateriali, ossia la non-rivalità, possa addirittura impedire il verificarsi di effetti anticompetitivi per effetto del possesso di raccolte massive di dati, potendo gli stessi essere raccolti e utilizzati molte volte e senza limiti. In tal senso, G. COLANGELO - M. MACCIOLINO *Big Data as Misleading Facility*, in *European Competition Journal*, 2017, vol. 13, n. 2, consultabile su <https://ssrn.com/abstract=2978465>, p. 3 ss., i quali osservano come il possesso di grandi quantità di dati di per sé non costituisca un problema, ed è improbabile che possa costituire un ostacolo alla concorrenza quando altre imprese sono in grado di ottenere dati uguali o simili, raccogliendoli dai propri utenti ovvero acquistando tali informazioni da altri operatori.

³⁵ Si legga sul tema F. VESSIA *Big data: dai vantaggi competitivi alle pratiche abusive*, in *Giur. Comm.*, fasc. 8, 2018, p. 1064 e ss.

³⁶ Si legga sul tema M. MACCIOLINO, *Big Data e prezzi personalizzati*, in *Concorrenza e mercato*, fasc. 1, 1 gennaio 2016, p. 95 e ss.; C. BUZZACCHI, *La politica*

Autorità che sinora si sono espresse su detta prassi hanno evidenziato una certa ambivalenza degli effetti, per un verso positivi e per un altro negativi, prodotti dalle offerte personalizzate; profilo, questo, evidenziato anche nell'*Indagine conoscitiva sui Big Data*, in cui si rileva come i prezzi personalizzati possono migliorare l'efficienza allocativa, statica e dinamica ma, sotto una diversa prospettiva, possono consentire l'aumento dei profitti per le imprese a danno dei consumatori e al tempo stesso avere un impatto eterogeneo su diversi gruppi di consumatori, aumentando il benessere di taluni, limitando il benessere di altri.

Non è mancato chi ha ravvisato nella discriminazione dei prezzi, praticata da un'impresa in posizione dominante o da due o più imprese all'esito di un'intesa restrittiva della concorrenza nei confronti di altre imprese, un illecito *antitrust*, sia comunitario, ai sensi degli artt. 101 e 102 del T.F.U.E., sia nazionale, in applicazione degli artt. 2 e 3 della L. n. 287/1990³⁷. Tuttavia, non è del tutto chiaro se le discriminazioni di prezzo siano vietate anche nei rapporti *business-to consumer*, giacché la normativa europea sulla concorrenza vieta espressamente solo le discriminazioni di prezzo nei confronti delle imprese e non anche nei confronti dei consumatori finali.

Di non minore importanza, per le valutazioni concorrenziali connesse al trattamento dei dati, sono le problematiche derivanti dalle concentrazioni tra imprese che detengono i *dataset*.

Difatti, tra i casi legati alla detenzione dei *Big Data* che finora hanno attirato la maggiore attenzione delle Autorità *Antitrust* vi sono state proprio le concentrazioni nel settore della *digital economy*, dalle quali sono emerse alcune criticità, che hanno portato la Commissione Europea ad adottare prima un Libro Bianco nel 2014 e poi ad avviare una Consultazione pubblica avente ad oggetto la revisione di alcuni aspetti del controllo sulle concentrazioni. Si pensi all'operazione di concentrazione *Facebook/WhatsApp*, nella quale la Società di Zuckerberg, dopo essere stata autorizzata all'acquisto di *WhatsApp*, ha disatteso le dichiarazioni di impegno rese nel corso della procedura di valutazione dell'operazione nel 2014, circa l'impossibilità tecnica di un collegamento tra gli indirizzi identificativi degli utenti *Facebook* e di quelli *WhatsApp*, operando nel 2016 un cambiamento delle impostazioni di *privacy* degli utenti *WhatsApp* per ottenere il

europea per i big data e la logica del single market: prospettive di maggiore concorrenza?, in *Concorrenza e mercato*, fasc. 1, 1 gennaio 2016, p. 171.

³⁷ Si cfr. A. FRIGNANI, *Le intese, Disci-*

plina della Concorrenza nella UE, cura di A. Frignani e S. BARIATTI, in *Tratt. dir. comm. dir. pubbl. econ.*, diretto da Galgano, Padova, 2012, p. 171.

matching con gli indirizzi *Facebook*, dichiarato tecnicamente impossibile poco tempo prima ³⁸.

Si consideri inoltre l'ulteriore caso che ha visto l'A.G.C.M. sanzionare *WhatsApp* per pratiche commerciali scorrette, ai sensi degli artt. 20, comma 2, 24 e 25 Codice del Consumo, per aver indotto i consumatori ad accettare la clausola di condivisione dei propri dati con *Facebook* nella fase di accettazione dell'aggiornamento dei termini di utilizzo di *whatsapp messenger*, facendo credere agli utenti che, senza l'accettazione di detta clausola, i medesimi non avrebbero più potuto continuare ad utilizzare il servizio *whatsapp messenger* ³⁹.

Parimenti degne di rilievo sono le situazioni di coordinamento tra le imprese rese più semplici nei mercati digitali dalla trasparenza dei prezzi su *Internet* e dall'utilizzo di algoritmi che consentono adattamenti automatici ed immediati al mutare delle condizioni di mercato ⁴⁰.

Come osservato dalle Autorità Garanti nell'*Indagine conoscitiva*, l'elevata trasparenza dei mercati *online*, ossia l'ampia disponibilità di dati sui prezzi dei concorrenti e di altre informazioni rilevanti, la frequenza di aggiustamento dei prezzi e le capacità di apprendimento delle strategie di prezzo ottimali attraverso il *machine learning* sono fattori in grado di agevolare potenzialmente fenomeni collusivi, più o meno taciti e dunque più o meno leciti.

Di fronte ad uno scenario così complesso e dall'intreccio ineludibile di problematiche di tutela della concorrenza e di protezione dei dati personali dei consumatori/utenti, diviene dunque una priorità nell'attività dell'A.G.C.M. la repressione dei comporta-

³⁸ Cfr. Commissione Europea "M.7217 Facebook/Whatsapp" in <http://ec.europa.eu/competition/mergers/cases/decisions>.

La Commissione, nel caso di specie, ha irrogato una sanzione di 110 milioni di euro a *Facebook* per aver fornito informazioni scorrette e fuorvianti durante l'istruttoria del 2014, laddove probabilmente la conoscenza preventiva dell'Autorità sulle possibilità di *matching* dei due *data set* avrebbe portato ad un diverso esito decisionale sull'operazione di concentrazione. Si legga ancora, G. GIANNONE CODICIONE, *I dati personali come corrispettivo della fruizione di un servizio di comunicazione elettronica e la "consumerizzazione" della privacy*, in questa *Rivista*, fasc. 2, 2017, p. 418 e ss., nota a Garante concurr. e mercato, 11 maggio 2017.

³⁹ Provvedimento dell'A.G.C.M. n. 26597/2017, PS 10601, in Bollettino, 15 maggio 2017 n. 18/2017. Come evidenziato nell'articolo di F. VESSIA, *Big Data: dai van-*

taggi competitivi alle pratiche abusive, cit., p. 1064, "il caso dimostra non soltanto che anche per la fruizione dei servizi gratuiti (come quelli offerti da WhatsApp) i contratti conclusi siano qualificabili come contratti dei consumatori, la cui valuta di scambio non è il denaro ma i dati personali, e conseguentemente andranno assoggettati alle norme del Codice del Consumo ivi incluse le disposizioni sulle PCS; ma conferma, altresì, che vi possano essere abusi conseguenti all'acquisita dominanza su un determinato mercato (i.e. quello dei social network per Facebook) capaci di estendersi su altri mercati (quello delle comunicazioni mediante messaggi di testo, vocali, fotografici e video chiamate in cui opera WhatsApp) per effetto della fusione realizzata tra i due colossi, che però nessuna Autorità ha saputo prevedere)".

⁴⁰ Si legga A.M. RIZZO, *I profili anti-trust del nuovo web e della nuova economia digitale*, in *Il Diritto industriale*, n. 2, 2019, p. 113 e ss.

menti abusivi da parte dei grandi *player* dell'economia digitale e delle intese restrittive della concorrenza ed auspicare una crescente cooperazione con l'Autorità garante della protezione dei dati personali essendo il "materiale informativo" determinante per un'offerta sul mercato maggiormente competitiva.

In questa prospettiva e al fine di perseguire l'obiettivo di tutela del benessere del consumatore, l'A.G.C.M. segnala nelle *Linee guida sui Big Data* l'opportunità di "non confinare l'analisi ai tradizionali parametri legati a prezzi e quantità, ma, con l'ausilio degli strumenti propri del diritto industriale, estenderla anche alla qualità, all'innovazione e all'equità" e la necessità, quantomeno con riferimento alle piattaforme digitali globali, di "misure volte ad incrementare la trasparenza all'utente circa la natura della propria profilazione in merito ai contenuti ricevuti, nonché meccanismi di *opt-in* circa il grado di profilazione prescelto, e ciò anche ai fini della tutela del pluralismo on-line, in relazione alla selezione dei contenuti operante attraverso la profilazione del consumatore" ⁴¹.

È interessante, pertanto, notare come la protezione dei dati e la tutela della *privacy* — seppur tematiche in sé e per sé estranee al diritto della concorrenza — possano invece attirare l'attenzione degli studiosi dei mercati, proprio perché incidenti sul modo di operare delle imprese negli stessi. D'altronde, la relazione tra protezione della *privacy* ed efficienza economica è caratterizzata sia da complementarità che da potenziali divergenze. Difatti, se è vero che l'applicazione della normativa *antitrust* non rappresenta lo strumento più adeguato ed efficace per affrontare tutte le questioni relative ai *Big Data*, è anche vero che la prospettiva *antitrust* ha alcune implicazioni per le norme sulla protezione dei dati che non possono essere sottovalutate; si pensi, ad esempio, ai casi in cui agevolare la raccolta dei dati, in taluni mercati, può avere effetti pro-concorrenziali, riducendo le barriere all'entrata ⁴².

⁴¹ Costituisce, inoltre, obiettivo dell'AGCM con una forte valenza pro-concorrenziale anche l'agevolare "la portabilità e la mobilità di dati tra diverse piattaforme, tramite l'adozione di standard aperti e interoperabili, anche oltre quanto previsto dal diritto alla portabilità di cui all'art. 20 del RGDP" e aumentare l'efficacia del proprio intervento rispetto alle operazioni di concentrazione attraverso: "1. una riforma a livello nazionale e internazionale che consenta alle autorità di concorrenza di poter valutare pienamente anche quelle operazioni di concentrazione sotto le attuali soglie richieste per la comunicazione preventiva, ma che potrebbero risultare ido-

nee a restringere sin dalla loro nascita importanti forme di concorrenza potenziale (come le acquisizioni da parte dei grandi operatori digitali di start-up particolarmente innovative anche soprannominate "killing acquisitions"); 2. La modifica dell'art. 6, comma 1, della legge n. 287/90, con l'introduzione di uno standard valutativo più adatto alle sfide dell'economia digitale, che faccia leva sul criterio dell'impedimento significativo della concorrenza effettiva (SIEC - "Substantial impediment to effective competition").

⁴² Si legga sul punto G. PETRUZZELLA, *Big Data, competition and privacy: a look from the antitrust perspective*, in *Concor-*

Ciò dimostra che è necessario trattare di *privacy*, concorrenza, benessere dei consumatori secondo un approccio interdisciplinare, perché l'obiettivo primario rimane quello di definire regole che consentano al mercato di funzionare in maniera efficiente ed equa, tutelando i diritti degli individui e, al contempo, soddisfacendo gli interessi dell'economia attraverso l'innovazione e la fiducia degli utenti. La tutela dei diritti delle persone deve necessariamente transitare attraverso l'attuazione dei principi costituzionali e non può esimersi da un'analisi applicativa dei criteri di liceità del consenso su cui è opportuno soffermarsi.

4. VALIDITÀ E LIMITI DEL CONSENSO NEL GDPR A FRONTE DEL VALORE COMPETITIVO DEI BIG DATA.

Dopo aver mostrato come la libertà di circolazione dei dati e il principio capitalistico sotteso al mercato sembrano essere il fondamento della legittimazione del titolare a trattare i dati ⁴³, occorre ora prestare, un'adeguata attenzione al consenso, perché solo se consapevole e non meramente "informato" esso consente un bilanciamento tra i diritti della persona e la libertà d'impresa. Sorgono criticità di fronte alla diffusione di un consenso indiscriminato, avviato alla sola acquisizione del trattamento dei dati che non siano tecnicamente o legalmente necessari. Le informazioni a cui l'utente, "fornitore" del dato, deve prestare attenzione sono troppo articolatamente esposte, con minuzie tecniche che sono non facilmente ponderabili da un utente medio ⁴⁴. La protezione dei dati personali si rivela di fatto sottesa *in primis* alla circolazione ⁴⁵ degli stessi, nella consapevolezza che i dati, una volta acquisiti dai soggetti operanti nel contesto dell'economia digitale

renza e mercato, fasc. 1, 1 gennaio 2016, p. 15 e ss.

⁴³ Sul punto si veda il lucido contributo di Aurelio Gentili, che spiega come, di fatto, fondamento della legittimazione del titolare di utilizzare i dati non è il consenso ma la libertà di circolazione dei dati. Così, A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in *Riv. trim. dir. e proc. civ.*, 1 settembre 2022, p. 701. Sulla natura del consenso *ex pluribus* si v. S. PATTI, *Il consenso dell'interessato al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, p. 455; G. RESTA, *Diritti fondamentali e diritto privato nel contesto digitale: un inventario di problemi*, in *Effettività e Drittwirkung: idee a confronto*, Atti del Convegno Pisa, 24-25 febbraio 2017, Torino, p. 182.

⁴⁴ Vi è chi discorre di "dinamiche di over information, che finiscono di escludere una reale consapevolezza nell'interessato/

utente". Così, V. D'ANTONIO, *Il consenso al trattamento dei dati personali tra autodefinizione informativa e dinamiche remuneratorie*, in AA.VV., *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, p. 162.

⁴⁵ Tra gli strumenti previsti dal legislatore europeo per aumentare il controllo dell'interessato sui propri dati, e favorire al contempo la libera circolazione degli stessi con l'obiettivo di stimolare l'economia digitale, viene in rilievo il diritto alla portabilità dei dati, disciplinato dall'art. 20 del Regolamento n. 679/2016/UE. In base a detta previsione normativa, l'interessato, quando i dati personali sono trattati con mezzi automatizzati, ha il diritto di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile, i dati personali che lo riguardano e di trasmetterli a un altro titolare del trattamento. Il predetto diritto viene, dunque, ad

possono essere utilizzati, trasferiti, elaborati, ceduti infinite volte, anche ad insaputa dell'interessato, e senza limitazioni geografiche, e che la disponibilità di molti *dataset*, ciascuno contenente una grande quantità di dati, può aumentare le probabilità di correlazione tra gli stessi, consentendo la reidentificazione di *database* precedentemente anonimizzati o la generazione, con l'impiego degli strumenti di *analytics*, di sempre nuove informazioni e nuovi dati personali. Consapevoli di questa destinazione dei dati è d'uopo verificare in che termini è possibile garantire la legittimità della circolazione dei dati. Il legislatore europeo, all'art. 5 del GDPR, stabilisce i sei principi cardine del sistema di protezione dei dati personali da rispettare ogni qualvolta vengano raccolti, trattati e memorizzati dati personali dei residenti nell'Unione Europea. Trattasi, nello specifico, dei principi di liceità, correttezza e trasparenza, di limitazione della finalità, di minimizzazione dei dati, di esattezza, di limitazione della conservazione, di integrità e riservatezza, da cui discendono nuovi obblighi e nuove responsabilità in capo al titolare del trattamento, ma anche nuovi diritti per i soggetti cui ineriscono i dati trattati (si pensi, ad esempio, al diritto ad essere informati; al diritto di accedere ai propri dati personali; al diritto di rettifica; al diritto di revoca del consenso e di opposizione al trattamento; al diritto di cancellazione e al diritto all'oblio). Ciò significa, nella sostanza, che i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato e che le finalità devono essere determinate, esplicite e legittime. I dati devono essere, poi, pertinenti, esatti e aggiornati, oltre che limitati a quanto necessario rispetto alle finalità, e comunque da trattare in modo da garantire una adeguata sicurezza. Deve essere rispettato il principio di specificità, ossia la c.d. granularità del consenso. Una maggiore specificità del consenso, infatti, garantisce maggiore consapevolezza e ponderazione in merito agli atti incidenti direttamente sulla personalità dell'utente. L'interessato, dunque, deve poter esprimere un consenso specifico e separato per ciascun distinto servizio, senza che l'erogazione di un dato servizio possa essere legata all'accettazione di altro servizio ⁴⁶. Spesso, invece, le piattaforme digitali impongono ai consumatori/utenti di cedere i propri dati, stabilendo quanti e quali informazioni debbano es-

assolvere a due importanti scopi: aumentare il controllo dell'interessato sui suoi dati, consentendo di accedervi e di riceverli in un formato che ne consenta la leggibilità e l'utilizzo; facilitare la loro trasmissione ad un altro titolare, anche tramite l'adozione di formati *standard* che consentano l'attuazione più semplificata di detto diritto.

⁴⁶ Il considerando 43 del Regolamento

GDPR afferma che "si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione".

sere oggetto di cessione, con un'offerta definita "prendere o lasciare"⁴⁷. Di fronte a simili situazioni, diventa sempre più importante far esprimere all'interessato un consenso informato, così da porlo nella condizione di conoscere come verranno trattati i propri dati, con quali modalità e per quali finalità, e quali diritti gli sono attribuiti dalla normativa. Tale inosservanza comporta la violazione del principio di trasparenza, sancito dall'art. 12 del Regolamento n. 679/2016, la cui violazione può rendere il consumatore vittima di una pratica commerciale ingannevole, oltre che vittima di una violazione della *privacy*⁴⁸.

Il consenso deve essere consapevole perché possa essere favorito un bilanciamento degli interessi in gioco, nei quali deve essere ricompresa non solo la libertà economica ma anche il diritto all'autodeterminazione, quale forma evolutiva del diritto della *privacy*. La pienezza del consenso, così intesa, può essere raggiunta attraverso interventi correttivi che investono l'operato del contraente forte, ossia del titolare del trattamento, per ovviare che l'utente si trovi costretto ad autorizzare il trattamento dei dati personali, anche laddove non tecnicamente strumentali al servizio, ove pertanto, il rapporto sinallagmatico sia ambiguo.

Lo specifico tema della liceità del consenso si palesa però con maggiori sfaccettature con la sopravvenuta crescente ed invasiva operatività dei cookies, quelle stringhe di testo che il browser colloca alla apertura della pagina web che oscurano la visualizzazione della pagina sino a quando non acquisiscono il consenso dell'utente a che vengano memorizzati i suoi dati. Le diverse tipologie degli stessi mostrano un sensibile *discrimen* tra loro, e quelli di tracciamento e di profilazione sono quelli più spinosi per la tutela dei dati personali, sebbene la memorizzazione dei dati avvenga in modo anonimo. Inoltre, non è di poco conto che la corresponsione di dati e l'utilizzazione degli stessi opera anche dopo la fruizione del servizio⁴⁹; se l'utente non provvede a rimuovere i cookies, questi continuano ad operare e a fornire informazioni in merito ai dati ricevuti senza che essi siano strumentali all'offerta di servizi in corso; come se ci fosse un punto di non ritorno salvo la salda determinazione di ostacolare questo protrarsi di sfruttamento, che tuttavia non sempre è, ad ogni modo, vincente.

⁴⁷ Si legga OCSE, *Data - driven Innovation for Growth and Well-being. Interim Synthesis Report*, ottobre 2014, disponibile su <https://www.oecd.org/sti/inno/data-driven-innovation-interim-synthesis.pdf>.

⁴⁸ Per una disamina completa delle questioni inerenti alla libertà del consenso al trattamento dei dati personali, si legga S. THOBANI, *La libertà del consenso al tratta-*

mento dei dati personali e lo sfruttamento economico dei diritti della personalità, in *Europa e Diritto privato*, fasc. 2, 1° giugno 2016, p. 513.

⁴⁹ In tal senso si v. G. RESTA - V. ZENO-ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. di dir. e proc. civ.*, fasc. 2, 2018, p. 417.

Verso la risoluzione di tali sopravvenuti aspetti sembra indirizzato il Regolamento ePrivacy, proposta di regolamento del Consiglio dell'UE che disciplina tutte le comunicazioni elettroniche sui servizi e reti disponibili al pubblico da parte di individui all'interno dell'Unione Europea, che ha l'obiettivo di proteggere le persone fisiche nell'UE dalle interferenze di terzi nelle loro comunicazioni, salvo che sia dato loro un consenso preventivo.

In attesa dell'approvazione del nuovo Regolamento europeo, il Garante per la protezione dei dati personali ha già dettato linee guida cookie e altri strumenti di tracciamento (10 giugno 2021) proprio con l'obiettivo di imporre il consenso esplicito degli utenti finali prima di poter utilizzare sul proprio sito web cookie, tracker, o qualsiasi altra tecnologia che memorizzi dati personali sulle apparecchiature terminali degli utenti ⁵⁰.

Si constata pertanto che, al di là degli intenti espressi nel GDPR, è emerso nella prassi come taluni dei principi applicabili al trattamento dei dati personali, sopra menzionati e tradizionalmente utilizzati per proteggere la *privacy*, si rivelino spesso inadeguati rispetto ai *Big Data* e non perfettamente rispondenti alle nuove logiche operative e trasmissive degli stessi.

Il tema del consenso al trattamento si scontra *in primis* con il fenomeno dell'acquisizione massiva di informazioni e dati personali tramite le *app*. Difficoltà sono state ravvisate, in modo peculiare, sul piano dell'attuazione del principio della "minimizzazione" e della limitazione delle finalità, stante l'intrinseca difficoltà di individuare, sin dalla fase iniziale, le finalità della raccolta e del trattamento dei dati ⁵¹. Ne consegue la complessità di rispettare il principio di esattezza giacché le notevoli quantità di dati raccolti possono derivare da molteplici fonti, senza che sia possibile *ab origine* verificare l'esattezza dei dati raccolti.

Tuttavia, sebbene il Regolamento non si occupi direttamente dei *Big Data*, lo stesso offre comunque strumenti per garantire la difesa della *privacy* e arginare parzialmente gli abusi anche in

⁵⁰ Vi è chi ritenga opportuna una ristretta limitazione del consenso offerta dall'art. 7 del GDPR, in ragione dei molteplici interessi che gravitano intorno al diritto della privacy e della centralità dell'esigenza di una circolazione dell'informazione non frammentata. Così, T.M. UBERTAZZA, *Models of Information Circulation and the Function of Privacy*, in *EuCML*, n. 6, 2022, p. 9.

⁵¹ La non semplice applicazione dei principi enunciati dal GDPR all'ecosistema dei *Big Data* fu dapprincipio evidenziata anche dall'allora Presidente del Garante per la protezione dei dati personali, Antonello Soro, in occasione del suo intervento al *World Economic Forum* di Davos, in cui ha

affermato che "[...] la nozione di titolarità del trattamento mostra, infatti, tutti i suoi limiti rispetto alla moltiplicazione dei gestori dei dati che caratterizza il processo di utilizzazione dei *Big Data*, lungo catene dagli anelli infiniti. I principi di minimizzazione, limitazione delle finalità e conservazione per il solo tempo indispensabile alla realizzazione del trattamento non si attagliano a raccolte così massive di dati, acquisiti spesso non per esigenze attuali ma in vista di future, eventuali necessità e riutilizzati per fini ulteriori non sempre compatibili con quelli originari". In <https://www.garrnews.it/rubriche-interne-18/speciale-1.8>.

detto ambito, mediante la previsione di una tutela preventiva (valutazione di impatto sulla protezione dei dati personali e protezione sin dalla progettazione e per impostazione predefinita, definite “*privacy by design*” e “*privacy by default*”). La tutela, dunque, deve essere anticipata ad un momento anteriore al trattamento dei dati personali ma è fondata sull’impegno dei titolari fin dalla progettazione dei prodotti e servizi, nella consapevolezza dell’incidenza sui dati degli utenti⁵².

In questa prospettiva, di grande utilità si rivela proprio la valutazione d’impatto prevista dall’art. 35 del Regolamento GDPR, cui dovranno essere sottoposti i trattamenti di dati posti in essere con la tecnica dei *Big Data*, soprattutto quando il trattamento comporti “una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basandosi su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche”⁵³.

L’attenzione è così rivolta alla volontà di evitare che un soggetto possa essere sollecitato ad una decisione basata su un trattamento automatizzato giacché anche numero limitato di dati può consentire l’uso di modelli decisionali sviluppati con strumenti automatizzati di vario livello e grado senza che il destinatario finale ne abbia piena consapevolezza. Ma questa circostanza non deve adombrare il tema dell’informativa che deve essere garantita affinché il consenso sia validamente prestato⁵⁴. Difatti, su questa criticità l’ordinanza della Corte di Cassazione n. 14381/2021 ha inteso intervenire sancendo che il presupposto del trattamento dei

⁵² Si legga “*Il Regolamento Europeo sulla privacy: origini e ambito di applicazione*”, in *Europa e Dir. privato*, fasc. 4, 1 dicembre 2016, p. 1249, in cui si osserva come le tecniche di protezione dei dati fin dalla progettazione e di protezione dei dati per impostazione predefinita, già conosciute e adottate dalle imprese, con il Regolamento n. 679/2016 sono state accolte nella disciplina europea, nella sezione relativa agli obblighi generali posti in capo al titolare e al responsabile del trattamento. Detti strumenti sono fondati su un’attenta valutazione dei rischi di violazione dei diritti e delle libertà fondamentali delle persone interessate, sulla cui base sorge l’obbligo per il titolare di predisporre misure e soluzioni tecniche specificamente mirate alla tutela dei dati personali (i cc.dd. servizi e prodotti *privacy oriented*).

⁵³ Si legga l’art. 35, par. 3, lett. a), GDPR. Invero, per far fronte alla molteplicità di rischi diretti o indiretti derivanti dalle tecniche di analisi basate sui *Big Data* dovranno essere adottate misure di sicu-

rezza adeguate, efficaci, realizzate a regola d’arte e continuamente valutate ed aggiornate, nel rispetto di quanto disposto dagli artt. 25 e 32 del Regolamento stesso.

⁵⁴ In tal senso si v. G. COMANDÈ, *Leggibilità algoritmica e consenso al trattamento dei dati personali, note a margine di recenti provvedimenti sui dati personali*, in *Danno e Responsabilità*, n. 2, 2022, p. 141 e ss. L’A. prende le mosse dalla decisione della Corte di Cassazione, Sez. I, 24 marzo 2021-25 marzo 2021, n. 14381. Ad ogni modo, una enfaticizzazione sul punto si rinviene anche nell’*Indagine conoscitiva sui Big Data — Linee guida e raccomandazioni di policy*, pubblicata nel luglio 2019 dall’Autorità Garante della Concorrenza e del Mercato, dall’Autorità per le Garanzie nelle Comunicazioni e dal Garante per la protezione dei dati personali, per minimizzare i rischi di violazione dei diritti individuali per il tramite dei *Big Data*, ove si evidenzia la necessità di adottare misure preventive e processi interni volti a commisurare il rischio sui diritti degli interessati.

dati personali è costituito dalla validità del consenso che si assume prestato al momento dell'adesione, specificando però che l'adesione ad una piattaforma da parte di consociati non comprende automaticamente l'accettazione di un sistema automatizzato per la valutazione oggettiva di dati personali. In tal modo è stata confermata la decisione del Garante per la protezione dei dati personali che ha ritenuto illegittimo un sistema di reputazione automatica per i rilevati vizi del consenso richiesto perché espresso sulla base di inadeguati elementi informativi. Le condizioni per la ponderatezza di una scelta consapevole sono pertanto centrali perché il consenso sia espressione di un consenso liberamente autodeterminato.

La condizioni per un consenso prestato liberamente ed "informato", nel senso di consapevole e specifico sono descritte nell'art. 6⁵⁵ GDPR. L'art. 7, comma 4, del medesimo Regolamento precisa, poi, che "nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento dei dati personali non necessario all'esecuzione di tale contratto". In altre parole, condizionare l'esecuzione del contratto alla presentazione del consenso al trattamento di dati personali non necessario e strumentale all'esecuzione del contratto stesso non è dalla norma vietato in sé e per sé, ma "tenuto nella massima considerazione"; va da sé che lo stesso ben può essere visto come un indizio di illiceità del trattamento, potendo il consenso non essere effettivo; e qui si riscontra una prima criticità. Altro aspetto problematico del consenso si palesa poi quando il trattamento ha ad oggetto dati sensibili, ricondotti dal legislatore nelle "categorie particolari di dati personali" ove, se da un lato, l'art. 9 del GDPR prevede basi giuridiche ancora più stringenti tramite il "consenso esplicito", ossia una forma di consenso rafforzato, per altro verso, consente di sfuggire a questi requisiti stringenti laddove interessi pubblici rilevanti si palesino. Nella prassi, tra l'altro, si registrano sempre più casi — spesso, oggetto di esame da parte del Garante per la protezione dei dati personali — in cui, a fronte dell'offerta di servizi digitali, viene richiesta la cessione di dati ulteriori rispetto a quelli strettamente necessari per la fornitura di detti servizi, oppure viene prevista la

⁵⁵ È bene tenere a mente che nei considerando n. 42 e n. 43 del Regolamento GDPR, il legislatore europeo precisa che "il consenso non dovrebbe essere considerato liberamente espresso se l'interessato non è in grado di operare una scelta autenticamente libera o è nell'impossibilità di rifiutare o revocare il consenso senza subire

pregiudizio" (considerando n. 42) e che il consenso si presume non liberamente espresso "se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione" (considerando n. 43).

possibilità per l'operatore economico di utilizzare i dati già prestatati anche per l'ulteriore attività di *marketing* ⁵⁶. La riduzione dell'asimmetria informativa tra utenti ed operatori digitali nella fase di raccolta dei dati deve essere posta tra gli obiettivi di policy da perseguire ⁵⁷, con la raccomandazione che l'informazione adeguata comprenda anche e soprattutto i termini della cessione dei dati sottesi al funzionamento del servizio.

5. RIFLESSIONI CONCLUSIVE.

La centralità dei dati per il funzionamento del mercato e la consapevole gestione degli stessi quale espressione dell'attuazione dei diritti della persona hanno reso il legislatore e gli operatori del diritto pienamente consci di come la rapidità dell'evoluzione tecnologica e la globalizzazione abbiano offerto una proiezione della circolazione dei dati personali molto distante da quella prevedibile ai tempi delle prime normative dettate sul tema. Le informazioni e i dati personali di cui beneficiano le imprese pubbliche al pari di quelle private per lo svolgimento delle loro attività, così come la disinvoltura, spesso imprudente, con la quale le persone rendono disponibili al pubblico informazioni personali che li riguardano, hanno completamente mutato i parametri di riferimento per un raggiungimento di un *fair* bilancia-

⁵⁶ Interrogativi vengono sollevati nella citata *Indagine conoscitiva* anche in ordine alla liceità del "farsi" dei *Big Data*, con riguardo alla possibilità di trattare, sulla scorta di una legittima base giuridica, i *dataset* oggetto di analisi, come pure del loro utilizzo, atteso che ciò comporta per lo più un uso "secondario" dei dati, che deve quindi misurarsi con il principio di compatibilità del trattamento in relazione alle finalità rispetto alle ragioni che hanno determinato l'originaria raccolta (art. 5, paragrafo 1, del Regolamento GDP). In relazione alla suddetta ipotesi, si rende necessario procedere ad una valutazione di impatto ex art. 35 del Regolamento GDP, indagando in primo luogo sulla finalità originaria della raccolta dei dati riversati nel *dataset* per, poi, valutare se la finalità del trattamento attuale possa dirsi compatibile con la finalità originaria e se costituisca o meno una lesione dei diritti degli interessati di allora. Anche per i dati presenti in *Internet* o tratti dai *social media*, il Garante per la protezione dei dati personali esclude che la circostanza per cui gli stessi siano resi pubblici (e quindi agevolmente "processabili") possa legittimarne un loro riutilizzo con tecniche *Big Data*, in particolare rispetto a finalità che nulla hanno a che vedere con quelle per

le quali tali informazioni erano state conferite.

⁵⁷ Lo stesso Garante per la protezione dei dati personali, nell'*Indagine conoscitiva*, evidenzia come un'attenta ponderazione dei principi di protezione dei dati personali e l'impiego delle misure volte a prevenire la violazione dei diritti fondamentali degli interessati rappresentano una cautela imprescindibile per lo sviluppo di tali tecnologie nel rispetto della dimensione individuale e collettiva dei diritti fondamentali (non limitati a quello alla protezione dei dati personali) in gioco. Le Autorità Garanti segnalano, inoltre, che "sia l'applicazione della normativa sulla protezione dei dati personali che la strumentazione propria della tutela del consumatore possono offrire un contributo importante per la riduzione di tale asimmetria informativa, garantendo che gli utenti ricevano un'adeguata, puntuale e immediata informazione circa le finalità della raccolta e dell'utilizzo dei loro dati e siano posti nella condizione di esercitare consapevolmente ed effettivamente le proprie scelte di consumo. In questa prospettiva, appaiono opportune misure volte a rendere maggiormente consapevoli i consumatori nel momento in cui forniscono il consenso al trattamento dei dati personali".

mento di interessi. Ed è in questo processo di veloce trasformazione che si deve investigare sulla opportunità o meno di un quadro normativo, o meglio operativo, coerente in materia di protezione dei dati nell'Unione, ovvero sull'utilità di una crescita di una cooperazione tra le Autorità Garanti che sia più fluida, seppur incardinata su definite regole di gerarchia dei ruoli, che siano in grado di creare il clima di fiducia che consenta lo sviluppo dell'economia digitale in tutto il mercato interno. Lo sviluppo del mercato digitale europeo deve essere concepito in un sistema ove le persone fisiche devono essere poste in condizione di controllare i propri dati personali, la cui tutela non è più riconosciuta in via assoluta nel diritto europeo ma alla luce della sua funzione sociale, nonché temperata con altri diritti fondamentali, in ossequio al principio di proporzionalità. La consapevolezza degli utenti del *web* di veder tutelata la propria *privacy*, nel momento in cui operano nei mercati digitali, deve essere motore di crescita e di competitività⁵⁸ ma non a discapito dei diritti della persona.

La complessità delle problematiche ingenerate dall'incessante processo di digitalizzazione e dallo sviluppo delle tecnologie dell'informazione e della comunicazione rivela come, che nell'attuale contesto sociale ed economico, non sia più possibile un'univoca percezione della *privacy* intesa *tout court* come diritto della personalità (assoluto, indisponibile, imprescrittibile, intransferibile e incommerciabile)⁵⁹. D'altronde, sostenere la depatrimonializzazione del dato personale appare oggi una affermazione del tutto decontestualizzata anche perché gli stessi individui hanno assunto un ruolo attivo nella creazione di raccolte di dati che li riguardano, attraverso le loro azioni nel *web*. Inoltre, i loro comportamenti ed abitudini, memorizzati nel mondo digitale, sono sempre più rappresentativi di comportamenti e abitudini non del singolo ma di individui simili (ossia, individui che sono stati raggruppati da un determinato algoritmo), attraverso il processo di profilazione, valutati e usati per fare previsioni e trarre conclusioni sul modo di agire dell'intero gruppo di individui simili. Tuttavia, il diritto ad escludere la condivisione di propri dati così come il potere di disporre una condivisione degli stessi devono essere riconosciuti e tutelati laddove la persona abbia compiuto coerenti scelte, frutto di una piena autodetermi-

⁵⁸ Si legga G. PITRUZZIELLA, *Big Data, Competition and privacy: a look from the antitrust perspective*, in *Concorrenza e mercato*, fasc. 1, 1 gennaio 2016, p. 15 e ss., secondo il quale "At the same time, a sufficient level of privacy is necessary to foster competition. In fact, privacy is an important element of trust and trust in digital services is necessary for online markets to

work smoothly and to be an engine of growth and competitiveness".

⁵⁹ Sulla nuova visione della persona non più identificata attraverso la triade assiologica integrità-inalienabilità-gratuità si v. R. SENIGAGLIA, *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contratto e Impresa*, 2020, 2, p. 780.

nazione, salvaguardia quest'ultima non solo dell'identità, dell'uguaglianza, della dignità della persona ma anche condizione preliminare per l'attuazione di scelte democratiche.

L'avvento della tecnologia dell'informazione, come si è cercato di enucleare, ha mutato la visione individualistica del concetto di sfera personale muovendo verso un ampliamento della nozione di sfera personale, che va oltre la vita domestica e familiare del singolo, la cui tutela oggi richiede sempre più il controllo dei propri dati personali a causa della massiccia diffusione degli stessi nella rete telematica e sempre più tutele avverso il rischio di "classificazione" in vario modo mediante la tecnica della profilazione. Inoltre, bisogna considerare che molto spesso la diffusione di un certo dato/informazione ha una finalità ulteriore rispetto a quella percepita *prima facie*. La diffusione del linguaggio dell'odio on-line, ad esempio, è spesso non fine a sé stessa ma volta ad attivare altri focolai; difatti, spesso, intende "modificare drasticamente la percezione dell'ambiente in cui si svolge la personalità dell'individuo, nel quadro di una profonda rimodulazione strutturale della società" ⁶⁰ foriera di nuovi diritti, come il diritto all'oblio.

Sotto il profilo degli interessi protetti, il diritto alla protezione dei dati personali condivide, però, con il più tradizionale diritto alla *privacy* la tutela della dignità della persona interessata (il Codice della *privacy*, all'art. 1, lo definisce diritto e lo fa rientrare nella categoria dei diritti della personalità), e costituisce anche una preconditione per l'esercizio di altri diritti civili, sociali e politici e, quindi — si ripete — strumento per il corretto funzionamento di una società democratica ⁶¹. È evidente, dunque, come oggi, proprio per effetto dell'impatto dei *Big Data* sulla società, la dimensione della *privacy* non sia più solo individuale, ma collettiva e, come, quindi, nuove e più complesse siano le sfide da affrontare a fronte del rischio della c.d. "dittatura dei dati"; ciononostante, non bisogna permettere che ciò avvenga attraverso la negazione dei diritti costituzionali. Il tema del consenso consapevole deve rimanere centrale sebbene le regole del mercato e il vorticoso e rapido evolversi del sistema economico, accelerato dalle potenzialità offerte dall'intelligenza artificiale, alterino la

⁶⁰ Così, testualmente G. GIANNONE CODICIONE, *Internet e tutele del diritto civile*, Torino, 2020, p. 81.

⁶¹ Il Garante per la protezione dei dati personali, Pasquale Stanzone, nella intervista resa in occasione dell'evento State of Privacy 22, in <https://www.garanteprivacy.it>, ha sottolineato come tra gli obiettivi primari del collegio della Privacy vi sia la diffusione della cultura della privacy e che pertanto bisogna "promuovere una sorta di

formazione digitale, di Paideia, a cominciare dai minori" al fine di favorire la "consapevolezza del fatto che i nostri dati personali sono un patrimonio inalienabile che fa parte della tutela integrale della persona". Il Garante, difatti, evidenzia come "nell'evoluzione di questi venticinque anni, l'Autorità è passata dalla tutela soltanto di alcuni diritti a tutelare la persona nella sua interezza".

visione antropocentrica che deve rimanere la premessa necessaria, almeno nella sua dimensione personalistica.

Parallelamente all'operato collaborativo delle Autorità garanti, custodi della tutela dei nuovi diritti e delle nuove dinamiche economiche e sociali, si deve auspicare una intensificazione dell'educazione digitale, ancora scarsa, nonché considerare che l'opinione pubblica non è sufficientemente informata sulla protezione dei dati personali e sulla *privacy*. Ciò comporta un gran divario tra quanto preteso dalle persone in termini di tutela dei propri dati e il loro comportamento *online* che spesso dimostra come non venga adottata alcuna cautela nella diffusione di proprie informazioni private.

Ed in questa nuova èra di apparente condivisione che si auspica il ritorno ad una ricerca della conoscenza che sia non solo più veloce ma anche più profonda. È di tutta evidenza, dunque, come solo con l'acquisizione della diversa e maggiore consapevolezza degli individui sulla rilevanza dei propri diritti e con una più analitica conoscenza del mondo digitale sarà possibile sviluppare un mercato altamente competitivo e performante ma al tempo stesso non invalidante la dignità della persona.

Abstract

The aim of this paper is to focus on the evolution of the concept of data and its reflection on the economy and legal issues, going beyond the original aspects of the right to privacy and the predicable rise of market welfare. Considering the pivotal role of the movement of data, the article shows the increased risk of unfair competition through the rapid technological evolution and underlines the need to ensure that consent is an expression of conscious choice. The suggested approach to this theme is an interdisciplinary one with increased cooperation between supervisory Authorities.