

JACOPO ALCINI*

*Profili etici del trattamento algoritmico dei dati nel contenzioso giudiziario***

Sommario: 1. Introduzione. - 2. I meccanismi di tutela. - 3. La responsabilità per illecito trattamento dei dati: spunti di riflessione. - 4. I provvedimenti giurisdizionali tra pubblicità ed anonimato. - 5. Conclusioni.

1. *Introduzione*

Il diritto alla protezione dei dati personali¹ ha ormai acquistato centralità nella società contemporanea, così fortemente caratterizzata dalla proliferazione delle informazioni disponibili su ogni individuo². Quando si parla di dato personale, può notarsi la peculiarità

* *Avvocato, Ph.D. UNIPG, assegnista di ricerca.*

** *Contributo sottoposto positivamente al referaggio secondo le regole del single blind peer-review.*

Il presente lavoro è un prodotto sviluppato nell'ambito del progetto UNI4JUSTICE: Universitas per la Giustizia. Programma per la qualità del sistema giustizia e per l'effettività del giusto processo, monitorato dal Ministero della Giustizia, promosso dall'Agenzia per la Coesione Territoriale, nell'ambito del PON Governance e Capacità Istituzionale 2014-2020 e realizzato in sinergia con gli interventi previsti dal Piano Nazionale di Ripresa e Resilienza (PNRR) a sostegno della riforma della giustizia. Le opinioni espresse dall'autore rispecchiano esclusivamente le visioni personali dello stesso.

¹ T. E. FROSINI, *Le sfide attuali del diritto ai dati personali*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Napoli, 2020, 395 ss.; G. VISINTINI, *Dal diritto alla riservatezza alla protezione dei dati personali*, in *Dir. inf.*, 2019, 1 ss.; C. FOCARELLI, *La privacy. Proteggere i dati personali oggi*, Bologna, 2015, 36 ss. Cfr. anche A. ASTONE, *Autodeterminazione dei dati e sistemi A.I.*, in *Contr. impr.*, 2022, 429 ss.

² C. PERLINGIERI, *Creazione e circolazione del bene prodotto dal trattamento algoritmico dei dati*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., 180. S. CALZOLAIO, *Protezione dei dati personali*, in *Dig. disc. pubbl.*, Torino, 2017, 614: «[...] riservatezza e protezione dei dati personali risultano distinguibili, sulla linea di confine fra libertà negativa (diritto di escludere) e libertà intrinsecamente positiva (diritto di controllare, autodeterminazione informativa) ed a loro volta si distinguono dal diritto all'identità personale (come "diritto a non vedere travisata la propria immagine sociale"): si tratta delle facce di un unico prisma, legato alla personalità umana»; M. DE CARO, *L'era delle macchine: tre problemi morali e politici*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., 7

che caratterizza tale nozione, giacché esso rappresenta uno strumento tecnico-giuridico mediante il quale si è scelto di tutelare quell'insieme di diritti relativi all'identità personale ed alla privacy. Esso è stato definito «contenitore vuoto all'interno del quale l'interprete inserisce di volta in volta uno specifico contenuto relativo al patrimonio informativo dell'interessato»³. Il dato personale, in sostanza, è così rilevante da determinare la portata applicativa della normativa, sebbene sia necessario sottolineare che tale locuzione non fa riferimento, né direttamente né indirettamente, alla privacy o alla riservatezza, risultando nuovamente come si tratti di diritti distinti⁴. A partire dal secondo dopoguerra, le tecnologie dell'informazione e della comunicazione (Information and Communication Technologies, ICTs) hanno assunto una fondamentale rilevanza per il benessere dei singoli cittadini e delle organizzazioni umane. Lo sviluppo di sistemi di raccolta e archiviazione di dati sempre più efficienti ha favorito la nascita dell'economia dell'informazione, in cui i soggetti economici hanno adottato modelli di business basati sullo scambio di dati e informazioni⁵.

In prima istanza, alcuni hanno parlato di economia digitale, focalizzando l'attenzione sull'utilizzo massiccio, esteso a ogni settore, delle tecnologie informatiche e digitali⁶. In tal senso, i dati sono definiti beni pubblici non rivali nel consumo, non deteriorabili e rinnovabili⁷.

Altri autori hanno focalizzato l'attenzione sulla nozione di economia dell'informazione (o economia informazionale)⁸. Come ha affermato Manuel Castells, l'età

ss.; A. ALPINI, *Identità, creatività e condizione umana nell'era digitale*, in *Tecn. dir.*, 2020, 4 ss.; L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2017, 106.; M.G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.*, 2016, 1949 ss.

³ F. DI RESTA, *La nuova "privacy europea". I principali adempimenti del Regolamento UE 2016/679 e profili risarcitori*, Torino, 2018, 4.

⁴ G. FINOCCHIARO, *Privacy e protezione dei dati personali*, Bologna, 2012, 36 ss.

⁵ J. RIFKIN, *L'era dell'accesso, La rivoluzione della new economy*, Milano, 2000, 5 ss.; L. FLORIDI, *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*, Oxford, 2014, 4 ss.

⁶ W.D. NORDHAUS, *Productivity growth and the new economy*, in *Brookings Papers on Economic Activity*, 2002, 221 ss.; M.R. FERRARESE, *La digital economy tra di più e di meno*, in V. BARSOTTI, M. GRAZIADEI (a cura di), *Il diritto oltre lo Stato*, Torino, 2021, 67 ss.

⁷ M. OREFICE, *I Big Data. Regole e concorrenza*, in *Pol. dir.*, 2016, 712, la quale rileva come i Big Data rappresenterebbero beni che, nella teoria economica di Ostrom, sono definiti commons, come risorsa immateriale condivisa, tendente ad essere non rivale e non esclusiva.

⁸ F. BRAVO, *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, Padova, 2018, 51 ss.: «è qualificabile come diritto soggettivo la situazione giuridica di chi, nell'ambito dell'attività di iniziativa economica privata e facendo uso dei poteri che gli derivano dall'autonomia privata, in presenza dei presupposti che legittimano il trattamento (condizioni di liceità previste dalla norma: artt. 6 e 9 reg. cit.) e che funzionano da meccanismi di selezione (e bilanciamento) degli interessi che l'ordinamento ha inteso tutelare, è facoltizzato a predisporre un

dell'informazione è dominata da una forma di capitalismo informazionale, in cui i modelli di business sono incentrati principalmente sull'innovazione tecnologica e sullo scambio di dati e informazioni.⁹

Nel nuovo scenario economico, beni intangibili quali dati e informazioni assumono un'importanza fondamentale, poiché il controllo dell'accesso a queste risorse è divenuto la forma privilegiata di capitalizzazione di tali utilità¹⁰.

Di recente, l'economia dell'informazione ha raggiunto uno stadio più evoluto grazie alla diffusione dei Big Data¹¹, per le quali si può procedere alla datizzazione generalizzata¹², vale a dire la trasformazione in formato digitale di qualsiasi aspetto del mondo reale e della

trattamento di dati personali per soddisfare le finalità che egli stesso unilateralmente determina, con le modalità, gli strumenti e l'organizzazione che egli stabilisce, nonché di trarre dal medesimo l'utilità economica connessa all'esercizio dell'attività – rilevante ex artt. 41 Cost. e 16 Carta dei diritti fondamentali dell'UE – in cui il trattamento si colloca».

⁹ G. FALCO, *Identità personale*, in *Nuovo dig. it.*, VI, Torino, 1938, 649; F. MESSINEO, *Problemi dell'identità delle cose e delle persone nel diritto privato*, in *Annali del seminario giuridico dell'Università di Catania*, Napoli, 1950, 64 ss.; G. PINO, *Il diritto all'identità personale ieri e oggi. Informazione, mercato, dati personali*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, I, Milano, 2006, 258 ss.; G. FINOCCHIARO, *Identità personale (diritto alla)*, in *Dig. disc. priv., Sez. civ.*, Torino, 2010, 730. In riferimento all'identità digitale cfr. G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 2017, 723 ss.

¹⁰ A. GORZ, *L'immateriale*, Torino, 2003, 23; G. D'IPPOLITO, *Monetizzazione, patrimonializzazione e trattamento di dati personali*, in E. CREMONA, F. LAVIOLA, V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, 2022, 54 ss.

¹¹ L. MERLA, *Big data e diritto: una sfida all'effettività*, in *MediaLaws*, 2021, 218 ss.; G. DELLA MORTE, *Big data e protezione internazionale dei diritti umani*, Napoli, 2018, 178 ss.; A. BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *Media Laws*, 2018, 206 ss.; M. COPPOLA, F. GUERRIERI, *Art. 4. Definizioni*, in G. M. RICCIO, G. SCORZA, E. BELISARIO (a cura di), *GDPR e normativa privacy. Commentario*, Milano, 2018, 47 ss.; G. D'ACQUISTO, M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017, 5 ss.; E. GIOVANNINI, *La rivoluzione dei big data a sostegno dell'Agenda 2030*, in *Equilibri. Rivista per lo sviluppo sostenibile*, 2016, 64 ss.; L. BOLOGNINI, *Principi del trattamento*, in L. BOLOGNINI, E. PELINO, C. BISTOLFI (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Milano, 2016, 103 ss.; M. MAGGIOLINO, *Big data e prezzi personalizzati*, in *Concorrenza merc.*, 2016, 95 ss.; J. SYLVESTRE BERGÉ, S. GRUMBACH, V. ZENO-ZENCOVICH, *The Data-sphere, Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law and Governance*, V, 2018, 149. In particolare, gli Autori differenziano i dati archiviati in base al modo in cui sono stati creati, suddividendoli in: 1) dati che sono il frutto della "datificazione" degli oggetti della vita reale che è stata finora uno dei modi più comuni attraverso cui i dati sono stati creati; 2) dati che vengono creati sin dall'origine come tali essendo il frutto dell'attività intellettuale ovvero della rappresentazione delle entità non materiali e quindi della datificazione dell'informazione (notizie, informazioni, risultati di ricerche); 3) dati prodotti dalle persone, che sono quasi interamente digitalizzate visto che la maggior parte delle informazioni relative alle loro attività, passate e presenti, vengono archiviate in formato digitale, essendo peraltro registrate, raccolte ed elaborate anche le loro caratteristiche fisiche; 4) dati che vengono generati automaticamente dalle tecnologie digitali e che costituiscono un'evoluzione dei casi precedenti.

¹² V. MAYER-SCHONBERGER, K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013, 130; A. STAZI, F. CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. inf.*, 2019, 442.

vita umana¹³.

La nascita dei Big Data ha portato con sé l'insorgere di una serie di questioni come il problema dell'intelligenza artificiale¹⁴ e dell'utilizzazione degli algoritmi¹⁵ e, pertanto, è necessario valutare le ripercussioni in un'ottica di libera circolazione dei dati personali.

La pervasività dei social network¹⁶, la moltiplicazione dei dispositivi in grado di

¹³ M. DELMASTRO, A. NICITA, *Big data. Come trasformano i mercati e la democrazia*, Bologna, 2019, 3 ss.; V. ZENOVICH, *Do data markets exist?*, in *MediaLaws*, 2019, 3 ss. In relazione alla problematica descritta, G. RESTA, *Identità personale e identità digitale*, in *Dir. inf.*, 2007, 522, specifica che le «tecniche di raccolta dei dati e profilazione individuale, rese possibili dalle nuove tecnologie, determinano il rischio che l'io venga frammentato, a sua insaputa, in una molteplicità di banche dati, offrendo così una raffigurazione parziale e potenzialmente pregiudizievole della persona, la quale verrebbe così ridotta alla mera sommatoria delle sue proiezioni elettroniche». ID., *La morte digitale*, in *Dir. inf.*, 2014, 891 ss. In riferimento alla digitalizzazione della dignità, cfr. R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. impr.*, 2019, 862 ss.

Anche se, secondo A. ALPINI, *Identità, creatività e condizione umana nell'era digitale*, in *Tecn. dir.*, 2020, 7 ss., l'uomo non si identifica con i propri dati e di conseguenza il controllo dell'uso dei dati non rappresenterebbe una garanzia di tutela per la persona. G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 1670 ss.; A. TURANO, *Diritto, robotica e teoria dei giochi: questioni e prospettive nazionali ed europee*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, 128 ss.; A. CONTALDO, F. CAMPARA, *Intelligenza artificiale e diritto*, in G. TADDEI ELMI, A. CONTALDO (a cura di), *Intelligenza artificiale*, Pisa, 2020, 61 ss.; G. SARTOR, F. LAGIOIA, *Le decisioni algoritmiche tra etica e diritto*, in U. RUFFOLO (a cura di), *Intelligenza artificiale*, Milano, 2020, 63 ss.

¹⁴ G. FINOCCHIARO, *Intelligenza artificiale e protezione dei dati personali*, cit., 1670 ss.; A. TURANO, *Diritto, robotica e teoria dei giochi: questioni e prospettive nazionali ed europee*, cit., 128 ss.; A. CONTALDO, F. CAMPARA, *Intelligenza artificiale e diritto*, in G. TADDEI ELMI, A. CONTALDO (a cura di), *Intelligenza artificiale*, cit., 61 ss.; G. SARTOR, F. LAGIOIA, *Le decisioni algoritmiche tra etica e diritto*, in U. RUFFOLO (a cura di), *Intelligenza artificiale*, Milano, 2020, 63 ss.

¹⁵ Per algoritmo si intende lo schema esecutivo della macchina che memorizza le opzioni decisionali in base ai dati che vengono progressivamente elaborati. Cfr. P. COMOGLIO, *Nuove tecnologie e disponibilità della prova*, Torino, 2018, 331 ss. Cfr. anche L. AVITABILE, *Il diritto davanti all'algoritmo*, in *Riv. it. sc. giur.*, 2017, 315 ss.; P. MORO, *Algoritmo e pensiero giuridico*, in *MediaLaws*, 2019, 13 ss.; S. VERNILE, *Verso la decisione amministrativa algoritmica?*, in *MediaLaws*, 2020, 136 ss.; B. ROMANO, *Algoritmi al potere*, Torino, 2018, 7 ss.

¹⁶ Cfr. C. PERLINGIERI, *Profilo civilistico dei social networks*, Napoli, 2014, 11 ss.; ID., *Social Networks and Private Law*, Napoli, 2017, 7 ss.; ID., *La tutela dei minori di età nei social networks*, in *Rass. dir. civ.*, 2016, 1324 ss.; R. CATERINA, *La libertà di comunicazione: il fenomeno dei social networks*, in C. PERLINGIERI, L. RUGGIERI (a cura di), *Internet e diritto civile*, Napoli, 2015, 117 ss.; A. COPPOLA, F.R. GRAZIANI, F. COLAPAOLI, M. ZONARO, M. MIRONE, *Social Network e diritto*, Torino, 2021, 1 ss.; M. BASSINI, *Libertà di espressione e social network, tra nuovi spazi pubblici e poteri privati. Spunti di comparazione*, in *Riv. it. inf. dir.*, 2021, 43 ss.: «Alle origini di Internet, il cyberspazio era stato immaginato da alcuni dei commentatori più vicini alla sensibilità libertaria e "cyberanarcoide" come il terreno di una possibile competizione "privata" tra comunità virtuali aliene dall'interferenza dei poteri statali. Ciascuna una piattaforma di libertà, caratterizzata da un novero di (poche e semplici) regole definite dagli amministratori e condivise dagli aderenti: in sostanza, il rispetto di limiti di contenuto e di continenza verbale, pena l'esclusione. Nessuna sanzione ulteriore, semmai la possibilità di transitare a una comunità diversa. Un sistema parallelo dominato da una sorta di "arbitraggio regolamentare", dove gli utenti avrebbero potuto "disporsi" e collocarsi a seconda delle rispettive inclinazioni e degli interessi coltivati. Per gli Stati, apparentemente, nessun ruolo e nessun potere: gli Stati, in questa ricostruzione, sono l'altrove, impossibilitati a predicare la propria sovranità e a estendere l'enforcement delle norme giuridiche entro uno spazio idealizzato come territorio separato. Questa ricostruzione dai toni idealistici si fondava su due illusioni che si sarebbero di lì a breve disvelate. In primo luogo, l'assunto che questa compartimentazione in comunità private non avrebbe generato posizioni di potere favorite dall'accumulo di risorse economiche, con un condizionamento sull'organizzazione, sulla mole, e conseguentemente sulla genuina circolazione dei contenuti condivisi dagli utenti, condizionamento costituente

raccogliere dati personali¹⁷, l'avanzamento tecnologico di software e algoritmi in grado di processare imponenti quantità di dati¹⁸, sono le cause principali dell'incremento esponenziale delle informazioni disponibili in rete¹⁹.

Queste vengono usualmente raccolte in grandi flussi omogenei, la cui analisi può fornire indicazioni, finanche in chiave predittiva²⁰, sui comportamenti individuali e collettivi. L'elaborazione dei dati individuali raccolti produce nuove informazioni²¹ riguardanti interi gruppi sociali, descrivendo così nel dettaglio tutta la generalità dei consociati²².

Il fenomeno in questione è in grado di trasformare profondamente la nostra società, influenzando tanto la sfera privata quanto quella pubblica²³.

Occorre, tuttavia, operare un distinguo ed una precisazione in merito. Quanto al distinguo, è necessario separare i dati di programmazione da quelli di lavorazione. I primi rappresentano la base informatica da cui principia il funzionamento degli algoritmi²⁴, mentre i secondi costituiscono l'oggetto mediato delle tecnologie.

La precisazione, invece, riguarda la collocazione ibrida dei dati personali tra soggetto ed oggetto, poiché da un lato gli stessi riguardano la persona, ne costituiscono una

un diretto precipitato del dischiudersi di strutture oligopolistiche nel mercato dei servizi (a tacitazione di quella pretesa concorrenza perfetta tra comunità virtuali). In secondo luogo, la ferrea convinzione inerente non soltanto all'impossibilità degli Stati di regolare il web ma anche alla non necessità di un loro intervento in un campo dove l'autonomia privata prometteva una governance efficiente, ridondando quel rifiuto della sovranità statale già predicato metaforicamente da John Perry Barlow nella Dichiarazione d'indipendenza del cyberspazio e fatto oggetto di un claim normativo».

¹⁷ S. RODOTÀ, Prefazione, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, I, cit., pp. XIII-XIV; F. GIOVANNELLA, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'Internet of Things diritto*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 3 ss.

¹⁸ P. PERLINGIERI, *Sul trattamento algoritmico dei dati*, in *Tecn. dir.*, 2020, 181 ss.

¹⁹ P. PERLINGIERI, *L'informazione come bene giuridico*, in *Rass. dir. civ.*, 1990, 333 ss., sottolinea che l'informazione, quale risultato del procedimento di elaborazione, è suscettibile di essere utilizzata sul mercato per gli scopi più vari.

²⁰ S. RODOTÀ, *Il mondo nella rete*, Bari, 2014, 33 ss.; M. DE FELICE, *Su probabilità, «precedente» e calcolabilità giuridica*, in *Riv. dir. proc. civ.*, 2017, 1546 ss. Sulla predittività, cfr. N. IRTI, *Per un dialogo sulla calcolabilità giuridica*, in *Riv. dir. proc.*, 2016, 923 ss.; ID., *Un diritto incalcolabile*, Torino, 2016, 11 ss.

²¹ C. DEL FEDERICO, A.R. POPOLI, *Disposizioni generali*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Torino, 2017, 60.

²² M.F. DE TULLIO, *La privacy e i Big Data verso una dimensione costituzionale collettiva*, in *Pol. dir.*, 2016, 651 ss.

²³ Sul rapporto fra il potere e la conoscenza che deriva dalle informazioni cfr. A. DI MARTINO, *La protezione dei dati personali. Aspetti comparatistici e sviluppo di un modello europeo di tutela*, in S. P. PANUNZIO (a cura di) *I diritti fondamentali e le corti in Europa*, Napoli, 2005, 377 ss.

²⁴ A. GARAPON, J. LASSÈGUE, *La giustizia digitale*, Bologna, 2021, 43: «La trasformazione digitale dei dati si scompone in tre momenti distinti: la loro digitalizzazione, il loro trattamento sotto forma di programma ed eventualmente, la loro ulteriore correlazione sotto forma statistica».

rappresentazione e spesso ne descrivono il comportamento e le relazioni. D'altro canto, sono oggetti di uso da parte di attori pubblici e privati, tanto da divenire obiettivo di apposita tutela²⁵.

In questo contesto, la protezione dei dati personali si rivela uno strumento fondamentale per consentire il libero sviluppo della personalità individuale²⁶.

Essa si concreta nei diritti dell'interessato, che ne costituiscono mezzi di tutela²⁷, nonché nel complesso degli obblighi posti a carico dei titolari e responsabili del trattamento. Consente, pertanto, di conservare un controllo sulle proprie informazioni quando giungono nell'altrui disponibilità. Oltre che sul piano soggettivo, la Data protection²⁸ assume una notevole importanza anche in una dimensione collettiva, contrastando la possibilità di derive orwelliane verso società del controllo digitale²⁹.

²⁵ Significative le parole di G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, 279: «personalità e patrimonialità [...] non sono due poli concettuali antitetici e mutualmente esclusivi: così come esistono beni patrimoniali costitutivi della persona, allo stesso modo gli attributi individuali del soggetto possono assumere un significativo valore di scambio, senza con ciò perdere la loro connotazione strutturalmente personale». Cfr. anche 245: «[...] riconoscere apertamente che il potere di controllo sullo sfruttamento commerciale della personalità rappresenti una parte integrante del diritto della personalità e che questo, pertanto, non possa più essere ricostruito come puro e semplice droit de défense, ma debba ormai essere ripensato [...] come diritto a struttura duplice e contenuto complesso».

²⁶ P. PERLINGIERI, *Privacy digitale e protezione dei dati personali tra persona e mercato*, in *Foro nap.*, 2018, 481 ss., evidenzia la necessità di un'ermeneutica assiologica che tenga precipuamente conto dei valori sottesi alla normativa in materia di data protection, divenendo così necessaria l'adozione di un approccio sistemico e realistico da parte del legislatore europeo, ove la protezione dei dati opera tra la più ampia funzione sociale e il paradigma dei diritti fondamentali. In tal senso, F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, II, Torino, 2016, 4 ss.; A. RICCI, *Sulla funzione sociale del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2017, 604, mette in luce come «l'assolutezza del diritto alla protezione dei dati personali trova nella "funzione sociale", così come interpretata, un principio alla stregua del quale coordinare fra loro la pretesa dell'interessato, gli interessi dei titolari del trattamento, le esigenze avvertite dalla società nel suo insieme. Essa non può che riferirsi all'oggetto del diritto, sebbene letteralmente riferita al diritto in quanto tale, e non può che essere interpretata come criterio di temperamento fra pretese individuali ed interessi generali. Sotto questo aspetto, la previsione del considerando conferma l'impianto descritto sin dalla dir. 95/46/CE che, come in precedenza ricostruito, muovendo dal presupposto che la libera circolazione delle informazioni è interesse connaturale al progresso economico e sociale, fonda la disciplina del trattamento dei dati sul bilanciamento tra la legittima pretesa individuale di protezione e il corretto funzionamento del mercato». Sulla dimensione anche collettiva della funzione del diritto alla protezione dei dati, si veda l'accurata ricostruzione di S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws*, 2019, 144 ss.

²⁷ C. COLAPIETRO, A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, 128 ss.

²⁸ Cfr. Corte giust., 2 marzo 2021, C-746/18, in *Dir. inf.*, 2021, 219.

²⁹ S. RODOTÀ, *Data Protection as a Fundamental Right*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWAGNE, S. NOUWT (a cura di), *Reinventing Data Protection?*, Springer, 2009, 82, secondo cui «reinventing data protection is an unrelenting process that is indispensable not only to afford adequate protection to a fundamental right but also to prevent our societies from turning into societies of control, surveillance and social

Il rapporto tra dati personali e tecnologie algoritmiche costituisce un punto nevralgico del dibattito europeo e nazionale che sembra non sempre trovare un punto di equilibrio, portando quindi a nuovi sviluppi dal punto di vista normativo e giurisprudenziale.

Dati e algoritmi sembrerebbero costituire infatti un binomio non del tutto risolutivo né esaustivo, se si considerano, per un verso, la molteplicità delle varie questioni giuridiche e, per altro verso, l'ambito apparentemente limitato entro cui le tutele previste dalla disciplina in materia di protezione dati spiegano la loro efficacia. In un tale contesto, risultano ancora diversi i nodi aperti in riferimento ai rapporti tra algoritmi, privacy e tutela dei dati personali.

Sarebbe sufficiente sottolineare le tensioni costituzionali che caratterizzano la relazione tra Big Data³⁰ e principi generali del GDPR, specialmente quando si guarda ai canoni di trasparenza e minimizzazione dei dati³¹.

In particolare, il consenso, quale base giuridica fondata sull'elemento volontaristico, sembra essere in crisi non solo per effetto della sempre maggiore asimmetria informativa tra individui e titolari del trattamento che implementano tecnologie algoritmiche, ma anche e soprattutto per via dalla complessità tecnologica.

Il consenso non è certo l'unica base giuridica³², dato che il GDPR, valorizzando il principio di accountability, sembra aver voluto attribuire nuova linfa a fondamenti normativi diversi, come il legittimo interesse, incentrati su una responsabilizzazione del titolare del trattamento. Tuttavia, lo stesso continua a rappresentare uno dei capisaldi della disciplina in materia³³, la cui validità come base giuridica deriva da una serie di predicati che devono essere

selection». F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, I, Torino, 2016, 12.

³⁰ Costituiti dal paradigma delle quattro V (Volume, Velocità, Varietà, Veracità). Cfr. G. D'ACQUISTO, M. NALDI, *Big data e privacy by design*, Torino, 2017, 5 ss.; T. MAURO, *I big data tra protezione dei dati personali e diritto della concorrenza*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019, 651 ss.

³¹ C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. impr.*, 2020, 893.

³² A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale*, Napoli, 2019, 165 ss.; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, 25 ss.

³³ S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, 583 ss.; ID., *La vita e le regole. Tra diritto e non diritto*, Milano, 2006, 82 ss.; M. BIN, *Privacy e trattamento dei dati personali: entriamo in Europa*, in *Contr. impr. eur.*, 1997, 459 ss.; S. PATTI, *Il consenso al trattamento dei dati personali*, in *Riv. dir. civ.*, 1999, 455 ss.; A. SCALISI, *Il diritto alla riservatezza*, Milano, 2002, 1 ss.; I. CHIRIACO, *Autonomia negoziale e dati personali*, Napoli, 2010, 42 ss.; M. MASNADA, *Il diritto alla protezione dei dati personali*, in G. ALPA, G. CAPILLI (a cura di), *Lezioni di diritto privato europeo*, Milano, 2007, 163 ss.; S. THOBANI, *Il consenso al trattamento dei dati*

rispettati. Tra questi, vi è senza dubbio la natura informata, presupposto affinché la manifestazione di volontà dell'interessato possa legittimare il trattamento dei dati da parte del titolare.

Un primo indirizzo³⁴, che nega la natura di bene ai dati personali, ravvisa una scriminante da fatto illecito in virtù del consenso dell'avente diritto ovvero di un atto unilaterale di tipo autorizzatorio.

Tale argomentazione risente della tradizionale impostazione volta a privilegiare il carattere non patrimoniale e indisponibile dei diritti della personalità³⁵.

Il soggetto consenziente non perde la titolarità del diritto e può in ogni tempo esercitare le relative facoltà, esponendosi semmai ad una responsabilità contrattuale per inadempimento, restando così salvo il principio di indisponibilità dei diritti della personalità³⁶.

Una seconda e diversa lettura del fenomeno, assimila i dati personali ai beni in senso giuridico, in quanto tali autonomamente suscettibili di essere oggetto di disposizione mediante contratto³⁷. In tal senso, l'acquisizione del consenso altrui al trattamento dei dati permette l'assunzione di specifiche informazioni. Questa lettura appare più coerente con il valore economico che hanno assunto i dati e trova riscontro non solo nelle strategie imprenditoriali, rispetto alle quali il patrimonio di informazioni è sempre più spesso considerato come una risorsa fondamentale, ma anche nelle valutazioni operate sul punto da parte del legislatore comunitario. Del resto, la problematica afferente alla qualificazione del diritto sui dati personali, funzionale alla relativa circolazione, non può essere risolta in modo semplicistico sulla sola base del fatto che tali informazioni abbiano assunto nel contesto attuale una valenza economica³⁸. Dal punto di vista giuridico, i dati sarebbero destinati ad essere commercializzati dal titolare originario del diritto e non è chiaro se quest'ultimo sia effettivamente abilitato a cederli. Gli stessi, quali entità immateriali, presentano un intrinseco

personali come condizione per la fruizione dei servizi on line, in C. PERLINGIERI, L. RUGGERI (a cura di), *Internet e diritto civile*, cit., 459 ss.

³⁴ G. MIRABELLI, *Le posizioni soggettive nell'elaborazione elettronica dei dati personali*, in *Dir. inf.*, 1993, 323.

³⁵ C. MIGNONE, *Identità della persona e potere di disposizione*, Napoli, 2015, 369; D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, 350.

³⁶ A. MANTELETO, *Il costo della privacy tra valore della persona e ragione d'impresa*, Milano, 2007, 70.

³⁷ G. ALPA, G. RESTA, *Le persone fisiche e i diritti della personalità*, Torino, 2006, 632; G. RESTA, *Diritti esclusivi e nuovi beni immateriali*, Torino, 2011, 38.

³⁸ A. OTTOLIA, *Big data e innovazione computazionale*, Torino, 2017, 111.

legame più con le reti di telecomunicazione che con un determinato territorio, motivo per cui non possono neanche essere radicati sul territorio di un solo Stato. A questo riguardo va tenuto presente che in taluni ordinamenti ed in particolare in quello tedesco, la possibilità di qualificare un'entità come bene è normativamente legata alla corporeità dell'oggetto³⁹. In tale contesto emerge, quindi, la difficoltà di applicare a entità come i dati il modello proprietario tradizionale, che prende come punto di riferimento il bene quale cosa materiale che può costituire oggetto di diritti e, attraverso lo strumento contrattuale, di una vicenda circolatoria⁴⁰. Sarebbe più plausibile la prospettazione di una generica titolarità dei dati⁴¹, la quale attribuisca al soggetto, sulla scia della consolidata tradizione dei beni⁴² immateriali, una serie di diritti di utilizzo e sfruttamento esclusivo delle informazioni, unitamente a limiti e rimedi volti a fronteggiare l'uso non autorizzato⁴³. Ben potrebbe, pertanto, in più contesti accantonarsi il concetto di protezione, invocando, di contro, il diritto al controllo dei dati personali (sinteticamente inteso come piena disponibilità⁴⁴ delle informazioni cedute con supervisione⁴⁵ del trattamento). Pertanto, è auspicabile la creazione di un diritto di proprietà fluido e relazionale, che, in deroga al *numerus clausus* dei diritti reali, possa esplicarsi sui dati mediante l'utilizzo della disciplina dei segreti commerciali, con l'applicazione di un apposito regime di licenza.

Scopo del presente lavoro è coniugare la disciplina del trattamento dei dati con le regole sottese al contenzioso giudiziario, al fine di individuare strumenti e soluzioni inidonee

³⁹ V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, 2018, 3.

⁴⁰ M. GRANIERI, *Proprietà, contratto e status nell'industria dell'informazione. Per una visione criticamente relazionale dell'economia digitale*, in *Merc. conc. reg.*, 2006, 114.

⁴¹ Cfr. Corte giust., 5 giugno 2018, c-210/16, in *Resp. civ. prev.*, 2019, 1987.

⁴² Sulla oggettivizzazione dei dati come beni giuridici, cfr. C. ANGIOLINI, *Lo statuto dei dati personali*, Torino, 2020, 110.

⁴³ V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, cit., 3.

⁴⁴ Da intendersi come possibilità di disporre dei dati ceduti, ad esempio revocando il consenso al trattamento e pretendendo la cancellazione dei dati o, semplicemente, modificando ed aggiornando gli stessi. Ciò rimanda all'esigenza di un ripensamento della categoria del bene e, conseguentemente, alla necessaria riformulazione del paradigma dominicale, anche con riferimento ai dati personali. Cfr. P. PERLINGIERI, *Il diritto dei contratti fra persona e mercato. Problemi del diritto civile*, Napoli, 2003, 333 ss.; A.C. NAZZARO, *Privacy, smart cities e smart cars*, in E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019, 340 ss.

⁴⁵ Già S. RODOTÀ, *Privacy e costruzione della sfera privata. Ipotesi e prospettive*, in *Pol. dir.*, 1991, 521 ss., intravedeva l'evoluzione in atto del diritto alla privacy, il cui oggetto si stava ampliando, così muovendosi dalla segretezza al controllo. ID., *Controllo e privacy della vita quotidiana. Dalla tutela della vita privata alla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2019, 9 ss.

a coniugare le esigenze di riservatezza con quelle di giustizia. Ad esempio, le modalità di pubblica comunicazione dei magistrati hanno dato luogo a frequenti critiche, a causa del dovere di riservatezza cui sono tenuti. Basti pensare alla prassi delle conferenze stampa o all'autocelebrazione delle proprie inchieste. Il dovere di informare è naturalmente irrinunciabile, purché esercitato nei limiti della legge, del rispetto della privacy e delle regole deontologiche⁴⁶, essendo necessario che i giudici si guardino bene dal contribuire a rafforzare un'ormai evidente degenerazione informativa, spesso giustizialista ed arbitraria⁴⁷. Nella prospettiva che vede l'esperienza giuridica incarnarsi nello spazio e nei tempi del processo, ciò che rileva è la coscienza, la sententia animi del giudice⁴⁸, sia nell'ambito processuale che nella vita privata. La discrezionalità del giudice⁴⁹ si collega alla natura stessa dell'attività interpretativa, operando giudizi di valore⁵⁰, che raccordano la valutazione del caso concreto alla meritevolezza degli interessi, secondo un ordine ragionevole di preferenze coerente al sistema ed alla sua irrinunciabile unità nel momento applicativo⁵¹. Questo aspetto portante dello *ius dicere*, si ritiene inscindibile dalla delicata operazione di anonimizzazione dei dati, che altrimenti rischiano di essere “fagocitati” da un tecnicismo professionale e degradante, perché privo della indispensabile ottica personalista⁵² che deve presiederne la tutela.

2. I meccanismi di tutela

Analizzando il corpo del reg. UE n. 679/2016 (GDPR)⁵³, emerge, una nuova

⁴⁶ G. CANZIO, *Un'efficace strategia comunicativa degli uffici giudiziari vs. il processo mediatico*, in *Dir. pen. proc.*, 2018, 1537 ss.

⁴⁷ Cfr. G.P. ACCINNI, *Civiltà giuridica della comunicazione*, Milano, 2018, 73 ss.

⁴⁸ G. CAPOGRASSI, *Opere*, V, Milano, 1959, 57 ss.

⁴⁹ P. PERLINGIERI, *L'interpretazione giuridica e i suoi canoni*, in *Rass. dir. civ.*, 2014, 418 ss.

⁵⁰ P. PERLINGIERI, *Principi generali e interpretazione integrativa nelle pagine di Emilio Betti*, in *Rass. dir. civ.*, 2019, 105 ss.

⁵¹ G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015, 16 ss.; A. ALPINI, *Compatibilità e analogia nell'unità del procedimento interpretativo. Il c.d. rinvio in quanto compatibili*, in *Rass. dir. civ.*, 2016, 701 ss.

⁵² P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico*, Napoli, 1972, 12 ss.; P. FEMIA, *Interessi e conflitti culturali nell'autonomia privata e nella responsabilità civile*, Napoli, 1996, 38 ss.; L. LONARDO, *Il valore della dignità della persona nell'ordinamento italiano*, in *Rass. dir. civ.*, 2011, 773; N. LIPARI, *Personalità e dignità nella giurisprudenza costituzionale*, in G. CONTE, S. LANDINI (a cura di), *Principi, regole, interpretazione, contratti e obbligazioni, famiglia e successioni*, I, Mantova, 2017, 261 ss.

⁵³ Cfr. M.G. STANZIONE, *Il regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Eur. dir. priv.*, 2016, 1249 ss.; G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1 ss.; ID., *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in *Quad. cost.*, 2018, 895 ss.; M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, 165 ss.; R. SENIGAGLIA, *Reg. UE 2016/679 e diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza*

strutturazione dei diritti e delle facoltà riconosciuti all'utente. A titolo esemplificativo si possono considerare: il diritto dell'interessato (art. 15) di accesso al trattamento; il diritto di rettifica (art. 16) ed il diritto di cancellazione ex art. 17 (connesso al più famoso diritto all'oblio⁵⁴); il diritto di limitare il trattamento in corso sui propri dati al ricorrere di esigenze specificamente individuate (art. 18), nonché il diritto alla loro portabilità (art. 20), ad esempio, dal fornitore di un servizio ad un altro; il diritto di opporsi al trattamento dei propri dati ed alla profilazione sulla base di questi (art. 21), così come di opporsi ad un processo decisionale automatizzato (art. 22).

Si può parlare di controllo dei dati personali con riguardo a tutte le facoltà partecipative previste dagli artt. 15 ss. GDPR, che realizzano la dimensione personalistica nella possibilità di pretendere che i propri dati siano trattati secondo canoni di ragionevolezza⁵⁵ e necessità (desumibili dal principio di lealtà di cui all'art. 8, par. 2, Carta UE). Sotto la disciplina precedente era forse possibile sostenere che l'utente avesse la proprietà dei propri dati e alcuni terzi avessero possibilità di accedervi⁵⁶. Superando le derive del proprietarismo⁵⁷, il reg. UE n. 679/2016 consente di accelerare il ripensamento del paradigma dominicale⁵⁸, offrendo, rispetto ai dati particolari, un approccio peculiare del

nell'ordine della dignità personale, in *Nuove leggi civ. comm.*, 2017, 1023 ss.; ID., *La dimensione patrimoniale del diritto alla protezione dei dati personali*, in *Contr. impr.*, 2020, 760 ss.; A. THIENE, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo Regolamento europeo*, in *Nuove leggi civ. comm.*, 2017, 410 ss.; F. BRAVO, *Lo scambio di dati personali nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. impr.*, 2019, 34 ss.; ID., *Sul bilanciamento proporzionale dei diritti e delle libertà fondamentali, tra mercato e persona: nuovi assetti nell'ordinamento europeo*, in *Contr. impr.*, 2018, 203 ss.; I.A. CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi giuridica e studi comportamentali*, in *Oss. dir. civ. comm.*, 2018, 67 ss.; V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contr. impr.*, 2018, 1098 ss.; A. IULIANI, *Note minime in tema di trattamento dei dati personali*, in *Eur. dir. priv.*, 2018, 293 ss.; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali: i principi ispiratori*, in *Contr. impr.*, 2018, 106 ss.; E. PELLECCIA, *Dati personali, anonimizzati, pseudoanonimizzati, deidentificati: combinazioni possibili di livelli molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm.*, 2020, 360 ss.; V. RICCIUTO, *Il contratto e i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 2020, 652 ss.; R. TREZZA, *Diritto ed intelligenza artificiale*, Pisa, 2020, 29 ss.

⁵⁴ Cfr. Corte giust., 24 settembre 2019, c-507/17, in *Foro it.*, 2019, c. 572.

⁵⁵ Cfr. E. GIORGINI, *Ragionevolezza e autonomia negoziale*, Napoli, 2010, 20 ss.

⁵⁶ G. ALPA, *La proprietà dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, 11 ss.; ID., *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 2017, 723 ss.

⁵⁷ P. FEMIA, *Una finestra sul cortile. Internet e il diritto all'esperienza metastrutturale*, in C. PERLINGIERI, L. RUGGERI (a cura di), *Internet e Diritto civile*, cit., 46.

⁵⁸ M. LIBERTINI, *Persona, ambiente e sviluppo: ripensare la teoria dei beni*, in *Benessere e regole dei rapporti civili*, Napoli, 2015, 479 ss.

controllo⁵⁹. Il regolamento pone una certa enfasi sul profilo del consenso⁶⁰, quale diritto personalissimo.

Nella difficoltà di rinvenire un unico paradigma⁶¹, le indagini dottrinali recenti hanno ricercato un punto di equilibrio fra consenso e consapevolezza delle implicazioni del trattamento, valorizzando la matrice personalistica della normativa di riferimento⁶². In virtù della sua intima connessione con l'obbligo informativo che deve precederne la richiesta, il consenso è il veicolo attraverso cui l'utente è posto nelle condizioni di giungere alla consapevolezza piena dell'utilizzo dei propri dati, nonchè dei poteri di controllo sui flussi informativi che lo riguardano.

L'art. 4, paragrafo 1, n. 11 del GDPR e l'art. 7, paragrafo 1, sanciscono il principio della spontaneità del consenso. Si fa riferimento, dunque, a un consenso libero, che va inteso sia come consapevolezza che come mancanza di condizionamenti, comprendendo tanto le conseguenze che potrebbero derivare da un rifiuto a far trattare i propri dati, quanto le eventuali pressioni psicologiche che ne inficerebbero le fondamenta. Si deve trattare, in altre parole, di una scelta vera, genuina e scevra da condizionamenti, che attenga al rapporto intercorrente tra titolare ed interessato. Al fine di garantire la massima espansione di suddetto principio, il legislatore europeo ha stabilito alcuni presidi, che si sostanziano, ad esempio, nel consenso informato ed in quello specifico.

Invero, si parla di consenso informato in quanto esso mira a colmare le possibili asimmetrie che, spesso, contraddistinguono i rapporti in questione e, per tale ragione, anche il Considerando 32 del Regolamento sancisce: «Il consenso dovrebbe essere prestato

⁵⁹ R. PICARO, *Le identità consumeristiche nella società della connettività e della condivisione*, Napoli, 2019, 102, mette in risalto il merito avuto dal GDPR che, nell'accentuare la valenza del diritto alla protezione dei dati come diritto fondamentale e dell'autodeterminazione informativa come condizione necessaria per il libero sviluppo della personalità del cittadino, ha segnato il passaggio da una concezione proprietaria del dato ad una concezione di controllo.

⁶⁰ Critici verso il ruolo attribuito dal legislatore al consenso, S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Riv. crit. dir. priv.*, 1984, 732 ss.; S. THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, cit., 147; C. CAMARDI, *Mercato delle informazioni e privacy. Riflessioni generali sulla L. n. 675/1996*, in *Eur. dir. priv.*, 1998, 1061; V. CARBONE, *Il consenso, anzi i consensi, nel trattamento informatico dei dati personali*, in *Danno resp.*, 1998, 30.

⁶¹ F.G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, Napoli, 2008, 183 ss.

⁶² Cfr. C. PERLINGIERI, *eHealth and Data*, in R. SENIGAGLIA, C. IRTI, A. BERNES (a cura di), *Privacy and Data Protection in Software Services*, Singapore, 2022, 130 ss.; A. VIVARELLI, *Il consenso al trattamento dei dati nell'era digitale*, cit., 72 ss.

mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano»⁶³. Viene, quindi, incoraggiato un salto di qualità da parte del titolare del trattamento⁶⁴ e può, dunque, evidenziarsi come il rapporto tra consenso e informativa, seppur rinnovato nelle sue dinamiche, sia giuridicamente molto stretto.

Si parla, invece, di consenso specifico avendo riguardo alle ipotesi in cui il trattamento abbia ad oggetto più finalità, per cui dovranno essere prestati tanti consensi quante sono gli obiettivi. Tale aspetto risponde ad un'esigenza di libertà, in quanto, in caso contrario, si priverebbe l'interessato della possibilità di scegliere a quali trattamenti acconsentire.

Si tratta, in sostanza, di una previsione che costituisce un'articolazione del concetto di controllo da parte dell'interessato, il quale, comprese le diverse finalità di un trattamento, può acconsentirvi consapevolmente e liberamente⁶⁵.

Inoltre, il consenso deve essere inequivocabile, ossia certo sia per quanto riguarda la circostanza che esso sia stato effettivamente prestato, sia con riferimento al contenuto.

Pertanto, salvo ipotesi specifiche, vige il principio della libertà della forma, per cui il consenso può essere prestato anche attraverso un comportamento concludente, purché la volontà dell'interessato sia inequivocabile ed espressa, non rilevando la semplice inazione, il silenzio o la preselezione della casella effettuata dal titolare del trattamento. Infine, il consenso deve essere dimostrabile, nel senso che il titolare è gravato dall'onere di provare l'avvenuta manifestazione del consenso e il momento in cui esso è stato espresso, attestando altresì di aver fornito un'informativa valida al momento della raccolta.

Ciò premesso, dare una corretta definizione del consenso è tutt'altro che semplice, in quanto esso è caratterizzato dalla sussistenza di una serie di elementi che appartengono a fattispecie giuridiche differenti, tanto che si suole parlare di pluralità di consensi⁶⁶.

⁶³ Cfr. Corte di giustizia U.E., 11 novembre 2020, C-61/19, in *Nuove leggi civ. comm.*, 2021, 247 ss. Cfr. anche M.C. MENEGHETTI, *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in *MediaLaws*, 2021, 266 ss.; Cass., 25 maggio 2021, n. 14381, in *Law. giur.*, 2022, 153; cfr. anche F. PAOLUCCI, *Consenso, intelligenza artificiale e privacy*, in *MediaLaws*, 2021, 259 ss.

⁶⁴ L. SCUDIERO, *Il consenso come condizione di libertà*, in G. CASSANO, V. COLAROCO, G. B. GALLUS (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018 n. 101*, Milano, 2018, 102.

⁶⁵ L. SCUDIERO, *Il consenso come condizione di libertà*, cit., 98.

⁶⁶ V. CARBONE, *Il consenso, anzi i consensi nel trattamento informatico dei dati personali*, cit., 23 ss. Seppure tale contributo sia antecedente all'emanazione del Codice della privacy, risulta estremamente attuale, in quanto la disciplina prevede diverse tipologie di consenso che si aggiungono alle numerose ipotesi rinvenibili nelle diverse branche

Esso, difatti, è uno strumento volto a comporre i contrapposti interessi del titolare e dell'interessato, che, in ragione dell'eterogeneità dei valori coinvolti, rappresentano l'incontro conflittuale tra il diritto di autodeterminare la propria personalità e la libertà informativa⁶⁷.

Il legislatore, pertanto, deve costantemente utilizzare tecniche di composizione delle diverse prerogative, adottando soluzioni che preservino la sfera privata dell'individuo ed al contempo garantiscano la circolazione dei dati personali quali beni economici⁶⁸. In tale ottica, il consenso funge da strumento di equilibrio fra il diritto all'autodeterminazione e la libertà informativa, divenendo prerogativa di libertà e assumendo il rango di diritto sui diritti che sorge dall'attività di trattamento.

L'art. 5, paragrafo 1, lett. a) del GDPR, nel prevedere che il trattamento dei dati personali debba essere lecito, non si limita a stabilire che esso non debba essere antigiusuridico, ma afferma, altresì, che in presenza dei presupposti previsti dalla normativa è pienamente lecito di per sé, qualificandolo come un vero e proprio diritto al trattamento, espressione del principio di libertà della circolazione dei dati⁶⁹.

In merito alla natura giuridica del consenso, la dottrina risulta divisa: un primo orientamento vi ravvisa un atto di autorizzazione, mentre una diversa corrente di pensiero è

del diritto. Ci si riferisce, ad esempio, al consenso informato in materia sanitaria o alla disciplina della tutela del diritto all'immagine. Cfr. anche F. STASSI, *Consenso dell'interessato e dati personali al tempo dei Big Data*, in *Riv. dir. econ., traspr., amb.*, 2021, 120 ss.

⁶⁷ S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, cit., 993.

⁶⁸ F. PIRAINO, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, pp. 375 s., sottolinea che «sotto il profilo dell'impostazione di fondo, rispetto alla dir. 95/46 il Regolamento si attegga in maniera più accentuata come una disciplina della circolazione dei dati personali, pur sensibile alle possibili conseguenze del trattamento sull'interessato, piuttosto che come un'ulteriore tappa del lungo e accidentato percorso riconoscimento giuridico della centralità della persona e della predisposizione di strumenti di realizzazione della persona umana e di salvaguardia contro le interferenze esterne».

⁶⁹ F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 149 s. L'A. sostiene che «l'autonomia privata non assume, nella prospettiva europea, un ruolo centrale ed esclusivo tra i criteri di selezione degli interessi relativi alla protezione dei dati quale diritto fondamentale della persona, trattandosi solo di uno dei criteri alternativi volti a dare fondamento legittimo all'attività di trattamento posta in essere dal titolare e, al contempo, operare quale meccanismo di primo livello nella selezione degli interessi protetti dall'ordinamento giuridico». Sempre secondo ID., *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, cit., 148, quanto detto «trae il suo fondamento, in ambito privatistico, in un insieme di diritti di libertà tra cui, in ambito economico, quella di iniziativa economica, che costituisce il riferimento primario, e quella di informazione. È diritto che non è riferibile esclusivamente allo svolgimento di un'attività imprenditoriale, né di un'ulteriore, pur sempre professionalmente svolta [...]: la libertà di iniziativa economica si estende oltre, comprendendo sia quelle po' anzi menzionate, sia l'attività economica anche occasionalmente esercitata».

propensa ad attribuirgli natura negoziale.

Per quanto concerne gli orientamenti dottrinali che escludono la natura negoziale del consenso, essi traggono la loro ratio nei caratteri di assolutezza, imprescrittibilità, indisponibilità e intrasmissibilità che contraddistinguono il dato personale, quale connotato del diritto della personalità⁷⁰.

Trattandosi di uno strumento di auto-determinazione, espressione della personalità umana, il consenso non potrebbe in alcun modo assumere valenza patrimoniale. Conseguentemente, non potrebbe essere valutato in un'ottica negoziale, ma solo come autorizzazione dell'interessato all'adozione da parte di un soggetto terzo di comportamenti in grado di coinvolgere la sua sfera personale⁷¹.

Una prima tesi qualifica il consenso come atto riconducibile alla scriminante di cui all'art. 50 c.p.⁷² Il consenso assolve a una duplice funzione: da un lato elimina il velo di riservatezza che copre l'informazione personale; dall'altra, garantisce all'interessato una circolazione dei dati personali conforme alla sua volontà. La sua natura giuridica sarebbe autorizzativa del compimento di un atto di per sé illegittimo⁷³. Pertanto, attraverso la manifestazione del consenso, lo stesso interessato regolamenterebbe il momento circolatorio e dunque, il rapporto con il titolare non assumerebbe natura negoziale, ma sarebbe conseguenza diretta ed inevitabile del potere di autodeterminazione. Il consenso implicherebbe la perdita dell'antigiuridicità in riferimento alla condotta del titolare del

⁷⁰ P. RESCIGNO, *Personalità (diritti della)*, in *Enc. giur.*, XXIII, Roma, 1991, 3 ss.; A. DI MAJO, *Profili dei diritti della personalità*, in *Riv. trim. dir. proc. civ.*, 1962, 94 ss.

⁷¹ «Visto nell'ottica della tutela assoluta della persona, esso è sovente interpretato come un mero strumento di autodeterminazione, di espressione della personalità umana: esso non è valutabile in termini patrimoniali, sicché gli effetti del suo svolgersi non sono qualificabili in termini di arricchimento/depauperamento delle ricchezze delle due parti di un rapporto (il soggetto che cede e quello che riceve i dati), e non sono in grado di determinare, quindi, la nascita di pretese di ordine patrimoniale da parte di chi cede i dati nei confronti di chi le riceve. In altri termini, il consenso cui non si dovesse riconoscere natura negoziale, non sta alla base di un fenomeno di negoziabilità dei dati, ma rappresenta, unicamente, un'autorizzazione della persona all'adozione di comportamenti in grado di coinvolgere la propria sfera personale». Così V. RICCIUTO, *Nuove prospettive del diritto privato dell'economia*, in E. PICOZZA e V. RICCIUTO (a cura di), *Diritto dell'economia*, Torino, 2013, 319, il quale, però, sottolinea che «da natura negoziale del consenso al trattamento dei dati personali, non è da escludere; al contrario, più di una voce si è espressa a favore del riconoscimento di una tale natura».

⁷² F. MANTOVANI, *Diritto penale*, Padova, 2017, pp. 245-249.

⁷³ A. FICI, E. PELLECCIA, *Il consenso al trattamento*, in R. PARDOLESI (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, I, Milano, 2003, 502 ss.

trattamento, impedendo l'insorgere di una responsabilità penale⁷⁴.

Una rielaborazione di tale teoria è avvenuta ad opera di chi ravvisa nel consenso un atto autorizzativo⁷⁵, ossia un atto a struttura unilaterale non negoziale la cui funzione sarebbe quella di consentire la realizzazione della propria sfera personale. Secondo tale opinione, il consenso assumerebbe i connotati dell'autorizzazione, divenendo condizione di accesso alla sfera personale e rappresentando un effetto connaturato allo stesso esercizio del potere autodeterminativo. Esso sarebbe caratterizzato dalla sussistenza di un profilo precettivo, fonte di regolamentazione per quel che attiene l'aspetto circolatorio dei dati. In altri termini, il consenso non avrebbe la mera funzione di rendere lecito il trattamento, ma garantirebbe la partecipazione dell'interessato alla circolazione dei propri dati personali⁷⁶. Il consenso così

⁷⁴ In altre parole, il trattamento dei dati personali sarebbe un'attività di per sé illecita e vietata, ma diverrebbe lecita, pur essendo circoscritta nel quantum e nel quomodo, tramite la manifestazione del consenso, che diverrebbe una vera e propria causa di giustificazione; inoltre, nel rispetto del carattere dell'imprescrittibilità, il consenso dell'avente diritto non comporterebbe una rinuncia definitiva né un'estinzione del diritto, ma la sua efficacia risulterebbe più circoscritta, riguardando esclusivamente la legittimazione alla lesione: non vi sarebbe un mutamento del diritto, bensì solo una sua parziale disponibilità. In ogni caso, il consenso dell'avente diritto influisce sul diritto soggettivo, poiché la tutela giuridica rispetto a determinati atti lesivi viene meno. Così A. DE CUPIS, *I diritti della personalità*, Milano, 1982, 94. L'A. evidenzia che, per quanto concerne l'applicabilità del consenso ai diritti della personalità, stante il loro carattere intrinseco di indisponibilità, «i diritti della personalità possono essere muniti di quel particolare e più modesto aspetto della facoltà di disposizione che è costituito dalla facoltà di consentire la lesione: quando si dice che essi sono indisponibili, sprovvisti della facoltà di disposizione, l'espressione deve essere intesa con questo temperamento».

⁷⁵ D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, pp. 350-351: «Il consenso al trattamento e alla circolazione dei dati personali, in altri termini, deve essere analizzato da diversi punti di vista, poiché le sue manifestazioni subiscono diverse trasformazioni. L'idea fondamentale e connettiva del quadro normativo che emerge dalla disciplina specifica è quella che il consenso dell'interessato, nella sua caratterizzazione di permesso autorizzativo, costituisce lo strumento che ha l'efficacia di rendere i dati intimi della persona non più assoggettati alla logica della repressione di qualunque circuito conoscitivo poste in essere. In questo senso, rappresenta l'elemento di connessione mediante il quale si attua una modificazione nelle forme particolari del potere».

⁷⁶ Questa teoria si basa sull'assunto per cui il consenso, avendo ad oggetto un diritto della personalità, può essere letto solamente in chiave autorizzativa-procedimentale e, dunque, in modo diverso rispetto ai casi in cui la circolazione abbia ad oggetto beni mercantili. Tale dottrina, quindi, attribuisce al consenso la natura di atto e trae la sua ratio nella circostanza per cui è pur sempre la legge a dettare una specifica disciplina in materia di circolazione dei dati personali, indicando esplicitamente le ipotesi in cui l'attività possa essere considerata legittima. Ciò che in realtà costituisce oggetto di circolazione e di negoziazione non è il dato personale di per sé, bensì la notizia in esso contenuta: il titolare di un diritto della personalità non può mai spogliarsi dello stesso trasferendolo ad un altro individuo. Pertanto, a prescindere dalla fase della circolazione in cui esso opera e che abbia, dunque, natura permissiva ovvero si tratti della fase patologica del rapporto, il consenso non potrebbe mai assumere natura contrattuale, configurandosi come atto necessariamente unilaterale e non creandosi un rapporto di natura bilaterale e neppure un concorso di volontà; la dichiarazione di volontà effettuata dal titolare del dato personale assumerebbe, pertanto, natura prettamente ricognitiva e, quindi, il regime della negoziazione non sarebbe caratterizzato da diverse manifestazioni di volontà, bensì da un rapporto regolamentare di creazione unilaterale. Così P. MANES, *Il consenso al trattamento dei dati personali*, Padova, 2001, 54. A fortiori, la dottrina in questione si basa sui frequenti richiami effettuati anche dallo stesso Garante per la protezione dei

considerato non darebbe vita ad un rapporto di natura negoziale e, pertanto, nel caso di trattamento illecito di dati personali, la responsabilità che sorgerebbe in capo al titolare sarebbe di tipo extracontrattuale ai sensi dell'art. 2043 c.c., in ragione della violazione del principio del *neminem laedere*.

Invero, in merito al danno da trattamento, il legislatore del 2003 si era limitato a richiamare all'art. 15 del Codice della privacy le regole civilistiche in materia di attività pericolose ex art. 2050 c.c., sebbene la dottrina risultasse discordante⁷⁷.

Con la novellazione del Codice della privacy, il citato art. 15 citato è stato abrogato e, dunque, è necessario prendere in considerazione l'art. 82 del Regolamento, il quale, a differenza della previgente disciplina nazionale, non contiene alcun espresso riferimento alle attività pericolose, ma prevede esclusivamente che il titolare risponderà qualora il trattamento sia stato realizzato nella sua sfera decisionale⁷⁸.

dati personali alla tutela dei diritti e delle libertà fondamentali, che impedirebbero di guardare al rapporto fra titolare ed interessato in un'ottica meramente negoziale. Il consenso, dunque, non potrebbe avere alcuna valenza traslativa o dispositiva, poiché i dati personali, afferendo alla persona, sfuggirebbero del tutto a una logica costitutiva o proprietaria e la manifestazione del consenso da parte dell'interessato si presenterebbe come un atto a struttura unilaterale e non negoziale.

Come notato anche da D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., 353, «si afferma, in tal modo, il principio che ogni relazione conoscitiva dell'identità personale del soggetto, perché sia lecita, debba essere sottoposta ad un atto autorizzativo il soggetto interessato. Si deve osservare, a questo proposito, come il concetto di effetto autorizzativo esprima linguisticamente un effetto costitutivo di legittimazione di una azione nella sfera soggettiva altrui».

⁷⁷ Una prima tesi, più tradizionale, ritiene che l'equiparazione con le attività pericolose tragga la sua ratio dalla circostanza per cui il trattamento dei dati personali mette sempre a rischio la sfera individuale, in quanto l'interessato può essere danneggiato sotto diversi punti di vista; il richiamo a tale forma di responsabilità deriverebbe, dunque, dal fatto che l'attività di trattamento dei dati personali risulta, di per sé, idonea a mettere in pericolo i diritti fondamentali dell'individuo come la riservatezza e l'identità personale, in ragione della vastità di fonti potenzialmente lesive. Così E. TOSI, *Diritto privato dell'informatica e Internet. I beni, i contratti, le responsabilità*, Milano, 2006, 461 ss.; G. P. CIRILLO, *La tutela civilistica del trattamento dei dati personali*, in A. LOIODICE, G. SANTANIELLO (a cura di), *La tutela della riservatezza*, Padova, 2000, 2734.

Più di recente, invece, gli studiosi si sono soffermati sul regime probatorio caratterizzante l'art. 2050 c.c., consistente nella prova liberatoria di aver adottato tutte le misure necessarie ad evitare il danno; pertanto, per escludere la responsabilità di cui all'art. 15, è necessario allegare il fatto specifico di rilievo che fa degradare l'evento verificatosi a una mera occasione e non a causa dell'evento, dimostrando la sua inevitabilità in quanto estraneo alla sfera di controllo del titolare del trattamento. Alla luce di ciò, per poter correttamente configurare un'ipotesi di responsabilità ex art. 15, è necessario allegare e dimostrare il pregiudizio subito a seguito del trattamento illecito, mentre il titolare, per sottrarsi all'obbligo risarcitorio, dovrà dimostrare di aver adottato tutte le misure idonee ad evitare il danno. Cfr. A. PINORI, *Internet e responsabilità per il trattamento dei dati personali*, in *Contr. e impr.*, 2007, 1568.

⁷⁸ L'obiettivo di assicurare un adeguato livello di tutela dell'interessato non può, però, essere perseguito solamente attraverso la previsione di norme che disciplinino il comportamento diligente da parte del titolare del trattamento e, pertanto, è stato creato un impianto regolamentare che, almeno teoricamente, prevede e, al contempo, previene i rischi derivanti dagli illeciti. Così P. TROIANO, *Misure minime di sicurezza*, in C.M. BIANCA,

Permane, invece, un meccanismo di inversione dell'onere della prova, in quanto ai sensi del paragrafo 3 della citata norma, il danneggiante non sarà gravato dall'obbligo risarcitorio qualora dimostri che l'evento dannoso non sia a lui in alcun modo imputabile, prefigurandosi una sorta di responsabilità oggettiva sui generis⁷⁹.

Ciò posto, le teorie che ravvisano nell'istituto del consenso un atto non negoziale presentano diverse criticità. Anzitutto, non valorizzano l'utilità patrimoniale del diritto sul dato personale, che, invece, costituisce uno degli aspetti di maggiore rilevanza, oltre a venire completamente tralasciata la valenza di bene economico. La seconda ragione risulta strettamente correlata alla prima, giacché viene del tutto trascurato il fatto che il trattamento dei dati personali può divenire causa fondante il rapporto tra titolare ed interessato. Infine, il presupposto dell'esercizio di un pieno controllo da parte dell'interessato è opinabile. Sebbene, difatti, il consenso assolve ad una funzione di monitoraggio, una volta che l'informazione personale è stata immessa nella rete, sarebbe pressoché impossibile controllarla o cancellarla definitivamente. Quindi, nonostante il legame fra interessato e dato personale non si estingua definitivamente a seguito della cessione per il trattamento, non si ritiene possa parlarsi di un pieno potere di controllo, in quanto la circolazione dei dati personali deve essere qualificata non con riferimento alla singola operazione economica, ma in un'ottica dinamica e negoziale.

L'articolo 10 del Regolamento contiene la disciplina riguardante il trattamento dei

F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al d.lgs. 30 giugno 2003, n. 196 (Codice della privacy)*, I, Torino, 2007, 685. Sul tema si è pronunciata anche Cass., 26 giugno 2012, n. 10646, in *Danno resp.*, 2013, 399, la quale ha stabilito che «in tema di trattamento dei dati personali, l'onere della prova per la mancata custodia degli stessi incombe al danneggiante, come disposto dall'art. 2050 c.c., richiamato dall'art. 15 d.lgs. 30 giugno 2003 n. 196, salvo che le notizie siano note già prima della loro diffusione da parte di questo, poiché, in tal caso, il danneggiato non è esentato dall'onere di dimostrare o, quanto meno, di indicare elementi presuntivi idonei a motivare la convinzione che la divulgazione sia riconducibile a chi possiede tali dati e non a chi abbia in precedenza pubblicato le medesime informazioni. Né può configurarsi un diritto al risarcimento quando il custode abbia divulgato i dati a salvaguardia della correttezza del proprio comportamento, perché i principi in tema di riservatezza vanno coordinati, oltre che con quelli che attengono all'interesse pubblico e al diritto della collettività all'informazione, con le esigenze di salvaguardia di interessi, pubblici e privati, all'onorabilità delle proprie frequentazioni nonché alla correttezza ed al rigore dei propri comportamenti [...]. Allorché le notizie che si assumono illecitamente diffuse risultino già pubblicamente note, il danneggiato non può ritenersi esentato da ogni onere di dimostrare, o quanto meno di indicare elementi presuntivi idonei a motivare la convinzione che la divulgazione di tali notizie sia riconducibile al convenuto-danneggiante, e non alle altre fonti che abbiano in precedenza pubblicato le medesime informazioni».

⁷⁹ G. MIRABILE, *Le tendenze evolutive della giurisprudenza riguardo alla nozione di attività pericolosa*, in *Resp. civ. prev.*, 2018, 454 ss.

dati personali relativi a condanne penali e reati. Si tratta di una prescrizione piuttosto semplice, che incarica legittimamente del trattamento di tali dati solo e soltanto l'autorità pubblica secondo il diritto dell'Unione o degli Stati membri, prevedendo che solo quest'ultima possa tenere un registro completo delle condanne penali, in modo da bilanciare il diritto alla riservatezza con il grado necessario di tutela dell'ordine pubblico.

Di fronte a questa disposizione, che può sembrare piuttosto scarna, va ricordato che le norme specifiche riguardanti i dati giudiziari e il loro trattamento da parte delle forze dell'ordine e degli altri titolari legittimi sono contenute nella Direttiva 2016/680 del Parlamento europeo e del Consiglio d'Europa relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati. Restano naturalmente valide le disposizioni riguardanti la liceità, la correttezza e la proporzionalità del trattamento così come indicate dal Regolamento. A questi principi si aggiungono poi numerose specificità introdotte dal decreto, ad esempio differenze nel trattamento a seconda della posizione giuridica dell'interessato (parte civile, testimone, persona informata sui fatti, ...) oppure la distinzione tra dati fattuali e valutazioni.

Dal combinato disposto delle discipline menzionate pare deducibile un principio generale, in base al quale è sancita la tutela dei dati personali nel giusto processo (sia penale che civile). Infatti, va ricordato come, seppure l'ambito penale sia quello che maggiormente afferisce a beni giuridici di rango costituzionale, tuttavia, non si può ignorare la personalizzazione del processo civile, quale strumento per la valorizzazione di interessi meritevoli di tutela⁸⁰.

3. La responsabilità per illecito trattamento dei dati: spunti di riflessione

Nel momento in cui si cerca di determinare l'entità e la tipologia del danno derivante dal trattamento illecito, occorre partire dall'assunto per cui l'interessato può trarre ed al contempo attribuire un'utilità di natura economica nel consentire il trattamento dei propri

⁸⁰ P. PERLINGIERI, *Il giusto rimedio nel diritto civile*, in *Il giusto processo civile*, 2011, 3.

dati personali. Posto che il rapporto intercorrente fra titolare del trattamento ed interessato abbia natura obbligatoria, è necessario esaminare l'ipotesi di mancato o inesatto adempimento dell'obbligazione assunta, consistente nella violazione dei limiti prefissati attraverso la manifestazione del consenso.

Quando il dato personale viene trattato al di fuori di tali limiti, ciò non comporta solamente una lesione della privacy, ma, altresì, un nocumento di natura patrimoniale. Può parlarsi anche di un danno da mancato sfruttamento economico delle proprie vicende, la cui fonte risiede nel pregiudizio subito dall'interessato a causa della pubblicazione non autorizzata di dati personali, con conseguente impossibilità di sfruttare le proprie vicende per fini di guadagno. Il risarcimento è previsto nell'ipotesi in cui la pubblicazione di tali vicende personali sia avvenuta senza il consenso dell'interessato, non solo come lesione della sfera intima e personale, ma anche come lucro cessante, consistente nell'impossibilità di dar vita ad un rapporto conveniente. La possibilità di ottenere siffatto risarcimento trova riscontro nella circostanza per cui un attributo della personalità, sebbene conservi in modo inalterato le proprie caratteristiche e prerogative⁸¹, può dar vita ad un vantaggio patrimoniale.

Il criterio adoperato è quello legale di quantificazione, che fa ritenere risarcibile tutto ciò che è direttamente riconducibile al calcolo differenziale tra situazione iniziale e finale del patrimonio del danneggiato⁸². Per tale ragione, stante l'esigenza di assicurare alla vittima l'utilità che avrebbe potuto ottenere dal diritto leso⁸³, si è parlato di prezzo del consenso,

⁸¹ Lungimirante G. SANTINI, *I diritti della personalità nel diritto industriale*, Padova, 1959, pp. 165-166: «Questo rilievo ne introduce subito un altro: fra il c.d. bene della personalità ed il bene patrimoniale, entrambi immateriali, esiste un solco che non può essere colmato: il bene della personalità può anche assumere valore economico, nel senso che una sua lesione provoca danni patrimoniali; lo pseudonimo, per esempio, ben poco si differenzia, sul piano economico, dalla ditta. Per contro, il bene patrimoniale immateriale può anche perdere ogni valore economico ed averne, se possibile, uno negativo, come accade per una ditta appena formata o appartenente ad un imprenditore da tempo dissestato. La differenza fra le due categorie non si apprezza dunque sul piano economico e (im)materiale, sotto il quale profilo sono, anzi, affini; si apprezza, invece, esclusivamente sotto il profilo giuridico. Invero, i beni della personalità sono tali perché sono l'oggetto dei diritti personalissimi indisponibili; i beni immateriali sono tali perché oggetto di un diritto esclusivo e disponibile, sulla natura del quale, come ho detto, rinvio all'insegnamento tradizionale, senza prendere posizione».

⁸² C. CASTRONOVO, *Le frontiere nobili della responsabilità civile*, in *Riv. crit. dir. priv.*, 1989, 654, il quale afferma che la teoria della differenza definisce il danno risarcibile come la differenza negativa che il patrimonio della vittima subisce rispetto allo stato in cui esso si trovava prima della commissione del fatto illecito.

⁸³ In riferimento al danno all'immagine, quale connotato della personalità, Cass., 16 maggio 2008, n. 12433, in *Giust. civ. Mass.*, 2008, 744, ha stabilito che «il danno patrimoniale va ravvisato, quanto meno, nella violazione del diritto della parte lesa allo sfruttamento economico dell'immagine stessa e va quantificato nel c.d. prezzo del consenso, cioè nella somma che il ritrattato avrebbe potuto ottenere quale corrispettivo della volontaria concessione a terzi del diritto di pubblicare la propria fotografia».

rappresentato dall'utilità che l'interessato avrebbe potuto ottenere cedendo lui stesso le proprie informazioni personali⁸⁴.

Il problema più rilevante in materia di risarcimento del danno concerne la necessità di operare un bilanciamento fra due distinte, ma parimenti rilevanti esigenze. In primis la necessità di dettare una disciplina che individui i limiti dell'esercizio del diritto al risarcimento, al fine di evitare un dilatarsi eccessivo del campo di applicazione della norma che impedisca la necessaria circolazione del dato personale. Inoltre, l'istanza ineludibile di prevedere un adeguato sistema di protezione dell'individuo sembra assicurare la tutela dei diritti costituzionalmente garantiti, ma, proprio in virtù del danno subito, il risarcimento del danno appare tutt'altro che semplice.

Invero, quando i dati personali vengono trattati in modo illecito, generando un nocumento a carico dell'interessato, egli, ha diritto di far valere a titolo di danno patrimoniale la perdita dei vantaggi economici che avrebbe potuto conseguire, anche in ragione del fatto che il titolare ha ingiustamente ottenuto dei benefici economici dalla circolazione delle informazioni personali. Quindi, il risarcimento dovrebbe consistere nel trasferimento dei vantaggi dal titolare all'interessato. Nel momento in cui il dato personale dell'interessato viene ceduto senza consenso, risultandone diminuito il valore patrimoniale e impedendo un suo diretto sfruttamento, vi è una lesione. Tuttavia, è estremamente difficile dimostrare l'entità del pregiudizio economico subito e stabilire quale sia il corretto ristoro da attribuire.

Come noto, la prima tipologia di risarcimento cui il danneggiato può beneficiare è quello in forma specifica⁸⁵, anche se pare estremamente arduo procedere ad una stima del danno. Conseguentemente, si potrebbe ritenere applicabile l'art. 1226 c.c. (liquidazione equitativa). Tuttavia, pur ravvisando il nocumento patrimoniale nella violazione del diritto della parte lesa allo sfruttamento economico del dato (quantificandolo nel prezzo del consenso) e pervenendo alla riallocazione dei vantaggi economici dal titolare del trattamento

⁸⁴ La nozione di danno patrimoniale ricomprende, infatti, anche la perdita di utilità economiche future. Pertanto, nel caso in cui il titolare utilizzi in modo illecito i dati personali dell'interessato facendoli circolare, quest'ultimo risulterà parte lesa e avrà diritto ad ottenere il risarcimento del danno come mancato guadagno. Così, P. VERCELLONE, *Diritti della personalità e «rights of publicity»*, in *Riv. trim. dir. proc. civ.*, 1995, 1163 ss.

⁸⁵ F. GRITTI, *La responsabilità civile*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, 145.

all'interessato⁸⁶, un siffatto ristoro pare difficilmente ipotizzabile, in quanto inquadrabile in una fattispecie di danno bagatellare.

In alternativa, potrebbero ritenersi applicabili i rimedi di natura restitutoria (come il regime dell'arricchimento senza causa)⁸⁷. In tal modo, invero, non solo si garantirebbe una diversa tutela dell'interessato, ma si potrebbe sopperire, seppur solo parzialmente, a quelle mancanze che caratterizzano la disciplina del trattamento illecito di dati personali. Tuttavia, si tratta di rimedi individuali e successivi, fortemente distopici rispetto al principio dell'accountability. Quest'ultimo, definito il principio dei principi⁸⁸, prevede un nuovo approccio al rischio, grazie al quale la tutela dell'interessato risulta rafforzata. Esso riguarda le misure che debbono essere adottate dal titolare al fine di proteggere i dati personali dell'interessato, evitando o quantomeno riducendo i rischi di accesso e divulgazione di dati non autorizzati e di perdita e distruzione degli stessi⁸⁹.

Il nuovo quadro normativo è improntato sui doveri e sulla responsabilizzazione del titolare del trattamento, il quale deve dimostrare di aver impiegato tutte le privacy policies e le misure necessarie in modo conforme al GDPR⁹⁰. Egli dovrà, dunque, valutare quali siano le misure tecniche ed organizzative da adottare in base alla natura dei dati personali, all'oggetto ed alle finalità del trattamento.

Tali misure, poi, devono essere adeguate, essendo necessario tener conto del contesto e delle specifiche circostanze in cui il trattamento viene effettuato, mediante una considerazione ex ante. Ma siccome l'art. 24 Regolamento non elenca espressamente quali siano suddette misure, la valutazione dovrà essere effettuata case by case, rimettendo al titolare la scelta⁹¹.

⁸⁶ M. CHIAROLLA, *Alla scoperta dell'America, ovvero: dal diritto al nome e all'immagine al right to publicity*, in *Foro it.*, 1992, 831; A. BARENGHI, *Diritto all'immagine e danno patrimoniale*, in *Giur. it.*, 1991, 975; A. DASSI, *Sulla lesione dell'immagine di persona nota*, in *Resp. civ. prev.*, 1991, 741.

⁸⁷ P. SIRENA, *La restituzione dell'arricchimento e il risarcimento del danno*, in *Riv. dir. civ.*, 2009, 65 ss.; ID., *Note critiche sulla sussidiarietà dell'azione generale di arricchimento senza causa*, in *Riv. trim. dir. proc. civ.*, 2005, 105 ss.

⁸⁸ R. CELELLA, *Il principio di responsabilizzazione: la vera novità del GDPR*, in *Ciber. dir.*, 2018, 211.

⁸⁹ G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 13.

⁹⁰ Cfr. M. GAMBINI, *Responsabilità civile e controlli del trattamento algoritmico*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, cit., 321.

⁹¹ Si potrebbe, a questo punto, ritenere che l'assenza di un'elencazione specifica costituisca una lacuna rispetto alla certezza delle azioni che il titolare deve porre in essere al fine di rispettare il principio di accountability. In realtà, tale norma deve essere interpretata nel senso che il Regolamento abbia lasciato suddetto margine di

Si tratta di un netto capovolgimento di prospettiva, in quanto una delle problematiche principali del Codice della privacy derivava dalla previsione di strumenti di tutela esclusivamente successivi.

Può dirsi, dunque, che si è passati da una concezione puramente formale di adempimento degli obblighi relativi alla privacy ad un approccio sostanziale di tutela, in cui vengono combinati due aspetti: l'adozione di misure efficaci da parte del titolare del trattamento e la capacità di dimostrarne la conformità delle stesse al Regolamento.

L'art. 30 stabilisce che il titolare (e il suo eventuale rappresentante) o il responsabile, ha l'obbligo di tenere un registro relativo alle attività di trattamento svolte sotto la propria responsabilità, finalizzato a dimostrare la conformità di tali trattamenti ai principi enunciati nel GDPR. Vi è, in sostanza, un vero e proprio obbligo di rendicontazione. L'accountability, pertanto, diviene un concetto dinamico e relazionale, che si rapporta alle conoscenze acquisite in base al progresso tecnologico, alla natura dei dati personali oggetto del trattamento, nonché alle specifiche caratteristiche delle operazioni di trattamento.

Il titolare, di conseguenza, non solo assume un ruolo proattivo, ma è gravato da obblighi fortemente pregnanti. Il riferimento riguarda i codici di condotta e le certificazioni di cui al paragrafo 3 dell'art. 32 del Regolamento. Trattasi di due istituti volti a dimostrare il rispetto degli obblighi da parte del titolare e, dunque, del principio dell'accountability. Egli, invero, dopo aver effettuato una valutazione relativa ai rischi⁹², alla natura dei dati, al contesto, ai costi, ai danni potenziali e allo stato dell'arte, compie un'attività di costante monitoraggio per verificare l'adeguatezza e la proporzionalità delle suddette misure⁹³.

La ratio di tale sistema è di garantire soluzioni orientate verso la massima protezione

manovra al titolare per garantire la «scalabilità» della protezione dei dati, cioè un adattamento delle misure al trattamento effettuato, affinché se ne possa garantire l'efficacia». Cfr. L. BOLOGNINI, E. PELINO, C. BISTOLFI, *Il Regolamento Privacy europeo*, Milano, 2016, 326.

⁹² A. MANTELERO, *Responsabilità e rischio nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, 163-164: «proprio l'analisi dei rischi ed in conseguente processo di mitigazione di questi ultimi rappresentano la chiave di volta di un modello a venire, in cui la centralità dell'individuo e della sua tutela muovono da una dimensione endogena verso una dimensione esogena. Partendo infatti dall'assunto che gli individui non possono (...) essere completamente consapevoli delle potenziali conseguenze del trattamento dei dati in sistemi complessi, si deve approdare alla conclusione che tali conseguenze devono necessariamente e preventivamente valutate ad opera di terzi, in maniera per certi versi analoga a quanto accade per la sicurezza dei prodotti».

⁹³ L. GRECO, *Il I ruoli: titolare e responsabile*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 255 s.

dei dati personali⁹⁴ ed un'applicazione di suddetti principi potrà in molti casi rendere superflua la valutazione finale del rischio, in quanto i diversi cicli di progettazione avranno già integrato l'analisi e la prevenzione dello stesso, mediante una consona modellazione del prodotto o del servizio stesso.

Il Regolamento contiene alcune disposizioni relative alla data breach, che possono essere annoverate fra le previsioni in materia di risk management, sebbene riguardino prevalentemente la gestione ex post di un evento pregiudizievole. Tale procedura risulta collegata al principio dell'accountability in ragione del fatto che la notifica della violazione non deve essere effettuata qualora il titolare sia in grado di dimostrare la mancanza di rischio per i diritti e le libertà delle persone fisiche nel caso di violazione dei dati personali. Il legame tra il principio dell'accountability e l'esclusione della notifica va rinvenuto nella circostanza per cui vanno applicate le misure di sicurezza ex art. 32, che il titolare deve attuare per garantire la tutela dei dati personali⁹⁵.

In ragione di questa ottica di responsabilizzazione, è stata inserita la figura del c.d. Data Protection Officer (DPO), che, per molti aspetti, costituisce il fulcro del nuovo apparato, in quanto gli viene riconosciuto un ruolo chiave nel sistema di gestione dei dati⁹⁶. Questo dimostra come l'intento del legislatore sia quello di garantire non solo l'adozione di misure adeguate, ma altresì la presenza di un soggetto che sorvegli la loro efficacia in modo da poterla comprovare di fronte alle Autorità di controllo, garantendo il rispetto dei principi e delle norme del GDPR.

Il DPO, tuttavia, non deve essere considerato un mero controllore dell'operato del titolare del trattamento, in quanto egli costituisce parte integrante del sistema di gestione della privacy ed agisce di concerto con il titolare al fine di ottimizzare le operazioni di trattamento. Il DPO, dunque, si caratterizza per la sua indipendenza, giacché, al di fuori delle ipotesi in cui deve essere obbligatoriamente coinvolto, può essere consultato in tutti i casi in cui il

⁹⁴ A. PRINCIPATO, *Verso nuovi approcci della tutela della privacy: privacy by design e privacy by default setting*, in *Contr. impr. Europa*, 2015, 202 s.

⁹⁵ Cfr. M. RENNA, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. prev.*, 2020, 1343 ss.

⁹⁶ S. COMELLINI, *Il responsabile della protezione dei dati: Data Protection Officer DPO aggiornato al d. lgs. del 10 agosto 2018, n. 101 in materia di privacy*, Santarcangelo di Romagna, 2018, 30; A. GRECO, *La nuova figura del Data Protection Officer*, in *MediaLaws*, 2021, 314.

titolare lo ritenga opportuno⁹⁷.

La scelta del legislatore di predisporre un impianto di tutela proattivo, caratterizzato da una serie di strumenti preventivi riguardanti la tutela dei dati personali oggetto di trattamento, non può che essere accolta positivamente, in quanto rappresenta un importante incentivo all'osservanza delle norme. Tuttavia, i rimedi descritti, anche alla luce del principio dell'accountability, non paiono sufficienti a tutelare concretamente l'interessato, in quanto si tratta di strumenti che quasi mai garantiscono il ripristino della situazione antecedente al verificarsi della lesione. Inoltre, non tengono conto dell'utilizzo collettivo dei dati personali, che può comportare conseguenze dannose in termini di discriminazione. Pertanto, in alternativa, si potrebbe applicare la disciplina di tutela collettiva prevista dal Codice del consumo (c.d. group privacy⁹⁸). In tal senso, si potrebbe pervenire al risultato utile di costituire delle associazioni rappresentative degli interessati⁹⁹. Ad oggi, difatti, un siffatto istituto è previsto solamente con riferimento ai consumatori, giacché l'art. 142 c. 2 Codice della privacy, il Considerando 142 e l'art. 80 del Regolamento si riferiscono esclusivamente alla possibilità per l'interessato di rivolgersi ad un organismo terzo per la protezione dei dati personali, affinché eserciti i diritti in sua vece. Qualora, invece, si prevedesse l'applicabilità del d.lgs. n. 205 del 2006 anche in materia di trattamento dei dati personali¹⁰⁰, l'ambito di garanzia potrebbe essere esteso notevolmente, assicurando una più intensa forma di tutela, posti i limiti di quella individuale.

Ai sensi dell'art. 37 del Codice del consumo, potrebbe ipotizzarsi l'intervento di un'associazione di categoria¹⁰¹ posta a salvaguardia degli interessati mediante il ricorso

⁹⁷ A. D'AGOSTINO, *Il sistema di gestione della privacy*, in G. CASSANO, V. COLAROCO, G.B. GALLUS (a cura di), *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018 n. 101*, cit., 39.

⁹⁸ Il concetto di group privacy, che ancora non trova una definizione univoca e pacifica, si propone di estendere ad un determinato gruppo, da intendersi non quale somma dei singoli membri ma come gruppo in sé, il diritto ad un'identità informazionale inviolata. Cfr. B. MITTELSTADT, *From Individual to Group Privacy in Big Data Analytics*, in *Philosophy & Technology*, 2017, 30, IV, 477 ss.; L. FLORIDI, *Group Privacy: a Defence and an Interpretation*, in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (a cura di), *Group Privacy. New Challenges of Data Technologies*, Springer, 2017, 103 ss.

⁹⁹ F. RICCI, *I contratti del consumatore: le clausole vessatorie*, in L. ROSSI CARLEO (a cura di), *Diritto dei consumi. Soggetti, atto, attività*, Torino, 2015, 77.

¹⁰⁰ Cfr. M. D'AMBROSIO, *Diritto all'immagine e reputazione nell'era dei social network*, in C. PERLINGIERI, L. RUGGERI (a cura di), *Internet e diritto civile*, cit., 161 ss.; ID., *Diritto all'immagine e utilizzo (in)consapevole della rete internet*, in *Foro nap.*, 2016, 153 ss.

¹⁰¹ A. QUERCI, *Le novità introdotte nel Codice del consumo dal d.l. 1/2012 ed il ruolo delle associazioni dei consumatori nella tutela contro le clausole vessatorie*, in *Contr. impr.*, 2013, 446 ss.

all'azione inibitoria. In tal modo, gli organismi associativi potrebbero convenire in giudizio il professionista (vale a dire il titolare del trattamento) richiedendo l'emanazione di un provvedimento che inibisca l'uso delle condizioni contrattuali considerate abusive.

Utilizzando tale strumento, si realizzerebbe una tutela sostanziale degli interessati che si inserirebbe in un ambito negoziale a latere delle azioni individuali.

L'obiettivo di una maggior tutela per l'interessato potrebbe, dunque, essere perseguito sia mediante una diretta applicazione delle norme contenute del Codice del consumo, ovvero attraverso la predisposizione di una normativa ad hoc, che, avendo come destinatari gli interessati, ricalchi quella consumeristica.

In tale contesto, occorre richiamare la sentenza del 25 gennaio 2018, causa C-498/16¹⁰², mediante la quale la terza sezione della Corte di Giustizia ha definito l'utente di Facebook un consumatore. La Corte ha affermato che «un ricorrente utilizzatore di tali servizi possa invocare la qualità di consumatore soltanto se l'uso essenzialmente non professionale di tali servizi, per il quale ha originariamente concluso un contratto, non ha acquisito, in seguito, un carattere essenzialmente professionale. Un'interpretazione della nozione di consumatore che escludesse tali attività si risolverebbe, infatti, nell'impedire una tutela effettiva dei diritti di cui i consumatori dispongono nei confronti delle loro controparti professionali, compresi quelli relativi alla protezione dei loro dati personali [...]. Alla luce delle considerazioni che precedono, [...] l'articolo 15 del regolamento n. 44/2001 deve essere interpretato nel senso che un utilizzatore di un account Facebook privato non perde la qualità di consumatore ai sensi di tale articolo allorché pubblica libri, tiene conferenze, gestisce siti Internet, raccoglie donazioni e si fa cedere i diritti da numerosi consumatori al fine di far valere in giudizio tali diritti»

Tale decisione, a cui si aggiunge anche la Direttiva 2019/770/UE (Digital Content and Service Directive), che, positivizzando la cessione del dato personale, definisce consumatore il cessionario di contenuti e servizi digitali¹⁰³, sembrano aprire la strada ad una

¹⁰² In *Giur. it.*, 2020, 1320.

¹⁰³ Cfr. G. MARINO, *Internet e tutela dei dati personali: il consenso ai cookie*, in *Jus civile*, 2021, 424 ss., secondo cui l'apporto fornito dalla DCSD è quello di aver avvicinato la disciplina della protezione dei dati personali allo statuto consumeristico, in modo da implementare il potenziale rimediabile a disposizione del consumatore-interessato.

possibile applicazione della disciplina consumeristica agli interessati al trattamento dei dati. La group privacy, infatti, sopperendo alle indubbie difficoltà che l'interessato può riscontrare nell'esercitare un'azione di tipo giudiziario, assicurerebbe una protezione concreta ed effettiva al soggetto pregiudicato dall'illecito trattamento.

4. I provvedimenti giurisdizionali tra pubblicità ed anonimato

Esaminate le conseguenze derivanti dall'illecito trattamento dei dati ed approntate alcune soluzioni, è opportuno verificare come la disciplina in questione venga declinata in ambito giudiziario.

La diffusione di banche di dati giuridiche ha messo in evidenza questioni sulle quali è tuttora aperto un acceso confronto, con l'obiettivo di coniugare la conoscibilità dei principi di diritto e della giurisprudenza proprie delle aule di Tribunale al diritto alla riservatezza ed all'oblio¹⁰⁴. Conoscere una sentenza costituisce una precisa garanzia offerta dallo Stato, in quanto emessa nel nome del popolo e conclusiva di un processo la cui pubblicità¹⁰⁵ si è storicamente affermata in funzione di garanzia del cittadino, rispetto alla tradizionale segretezza del potere esercitato mediante l'istruttoria giudiziale¹⁰⁶.

In questo contesto, il legislatore ha disciplinato la materia dei dati personali, distinguendo il profilo del trattamento dei dati personali da parte degli organi di giustizia (art. 2-duodecies d.lgs. 196/2003, integrato dal d.lgs. 101/2018 di recepimento del GDPR) da quello relativo alla divulgazione all'esterno, per finalità di informazione e di informatica giuridica, del contenuto dei provvedimenti giurisdizionali (di cui agli artt. 51 e 52 del d.lgs.

¹⁰⁴ P. PERLINGIERI, *La pubblica amministrazione e la tutela della privacy. Gestione e riservatezza dell'informazione nell'attività amministrativa*, in *Ann. fac. econ. Benevento*, 2003, 211 ss.; ID., *La persona e i suoi diritti*, Napoli, 2005, 255 ss.; G. FINOCCHIARO, *La memoria della rete e il diritto all'oblio*, in *Dir. inf.*, 2010, 391 ss.; ID., *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. inf.*, 2014, 591 ss.; M. COCUCCIO, *Il diritto all'oblio fra tutela alla riservatezza e diritto all'informazione*, in *Dir. fam. pers.*, 2015, 741; M. RIZZUTI, *Il diritto e l'oblio*, in *Corr. giur.*, 2016, 1077 ss.; Corte giust, 13 maggio 2014, n. 131/12, in *Foro it.*, 2014, IV, c. 295.

¹⁰⁵ A. FRASSINETTI, *Pubblicità dei giudizi e tutela della riservatezza*, in *Riv. dir. civ.*, 2002, 665 ss.; ID., *Codice della privacy e processo civile*, in *Riv. dir. proc.*, 2005, 465 ss.; R. G. ALOISIO, M. CICALA, *Il codice della privacy tutela l'anonimato delle parti nel processo?*, in *Riv. dir. priv.*, 2005, 503 ss.

¹⁰⁶ G. GRASSO, *Il trattamento dei dati di carattere personale e la riproduzione dei provvedimenti giudiziari*, in *Foro it.*, 2018, c. 349; G. RESTA, *Privacy e processo civile: il problema della litigation anonima*, in *Dir. inf.*, 2005, 696 ss. Sulle ragioni della scelta di rendere pubbliche le pronunce, cfr. S. SCAGLIARINI, *La pubblicazione delle sentenze della Cassazione: attentato alla privacy o scelta di trasparenza?*, in *Quad. cost.*, 2015, 184.

196 del 2003, integrate dal d.lgs. 101/2018).

Per quanto attiene al trattamento di dati personali per ragioni di giustizia (art. 2-duodecies), il Codice identifica tali trattamenti in quelli direttamente correlati alla trattazione giudiziaria di affari e di controversie, o che, in materia di trattamento giuridico ed economico del personale di magistratura, hanno una diretta incidenza sulla funzione giurisdizionale, nonché nelle attività ispettive su uffici giudiziari. Restano pertanto esclusi i trattamenti relativi all'ordinaria attività amministrativo-gestionale di personale e mezzi, rispetto ai quali trova applicazione la ordinaria disciplina dei trattamenti in ambito pubblico.

Per quel che attiene al regime di riservatezza degli atti trattati in ambito giudiziario, va rammentata la regola generale secondo cui non sussistono le garanzie della privacy per quei dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati (artt. 24 c. 1 lettera c; 38 c. 6; 43 c. 1, lettera f). Peraltro, nella vigenza della precedente normativa, il Garante aveva affermato che il calendario dei processi, le udienze e le sentenze sono pubblici e conoscibili da chiunque vi abbia interesse, secondo le modalità regolate dal codice di rito e dalle altre norme processuali. Così aveva ritenuto lecita la diffusione della notizia della richiesta di rinvio a giudizio, anche quando l'imputato sia indicato nominativamente, in quanto la diffusione di tale tipo di notizia non risultava vietata da norme specifiche.

Maggiori restrizioni sono previste dal Codice nel caso del trattamento, fuori dall'ambito sopra descritto, dei dati giudiziari, definiti dall'art. 4 come i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

Il Codice considera legittimo il trattamento di tali dati da parte di soggetti pubblici o privati solo se autorizzato da espressa disposizione di legge o da provvedimento del Garante che specifichino le finalità di rilevante interesse pubblico del trattamento, i tipi di dati trattati e di operazioni eseguibili (artt. 21 e 27)¹⁰⁷.

¹⁰⁷ Cfr. Cass., 25 maggio 2017, n. 13151, in *Foro amm.*, 2017, 1515.

Nel caso di soggetti pubblici, è rafforzato il principio di proporzionalità nel trattamento di queste informazioni, ritenendosi legittimo il trattamento dei soli dati giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa (art. 22).

Tra le autorizzazioni di ordine generale rilasciate dal Garante per il trattamento di dati giudiziari da parte di soggetti pubblici o privati vi è quella relativa alla documentazione giuridica, secondo cui è autorizzato il trattamento, ivi compresa la diffusione, di dati per finalità di documentazione, di studio e di ricerca in campo giuridico, in particolare per quanto riguarda la raccolta e la diffusione di dati relativi a pronunce giurisprudenziali, se pur con la prescrizione di tipo generale che possono essere trattati i soli dati essenziali per le finalità per le quali è ammesso il trattamento e che non possano essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa. A differenza degli altri trattamenti, i dati da utilizzare per la documentazione giuridica, come rimarca l'autorizzazione suddetta, non devono essere forniti dagli interessati, nel rispetto della disciplina prevista dal D.P.R. 14 novembre 2002, n. 313. In ogni caso, l'autorizzazione richiama gli artt. 51 e 52 del Codice, che dettano una particolare disciplina per la diffusione dei dati giudiziari in via informatica.

Più precisamente, l'art. 51 del Codice in materia di protezione dei dati personali, disciplina la diffusione dei provvedimenti giudiziari, prevedendo la piena accessibilità degli stessi da parte di chi vi abbia interesse anche mediante reti di comunicazione elettronica (ad esempio, Italgireweb), ivi compreso il sito istituzionale, precisando che le sentenze e le altre decisioni dell'autorità giudiziaria di ogni ordine e grado depositate in cancelleria o segreteria, sono rese accessibili anche attraverso il sistema informativo e il sito istituzionale, osservando opportune cautele. Queste ultime sono disciplinate dal successivo art. 52¹⁰⁸, che individua i limiti alla diffusione del contenuto, integrale o parziale, delle sentenze e degli altri provvedimenti giurisdizionali. Tali limiti si applicano sia alle ipotesi di divulgazione per finalità di informazione giuridica su riviste scientifiche o su supporti elettronici, sia ad ogni altra ipotesi di riproduzione di pronunce giudiziarie, come nel caso della diffusione di notizie

¹⁰⁸ R. DE NICTOLIS, V. POLI, *Il diritto all'anonimato nel processo (art. 52 d. lgs. 30 giugno 2003, n. 196)*, in *Giust. civ.*, 2003, 495 ss.

su organi di stampa. L'art. 52 c. 1 d.lgs. 196/2003 autorizza l'interessato a chiedere l'annotazione volta a precludere, in caso di riproduzione della sentenza o provvedimento in qualsiasi forma, per finalità di informazione giuridica su riviste, supporti elettronici o mediante reti di comunicazione elettronica, l'indicazione delle generalità e di altri dati identificativi del medesimo interessato riportati sulla sentenza o provvedimento. In altri termini, la norma disciplina le modalità operative attraverso le quali avviene l'anonimizzazione¹⁰⁹ dei dati identificativi degli interessati nei provvedimenti giudiziari. In particolare, nel definire i casi nei quali è garantito il diritto all'anonimato delle parti in giudizio o dei soggetti interessati, distingue due ipotesi. In primo luogo, individua espressamente specifiche ipotesi nelle quali il bilanciamento tra gli opposti interessi (esigenze di riservatezza e pubblicità degli atti giudiziari) è compiuto a monte dal legislatore in considerazione della delicatezza di determinate categorie di dati (art. 52 c. 5 e art. 9 GDPR): l'oscuramento obbligatorio e d'ufficio riguarda le generalità e gli altri dati identificativi, ovvero altri dati anche relativi a terzi dai quali possa desumersi direttamente o indirettamente l'identità di minori o delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone¹¹⁰. In secondo luogo, la medesima disposizione prevede il giudizio di bilanciamento a valle della verifica della sussistenza di motivi legittimi¹¹¹ a fondamento della richiesta di

¹⁰⁹ Corte giust., 14 marzo 2017, c-188/15, in *Foro it.*, 2015, c. 239; Corte giust., 22 dicembre 2010, c-497/10, in *Riv. dir. internaz. priv.*, 2011, 812 ss.

¹¹⁰ G. ELLI, R. ZALLONE, *Il nuovo Codice della privacy*, Torino, 2004, 73 ss.

¹¹¹ Cass., 15 febbraio 2017, n. 11959, in *Giust. civ. Mass.*, 2010, 757, secondo la quale la corretta interpretazione dell'espressione motivi legittimi deve essere intesa come sinonimo di motivi opportuni, la cui valutazione impone un equilibrato bilanciamento tra esigenze di riservatezza del singolo e di pubblicità della sentenza. A guidare il suddetto bilanciamento, peraltro, vengono in rilievo le linee guida del Garante della privacy, pubblicate il 2 dicembre 2010, le quali pongono una duplice tipologia dei motivi legittimi: l'una relativa alla particolare natura dei dati contenuti nel provvedimento; l'altra alla delicatezza della vicenda oggetto del giudizio. Invero, mentre per la nozione di particolare natura dei dati non sono sorti dubbi, risultando pacifico il riferimento ai dati sensibili (espressamente indicati dalla normativa speciale), per il concetto di delicatezza della vicenda è stata necessaria un'ulteriore specificazione da parte della Suprema Corte, laddove ha precisato che «l'estrema latitudine del sostantivo abbia necessità di essere riempita di contenuti concreti, sintomatici della peculiarità del caso e della capacità, insita nella diffusione dei relativi dati, di riverberare [...] negative conseguenze su vari aspetti di vita sociale e di relazione dell'interessato [...], così andando ad incidere pesantemente sul diritto alla riservatezza del singolo». Cfr. anche Cass., 10 agosto 2021, n. 22561, in *Nuova giur. civ. comm.*, 2022, 32, secondo cui l'art. 52 non specifica, peraltro, neppure esemplificativamente, quali sono i motivi legittimi: essa si traduce dunque in una clausola generale, in un concetto giuridico a contenuto indeterminato. Tale tecnica normativa difetta di una puntuale tipizzazione ma è sovente utilizzata dal legislatore. Per cui, in presenza della stessa, per la sussunzione del fatto concreto nell'ipotesi normativa è necessaria un'integrazione che il Legislatore stesso ha affidato al potere ricostruttivo dell'interprete con l'utilizzo di parametri che, in conformità ai principi fondamentali dell'ordinamento, vanno completati e specificati con gli elementi e i criteri fattuali della singola

oscuramento dei dati identificativi delle parti¹¹², onde consentire al giudice il vaglio sulla meritevolezza delle ragioni per le quali la decisione dovrebbe derogare al principio di pubblicità degli atti.

Del resto, lo stesso art. 52 c. 7 d.lgs. 196/2003 prevede che al di fuori degli indicati casi, è ammessa la diffusione in ogni forma del contenuto anche integrale di sentenze e di altri provvedimenti giurisdizionali.

Qualora sia diffusa una pronuncia sottoposta in via obbligatoria all'oscuramento (giacché sussumibile nell'ambito applicativo dell'art. 9 del Regolamento (UE) 2016/679; dell'art. 10 del Regolamento 2016/679, letto in combinato con l'art. 2-octies, comma 3, lett. e del Codice della privacy; dell'art. 52, comma 5, del medesimo codice, dell'art. 734-bis del cod. pen.) o in relazione alla quale il giudice non abbia provveduto sulla richiesta di anonimizzazione, le parti o i terzi interessati possono attivare alcuni possibili rimedi a loro tutela, in disparte delle iniziative di public enforcement.

Fra essi, in primo luogo, potrebbe ricorrere la richiesta all'amministrazione, e segnatamente al responsabile del sito istituzionale, di interrompere la divulgazione di dati sensibili attraverso la pubblicazione in rete, nonostante il divieto posto direttamente dalla legge alla diffusione dei dati in determinate ipotesi. Il che pone il dubbio se l'amministrazione sia titolare di poteri autonomi rispetto al provvedimento di anonimizzazione del giudice destinati a operare a prescindere dal dato processuale.

Il secondo rimedio di carattere giurisdizionale, si sostanzia in un'istanza rivolta al giudice e in quanto tale destinata ex post a sollecitare a disporre l'oscuramento supposto come obbligatorio o a ottenere una pronuncia sulla richiesta previamente depositata e non ancora deliberata. In ogni caso, resta sempre percorribile dalla parte interessata la tutela risarcitoria azionabile innanzi all'autorità giudiziaria ordinaria avverso il plesso burocratico, costituendo fatto illecito la diffusione, anche a meri scopi di informazione giuridica, di

fattispecie. Tale ricostruzione è quindi volta a declinare il concetto giuridico indeterminato non in sé e per sé ma di volta in volta sullo specifico caso in esame, prendendo a riferimento i parametri oggettivi e soggettivi caratterizzanti la singola fattispecie concreta. E ciò al fine di valutare, in concreto, se è stato salvaguardato il fine considerato dalla norma.

¹¹² A. MAIETTA, *I trattamenti in ambito giudiziario, da parte delle forze di polizia e per la difesa e la sicurezza dello Stato*, in F. CARDARELLI, S. SICA, V. ZENO ZENCOVICH (a cura di), *Il codice dei dati personali*, Milano, 2004, pp. 188-189; I. FAGANELLO, *Il diritto alla protezione dei dati personali*, Rimini, 2004, 394; P. PERRI, *Privacy, diritto e sicurezza informatica*, Milano, 2007, 195 ss.

pronunce giurisdizionali in via integrale, comprensiva cioè di dati che, in via obbligatoria per legge o per annotazione del giudice, devono rimanere oscurati¹¹³.

5. Conclusioni

Ad oggi, i software in uso presso gli uffici giudiziari, seppure si siano maggiormente evoluti, non sono ancora in grado di prendere autonomamente decisioni che siano coscienti e morali, in quanto non godono della qualità etica della consapevolezza¹¹⁴. Sul tema è intervenuta, il 4 dicembre 2018, la Commissione Europea per l'efficacia della giustizia

¹¹³ Cass., 20 maggio 2016, n. 10510, in *Rass. dir. farm.*, 2016, 529: «richiamava il giudice a quo l'art. 52 D. Lgs. n. 196 che disciplina i modi di diffusione delle sentenze o dei provvedimenti giurisdizionali, per finalità di informativa giuridica, precisando che l'interessato può esplicitamente chiedere, per motivi legittimi, con domanda depositata nella cancelleria, prima che sia definito il grado di giudizio, che, in caso di riproduzione del provvedimento in qualsiasi forma, per finalità di informazione giuridica, sia esclusa l'indicazione delle generalità e di altri dati identificativi del soggetto interessato, riportati nel provvedimento stesso; più specificamente, nel settore civile, vanno omessi, anche in mancanza di richiesta, le generalità, nonché altri dati identificativi, anche relativi a terzi, dai quali possa desumersi l'identità di minori oppure delle parti nei procedimenti in materia di rapporti di famiglia e di stato delle persone. Va peraltro osservato che l'art. 22 Codice Privacy afferma il principio generale per cui i dati sensibilissimi, e specificamente quelli idonei a rivelare lo stato di salute, non possono essere diffusi. Tale indicazione, che non pare ammettere eccezioni, supera il punto di equilibrio indicato dall'art. 52, con riferimento ai provvedimenti giurisdizionali, tra gli interessi della persona alla privacy, di sicura rilevanza costituzionale, e quelli, altrettanto rilevanti, all'integrale pubblicazione dei provvedimenti giurisdizionali, a scopo di informativa giuridica.

Del resto, ad colorandum, anche se successiva alla fattispecie dedotta, può ricordarsi l'Autorizzazione n. 7/2008 al trattamento dei dati a carattere giudiziario, anche da parte di soggetti pubblici, del Garante della privacy, ove si evidenzia la necessità di favorire l'attività di documentazione, studio e ricerca in campo giuridico ma pure, quella di ridurre al minimo i rischi che i trattamenti potrebbero comportare per i diritti e le libertà fondamentali nonché per la dignità della persona; ne consegue che devono essere trattati i soli dati essenziali ai fini della informativa giuridica, e che il trattamento va effettuato unicamente con operazioni, con logiche e mediante forme di organizzazione di dati strettamente indispensabili, in rapporto ai predetti obblighi informativi. Ancor più recentemente la Deliberazione del Garante della Privacy del 2 dicembre 2010 circa le "Linee guida sul trattamento dei dati personali nella riproduzione di provvedimenti giurisdizionali, per finalità di informazione giuridica" precisa che, relativamente ai dati idonei a rivelare lo stato di salute, esiste uno specifico divieto di diffusione anche per i soggetti pubblici, e chiarisce che la salvaguardia dei diritti degli interessati attraverso un oscuramento delle loro generalità, non pregiudica la finalità di informazione giuridica, ma può risultare necessaria nella prospettiva di un bilanciamento dei diversi interessi per tutelare la sfera di riservatezza dei soggetti coinvolti. Appare pertanto illecita la diffusione delle generalità del ricorrente, con riferimento ad un provvedimento giurisdizionale, ove si indicava il suo stato di salute e le sue invalidità. Il ricorrente chiede la condanna del titolare del trattamento dei dati al risarcimento del danno, ma non è in grado di indicare specificamente chi egli sia (si limita ad affermare che non sarebbe il giudice) né di individuare la consistenza del danno occorso che, come afferma la giurisprudenza consolidata di questa Corte (tra le altre, Cass. n. 222 del 2016), anche in materia di diritti fondamentali, non può configurarsi in re ipsa: il richiedente deve fornire prova di tutti i presupposti di cui all'art. 2043 c.c., non solo il comportamento illegittimo, ma pure il danno occorso e il nesso di causalità tra comportamento ed evento dannoso».

¹¹⁴ J. NIEVA-FENOLL, *Intelligenza artificiale e processo*, Torino, 2019, 21.

(CEPEJ) del Consiglio d'Europa che ha emanato la Carta etica europea per l'uso dell'intelligenza artificiale nei sistemi di giustizia e nei relativi ambienti. Per la prima volta a livello europeo si è preso atto della crescente importanza dell'intelligenza artificiale e dei benefici attesi quando sarà pienamente utilizzata al servizio della efficienza e qualità della giustizia, individuando alcune linee guida fondamentali.

In particolare, la Carta etica, nel tentativo di bilanciare l'interesse di un progresso dell'efficienza del sistema giudiziario e la tutela dei diritti fondamentali, enuncia i seguenti principi: 1) rispetto diritti fondamentali; 2) non discriminazione; 3) qualità e sicurezza; 4) trasparenza; 5) garanzia dell'intervento umano. Questo principio è particolarmente rilevante in ambito giudiziario, ove il giudice deve mantenere il potere di verificare l'output intelligente rispetto al caso specifico, per garantire l'effettiva applicazione del diritto al caso specifico. Ogni utente deve essere informato sulla natura della soluzione proposta tramite intelligenza artificiale, le possibili opzioni ed il diritto al contraddittorio.

La Carta etica è indirizzata sia alle start up che progettano piattaforme di nuovi servizi, sia agli sviluppatori di tools, sia alle autorità a cui spetta la decisione di regolare questo campo, nonché ai professionisti del settore giuridico (magistrati, avvocati, notai).

L'idea di fondo è che l'intelligenza artificiale utilizzata come strumento di ausilio del giudice, possa in determinate circostanze favorire la prevedibilità nell'applicazione della legge e l'uniformità degli orientamenti giurisprudenziali¹¹⁵.

Sotto questo profilo, ad esempio, si può pensare a forme di certificazione volte ad attestare la conformità di un sistema di intelligenza artificiale rispetto a determinati requisiti, volti a garantire il rispetto dei diritti fondamentali, anche nel settore giustizia¹¹⁶.

La circostanza che tali sistemi possano agire come una sorta di black box¹¹⁷ non esclude infatti la possibilità di assoggettarli a controlli di tipo controfattuale, volti ad attestare la loro attendibilità. Appare quindi possibile e auspicabile affidare ad apposite autorità pubbliche compiti di certificazione e controllo sul concreto funzionamento dei sistemi di

¹¹⁵ A. CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in A. NUZZO, G. OLIVIERI (a cura di), *Algoritmi*, Roma, 2019, 47 ss.

¹¹⁶ J. NIEVA-FENOLL, *Intelligenza artificiale e processo*, cit., 64 ss.

¹¹⁷ E. PELLECCIA, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *Nuove leggi civ. comm.*, 2018, 1224 ss.

intelligenza artificiale, per verificarne l'attendibilità e la legittimità dell'impiego nel settore giustizia¹¹⁸, tenendo in considerazione che la condizione indispensabile è la disponibilità e la sicurezza dei dati personali.

Basti pensare che manca ancora oggi un archivio completo delle sentenze dei giudici di merito accessibile a tutti gli interessati e che sussistono problemi riguardanti la conservazione dei documenti digitali giudiziari. La creazione di una raccolta dei provvedimenti in formato digitale dovrà garantire il rispetto dei principi sanciti dal GDPR, considerando che potrebbe rendersi necessario un intervento volto ad assicurare l'anonimizzazione, la pseudonimizzazione o la cifratura dei dati personali, al fine di tutelare il diritto alla riservatezza ed al controllo sui dati personali, evitando così il rischio di profilazione da parte degli organi giudicanti.

Abstract

Il diritto alla protezione dei dati personali sembra richiedere una attenzione particolare in particolare riferimento agli imprevedibili effetti dell'A.I. Se il GDPR appronta strumenti di difesa indispensabili per la navigazione in rete, d'altro canto il principio del consenso al trattamento pare doversi potenziare a vantaggio di ulteriori tutele. In particolare, nell'ambito del contenzioso giudiziario, significativa appare l'esigenza di riservatezza, da coniugare con le imprescindibili necessità di giustizia.

Abstract

The right to the protection of personal data seems to require special attention, with particular reference to the unpredictable effects of A.I. If the GDPR provides indispensable defence tools for surfing the net, on the other hand, the principle of consent to processing seems to have to be strengthened for the benefit of further protections. In particular, in the context of legal disputes, the need for confidentiality, to be combined with the unavoidable need for justice, appears significant.

Camerino, aprile 2023.

¹¹⁸ F. DONATI, *Intelligenza artificiale e giustizia*, in *Riv. ass. it. cost.*, 2020, 435.