RIVISTA INTERNAZIONALE DI FILOSOFIA ONLINE
CON *PEER REVIEW*
WWW.METABASIS.IT
novembre 2024 anno XIX n° 38

IL COMPLESSO RAPPORTO TRA AUTOMATISMO DIGITALE E PROTEZIONE DEI DATI PERSONALI: IL PRINCIPIO DI NON ESCLUSIVITÀ DELLA DECISIONE AUTOMATIZZATA.

DOI: 10.7413/18281567276

di Giulia Cesaro
Università degli Studi Insubria, Varese e Como

The complex relationship between digital automation and data protection: the principle of non-exclusivity of automated decision-making.

Abstract
Article 22 of the General Data Protection Regulation (GDPR) enshrines the principle of non-exclusivity of automated decision-making. This provision is part of a broader framework aimed at protecting and safeguarding the individual's privacy, which underpins the entire regulatory structure established at the European Union level by the GDPR. The legislative provision seeks to prevent individuals from being harmed in their rights and freedoms using automated decisions: decisions made without any human intervention, relying solely on fully standardized algorithms. The current formulation of the provision raises questions about the practical effectiveness of this principle and the need for a revision that can address the new challenges posed by technological advancements.

Keywords: privacy, personal data, GDPR, digital automation, artificial intelligence.

1. Privacy e protezione dei dati personali

La disamina del rapporto tra automazione digitale e tutela dei dati personali implica la necessità, sul piano dell'inquadramento teorico-sistematico, di alcune considerazioni di carattere generale.

In via preliminare, è opportuno chiarire il significato di termini che, per quanto apparentemente simili, sono, in realtà, profondamente diversi.

In questa prospettiva, occorre distinguere tra privacy e protezione dei dati personali.

I concetti si differenziano anzitutto quanto alla loro origine ed evoluzione storica[1].

1.1 Diritto alla privacy

Il moderno concetto di privacy[2] rinviene le proprie origini negli Stati Uniti d'America di fine Ottocento, con la pubblicazione, nel 1890, del saggio *"The Right to Privacy"*[3] ad opera di due giuristi americani: Samuel Warren e Louis Brandeis.

Lo scritto concepiva la privacy come corollario della riservatezza e, più specificamente, come *"diritto a essere lasciati soli"*[4], sottolineando l'esigenza di protezione della sfera privata dell'individuo dalle intrusioni esterne.

Nel fornire una definizione del diritto alla privacy, gli autori introducono una netta separazione tra privacy materiale, che riguardava proprietà e possesso, e *"inviolate personality"*, entità stessa del diritto bisognoso di tutela[5].

Nei primi passaggi del testo, i due avvocati indicano immediatamente il loro obiettivo: oggetto della loro analisi non sarà né il diritto alla proprietà privata, né il diritto alla vita ed all'integrità fisica[6], entrambi già ampiamente tutelati in un ordinamento di *common law* quale è quello giuridico statunitense.

---

[1] Storicamente, è possibile rinvenire una forma embrionale di riservatezza, che accomuna i concetti di privacy e di protezione dei dati personali, nella classica distinzione che Aristotele fa tra la sfera pubblica, connessa all'attività politica e corrispondente al termine greco *polis*, e la sfera privata, la *oikos*, associata alla famiglia ed alla vita domestica. Sul punto, si veda Aristotele, *La Politica*, Le Monnier, Firenze, 1981.

[2] Per una compiuta trattazione del concetto di "privacy", si veda S. Rodotà, in P. Conti (a cura di), *Intervista su privacy e libertà*, Laterza, Roma-Bari 2005.

[3] Per approfondimenti, si rinvia a S. Warren – L. Brandeis, *The Right to Privacy*, in «Harvard Law Review», 5/1990, pp. 193-220.

[4] *"The right to be let alone":* il diritto a essere lasciati soli, a godere del proprio privato.

[5] N. Lugaresi, *Internet, Privacy e Pubblici Poteri negli Stati Uniti*, Giuffrè Editore, Milano 2000, p. 47.

[6] Il saggio si apre, infatti, con una considerazione di carattere generale: *"that the individual shall have full protection in person and in property is a principle as old as the common law*": il fatto che l'individuo debba avere una protezione completa nella persona e nella proprietà è un principio antico quanto il diritto comune. S. Warren – L. Brandeis, cit., p. 193.

Gli autori intendono soffermarsi, invece, sulle conseguenze dell'evoluzione sociale e giuridica di questi due diritti, secondo un percorso che ha portato al riconoscimento di ciò che è considerato un patrimonio più intimo dell'individuo: l'essenza stessa della persona, lesa nei propri sentimenti più privati.

Warren e Brandeis, colpiti dall'intrusione nella vita delle persone[7], trasformano il concetto di riservatezza, già in parte interiorizzato dall'ordinamento, in uno standard morale, e gli conferiscono un profilo etico.

Essi inquadrano, poi, la privacy come categoria indipendente, che scaturisce dalla necessità di proteggere la natura più intima degli uomini, cioè quello spazio di autonomia, di sfera chiusa, che va preservato dall'intrusione altrui, che siano terzi o lo Stato.

Il diritto alla privacy, frutto dell'esperienza americana di fine XIX secolo, approda successivamente in Europa. Nel Vecchio Continente, l'istituto si sviluppa in un contesto successivo alla Seconda guerra mondiale e segnato dall'avvento dei regimi totalitari, che utilizzavano forme di sorveglianza e di raccolta di dati per controllare e reprimere ogni forma di dissenso politico[8].

Nell'esperienza europea, quindi, la privacy ha una genesi del tutto diversa, ricollegata alla dicotomia hobbesiana potere *versus* libertà[9] e derivante dall'esigenza di tutelare i cittadini dal controllo illimitato dell'Autorità pubblica.

---

[7] L'ispirazione del saggio deriva, infatti, dalla vita professionale e personale degli autori. I due giovani avvocati di Boston erano in procinto di intentare una causa contro un noto giornale locale che aveva fatto trapelare indiscrezioni sulla vita matrimoniale della moglie di uno di loro. In questa prospettiva, le minacce che mettono in pericolo il *"right to be let alone"* riguardano principalmente l'invasione della sfera della riservatezza dell'individuo da parte di quelle che, all'epoca, erano innovazioni tecnologiche e mediatiche. Tali nuovi strumenti di comunicazione e informazione finiscono per abbattere le barriere che separano la sfera privata da quella pubblica, con il rischio di esporre dettagli intimi e personali della vita individuale.

[8] Cfr. P. Bellini, *Osservazione, Sorveglianza e Controllo,* in *www.metabasis.it*, n. 34/2022; sul punto si veda anche: Id, *Cyberfilosofia del potere. Immaginari, Ideologie e conflitti della civiltà tecnologica*, Mimesis, Milano-Udine 2007.

[9] Per una più compiuta disamina del rapporto autorità-libertà, si rinvia a C. Schmitt, *The Leviathan in the State Theory of Thomas Hobbes: Meaning and Failure of a Political Symbol,* trans. by G. Schwab and E. Hilfstein, Greenwood, Westport-London 1996.

1.2 Il diverso diritto alla protezione dei dati personali e l'importanza dei dati personali nell'era del digitale

Il concetto di "dati personali" è successivo a quello di "privacy", essendo frutto dell'evoluzione tecnologica avutasi nel corso del tempo.

Con il progresso del digitale e l'avvento di software di gestione ed organizzazione dati, la necessità di proteggere le informazioni personali è diventata sempre più urgente e complessa.

In questo contesto di digitalizzazione, il concetto di riservatezza ha assunto una nuova e diversa dimensione, costituendo oggetto non più di un diritto difensivo, fondato sull'esclusione degli altri dalla sfera individuale, ma di un diritto attivo, che attribuisce al singolo il potere di controllare e proteggere informazioni strettamente personali.

Pertanto, mentre il diritto alla privacy è da intendersi in senso passivo (escludere gli altri), il diritto alla protezione dei dati personali si inserisce in un contesto attivo (controllo sull'uso e sulla gestione dei propri dati).

Sul piano concettuale, tra i due diritti sussiste un rapporto di *genus ad speciem*, rientrando i dati personali nel più ampio concetto di "privacy" e, dunque, di "riservatezza".

La privacy in senso stretto è oggetto di un diritto più ampio, che tutela il singolo nella sua individualità (diritto al rispetto della propria sfera personale); il diritto alla protezione dei dati personali si colloca, invece, in una dimensione settoriale e, più specificamente, meta-individuale. Esso consente la tutela della persona oltre la sfera privata, e, in particolare, nell'area delle relazioni sociali (diritto alla tutela della propria individualità nell'ambito della collettività).

In un mondo sempre più interconnesso e digitalizzato, per relazioni sociali si intendono, anche e soprattutto, interazioni digitali.

La rivoluzione tecnologica avutasi con la diffusione di internet e della tecnologia distribuita ha senz'altro rafforzato l'esigenza di protezione della riservatezza, stanti i rischi – derivanti, soprattutto, dall'impiego delle banche dati – di raccogliere e distribuire informazioni personali anche senza il pieno consenso o la totale consapevolezza degli individui.

Il successivo progresso scientifico ha, poi, complicato ulteriormente la protezione dei dati personali, rendendo necessaria una tutela più elevata.

L'avvento dell'intelligenza artificiale ha, infatti, innescato una vera e propria rivoluzione tecnologica nella storia dell'umanità, caratterizzata da un crescente utilizzo di algoritmi in una varietà sempre più

ampia di settori. Tra i vari: la sanità, la finanza ed i servizi bancari[10]; i trasporti e la mobilità; l'educazione; il marketing, la pubblicità, la comunicazione; il versante legale e giuridico[11].

Le interazioni digitali ampliano enormemente le modalità di comunicazione ed interazione; al contempo, però, introducono nuove sfide per la protezione della privacy e dei dati personali.

Dati ed informazioni personali sono, infatti, condivisi, raccolti e spesso memorizzati su piattaforme digitalizzate e lontane dal controllo diretto dell'individuo.

In un contesto ormai quasi completamente automatizzato, il diritto alla protezione dei dati personali assurge a meccanismo di garanzia, consentendo agli individui di esercitare un controllo sul rispetto della propria identità digitale e di preservare, in tal modo, l'autodeterminazione decisionale.

2. La protezione dei dati personali nella legislazione europea: il GDPR

A livello comunitario, il diritto alla protezione dei dati personale rinviene una compiuta regolamentazione all'interno del Regolamento 2016/679, meglio noto come GDPR *(General Data Protection Regulation)*[12].

Il Regolamento ha sostituito le precedenti normative[13], rafforzando il concetto di protezione dei dati personali come diritto fondamentale dell'individuo e, quindi, come diritto inviolabile e centrale nello sviluppo dell'economia digitale. Al centro della nuova disciplina vi è l'effettiva protezione dei dati personali, non solo attraverso l'adempimento formale degli obblighi gravanti sui vari soggetti coinvolti, ma con un approccio basato anche sulla consapevolezza e sulla conseguente responsabilità

---

[10] Si consideri, ad esempio, il fenomeno del *credit scoring*, meglio analizzato al par. 5.

[11] L'impatto delle nuove tecnologie e delle cyber-innovazioni nel campo del diritto è significativo: si pensi, a titolo esemplificativo, alla digitalizzazione dei processi e all'introduzione del Processo Civile Telematico (PCT) , realizzata con la riforma Cartabia (provvedimento Direzione Generale per i Sistemi Informativi Automatizzati del 2 agosto 2024); alla nascita di nuove forme di contenzioso, derivate dall'impiego di tecnologie innovative (la *blockchain*); ancora, e soprattutto, all'automazione delle decisioni, cioè all'impiego, nei processi decisionali (sia pubblici che privati), di decisioni completamente automatizzate. Per un'analisi più approfondita dell'automatismo digitale e dei rischi connessi all'impiego dello stesso, si rimanda al par. 5.

[12] Il Regolamento Generale sulla Protezione dei Dati, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, è stato approvato con Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 ed è applicabile a decorrere dal 25 maggio 2018.

Il testo integrale è disponibile al seguente link: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=it.

[13] Il riferimento va, in particolare, alla direttiva 95/46/CE (recepita dai Paesi membri, tra cui l'Italia, con la legge n. 675 del 1996).

degli stessi. Nel contesto della protezione dei dati personali, il Regolamento fornisce un quadro dettagliato su come devono essere gestite le informazioni personali di una persona fisica.

In questa prospettiva, la normativa specifica anzitutto quali sono le operazioni che costituiscono il trattamento dei dati personali e l'identità dei principali soggetti coinvolti nell'ambito delle stesse.

Sul primo versante, il termine "trattamento", come definito dal GDPR, copre una gamma estremamente ampia di attività che possono essere eseguite su dati personali.

Queste operazioni includono, tra le altre, la raccolta, l'organizzazione, la conservazione, la modifica, la cancellazione e anche la distruzione dei dati[14].

Il concetto di trattamento include, pertanto, qualsiasi azione eseguita sui dati di una persona, anche se apparentemente banale, come il semplice accesso ad un database o la cancellazione di un file; ciò testimonia l'ampiezza della tutela fornita dal GDPR.

Altrettanto vasta è la nozione di "dato personale", definito come *"qualsiasi informazione riguardante una persona fisica identificata o identificabile"*[15].

La portata del concetto di dato personale implica che anche dettagli che, di per sé, non sembrano identificare direttamente una persona (come un indirizzo IP), possono essere considerate dati personali se, combinate con altre informazioni, portano all'identificazione della persona fisica.

Sul piano soggettivo, il GDPR identifica i principali soggetti che partecipano al trattamento dei dati personali. Ogni attore ha un ruolo e una responsabilità specifici nel gestire le informazioni, garantendo il rispetto della normativa.

In questa prospettiva, si distingue tra titolare del trattamento, responsabile del trattamento ed interessato.

---

[14] L'articolo 4, comma 2, del Regolamento reca la definizione di "trattamento", intendendo per esso*: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione"*.

[15] Cfr. articolo 4, comma 1, del Regolamento. La persona fisica alla quale si riferiscono i dati personali – l'interessato – è considerata identificabile quando può essere riconosciuta direttamente o indirettamente attraverso una serie di indicatori. Questi includono: nome; numero di identificazione; dati relativi all'ubicazione; identificativi online (come indirizzi IP o *cookies*); caratteristiche fisiche, genetiche, fisiologiche, psichiche, economiche, culturali o sociali.

Il titolare è il soggetto[16] che determina le finalità e i mezzi del trattamento di dati personali; egli ha il potere di decidere perché e come i dati personali devono essere trattati, stabilendo gli scopi per cui le informazioni vengono raccolte e le modalità con cui esse saranno utilizzate.

Il responsabile è, invece, il soggetto[17] che agisce per conto del titolare; costui ha il compito di eseguire le operazioni sui dati attenendosi scrupolosamente alle indicazioni fornite dal titolare.

L'interessato è la persona fisica alla quale si riferiscono i dati personali oggetto di trattamento[18]. Costui rappresenta il fulcro della protezione offerta dal GDPR. In questa prospettiva, la normativa riconosce agli interessati diritti ben precisi, come il diritto di accesso ai propri dati, la possibilità di richiederne la rettifica o la cancellazione, il diritto di opporsi a determinati trattamenti, il diritto a non essere sottoposto a decisioni completamente automatizzate[19].

Il trattamento dei dati personali, così come regolato dal GDPR, implica una serie complessa di operazioni e coinvolge più soggetti, ciascuno con ruoli ben definiti. Il titolare e il responsabile del trattamento operano insieme per garantire che i dati vengano gestiti in modo conforme alle normative; l'interessato gode, invece, di una protezione rafforzata, stante il rischio di abuso delle proprie informazioni personali.

Il GDPR rappresenta, quindi, un sistema normativo robusto, volto a garantire un equilibrio tra l'uso legittimo dei dati personali e la protezione dei diritti fondamentali degli individui, definendo con chiarezza ogni operazione e attore coinvolto nel processo di trattamento.

---

[16] L'articolo 4, comma 7, del Regolamento, recante la definizione di "titolare del trattamento", specifica che costui può essere una persona fisica o giuridica, un'autorità pubblica o qualsiasi altro ente.

[17] Anche in tal caso, come specificato dal Regolamento, può trattarsi di una persona fisica o giuridica, un'autorità pubblica o un altro ente (articolo 4, comma 8, GDPR).

[18] Cfr. articolo 4, comma 1, del Regolamento che, nel precisare cosa si intende per "dato personale", fa riferimento all'"interessato".

[19] L'articolo 22 del Regolamento, rubricato *"Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione"*, sancisce *"il diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona"*. Sul punto, amplius, par. 5.

3. I principi cardine in materia di protezione dei dati personali: liceità, minimizzazione dei dati e *accountability*

Il trattamento dei dati personali diventa illecito quando il titolare del trattamento non rispetta le disposizioni stabilite dal GDPR.

Ciò accade, ad esempio, quando il trattamento è eseguito in violazione dei principi generali stabiliti dal Regolamento. Questi principi, delineati principalmente al Capo II e, specificamente, all'articolo 5 del GDPR, costituiscono le fondamenta del sistema di protezione dei dati personali in Europa.

Essi rivestono un ruolo essenziale nell'ambito dell'interpretazione del Regolamento, permettendo di valutare, caso per caso, la legittimità delle attività di trattamento.

Principio cardine è, anzitutto, il principio di liceità, enunciato all'articolo 5, comma 1, del Regolamento, e meglio esplicitato al successivo articolo 6.

L'articolo 5[20] sancisce, genericamente, la liceità, la correttezza e la trasparenza dei dati personali; l'articolo 6 stabilisce, invece, le condizioni in sussistenza delle quali il trattamento è considerato lecito. Tali condizioni[21], note come "basi giuridiche del trattamento", costituiscono la base per l'utilizzo delle informazioni personali.

Il medesimo articolo 5, comma 1, del Regolamento detta, poi, il principio della minimizzazione dei dati[22], in ossequio al quale i dati personali trattati devono essere «adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati».

Ciò impone ai soggetti titolari e responsabili del trattamento di trattare solo i dati strettamente necessari, evitando l'accumulo indiscriminato tipico dei Big Data[23].

---

[20] Articolo 5, comma 1, lettera a), GDPR: "*I dati personali sono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato*".

[21] Ai sensi dell'articolo 6 del Regolamento, condizioni di liceità del trattamento sono ad esempio: il consenso dell'interessato; l'esecuzione di un contratto; il rispetto di obblighi di legge; la tutela degli interessi vitali dell'interessato o di un'altra persona; l'esecuzione di un compito di interesse pubblico; il perseguimento di legittimi interessi del titolare o di terzi.

[22] Articolo 5, comma 1, lettera c), GDPR: *"I dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati"*.

[23] I Big Data si riferiscono, in particolare, a grandi quantità di dati caratterizzati da velocità, varietà e volume. In quanto tali, essi richiedono strumenti avanzati di analisi per estrarre informazioni utili. Questi dati provengono da diverse fonti, come social media, dispositivi mobili, sensori e transazioni online, e sono utilizzati per scopi commerciali, di ricerca e per migliorare i servizi offerti all'utenza.

Altro principio fondamentale sancito dal GDPR è il principio di *accountability*[24] (cd. responsabilizzazione), di cui all'articolo 5, comma 2.

Tale principio si sostanzia in un duplice obbligo sancito in capo al titolare del trattamento: obbligo di adottare le misure volte alla tutela dei dati personali e di comprovare la conformità delle stesse al Regolamento. Il titolare del trattamento deve, quindi, autoresponsabilizzarsi effettuando una corretta analisi dei rischi connessi al trattamento dei dati, in modo da adottare le misure di sicurezza ritenute più adeguate. Fondamentale è che tali misure siano conformi al Regolamento e, cioè, alle condizioni di liceità.

4. Profili di responsabilità

La portata dei principi applicabili al trattamento dei dati personali induce a riflettere sulle implicazioni derivanti dalla loro violazione.

Il trattamento eseguito in violazione[25] delle normative stabilite dal GDPR è illecito, con conseguenze che possono essere di diversa natura: amministrativa, penale, o civile.

Sul piano amministrativo, il titolare che adotta un trattamento illecito andrà incontro all'erogazione di una sanzione pecuniaria, il cui importo sarà determinato in base ai parametri di cui all'articolo 83, commi 4 e 5 del Regolamento. Le sanzioni amministrative variano in base alla gravità delle violazioni: per violazioni meno gravi, come la mancata notifica di una violazione dei dati *(data breach)* o la mancata adozione di misure di sicurezza adeguate, l'importo può arrivare fino a 10.000.000 di euro, o al 2% del fatturato annuo mondiale, se superiore; per violazioni più gravi, come quelle relative ai principi fondamentali, la sanzione può arrivare fino a 20.000.000 euro, o al 4% del fatturato annuo mondiale[26].

---

[24] Articolo 5, comma 2, GDPR: *"il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo"*. Per approfondimenti sul principio di *accountability*, si rimanda a G. Comandè, *Intelligenza artificiale e responsabilità tra liability e accountability. Il carattere trasformativo dell'IA e il problema della responsabilità,* in «Analisi giuridica dell'economia», n. 1/2019, pp. 169-188.

[25] Si consideri, ad esempio, l'ipotesi in cui il titolare non richieda il consenso dell'interessato per inviare comunicazioni commerciali. O, ancora, il caso in cui vi sia un accesso non autorizzato da parte di soggetti terzi, diversi dal titolare e dal responsabile del trattamento *(hacker)*.

[26] Cfr. articolo 83 del Regolamento, recante le *"Condizioni generali per infliggere sanzioni amministrative pecuniarie"*.

Sul versante penale, si sottolinea che il GDPR non prevede direttamente sanzioni penali, lasciando agli Stati membri la facoltà di introdurre disposizioni interne per le violazioni della normativa sulla protezione dei dati personali. In Italia, la responsabilità penale è disciplinata dal Codice in materia di protezione dei dati personali[27], recante una serie di reati legati al trattamento illecito dei dati personali. Tra le principali fattispecie penali, figura, ad esempio, la comunicazione o diffusione di dati illeciti su larga scala, punibile con la reclusione fino a sei anni; ancora, la falsità nelle dichiarazioni al Garante o l'inosservanza dei provvedimenti dell'Autorità Garante, punite con pene detentive che presentano un massimo edittale di tre anni[28].

Oltre alle responsabilità amministrative e penali, il titolare del trattamento può essere chiamato a rispondere civilmente per il danno causato all'interessato a seguito di una violazione dei dati personali. Riferimento normativo in materia è il considerando 83 del GDPR.
La norma, in attuazione del principio di *accountability* di cui all'articolo 5, comma 2, prevede che, per mantenere la sicurezza e prevenire trattamenti in violazione al Regolamento, il titolare del trattamento dei dati personali deve valutare i rischi inerenti al trattamento e adottare le misure, tecniche ed organizzative, volte a limitare tali rischi[29].
In ambito giurisprudenziale, sono stati offerti diversi spunti di riflessione sull'interpretazione del disposto normativo. La recente giurisprudenza, sia comunitaria[30], sia nazionale[31], ha qualificato la responsabilità civile del titolare del trattamento come responsabilità aggravata per colpa presunta[32].

---

[27] Per "Codice in materia di protezione dei dati personali", anche noto come "Codice della privacy", si intende il Decreto legislativo n. 196 del 2003, così come modificato, in ultimo, dal Decreto legislativo n. 101 del 2018.

[28] Cfr. articolo 160 del Codice della privacy.

[29] Cfr. considerando 83 del GDPR.

[30] Corte di Giustizia dell'Unione Europea (CGUE), Sez. III, 14 dicembre 2023, n. C-340/2. Nel caso di specie, la Corte UE è stata chiamata a definire, in base al Regolamento Generale sulla Protezione dei Dati, le condizioni per il risarcimento del danno morale subito da un soggetto i cui dati personali, a seguito di un attacco *hacker*, erano stati illecitamente pubblicati su internet da un'agenzia pubblica. Per approfondimenti, si rinvia a M. Cocuccio, *Violazione in materia di tutela di dati personali: profili di responsabilità civile*, in «Giurimetrica», n. 1/2023, pp. 1-20.

[31] Il riferimento va, *ex multis*, a Cass. Civ., 23 gennaio 2013, n. 1593.

[32] Per una più compiuta trattazione della responsabilità civile dell'ideatore o del programmatore dell'algoritmo, si rinvia a M. Gambini, *Responsabilità civile e controlli nei trattamenti algoritmici*, in «Rivista di diritto dell'impresa», n. 2/2020, pp. 305-340.

Tale ricostruzione vede operare, a carico del danneggiante (il titolare del trattamento), una presunzione di inadeguatezza delle misure adottate in attuazione del considerando 83 GDPR.
La presunzione è, però, non assoluta, ma relativa: è ammessa, cioè, una prova contraria.
Il danneggiante, quindi, si presume responsabile, a meno che non fornisca prova liberatoria dell'adeguatezza delle misure. In tal caso, egli andrà esente da responsabilità.
Diversamente, sarà responsabile civilmente e, in quanto tale, tenuto al risarcimento del danno nei confronti del danneggiato (l'interessato).
Profili di responsabilità sono, poi, in ogni caso rinvenibili anche in capo al responsabile del trattamento. Egli, operando per conto del titolare è tenuto ad agire nel rispetto delle direttive impartite da quest'ultimo e della normativa in materia di protezione dei dati personali.
Si profila, allora, un duplice regime di responsabilità (del titolare e del responsabile).
Il rapporto tra i due è, infatti, regolamentato da un contratto, in cui sono definiti gli obblighi del responsabile. Se questi obblighi non vengono rispettati, il responsabile può incorrere in una responsabilità contrattuale nei confronti del titolare, oltre a violare il GDPR, il che rappresenta un illecito di natura extracontrattuale.

5. Decisioni automatizzate: quali rischi per l'interessato?

Con l'avvento dell'intelligenza artificiale, il trattamento dei dati personali è diventato sempre più automatizzato. Gli algoritmi e i sistemi intelligenti sono in grado di raccogliere, analizzare ed elaborare grandi quantità di informazioni in modo rapido ed efficiente, riducendo al minimo, se non addirittura eliminando, l'intervento umano. Questo approccio ha portato a significativi miglioramenti in termini di velocità delle decisioni, ma ha anche sollevato preoccupazioni riguardo alla protezione della privacy, alla sicurezza dei dati e, in particolare, alla possibilità di errori o discriminazioni nei processi decisionali automatizzati.
Prima di esaminare i rischi connessi all'impiego di tali sistemi, è fondamentale comprendere che cosa si intenda per "processo decisionale automatizzato" e "profilazione".
"Decisioni automatizzate" sono decisioni basate esclusivamente sull'automatismo digitale; assunte, cioè, mediante l'ausilio di algoritmi standardizzati e senza alcun coinvolgimento umano. Caratteristica peculiare di tali decisioni è, quindi, la totale assenza di un soggetto in grado, attraverso

la propria autorità o competenza, di influenzare i risultati conseguiti (o, quantomeno, di controllarne gli esiti)[33].

Per "profilazione", invece, si intende il processo che comprende la raccolta e l'elaborazione dei dati relativi agli utenti di un servizio, con l'obiettivo di suddividerli in gruppi o categorie in base ai loro comportamenti, preferenze o altre caratteristiche specifiche (segmentazione) [34].

Non necessariamente un processo decisionale automatizzato è basato su profilazione; così come, d'altro canto, la profilazione può non avvenire in base ad un processo decisionale automatizzato; spesso, tuttavia, i due fenomeni coincidono.

Sia nel caso di decisioni automatizzate che di profilazione, l'adozione di processi decisionali basati sull'automatismo digitale comporta, nella pratica, diversi rischi.

Il rischio principale riguarda, in particolare, il fatto che le valutazioni algoritmiche possano insinuarsi nelle vite delle persone, finendo con il prevalere progressivamente su decisioni ragionate e ponderate dell'intelligenza umana. In questa prospettiva, l'intelligenza artificiale tenderebbe quasi a sostituire l'intelligenza umana, agendo a mo' di surroga di quest'ultima.

Questa problematica si presenta in modo diverso, a seconda dell'entità e della complessità del processo decisionale coinvolto.

Nei processi decisionali più semplici[35], riguardanti esclusivamente oggetti, i rischi appaiono piuttosto limitati.

Quando, però, gli algoritmi coinvolgono soggetti e trattano aspetti strettamente connessi alla vita delle persone, emerge la necessità di un controllo molto più rigoroso, stante il rischio di lesione della sfera della riservatezza dell'individuo e, con essa, del principio di liceità del trattamento dei dati personali.

---

[33] Nel novero dell'automatismo digitale rientrano operazioni di diversa natura. Ad esempio, nel settore bancario e finanziario, il rifiuto o l'approvazione automatica di una domanda di credito; ancora, nei processi di selezione del personale, l'impiego di meccanismi che prevedono l'analisi computerizzata dei vari curricula presentati.

[34] La profilazione consente di personalizzare offerte, comunicazioni e servizi in modo più mirato ed efficace. Per tale ragione, essa è utilizzata particolarmente in ambito commerciale, come mezzo che consente la fornitura di servizi personalizzati oppure l'invio di pubblicità comportamentale. Sulla profilazione, cfr. R. Lener, *Tecnologie e attività finanziaria*, in P. Perlingieri – S. Giova – I. Prisco (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto ed economia*, Esi, Napoli, 2020, pp. 197 ss.

[35] Si pensi, ad esempio, all'approvazione di una richiesta di acquisto online. In questo caso, l'algoritmo analizza i dati relativi alla disponibilità del prodotto, al prezzo e alla corretta compilazione dei dati di pagamento per determinare automaticamente se approvare o meno la transazione. Il processo, che riguarda esclusivamente un oggetto (il prodotto) e non coinvolge variabili soggettive, costituisce un valido esempio di decisione automatizzata semplice.

Nella seconda categoria di automatismi, si consideri, ad esempio, il fenomeno del *credit scoring*: un sistema completamente automatizzato, utilizzato dalle banche e dagli istituti finanziari per valutare l'affidabilità creditizia di un individuo o di un'impresa[36].

In tale automatismo, la decisione finale dell'istituto di credito di concedere o meno un finanziamento dipende esclusivamente dal calcolo meccanico del punteggio numerico di capacità creditizia[37].

Molteplici sono i rischi connessi all'impiego di questo meccanismo, e tutti legati all'assenza di un intervento umano.

Si consideri, ad esempio, il caso di un investitore la cui richiesta di credito (mutuo, prestito, finanziamento) venga respinta dall'ente deputato ad erogarla a causa di una valutazione algoritmica successivamente risultata errata.

L'algoritmo di *credit scoring* potrebbe aver commesso un errore che ha influito negativamente sulla decisione finanziaria. Questo errore potrebbe essere stato causato da diversi fattori, come ad esempio la mancanza di precisione nell'elaborazione dei dati, l'uso di un numero inferiore di informazioni rispetto a quelle realmente disponibili, o la selezione incompleta dei dati da analizzare.

Inoltre, l'algoritmo potrebbe aver erroneamente valutato la qualità e la quantità dei dati, riducendoli sinteticamente a un singolo punteggio numerico. Un altro rischio significativo riguarda i bias potenziali presenti nei dati o nei modelli, che potrebbero portare a decisioni ingiuste o discriminatorie, influenzando negativamente determinate persone o gruppi[38].

---

[36] Si tratta, più specificamente, di un punteggio numerico che riflette il rischio di insolvenza di un cliente in relazione alla sua capacità di restituire il capitale investito o di adempiere ad altre obbligazioni finanziarie. Tale punteggio aiuta le banche e le altre istituzioni finanziarie a determinare la solvibilità di un individuo e, quindi, decidere se erogare un finanziamento o una linea di credito e a quali condizioni. Un punteggio più alto indica un rischio minore di insolvenza, mentre un punteggio basso suggerisce un rischio maggiore. Per approfondimenti, si rinvia a L. Ammannati – G. L. Greco, *Piattaforme digitali, algoritmi e big data: il caso del credit scoring,* in «Rivista Trimestrale di Diritto dell'Economia», n. 2/2021, pp. 290 ss.; Id., *Il credit scoring alla prova dell'intelligenza artificiale*, in U. Ruffolo (a cura di), *XXVI Lezioni del diritto dell'intelligenza artificiale*, Giappichelli, Torino, n. 2/2021, pp. 379 ss.

[37] Cfr. G. Biferali, *Big data e valutazione del merito creditizio per l'accesso al peer to peer lending*, in «Diritto dell'informazione e dell'informatica», n. 3/2018, p. 487.

[38] R. Berti, F. Zumerle, *Il nostro "credit score" deciso dall'AI: ecco come e quali rischi*, in www.aziendadigitale.eu, 7 giugno 2021. Sui rischi connessi al *credit score*, si veda anche: E. Falletti, *Discriminazione algoritmica. Una prospettiva comparata*, Giappichelli, Torino 2022.

L'intelligenza artificiale è stata selezionata per eseguire tale operazione perché, in astratto, ha la capacità di fare previsioni, identificando elementi specifici ed analizzando enormi quantità di dati provenienti da fonti diverse.

Il punto cruciale, però, è che gli algoritmi non sono infallibili: nella vita reale ci sono situazioni specifiche che solo una mente umana, in grado di cogliere diverse sfumature e di applicare il buon senso, può valutare adeguatamente.

Nel caso sopra riportato, un controllo umano, anche successivo o a fini di validazione, avrebbe probabilmente condotto a una decisione più equa e corrispondente alla realtà, permettendo, così all'investitore, di vedere accolta la propria richiesta di finanziamento.

6. Il diritto a non essere soggetto a decisioni completamente automatizzate e il cd. principio di non esclusività della decisione automatizzata

L'interessato, vittima di un trattamento automatizzato discriminatorio o lesivo, è tutelato dal Regolamento Generale sulla Protezione dei Dati attraverso il riconoscimento di una serie di diritti specifici. Il GDPR ha introdotto un quadro normativo chiaro ed articolato, finalizzato alla tutela dei diritti delle persone fisiche nel contesto del trattamento dei dati personali.

I diritti in questione sono essenziali per garantire che ogni individuo possa mantenere il controllo sulle proprie informazioni personali, favorendo, al contempo, la trasparenza e la responsabilità nelle pratiche di trattamento da parte di titolari e responsabili.

I diritti dell'interessato sono disciplinati dagli articoli 15 e seguenti del Regolamento[39].

Tra le varie tutele accordate all'interessato rileva, in particolar modo, il diritto a non essere soggetto a decisioni completamente automatizzate, di cui all'articolo 22 GDPR[40]: «l''interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona».

---

[39] Gli articoli da 15 a 22 del Regolamento disciplinano il catalogo dei diritti dell'interessato. Tra questi, figurano: il diritto di accesso; il diritto alla rettifica; il diritto alla cancellazione (o all'oblio); il diritto alla limitazione del trattamento; il diritto alla portabilità dei dati; il diritto di opposizione; infine, il diritto a non essere soggetto a decisioni completamente automatizzate.

[40] La norma è rubricata: *"Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione"*.

Questo diritto, in cui è cristallizzato il cd. principio di non esclusività della decisione automatizzata, si traduce sostanzialmente nella facoltà, riconosciuta al soggetto danneggiato da un trattamento lesivo o discriminatorio, di chiedere ed ottenere l'intervento umano nel processo decisionale.

Nel sancire un divieto generale di essere sottoposti a decisioni significative basate unicamente su un processo automatizzato, l'articolo 22 del GDPR offre una protezione formidabile contro la distorsione dei giudizi nei processi decisionali; aspetto, quest'ultimo, che, come osservato, costituisce una delle principali problematiche legate all'impiego delle decisioni algoritmiche.

Il divieto stabilito dall'articolo 22 trova oggi la sua applicazione più significativa proprio nel settore dell'intelligenza artificiale.

La disposizione, sebbene solida e risalente nel tempo[41], presenta, tuttavia, numerose vulnerabilità, che rendono auspicabile una revisione normativa.

Uno dei punti critici più evidenti risiede nell'avverbio *"*unicamente*"*, che, in senso figurato, funge da interruttore, attivando o disattivando automaticamente la tutela approntata dalla norma. In altri termini, per come la disposizione è attualmente formulata, è sufficiente un intervento umano significativo per escludere l'applicazione dell'articolo 22[42].

La realtà, però, è decisamente più complessa: esistono, infatti, diversi livelli di automazione e vari gradi di coinvolgimento umano, che possono essere più o meno significativi.

Appare, quindi, preferibile esaminare, caso per caso, il contesto che fa da sfondo alla decisione automatizzata, invece di disattivare *tout court* la protezione di cui all'articolo 22 al solo verificarsi di un intervento umano.

Un altro aspetto che necessita di un intervento correttivo riguarda, poi, le numerose deroghe contemplate dalla norma al comma 2[43].

---

[41] La disposizione, infatti, nel suo nucleo essenziale, era già presente nella direttiva 95/46/CE sulla protezione dei dati personali, precisamente all'articolo 15, rubricato *"Decisioni individuali automatizzate"* e così formulato: *"gli Stati membri riconoscono a qualsiasi persona il diritto di non essere sottoposta ad una decisione che produca effetti giuridici o abbia effetti significativi nei suoi confronti fondata esclusivamente su un trattamento automatizzato di dati destinati a valutare taluni aspetti della sua personalità, quali il rendimento professionale, il credito, l'affidabilità, il comportamento, ecc."*.

[42] Cfr. *"Allucinazioni" dell'AI, dati personali e tutele: il GDPR va rafforzato*, in www.aziendadigitale.eu, 9 maggio 2023.

[43] Articolo 22, comma 2, GDPR: *"Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto*

Tra le varie esenzioni, rileva, in particolare, quella[44] che interviene quando le decisioni unicamente basate su trattamento automatizzato siano autorizzate da disposizioni normative, pur nel rispetto di misure adeguate. L'eccezione in questione, di cui beneficiano gli algoritmi autorizzati dalla legge, è attualmente formulata in termini così ampi da renderla assimilabile a un vero e proprio *bug* nella disciplina normativa. Essa finisce, cioè, idealmente, per rappresentare la porta attraverso cui si consente l'ingresso a iniziative che sarebbe, invece, preferibile escludere[45].

Le criticità presenti nel dato normativo sollevano interrogativi sull'effettiva efficacia applicativa del principio, in esso contenuto, di non esclusività della decisione algoritmica.

Una formulazione normativa così ambigua esige una revisione, in grado di adattare il nucleo di tutela e la *ratio* della norma al nuovo scenario tecnologico che, in seguito all'avvento dell'intelligenza artificiale, ha fatto irruzione nelle nostre vite.

In questa prospettiva, risulta opportuno ricalibrare l'articolo 22 del GDPR; non con l'obiettivo di ridurre le garanzie di tutela attualmente riconosciute all'interessato, ma, al contrario, per assicurare almeno lo stesso livello di protezione, integrando, al contempo, riferimenti a una realtà certamente più complessa e variegata rispetto a quella descritta dalla norma attuale.

7. Riflessioni conclusive: il paradosso di Achille e la "*cyber*-tartaruga"

In definitiva, il GDPR continua a costituire il più solido e avanzato corpo normativo a tutela dei diritti della persona, anche di fronte alle innovazioni dirompenti nel campo dell'intelligenza artificiale. Tuttavia, è evidente che gli istituti previsti dal Regolamento necessitano di aggiornamenti e integrazioni, in particolare per quanto riguarda l'articolo 22.

La norma, che rappresenta un baluardo fondamentale a tutela dell'interessato, va adeguatamente custodita e innovata per affrontare le nuove sfide imposte dall'evoluzione tecnologica.

Sottolineata l'esigenza di novellare la disposizione di cui all'articolo 22 del GDPR, resta da stabilire a chi affidare tale compito.

---

dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato".

[44] Si fa riferimento alla deroga di cui all'articolo 22, comma 2, lettera b), GDPR.

[45] *"Allucinazioni" dell'AI, dati personali e tutele: il GDPR va rafforzato*, cit.

La giurisprudenza[46] potrebbe essere certamente d'aiuto; tuttavia, in una prospettiva *de iure condendo*, sarebbe auspicabile un intervento del Legislatore, in grado di fornire una regolamentazione chiara ed esaustiva, che rispecchi adeguatamente il progresso digitale e che garantisca, al contempo, la protezione dei diritti fondamentali degli individui.

> «Sul rapporto tra la legge e la tecnologia: l'uomo ha, nello spirito libero che lo contraddistingue, la capacità dell'invenzione e, per quanto riguarda la produzione normativa, tante volte ci troviamo in quello che il filosofo – Zenone – chiamava 'il paradosso di Achille e della tartaruga': a mano a mano che Achille cerca di raggiungere la tartaruga, la tartaruga fa un passo avanti e Achille non la raggiungerà mai. […] quando vi è un'innovazione tecnologica, la legge molto spesso manca, ed il Legislatore è tenuto ad inseguire le problematiche che emergono dall'innovazione tecnologica. Questo […] ci impone di lavorare di fantasia, per comprendere quali saranno i problemi che l'innovazione tecnologica ci pone»[47].

È atteso, allora, un intervento chiarificatore in materia, così da fare in modo – riprendendo l'invito del Guardasigilli – che la produzione normativa riesca a vincere il paradosso e a raggiungere il passo dell'innovazione tecnologica.

---

[46] Devono, però, considerarsi i rischi connessi all'evoluzione giurisprudenziale: orientamenti contrastanti, posizioni divergenti, possibili critiche da parte della dottrina.

[47] La citazione è tratta da un intervento del Ministro della Giustizia, Carlo Nordio, in occasione del convegno *"Spazio virtuale. Le garanzie di giurisdizione nella resilienza e nella difesa della sicurezza nazionale"*, organizzato dalla Presidenza del Consiglio dei Ministri e dalla Fondazione Vittorio Occorsio e svoltosi a Roma, presso il Ministero degli Affari Esteri e della Cooperazione Internazionale, l'11 ottobre 2024.

RIVISTA INTERNAZIONALE DI FILOSOFIA ONLINE
CON *PEER REVIEW*
WWW.METABASIS.IT
novembre 2024 anno XIX n° 38

MIMESIS
Sesto San Giovanni (MI)
via Monfalcone, 17/19

AlboVersorio Edizioni
& AlboVersorio Edizioni
di Ass. NonsoloSophia
nonsolosophia@gmail.com

Autorizzazione del Tribunale di Varese n. 893 del 23/02/2006.
ISSN 1828-1567