INTELLIGENZA ARTIFICIALE E DIRITTO: UNA RIVOLUZIONE?

A CURA DI
ALESSANDRO PAJNO, FILIPPO DONATI E ANTONIO PERRUCCI

VOLUME I
DIRITTI FONDAMENTALI, DATI PERSONALI E REGOLAZIONE

SOCIETÀ EDITRICE IL MULINO

Alla pubblicazione di questa ricerca ha contribuito il Gruppo AlmavivA, che Astrid vivamente ringrazia

ISBN 978-88-15-29967-3

Redazione e produzione: Edimill srl - www.edimill.it

Capitolo decimo

IL RUOLO DI TITOLARE, RESPONSABILE E CONTITOLARE DEL TRATTAMENTO NEI TRATTAMENTI DI DATI PERSONALI MEDIANTE INTELLIGENZA ARTIFICIALE

1. *L'intelligenza artificiale nella «data-driven economy»*

Quando si parla di intelligenza artificiale, il primo pensiero va alla *science fiction* e ai libri di Asimov, dove robot e androidi sembravano rappresentare un futuro molto lontano. «L'intelligenza artificiale non è fantascienza: fa già parte delle nostre vite»[1].

Oggi invece l'intelligenza artificiale è realtà e lo sviluppo tecnologico, ma anche industriale e sociale[2], si basa sempre

Questo capitolo è di Giusella Finocchiaro e Laura Greco.

[1] Così la Commissione europea nella Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *L'intelligenza artificiale per l'Europa*, COM(2018) 237, 25/4/2018, p. 1.

[2] Le istituzioni europee hanno da subito riconosciuto il rilevante impatto delle tecnologie basate sull'intelligenza artificiale nei settori sociali e industriale. «L'uso dei sistemi di IA può svolgere un ruolo significativo nel conseguimento degli obiettivi di sviluppo sostenibile e nel sostegno al processo democratico e ai diritti sociali. (…) Le tecnologie digitali quali l'IA sono fattori abilitanti fondamentali per conseguire gli obiettivi del *Green Deal*», la strategia europea volta ad affrontare le sfide legate al clima e all'ambiente (cfr. COM[2020] 65, *Libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, p. 2). Anche nel contesto industriale e manifatturiero, è evidente la rilevanza e la diffusione dei sistemi di intelligenza artificiale: «L'Europa produce più di un quarto di tutti i robot di servizio industriali e professionali (ad esempio per l'agricoltura di precisione, la sicurezza, la salute e la logistica) e svolge un ruolo importante nello sviluppo e nell'utilizzo di applicazioni software per le imprese e le organizzazioni (applicazioni *business-to-business* quali i software per l'ingegneria, il design, e la pianificazione delle risorse aziendali), nonché di applicazioni a sostegno dell'*e-government* e dell'impresa intelligente. L'Europa svolge un ruolo guida per quanto riguarda la diffusione dell'IA nell'industria manifatturiera: oltre la metà dei principali fabbricanti implementano almeno un'istanza di IA nelle operazioni di fabbricazione» (COM[2020] 65, cit., p. 4).

più sui sistemi di *Artificial Intelligence*, intesi come «sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi»[3]. Come si legge nella Comunicazione della Commissione europea *L'intelligenza artificiale per l'Europa*, questi sistemi possono consistere in software che agiscono nel mondo virtuale (per esempio assistenti vocali, software per l'analisi delle immagini, motori di ricerca, sistemi di riconoscimento vocale e facciale) oppure incorporare l'intelligenza artificiale in dispositivi hardware (per esempio in robot avanzati, auto a guida autonoma, droni o applicazioni dell'internet delle cose).

Non si tratta però di un fenomeno nuovo. La nascita dell'intelligenza artificiale si fa risalire alla Conferenza di Dartmouth del 1956, dove per la prima volta si cercò di definire l'intelligenza artificiale «sulla base della congettura per cui, in linea di principio, ogni aspetto dell'apprendimento o una qualsiasi altra caratteristica dell'intelligenza possano essere descritte così precisamente da poter costruire una macchina che le simuli»[4].

Soltanto oggi, però, i progressi compiuti nell'ambito del calcolo computazionale e la crescente disponibilità di dati hanno consentito l'effettivo sviluppo dell'intelligenza artificiale. Da un lato, le infrastrutture di calcolo sono senz'altro essenziali per il funzionamento di questi sistemi che richiedono risorse digitali ed elettroniche ad alte prestazioni. Dall'altro lato, i dati – personali e non[5] – rappresentano

[3] Cfr. la già citata COM(2018) 237, p. 1.

[4] Cfr. il testo della proposta con cui gli organizzatori della conferenza (nonché «padri fondatori» di questa tecnologia) affrontarono i temi principali del campo di ricerca, tra cui le reti neurali, la teoria della computabilità, la creatività, l'elaborazione e il riconoscimento del linguaggio naturale: J. McCarthy, M.L. Minsky, N. Rochester e C.E. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, https://aaai.org/ojs/index.php/aimagazine/article/view/1904/1802.

[5] I dati non personali sono oggetto della disciplina dettata dal Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea. Questo Regolamento, adot-

la materia prima di queste tecnologie, che si alimentano e imparano costantemente dalle informazioni che gli vengono fornite. Come ha affermato la Commissione europea, «l'intelligenza artificiale è un insieme di tecnologie che combina dati, algoritmi e potenza di calcolo»[6].

Non è dunque un caso che, in un'epoca in cui tecnica, scienza e dati sono i principali *asset*, l'intelligenza artificiale stia progredendo in modo esponenziale. Questa è d'altronde anche l'era della cd. «quarta rivoluzione industriale» legata, tra l'altro, allo sfruttamento delle nuove tecnologie al servizio delle attività finanziarie, il cd. fenomeno *FinTech*[7].

Siamo di fronte a fenomeni e a tecnologie che traggono le proprie origini dalla e, allo stesso tempo, beneficiano della *data-driven economy*. «I dati sono la linfa vitale dello sviluppo economico»[8] e il legislatore europeo mostra di

tato «per potenziare ulteriormente lo scambio transfrontaliero dei dati e promuovere l'economia dei dati», si è affiancato al Regolamento (UE) 2016/679 in materia di protezione dei dati personali. A tal proposito, la Commissione europea, COM(2019) 250, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, 29/5/2019, p. 2, rileva che «ora esiste un quadro globale per uno spazio comune europeo dei dati e per la libera circolazione di tutti i dati all'interno dell'Unione europea».

[6] Cfr. COM(2020) 65, cit., p. 2.

[7] Il termine *FinTech* descrive, in particolare, il fenomeno in base al quale si assiste ad una offerta di servizi di finanziamento, di pagamento, di investimento e di consulenza ad alta intensità tecnologica. Tale innovazione finanziaria, resa possibile dalla tecnologia, riverbera i suoi effetti sia nel campo dei servizi finanziari sia bancari, modificandone la struttura. La Commissione europea, nella COM(2018) 109, *Piano d'azione per le tecnologie finanziarie: per un settore finanziario europeo più competitivo e innovativo*, 8/3/2018, definisce «le tecnologie finanziarie (*fintech*), ossia l'innovazione nel settore dei servizi finanziari resa possibile dalla tecnologia» come «il punto di incontro dei servizi finanziari e del mercato unico digitale» (p. 2). Sul punto, cfr. anche G. Finocchiaro e V. Falce (a cura di), *«Fintech»: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Bologna, 2019; G. Finocchiaro e V. Falce, *La «digital revolution» nel settore finanziario. Una nota di metodo*, in «Analisi Giuridica dell'Economia», 2019, n. 1, pp. 313-326.

[8] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *Una strategia europea per i dati*, COM(2020) 66, 19/2/2020, p. 3.

averne consapevolezza facendosi promotore di molteplici iniziative volte a garantire la circolazione di questa importante risorsa. A partire dall'ormai non più tanto recente Regolamento in materia di protezione dei dati personali[9] (di seguito anche solo «Regolamento»), tra gli interventi di maggiore rilievo per lo sviluppo dell'economia dei dati si annoverano il Regolamento sulla libera circolazione dei dati non personali[10], la Direttiva sulla cybersicurezza[11] e

[9] *Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*. In generale, sul Regolamento cfr. G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in «Contratto e impresa», 2017, III, pp. 723-733; G. Busia, L. Liguori e O. Pollicino (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma, 2016; L. Califano e 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; V. Cuffaro, R. D'Orazio e V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019; R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta (a cura di), *Codice della privacy e data protection*, Milano, 2021; G. Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; R. Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice privacy)*, Milano, 2019; F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016; G.M. Riccio, G. Scorza e E. Belisario (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, 2018; S. Sica, V. D'Antonio e G.M. Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016; E. Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019; N. Zorzi Galgano (a cura di), *Persona e mercato dei dati: riflessioni sul GDPR*, Padova, 2019.

[10] Cfr. già citato *Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea*.

[11] *Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione* (meglio nota come «Direttiva NIS»). Si noti che sono state recentemente proposte dalla Commissione europea l'abrogazione della direttiva qui citata e la contestuale adozione di una nuova direttiva, la cd. «NIS2», volta a rafforzare il quadro normativo sulla *cybersecurity* in Europa estendendo l'ambito

la Direttiva sull'apertura dei dati[12]. Da ultimo, la recente proposta del *Data Governance Act* con cui il legislatore europeo mira a «promuovere la disponibilità dei dati utilizzabili rafforzando la fiducia negli intermediari di dati e potenziando i meccanismi di condivisione dei dati in tutta l'Unione europea»[13], nonché la proposta di *Data Act*[14] che affronta, invece, il tema della circolazione e dello sfruttamento dei dati generati da prodotti e servizi.

È dunque in questo panorama normativo che anche le tecnologie fondate sull'intelligenza artificiale devono necessariamente muoversi nel rispetto dei valori e dei diritti fondamentali dell'Unione europea, tra i quali la dignità umana, la tutela della riservatezza e la protezione dei dati personali. Questa esigenza è stata recentemente ribadita dalla Commissione europea, che ha affermato:

> I cittadini daranno fiducia alle innovazioni basate sui dati e le faranno proprie solo se saranno convinti che la condivisione dei dati personali nell'Ue sarà soggetta in ogni caso alla piena conformità alle rigide norme dell'Unione in materia di protezione dei dati[15].

applicativo della NIS1 e rafforzandone l'apparato sanzionatorio. Il testo della Proposta è disponibile al sito https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union, consultato il 3/5/2021.

[12] Si tratta della *Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico*. La direttiva promuove l'utilizzo dei dati aperti, ossia conferiti in un formato indipendente dalla piattaforma e resi disponibili al pubblico senza alcuna restrizione che impedisca il riutilizzo dei medesimi.

[13] Cfr. COM(2020) 767, *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati)*, 25/11/2020, p. 1. La citata Proposta è stata recentemente approvata, prima, dal Parlamento europeo, poi, dal Consiglio ed il testo definitivo è stato pubblicato in Gazzetta Ufficiale dell'Unione europea del 3/6/2022, L 152.

[14] Cfr. COM(2022) 68, *Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, 23/2/2022.

[15] Cfr. COM(2020) 66, cit., p. 1.

2. *L'architettura giuridica nel trattamento di dati personali*

Dall'analisi delle interazioni tra applicazioni di intelligenza artificiale e la disciplina concernente la protezione dei dati personali emergono molteplici profili, alcuni dei quali sono affrontati nei contributi di questo volume.

Fra tutti, uno degli aspetti più complessi riguarda le responsabilità e l'imputazione delle scelte di come e perché trattare i dati personali mediante le tecnologie di intelligenza artificiale.

Per meglio comprendere i ruoli dei soggetti coinvolti nel trattamento di dati personali, occorre preliminarmente ripercorrere le caratteristiche fondanti i ruoli di titolare e di responsabile del trattamento di dati personali e descriverne le rispettive responsabilità.

2.1. *Il titolare del trattamento di dati personali*

Il titolare del trattamento di dati personali è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali»[16].

[16] Cfr. art. 4, 1° comma, n. 7 del Regolamento. Cfr. *ex multis* S. Calzolaio, L. Ferola, V. Fiorillo, E.A. Rossi e M. Timani, *La responsabilità e la sicurezza del trattamento*, in Califano e Colapietro (a cura di), *Innovazione, tecnologia e valore della persona*, cit., pp. 137-202; A. D'Ottavio, *Ruoli e funzioni privacy principali ai sensi del Regolamento*, in Panetta (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, cit., pp. 143-184; D. Farace, *Il titolare e il responsabile del trattamento*, in Cuffaro, D'Orazio e Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., pp. 731-774; L. Greco, *L'organigramma privacy: i soggetti del trattamento*, in Finocchiaro (a cura di), *La protezione dei dati personali in Italia*, cit., pp. 321-354; E. Maio, *Sub Art. 24*, in A. Barba e S. Pagliantini (a cura di), *Delle persone*, vol. II, in E. Gabrielli (diretto da), *Commentario del codice civile*, Milano, 2019, pp. 503-512; A. Mantelero, *Gli autori del trattamento dati: titolare e responsabile*, in «Giurisprudenza italiana», 2019, n. 12, pp. 2799-2805; F. Pizzetti e L. Greco, *Sub Art. 24*, in D'Orazio, Finocchiaro, Pollicino e Resta (a cura di), *Codice della privacy e data protection*, cit., pp. 398-410; G.M. Riccio, *Titolarità e contitolarità nel trattamento dei dati personali*

Si tratta dunque del soggetto che definisce l'obiettivo al quale è orientato (finalizzato) il trattamento e in ragione del quale organizza la sua attività, determinando quali tecniche (elettroniche o analogiche) utilizzare; quali misure di sicurezza adottare; quali soggetti coinvolgere nel trattamento, e così via[17].

Titolare del trattamento di dati personali è colui che esercita concretamente un potere sul trattamento, colui che guida e dà impulso al trattamento di dati personali ed è in grado di mutarne le finalità e i mezzi con cui viene posto in essere.

A fronte di così ampi poteri, sul titolare del trattamento di dati personali grava una corrispondente responsabilità rispetto ai diritti e alle libertà delle persone fisiche i cui dati personali sono trattati.

Il titolare del trattamento di dati personali deve infatti garantire il rispetto delle norme del Regolamento e, se richiesto, dimostrare e dare prova di tale osservanza[18]. Questo principio generale, che deve orientare l'azione del titolare del trattamento di dati personali nel suo complesso, prende il nome di *accountability* e rappresenta il nuovo approccio alla tutela dei dati personali improntato alla gestione del rischio.

Rispetto a quanto previsto dalla previgente normativa dettata dalla Direttiva 95/46/CE, il Regolamento non prevede più soltanto prescrizioni dirette e precise alla cui mancata applicazione consegue una sanzione, bensì un obiettivo da realizzare, secondo modalità che lo stesso titolare di trattamento deve di volta in volta determinare e che saranno

tra Corte di giustizia e Regolamento privacy, in «Nuova Giurisprudenza Civile Commentata», 2018, n. 12, pp. 1805-1819; M. Siano, *Sub Art. 24*, in Riccio, Scorza e Belisario (a cura di), *GDPR e normativa privacy. Commentario*, cit., pp. 236-244.

[17] Secondo il Gruppo di lavoro art. 29, *Parere 1/2010*, adottato il 16/2/2010, il concetto di «"strumenti" non si riferisce solo ai mezzi tecnici per trattare i dati personali, ma anche al "come" del trattamento, cioè "quali dati saranno trattati", "quali terzi avranno accesso ai dati", "quando tali dati saranno eliminati" ecc. La determinazione degli "strumenti" ingloba quindi questioni sia tecniche che organizzative» (p. 14).

[18] Sul principio di *accountability*, cfr. ampiamente G. Finocchiaro, *L'accountability nel Regolamento europeo*, in Barba e Pagliantini (a cura di), *Delle persone*, vol. II, cit., pp. 513-523.

oggetto di successiva valutazione da parte dell'autorità di controllo e del giudice.

Si passa quindi da un approccio normativo che dettava indicazioni assai precise ad un sistema basato sui principi e volto a responsabilizzare il titolare del trattamento di dati personali.

In virtù del principio di *accountability*, il titolare del trattamento di dati personali deve garantire in primo luogo di trattare i dati personali sulla base di una adeguata condizione di liceità del trattamento[19]. In secondo luogo, deve adottare misure, tecniche ed organizzative, che garantiscano la sicurezza del trattamento di dati personali in maniera proporzionale al rischio che potrebbe derivare dallo stesso trattamento[20]. Ciò comporta anche la strutturazione della propria organizzazione secondo principi di *privacy by design* e *by default* e la formalizzazione dei rapporti con altri eventuali soggetti coinvolti nel trattamento di dati personali. In capo al titolare del trattamento di dati personali sono previsti ulteriori adempimenti che riflettono il citato principio di *accountability*, tra cui la valutazione d'impatto sulla protezione dei dati personali, la gestione e la notifica dei *data breach*, la tenuta del registro delle attività di trattamen-

[19] I presupposti di liceità del trattamento di dati personali sono individuati agli artt. 6 e 9 del Regolamento. Cfr. ampiamente in S. Bosa, *Sub Art. 6* e R. Tuccillo, *Sub Art. 9*, in Barba e Pagliantini (a cura di), *Delle persone*, vol. II, cit., pp. 118-133 e 152-186; F. Bravo, *Le condizioni di liceità del trattamento di dati personali*, in Finocchiaro (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., pp. 110-193; M. Dell'Utri, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in Cuffaro, D'Orazio e Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., pp. 179-248; G. Druetta, *Sub Art. 9* e F. Resta, *Sub Art. 6*, in Riccio, Scorza e Belisario (a cura di), *GDPR e normativa privacy. Commentario*, cit., pp. 89-106, in part. 63-76.

[20] Cfr. art. 32 del Regolamento. Cfr. F. Bravo, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in Cuffaro, D'Orazio e Ricciuto (a cura di), *I dati personali nel diritto europeo*, cit., pp. 775-854; M. Renna, *Sub Art. 32*, in Barba e Pagliantini (a cura di), *Delle persone*, vol. II, cit., pp. 618-636; F. Rotolo, *Sub Art. 32*, in Riccio, Scorza e Belisario (a cura di), *GDPR e normativa privacy. Commentario*, cit., pp. 293-303.

to, che qui, per ragioni di necessaria brevità, non possono essere esaminati nel dettaglio.

In sintesi, per comprendere il nuovo concetto di responsabilità del titolare del trattamento di dati personali, basti evidenziare che la valutazione complessiva dell'intero trattamento compete, prima che a chiunque altro, a tale soggetto, che deve adottare misure, *policy*, procedure adeguate alla tutela dei dati personali e successivamente giustificare l'iter decisionale che l'ha portato a tali determinazioni.

2.2. *Il responsabile del trattamento di dati personali*

Il responsabile del trattamento di dati personali è invece privo di un potere decisorio circa le finalità e le modalità del trattamento. Il responsabile del trattamento di dati personali è infatti «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»[21].

Ne consegue che questi può agire soltanto su istruzione del titolare del trattamento di dati personali[22] e solo in virtù del suo rapporto con quest'ultimo può effettuare un trattamento di dati che rinviene la sua base giuridica nella posizione del titolare del trattamento. In altre parole, il trattamento effettuato dal responsabile trae legittimazione unicamente dalla designazione effettuata dal titolare del trattamento di dati personali e dal rapporto che lega il titolare al responsabile.

[21] Cfr. art. 4, 1° comma, n. 8 del Regolamento. Oltre ai contributi segnalati alla precedente nota 16, cfr. E. Maio, *Sub Art. 28*, in Barba e Pagliantini (a cura di), *Delle persone*, vol. II, cit., pp. 564-572; F. Pizzetti e L. Greco, *Sub Art. 28*, in R. D'Orazio, G. Finocchiaro, O. Pollicino e G. Resta (a cura di), *Il nuovo Codice della privacy*, Milano (in corso di pubblicazione), pp. 456-478; L.M. Salvati e G. Scorza, *Sub Art. 28*, in Riccio, Scorza e Belisario (a cura di), *GDPR e normativa privacy. Commentario*, cit., pp. 261-272.

[22] EDPB, *Guidelines 7/2020 on the concepts of controller and processor in the GDPR*, 2/9/2020: «The processor must not process the data otherwise than according to the controller's instructions» (p. 3).

Sebbene rimanga una figura gerarchicamente subordinata al titolare del trattamento e svolga un'attività strumentale al raggiungimento degli obiettivi fissati dal titolare, il responsabile del trattamento di dati personali gode di alcuni, seppure circoscritti, margini di discrezionalità nell'esecuzione delle operazioni di trattamento delegate.

Ad esempio, il Regolamento ha previsto che l'autonomia gestionale del responsabile del trattamento di dati personali possa spingersi fino all'individuazione di un nuovo soggetto nella filiera dei soggetti attivi del trattamento, il cd. sub-responsabile del trattamento, facoltà che tuttavia non è incondizionata[23]. Inoltre, è ormai pacifico che il responsabile del trattamento goda di una certa libertà nella definizione dei mezzi del trattamento necessari «to best serve the controller's interests»[24].

Allo stesso tempo però è posto un limite alla discrezionalità del responsabile del trattamento di dati personali, come sancito dall'art. 28, 10° comma, secondo cui «se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione». Tale disposizione risponde direttamente a quell'approccio

[23] Si ritiene infatti che, da un lato, il responsabile del trattamento di dati personali debba individuare il sub-responsabile alla luce dei criteri di conoscenza, risorse e affidabilità previsti anche ai fini della nomina del responsabile principale da parte del titolare del trattamento di dati personali. Dall'altro lato, poi, la nomina è subordinata all'autorizzazione del titolare del trattamento a cui dunque compete, in ultima battuta, la decisione se consentire ovvero negare l'ingresso di un nuovo soggetto nello scenario del trattamento dei dati oggetto del suo rapporto col responsabile. Cfr. Pizzetti e Greco, *Sub Art. 28*, cit., pp. 468-469.

[24] EDPB, *Guidelines 7/2020*, cit., p. 4. L'EDPB distingue anche tra mezzi del trattamento essenziali e non essenziali per tracciare una linea tra le decisioni che competono al titolare del trattamento e quelle che ricadono nella discrezionalità del responsabile del trattamento: «"Essential means" are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller. (…) "Non-essential means" concern more practical aspects of implementation, such as the choice for a particular type of hard- or software or the detailed security measures which may be left to the processor to decide on» (p. 14).

funzionale e sostanzialista che, ai fini della configurazione dei rapporti e dell'individuazione delle responsabilità, dà rilevanza alla realtà del trattamento. In tale ottica, dunque, ove dall'analisi fattuale delle modalità concrete del trattamento derivi che il responsabile del trattamento di dati personali abbia assunto un ruolo rilevante nella determinazione delle finalità o degli aspetti fondamentali dei mezzi del trattamento, questi deve essere considerato titolare (o contitolare) del trattamento.

Dunque la qualificazione di un soggetto come responsabile del trattamento di dati personali è subordinata ad un riscontro effettivo, *case-by-case*, del grado di subordinazione di quest'ultimo e dell'assenza di autonomia nella determinazione di mezzi e di finalità del trattamento.

2.3. *Il contitolare del trattamento di dati personali*

La contitolarità di un trattamento di dati personali ha luogo qualora il trattamento sia comune a più soggetti e da questi siano condivise le decisioni circa i mezzi e le finalità di trattamento[25].

Sotto il profilo operativo, la gestione della contitolarità del trattamento si presenta particolarmente onerosa, richiedendo un continuo contatto fra i contitolari. L'art. 26 del Regolamento, infatti, prevede espressamente la stipulazione di un accordo interno tra contitolari, ove questi debbano determinare in modo trasparente «le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14».

Dalla fattispecie ora descritta va tuttavia tenuta distinta quella in cui più soggetti si trovino coinvolti nel medesimo trattamento, provvedendo ciascuno ad adottare decisioni

[25] Per approfondimenti, cfr. F. Pizzetti e L. Greco, *Sub Art. 26*, in D'Orazio, Finocchiaro, Pollicino e Resta (a cura di), *Codice della privacy e data protection*, cit., pp. 422-449.

autonome in merito alle finalità e modalità del trattamento. In questo caso, anziché di contitolari, si parlerà più propriamente di titolari autonomi del trattamento di dati personali.

3. *La responsabilità dei sistemi di intelligenza artificiale*

Il tema della responsabilità è quanto mai rilevante anche nel caso di applicazioni di intelligenza artificiale, rispetto alle quali è ancora aperto un dibattito circa il modello di responsabilità più adeguato[26].

La questione rileva senza dubbio ai fini dell'individuazione del soggetto responsabile nel caso di danni cagionati dalle applicazioni di intelligenza artificiale. In particolare, in quei casi in cui l'esito dell'elaborazione effettuata dall'applicazione di intelligenza artificiale non sia del tutto determinabile a priori e sia caratterizzato da un certo grado di imprevedibilità: non sia cioè un processo deterministico, ma sia caratterizzato da una certa autonomia elaborativa. Sono le ipotesi, ad esempio, delle applicazioni di intelligenza artificiale costituite da modelli di *machine learning* che usano reti neurali e algoritmi di *deep learning*[27], a cui talvolta ci si riferisce come algoritmi *black-box*, che costituiscono una nuova tipologia di rischio anche nel mondo finanziario[28].

Come si legge nella Comunicazione *L'intelligenza artificiale per l'Europa*,

[26] In tema di responsabilità delle applicazioni di intelligenza artificiale cfr. U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2018; A. Santosuosso, C. Boscarato e F. Caroleo, *Robot e diritto: una prima ricognizione*, in «Nuova Giurisprudenza Civile Commentata», 28, 2012, n. 7-8, pp. 494-516.

[27] Le diverse tipologie di *machine learning* sono illustrate dall'Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), *30 Recommendations on Regulation, Innovation and Finance - Final Report to the European Commission*, December 2019, p. 28, che definisce il *deep learning* un tipo di *machine learning* che utilizza le reti neurali.

[28] Cfr. ROFIEG, *Report*, cit., pp. 11 e 39. Tuttavia, i rischi della *black box* possono essere limitati con un approccio che coinvolga contestualmente la rappresentazione della conoscenza, *deep learning*, *machine learning* e *natural language processing* (cfr. ROFIEG, *Report*, cit., p. 31).

l'apprendimento automatico, un tipo di IA, opera mediante l'individuazione di modelli a partire dai dati disponibili e la successiva applicazione di questa conoscenza ai dati nuovi. Quanto più è grande il set di dati, tanto più accurata sarà l'individuazione delle relazioni anche impercettibili tra i dati. Quando si tratta di utilizzare l'IA, gli ambienti ad alto contenuto di dati offrono anche le maggiori opportunità, perché i dati sono il mezzo attraverso il quale l'algoritmo apprende e interagisce con il suo ambiente[29].

Si comprende, dunque, come il tema della responsabilità assuma una rilevanza significativa anche sotto il profilo della protezione dei dati personali, in particolare ai fini della determinazione del soggetto che deve rispondere del trattamento di dati personali effettuato tramite le applicazioni di intelligenza artificiale.

Ai fini di tale riflessione, complessa e non ancora giunta a compiuta definizione, giova ripercorrere alcune delle ipotesi che sono state sino ad oggi avanzate.

Se da un lato parte della dottrina, muovendo dalla legislazione vigente, ha pensato di applicare le norme in materia di responsabilità civile e responsabilità del produttore[30], dall'altro

[29] Cfr. la già citata COM(2018) 237, p. 10.

[30] Il rapporto tra responsabilità civile e intelligenza artificiale è esaminato approfonditamente all'interno della sezione monografica della rivista «Giurisprudenza italiana» dedicata al tema «Intelligenza artificiale e responsabilità», a cura di Ruffolo e di Gabrielli. In particolare, si vedano i contributi di M. Costanza, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, pp. 1686-1689, che individua la responsabilità in capo al soggetto più vicino al fatto lesivo causato dall'applicazione di intelligenza artificiale; di U. Ruffolo, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, pp. 1689-1704, che vaglia le possibilità di individuazione e qualificazione della responsabilità da intelligenza artificiale alla luce del Codice civile, esaminando altresì le ipotesi di riconoscimento di personalità giuridica; di M. Gambini, *Algoritmi e sicurezza*, pp. 1726-1740, che affronta il tema della sicurezza nel settore dell'intelligenza artificiale esaminando le soluzioni già esistenti e adottate nell'ambito dei servizi della società dell'informazione e dei trattamenti automatizzati di dati personali. Con particolare riferimento al tema della responsabilità civile delle cd. *autonomous car*, si rinvia a E. Al Mureden, *«Autonomous cars» e responsabilità civile tra disciplina vigente e prospettive «de iure condendo»*, in «Contratto e impresa», 2019, III, pp. 895-924. Approfondisce il tema della responsabilità

lato vi è stato invece chi, con il proposito di definire nuove norme e nuovi modelli, ha proposto di riconoscere una soggettività giuridica al programma e conseguentemente attribuire ad esso una responsabilità[31]. Questa possibilità è stata menzionata anche nella Risoluzione del Parlamento europeo del 16/2/2017, ove si invitava la Commissione europea a valutare

l'istituzione di uno status giuridico specifico per i robot nel lungo termine, di modo che almeno i robot autonomi più so-

derivante dalle applicazioni di sistemi di intelligenza artificiale anche il libro curato da F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018 e in particolare il contributo di M. Bassini, L. Liguori e O. Pollicino, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, pp. 333-371, nel quale gli autori offrono una panoramica dei diversi orientamenti espressi da dottrina e giurisprudenza in relazione al tema della responsabilità civile e penale derivante da eventuali danni causati da sistemi di intelligenza artificiale; A. Massolo, *Responsabilità civile e IA*, pp. 373-382, valuta invece l'idoneità del quadro giuridico nazionale ed europeo a regolare i rapporti civili nell'era dell'intelligenza artificiale. Per una rassegna delle problematiche sollevate, cfr. anche il volume curato da A. De Franceschi e R. Schulze (a cura di), *Digital Revolution. New challenges for Law*, München, 2019, e in particolare i contributi di G. Mazzini, *A System of Governance for Artificial Intelligence through the Lens of Emerging Intersections between AI and EU Law*, pp. 245-298, e di F. Mezzanotte, *Risk Allocation and Liability Regimes in the IoT*, pp. 169-189; O. Rachum-Twaig, *Whose Robot Is It Anyway?: Liability for Artificial-Intelligence-Based Robots*, in «University of Illinois Law Review», 2020; R.H. Weber e D.N. Staiger, *New Liability Patterns in the Digital Era*, in T.E. Synodinou, P. Jougleux, C. Markou e T. Prastitou (a cura di), *EU Internet Law*, Cham, 2017, pp. 197-214.

[31] Approfondiscono il tema del riconoscimento della personalità giuridica, cfr. U. Pagallo, *The Laws of Robots*, Dordrecht, 2013; G. Sartor, *Cognitive automata and the law: electronic contracting and the intentionally of software agents*, in «Artificial Intelligence Law», 17, 2009, n. 4, pp. 253-290; G. Teubner, *Rights of Non-Humans? Electronic Agents and Animals as New Actors in Politics and Law*, in «Journal of Law and Society», 33, 2016, pp. 497-521. In senso contrario, invece, cfr. L. Coppini, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in «Politica del diritto», 2018, IV, pp. 713-739; S. Toffoletto, *IoT e intelligenza artificiale: le nuove frontiere della responsabilità civile (e del risarcimento)*, note a margine del convegno «Intelligenza artificiale e primi profili applicativi: Giustizia, IoT e Lavoratori» (Aula Magna del Palazzo di Giustizia di Milano, 17/4/2018).

fisticati possano essere considerati come persone elettroniche responsabili di risarcire qualsiasi danno da loro causato, nonché eventualmente il riconoscimento della personalità elettronica dei robot che prendono decisioni autonome o che interagiscono in modo indipendente con terzi[32].

Tuttavia, questa soluzione, che – a ben vedere – cede al fascino retorico della soggettività delle applicazioni di intelligenza artificiale, è stata presto esclusa dallo stesso Parlamento europeo. Si legge infatti nella recente Risoluzione del 20/10/2020:

> Non è necessario conferire personalità giuridica ai sistemi di intelligenza artificiale; (…) l'opacità, la connettività e l'autonomia dei sistemi di intelligenza artificiale potrebbero rendere, nella pratica, molto difficile o addirittura impossibile ricondurre specifiche azioni dannose dei sistemi di intelligenza artificiale a uno specifico *input* umano o a decisioni adottate in fase di progettazione; (…) conformemente a concetti di responsabilità ampiamente accettati, è tuttavia possibile aggirare tale ostacolo considerando responsabili le varie persone nella catena del valore che creano il sistema di intelligenza artificiale, ne eseguono la manutenzione o ne controllano i rischi associati[33].

Infatti, se pure fosse riconosciuta all'applicazione una soggettività giuridica, nel caso in cui l'applicazione fosse ritenuta responsabile, occorrerebbe comunque risolvere il problema del risarcimento del danno cagionato. Il programma

[32] Cfr. punto 59, lett. *f* della Risoluzione del Parlamento europeo del 16/2/2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103 [INL]).

[33] Cfr. punto 7 della citata Risoluzione del Parlamento europeo del 20/10/2020 recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014 [INL]). Non sembra invece accantonata l'eventualità di aderire a prodotti del settore assicurativo, nei confronti del quale il Parlamento sollecita la collaborazione al fine di verificare «in che modo sia possibile utilizzare dati e modelli innovativi per creare polizze assicurative che offrano coperture adeguate a prezzi accessibili». Ritiene invece che non sia necessaria una revisione completa dei sistemi di responsabilità e che la configurazione della responsabilità per danni da prodotto difettoso costituisca un mezzo efficace che, tuttavia, debba essere adeguato al mondo digitale.

di intelligenza artificiale non avrebbe, infatti, un patrimonio di cui poter disporre con il quale risarcire il danno. Rimarrebbe dunque non risolto il problema del risarcimento.

Per gli stessi motivi è stato ritenuto fuorviante e poco efficace tentare di applicare categorie e criteri di natura soggettiva, quali il dolo o la colpa, all'applicazione informatica cui si sarebbe attribuita la soggettività.

3.1. *L'individuazione dei ruoli e delle responsabilità previste dal Reg. (UE) 2016/679 nelle applicazioni di intelligenza artificiale*

Se all'applicazione di intelligenza artificiale non è riconosciuta soggettività giuridica, evidentemente, non potrà essere considerata titolare del trattamento di dati personali né responsabile del trattamento di dati personali, posto che tali concetti – come sopra illustrato – presuppongono l'individuazione di un centro di imputazione di responsabilità.

Oggi sembra che il quadro in materia di responsabilità dei prodotti di intelligenza artificiale stia prendendo forma nella direzione di una responsabilità oggettiva e solidale in capo ai molteplici soggetti coinvolti.

Occorre dunque riflettere se possa essere considerato responsabile, sotto il profilo della protezione dei dati personali, il produttore del sistema di intelligenza artificiale, il venditore o l'utilizzatore che trae vantaggio dall'utilizzo di sistemi di intelligenza artificiale. È quindi necessario individuare, nelle varie fasi di costruzione, *training*, immissione nel mercato e sfruttamento del sistema di intelligenza artificiale, chi definisce le modalità e le finalità del trattamento di dati personali.

A tal fine sembra offrire spunti interessanti la *Proposal for a Regulation laying down harmonised rules on artificial intelligence* della Commissione europea (di seguito, per brevità, anche «Proposta»)[34] che, tra le altre disposizioni volte a

[34] Si tratta della COM(2021) 206 del 21/4/2021, disponibile al seguente link https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206.

delineare un quadro normativo per i sistemi di intelligenza artificiale, distingue le categorie di soggetti coinvolti nella filiera di creazione e utilizzo di un prodotto di intelligenza artificiale.

In particolare, la Proposta prevede specifici adempimenti in capo, rispettivamente, al *provider* definito come la persona fisica o giuridica, l'autorità pubblica, l'agenzia o un altro organismo che sviluppa o dispone di un sistema di intelligenza artificiale sviluppato al fine di immetterlo sul mercato con il proprio nome o marchio; allo *user*, vale a dire qualsiasi persona fisica o giuridica, autorità pubblica, agenzia o altro ente che utilizza, per scopi professionali e non personali, un sistema di intelligenza artificiale sotto la propria autorità; al cd. *importer*, ossia qualsiasi persona fisica o giuridica stabilita nell'Unione che immette sul mercato o concede in servizio un sistema di intelligenza artificiale che reca il nome o il marchio di una persona fisica o giuridica stabilita al di fuori dell'Unione; al *distributor*, qualsiasi persona fisica o giuridica nella catena di fornitura, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di intelligenza artificiale sul mercato dell'Unione senza influire sulle sue proprietà.

Nella Proposta non è invece oggetto di definizione il cd. *product manufacturer*, a cui tuttavia è dedicato l'art. 24 che, quanto ad obblighi in relazione al sistema di intelligenza artificiale prodotto, pone il produttore sullo stesso piano del *provider*[35].

Ebbene, dall'esame degli obblighi imposti in capo alle figure sopra elencate e dalle attività da queste espletate è possibile desumere un diverso grado di responsabilità sotto il profilo della protezione dei dati personali.

Tra i doveri previsti dall'art. 16 della Proposta, il *provider* è responsabile, in particolare, della predisposizione e della tenuta del cd. *quality management system*, il quale

[35] Cfr. art. 24 della Proposta: «(…) the manufacturer of the product shall take the responsibility of the compliance of the AI system with this Regulation and, as far as the AI system is concerned, have the same obligations imposed by the present Regulation on the provider».

comprende, tra gli altri, sistemi e procedure di gestione dei dati, incluse le fasi di raccolta, analisi, etichettatura, archiviazione, filtraggio, minimizzazione, aggregazione e qualsiasi altra operazione che coinvolga dati ai fini della commercializzazione del sistema di intelligenza artificiale.

Fatta salva l'eventualità in cui tali dati non abbiano natura personale, è evidente che il *provider*, così come il produttore in ragione dell'analogia stabilita dalla stessa Proposta, siano da considerare titolari del trattamento di dati personali, quando determinino i dati personali che vengono raccolti ed analizzati dal sistema di intelligenza artificiale per il raggiungimento degli obiettivi a cui questo è preordinato. Sono infatti questi soggetti a detenere, nell'ambito della creazione e della fornitura del prodotto, il potere di individuare il dataset da fornire al sistema, anche nelle fasi di progettazione, *training* e *testing* dove i dati potrebbero pure essere diversi da quelli che saranno poi utilizzati dal prodotto finale[36].

Analogamente, lo *user* dovrebbe essere considerato titolare del trattamento di dati personali fintanto che eserciti un controllo sugli *input data*, dovendo garantire che tali dati siano rilevanti ai fini del perseguimento degli scopi del sistema di intelligenza artificiale[37]. A tal riguardo infatti è espressamente previsto che lo *user* debba compiere una valutazione di impatto sulla protezione dei dati personali ai sensi dell'art. 34 del Regolamento (UE) 2016/679[38].

Al contrario, invece, sembrerebbe che il distributore e l'importatore non abbiano alcun potere decisionale in ordine al trattamento dei dati personali che (eventualmente) alimentano il sistema di intelligenza artificiale. La loro

[36] «High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become the source of discrimination prohibited by Union law. High quality training, validation and testing data sets require the implementation of appropriate data governance and management practices» (cfr. Considerando n. 44 della Proposta).

[37] Cfr. art. 29, 3° comma della Proposta.

[38] Cfr. art. 29, 6° comma della Proposta.

attività si limita infatti al collocamento e alla circolazione del prodotto sul mercato, ragione per cui gli obblighi loro in capo hanno natura meramente di vigilanza e di controllo circa l'osservanza dei requisiti di conformità, di marcatura CE e di supporto documentale che devono essere garantiti dal *provider* o del *manufacturer*.

Nello scenario così ipotizzato, potrebbero allora individuarsi quali responsabili del trattamento di dati personali ai sensi dell'art. 28 del Regolamento i soggetti, esterni all'organizzazione del *provider*, del *manufacturer* o dello *user*, a cui siano affidate e impartite istruzioni circa, ad esempio, le operazioni di raccolta dei dati o di conservazione dei medesimi.

L'impostazione che deriva dalla configurazione dei ruoli individuata dalla Proposta non sorprende e anzi riflette quel principio di *accountability* già accennato, la cui applicazione in questo ambito risulta quanto mai appropriata alla materia, dal momento che alloca il rischio presso il soggetto, cioè il titolare del trattamento di dati personali, che meglio è in grado di esaminare il contesto e di valutare come affrontarlo e che sarà chiamato a dimostrare l'adeguatezza delle scelte adottate.

Questo orientamento sembra d'altronde adottato dallo stesso Parlamento europeo, secondo il quale

> la responsabilità dell'operatore è giustificata dal fatto che tale persona sta controllando un rischio associato al sistema di intelligenza artificiale, in modo analogo al proprietario di un'automobile (…) e che, vista la complessità e la connettività di un sistema di intelligenza artificiale, l'operatore sarà, in molti casi, il primo punto di contatto visibile per la persona interessata[39].

4. *Conclusioni*

Nella ricerca di un centro di imputazione di responsabilità per il trattamento di dati personali nelle applicazioni

[39] Cfr. punto n. 10 della Risoluzione citata.

di intelligenza artificiale, gioca ancora una volta un ruolo essenziale il metodo e l'approccio con cui gestire fenomeni – apparentemente – nuovi.

Benché si possa essere tentati (ed effettivamente lo si è stati, come sopra illustrato) di pensare a nuove norme e a nuove soluzioni, finanche attribuendo personalità giuridica al robot, l'indagine sembra essersi oggi indirizzata verso l'applicazione delle norme vigenti in materia di responsabilità e di protezione dei dati personali.

L'interpretazione più in linea con il quadro normativo a disposizione è attualmente quella di ritenere titolari del trattamento di dati personali i soggetti che hanno un effettivo potere decisionale sui dati personali da fornire ai sistemi di intelligenza artificiale, dati che devono essere «relevant, representative, free of errors and complete», in evidente corrispondenza con il Regolamento che richiede che i dati siano sempre aggiornati, corretti, completi.