ranno tecnicamente possibili trapianti di cervello (la prospettiva non sembra così lontana; a Torino ci si dichiara pronti a realizzarli) e, in futuro, quelli di testa su corpo altrui (o viceversa); con conseguenti analoghi problemi persino circa la "identità" del trapiantato (tali trapianti sono attualmente vietati. Ma in caso di violazione del divieto – forse prossimo a venir meno – tutti i richiamati problemi permarrebbero).

Intelligenza Artificiale e protezione dei dati personali

Giusella Finocchiaro

La riflessione giuridica sull'intelligenza artificiale è innanzitutto una riflessione sul metodo. Si tratta di un fenomeno che, seppur nuovo, va analizzato alla luce delle norme già esistenti, in particolare quelle dettate dal nuovo Reg. (UE) 2016/679 in materia di protezione dei dati personali. L'A. valuta la necessità di operare un bilanciamento di interessi tra il diritto alla protezione dei dati e l'esigenza di disporre di un'ingente mole di dati per lo sviluppo di questa nuova tecnologia, interrogandosi altresì sui criteri di allocazione della responsabilità in caso di danni cagionati da applicazioni di intelligenza artificiale.

Sul metodo

L'intelligenza artificiale e le sue applicazioni [1] costituiscono il tema del momento [2]. Esso investe il vivere comune sotto diversi profili: politici, etici, sociologici e naturalmente, come ogni fenomeno sociale, anche sotto il profilo giuridico.

Come sempre il metodo da adottarsi non può che consistere nel qualificare il fenomeno secondo la normativa vigente e nell'individuare le conseguenze dell'eventuale mancato rispetto delle norme, per verificare l'esigenza di una normativa *ad hoc*.

Proprio dal metodo sembra opportuno muovere oggi. Si è diffusa, infatti, la tendenza, esaltata dai mezzi di comunicazione, di richiedere una norma nuova per ogni nuovo fenomeno illecito. L'allarme sociale, assolutamente condivisibile in molti casi, produce quasi automaticamente la richiesta di norme *ad hoc*. Mentre è comprensibile la richiesta di una sicura dichiarazione di illiceità del fenomeno con le eventuali conseguenze sotto il profilo sanzionatorio, l'esigenza di prevedere una norma specifica per ogni nuova fattispecie appare l'esito di una carenza metodologica. Tale ragionamento può essere compreso se svolto da non giuristi, in quanto frutto di mancanza di competenza tecnica, ma non può essere giustificato se svolto, invece, dai giuristi.

Il giurista, infatti, non si può limitare ad applicare la norma all'esatta fattispecie da questa tratteggiata, ma deve utilizzare il principale strumento a sua disposizione che è costituito dall'interpretazione. Dunque deve non solo applicare le disposizioni rilevanti, ma cercare nel sistema giuridico, considerato nella sua complessità, le risposte. Se la corrispondenza fra fattispecie e norma fosse univoca, allora non occorrerebbe alcuna competenza giuridica. Chiunque potrebbe svolgere questo semplice compito. Al contrario, la visione sistematica e il metodo interpretativo sono peculiarità del lavoro del giurista, che va orgogliosamente rivalutato.

Purtroppo il nostro legislatore sempre più frequentemente cede al richiamo mediatico e alla lusinga del consenso che si riscuote con una facile risposta, attraverso il noto approccio della legislazione dell'emergenza. L'ultimo atto in questo senso è la disposizione contenuta nell'art. 8 *ter* [3], D.L. 14 dicembre 2018, n. 135 (meglio noto come, "Decreto Semplificazioni") [4], che definisce la tecnologia della *blockchain* e le applicazioni di *smart contract* [5].

La norma citata, sotto il profilo giuridico, è errata per almeno due ordini di ragioni. In primo luogo, nel dibattito internazionale è ormai un principio consolidato quello della neutralità tecnologica, in virtù del quale la norma giuridica deve essere tecnologicamente neutra e dunque non riferirsi ad una particolare tecnologia, affermata in un particolare

[1] In generale sull'attuale sviluppo dell'intelligenza artificiale e su alcune problematiche, si rinvia ad alcuni recenti rapporti: Centre for European Policy Studies, *Artificial Intelligence: Ethics, Governance and Policy Challenges*, curato da Renda, 2019; AI Now Insititute at New York University, *AI Now Report 2018*.

[2] Specificamente sul tema di questo articolo, v. Robert van den Hoven van Genderen, *Privacy and Data Protection in the Age of Pervasive Technologies in AI and Robotics*, in *Eur. Data Prot. L. Rev.*, III/2017, 338 e segg.; Kuner-Cate-Lynskey-Millard-Loideain-Svantesson, *Expanding the artificial intelligence-data protection debate*, in *International Data Privacy Law*, VIII/2018, 289 e segg.; Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

[3] Questa disposizione non era presente nel testo originario del decreto legge citato, ma è stata introdotta dalla legge di conversione 11 febbraio 2019, n. 12 (in G.U. 12 febbraio 2019, n. 36).

[4] D.L. 14 dicembre 2018, n. 135, *Disposizioni urgenti in materia di sostegno e semplificazione per le imprese e per la pubblica amministrazione*, pubblicato in G.U. del 14 dicembre 2018, n. 290.

[5] L'art. 8 *ter* così dispone: "1. Si definiscono 'tecnologie basate su registri distribuiti' le tecnologie e i protocolli informatici che usano un registro condiviso, distribuito, replicabile, accessibile simultaneamente, architetturalmente decentralizzato su basi crittografiche, tali da consentire la registrazione, la convalida, l'aggiornamento e l'archiviazione di dati sia in chiaro che ulteriormente protetti da crittografia verificabili da ciascun partecipante, non alterabili e non modificabili. 2. Si definisce '*smart contract*' un programma per elaboratore che opera su tecnologie basate su registri distribuiti e la cui esecuzione vincola automaticamente due o più parti sulla base di effetti predefiniti dalle stesse. Gli '*smart contract*' soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate, attraverso un processo avente i requisiti fissati dall'Agenzia per l'Italia digitale con linee guida da adottare entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto. 3. La memorizzazione di un documento informatico attraverso l'uso di tecnologie basate su registri distribuiti produce gli effetti giuridici della validazione temporale elettronica di cui all'art. 41, Reg. (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014. 4. Entro novanta giorni dalla data di entrata in vigore della legge di conversione del presente decreto, l'Agenzia per l'Italia digitale individua gli standard tecnici che le tecnologie basate su registri distribuiti debbono possedere ai fini della produzione degli effetti di cui al comma 3".

momento storico. I vantaggi della neutralità tecnologica sono evidenti: il diritto non condiziona il mercato, favorendo questa o quella tecnologia; non condiziona lo sviluppo della tecnica e non deve rincorrerla. L'approccio del diritto, nella neutralità tecnologica, è "funzionale". Non si concentra sul "cosa", ma sul "come". Legiferare in questo modo può essere più difficile, perché non si norma l'oggetto, ma la funzione. Questo principio è stato, ad esempio, affermato dall'UNCITRAL nella regolazione sulla firma elettronica, che appunto è fondata sui principi della "neutralità tecnologica" e dell'"equivalenza funzionale". Così si stabiliscono dei principi generali che possono rimanere invariati per un certo periodo di tempo, senza essere vincolati al mutamento delle tecnologie[6].

La norma italiana, invece, tenta di descrivere la tecnologia della *blockchain* e le applicazioni di *smart contract*, allo stato attuale, cristallizzandoli.

Oltre a ciò, effettua un'ulteriore operazione inutile e, anzi, dannosa. Attribuisce agli *smart contract*, dopo averli inutilmente definiti, secondo quel processo contrario al principio della neutralità tecnologica che prima si è illustrato, la forma scritta, solo se le parti sono identificate secondo un processo che dovrà essere disciplinato da AgID. Ora, l'identificazione delle parti, secondo i principi generali, non è requisito del contratto. Oltre a ciò, la forma scritta del documento informatico è materia già ampiamente disciplinata dal Codice dell'amministrazione digitale[7] che certamente non richiede ulteriori precisazioni.

Il tema che qui ci occupa, intelligenza artificiale e *privacy*, va dunque inquadrato nel contesto attuale di disordine intellettuale e l'obiettivo che si cercherà di perseguire sarà quello di razionalizzare le esigenze e le risposte normative.

L'Intelligenza Artificiale e l'approccio del legislatore europeo

L'intelligenza artificiale costituisce oggi uno strumento ormai diffuso, benché ancora suscettibile di grande espansione. Si tratta, dunque, di una realtà e non di una eventualità futura. "L'intelligenza artificiale non è fantascienza: fa già parte delle nostre vite"[8]. Le applicazioni di intelligenza artificiale sono moltissime e a titolo esemplificativo si possono annoverare: *Natural Language Processing, Speech Recognition*, *Virtual Agent*, *Machine Learning, AI-optimized Hardware, Decision Management*, *Deep Learning, Biometrica, Robotic Process Automation* e *Text Analytics*[9].

L'intelligenza artificiale[10] si basa sui dati. Una delle ragioni per le quali, pur essendo stata ampiamente studiata già molti anni fa[11] e pur essendo sotto molti aspetti già matura, non era una tecnologia ancora applicabile, era costituita dall'assenza di una grande quantità di dati a disposizione.

Oggi i dati sono disponibili e spesso sono forniti dagli stessi utenti, soprattutto tramite i *social network* e i motori di ricerca. La mente vola subito a Facebook, a Instagram e a Google, ma una mole di dati addirittura superiore è quella a disposizione dei grandi attori del *web* cinesi, come Ali Baba e Baidu, i quali ci appaiono lontani per la barriera linguistica che naturalmente ci separa.

Si stimano in miliardi gli utenti che quotidianamente forniscono dati, più o meno consapevolmente, in tutto il mondo[12].

L'IA si nutre di dati[13] e ora i dati sono certamente disponibili, spesso addirittura gratuitamente. Il nuovo petrolio, secondo la celebre metafora dell'*Economist*[14], costituisce la risorsa della nuova economia digitale[15].

---

[6] Sul tema v. il mio articolo, *Riflessioni su diritto e tecnica*, in *Dir. Inf.*, IV-V/2012, 831 e segg.

[7] D.Lgs. 7 marzo 2005, n. 82, successivamente modificato e integrato con il D.Lgs. 22 agosto 2016, n. 179 e poi con il D.Lgs. 13 dicembre 2017, n. 217.

[8] 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 aprile 2018, 1.

[9] Per maggiori approfondimenti, si rinvia al mio contributo *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. Trim. Dir. Proc. Civ.*, II/2018, 441-460. V. inoltre alcuni atti di fonte europea rilevanti in tema di intelligenza artificiale: Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)); Comunicazione della Commissione, *Piano di coordinamento per l'IA*, e Allegato, *Piano coordinato per lo sviluppo e l'utilizzo dell'intelligenza artificiale "*Made in Europe*"*, COM(2018) 795, 7 dicembre 2018; Consiglio dell'Unione europea, *Conclusioni dell'11 febbraio 2019 relative al "Piano coordinato sull'intelligenza artificiale"*; Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale, 2018/2088(INI).

[10] Nella citata Comunicazione della Commissione europea del 25 aprile 2018, si rinviene una definizione di intelligenza artificiale, secondo la quale l'espressione "indica sistemi che mostrano un comportamento intelligente analizzando il proprio ambiente e compiendo azioni, con un certo grado di autonomia, per raggiungere specifici obiettivi" (1).

[11] La nascita dell'intelligenza artificiale si fa risalire alla Conferenza di Dartmouth (Hanover, New Hampshire) del 1956. V. 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: McCarthy-Minsky-Rochester-Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, https://aaai.org/ojs/index.php/aimagazine/article/view/1904/1802.

[12] Secondo il *Global Digital Report 2019* di *We are Social* e *Hootsuite* (note agenzie di *social media management*), sono 4.39 miliardi gli utenti che si collegano a Internet nel 2019, con un aumento di 366 milioni (9%) rispetto a gennaio 2018; sono invece 3.48 miliardi gli utenti che frequentano *social media*, con un totale mondiale in crescita di 288 milioni (9%) rispetto allo scorso anno (il *report* integrale è disponibile al seguente *link* https://datareportal.com/reports/digital-2019-global-digital-overview, consultato in data 25 marzo 2019). Interessante è anche lo spaccato che offrono Lori Lewis e Chadd Callahan di *Cumulus Media* che mostra le attività svolte su varie piattaforme *web* nell'intervallo di un minuto: ad esempio, è stato rilevato che, nel 2018, ogni 60 secondi sono state effettuate 3.7 milioni di ricerche su Google; 973.000 accessi a Facebook; 481.000 post su Twitter; 187 milioni di *e-mail* inviate; 38 milioni di messaggi inviati attraverso il servizio *chat* di WhatsApp; 4.3 milioni di video visualizzati su YouTube (tale analisi, sotto forma di infografica, è ripresa da diverse testate, tra cui il Sole24Ore, ed è disponibile al seguente *link https://www.infodata.ilsole24ore.com/2018/05/17/cosa-accade-internet-un-minuto/*).

[13] Cfr. Mantelero, *Report on Artificial Intelligence. Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, Commissione consultiva della Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, 25 gennaio 2019.

[14] *The Economist*, *The world's most valuable resource is no longer oil, but data*, pubblicato il 6 maggio 2017.

[15] Cfr. Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. Inf*, 4-5/2018, 689-726.

È palese che il campo di gioco è quanto meno continentale: gli Stati Uniti e la Cina hanno i mercati più ampi e le tecnologie più avanzate e dunque giocano il ruolo più importante. L'Europa cerca di essere il terzo attore e di consolidare il mercato digitale europeo, ma il singolo Stato non può svolgere alcun ruolo. Le scelte politiche, economiche e quindi giuridiche sono necessariamente europee.

I dati personali costituiscono al tempo stesso la risorsa sulla quale si basa l'economia digitale e l'oggetto del diritto alla protezione dei dati personali, riconosciuto dall'art. 8 della Carta dei diritti fondamentali dell'Unione europea.

L'azione dell'Unione europea è volta a favorire un nuovo mercato, il mercato unico digitale europeo. In questo senso recentemente militano il Reg. (UE) 2016/679 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 Dir. 95/46/CE" [16] (nel prosieguo, per brevità, "Regolamento") e il Reg. (UE) 2014/910 del Parlamento europeo e del Consiglio del 23 luglio 2014, "in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE" [17].

I due regolamenti, considerati in una prospettiva unitaria, indicano chiaramente l'intento del legislatore europeo di disegnare un mercato unico digitale, rimuovendo gli ostacoli giuridici costituiti dalla disomogeneità delle norme applicabili. Si tratta, ed è certamente superfluo intrattenersi sul punto, di regolamenti e non di direttive: dunque direttamente applicabili e volti a costituire un sistema di riferimento giuridico uniforme ed omogeneo.

Oltre a ciò, emerge, inoltre, la volontà del legislatore europeo di consolidare la posizione europea nel quadro globale, affermando un approccio unitario, che declina i principi fondamentali statuiti dalla Carta dei diritti fondamentali dell'Unione europea.

Come con molti altri atti normativi europei in questo settore, con esso si intende rafforzare la fiducia nelle transazioni elettroniche nel mercato interno, assicurando la protezione dei dati personali, e aumentando così l'efficacia dei servizi on line pubblici e privati nell'Unione europea. Fin dai primi studi della Commissione europea sul commercio elettronico negli anni '90 [18], l'obiettivo è stato quello di rafforzare la fiducia, innanzitutto del consumatore, per favorire lo sviluppo del mercato.

Mercato digitale e protezione dei dati personali

Dunque il legislatore europeo si muove fra due diverse esigenze: quella di favorire lo sviluppo del mercato digitale europeo, il cui bene di scambio è costituito dall'informazione e dai dati personali, e quella di tutelare la persona nei suoi diritti fondamentali.

Da questa duplice esigenza nasce il Reg. europeo 2016/679, il quale, fin dal titolo, chiarisce il duplice oggetto: la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione dei dati.

In questa tensione si sviluppa la disciplina dettata dal Regolamento europeo che si snoda intorno al principio del necessario bilanciamento di diritti e interessi.

Nei numerosi atti delle istituzioni europee concernenti l'intelligenza artificiale si legge questo tentativo di bilanciamento. Condivisione e disponibilità dei dati sono infatti annoverate tra le azioni strategiche volte a promuovere lo sviluppo dei sistemi di intelligenza artificiale, purché tali

---

[16] Reg. (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 Dir. 95/46/CE (regolamento generale sulla protezione dei dati), pubblicato in G.U.U.E. L 119/1 del 4 maggio 2016. In generale, sul Regolamento v. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. Impr.*, III/2017, 723-733; Bassini, *La svolta della privacy europea: il nuovo pacchetto sulla tutela dei dati personali*, in *Quad. Cost.*, 2016, 587-590; Busia-Liguori-Pollicino (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali*, Roma, Aracne, 2016; Califano, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in Califano-Colapietro (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, Editoriale Scientifica, 2017; Califano, *Privacy: affermazione e pratica di un diritto fondamentale*, Editoriale Scientifica, Napoli, 2016; Cuffaro, *Il diritto europeo alla protezione dei dati personali*, in *Contr. Impr.*, III/2018, 1098-1119; Finocchiaro, *Introduzione al Regolamento Europeo sulla protezione dei dati*, in *Leggi Civ. Comm.*, I/2017, 1-18; 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; Piraino, *Il Regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Leggi Civ. Comm.*, II/2017, 369-409; 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; Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679*, Torino, 2016; Riccio-Scorza-Belisario (a cura di), *GDPR e Normativa Privacy. Commentario*, Milano, Ipsoa, 2018; Sica-D'Antonio-Riccio (a cura di), *La nuova disciplina europea della privacy*, Padova, 2016; Stanzione, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione*, in *Europa e Dir. Priv.*, IV/2016, 1249-1264; Tosi (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, 2019.

[17] Pubblicato in G.U.U.E. L 257 del 28 agosto 2014. Il Regolamento è, in sigla, comunemente denominato "eIDAS", dove "e" sta per "electronic", "ID" per "identification", "A" per "authentication" e "S" per "signature". Per un commento si rinvia al mio, *Una prima lettura del regolamento europeo eIDAS: identificazione on line, firme elettroniche e servizi fiduciari*, in *Leggi Civ. Comm.*, 2015, 419 e segg., nonché al volume da me curato con Delfini, *Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, commento al regolamento UE 910/2014*, Torino, 2017.

[18] Cfr. Comunicazione della Commissione delle Comunità europee al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni, *Un'iniziativa europea in materia di commercio elettronico*, COM(97) 157, 15 aprile 1997, ove la creazione della fiducia figura tra i primi obiettivi nello sviluppo del commercio elettronico: "Perché possa svilupparsi il commercio elettronico, i consumatori e le imprese debbono essere certi che le rispettive transazioni non siano intercettate o modificate, che il venditore e l'acquirente siano effettivamente coloro che affermano di essere e che siano accessibili meccanismi per effettuare le transazioni legali e sicuri. La creazione di tale fiducia è la condizione essenziale affinché le imprese e i consumatori possa adottare il commercio elettronico" (22). Analogamente, nella Comunicazione della Commissione delle Comunità europee al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni, *Garantire la sicurezza e l'affidabilità nelle comunicazioni elettroniche. Verso la definizione di un quadro europeo in materia di firme digitali e di cifratura*, COM(97) 503, 8 ottobre 1997, si legge che "the present communication aims at developing such a policy framework with a view to (...) stimulating and enabling users in all economical sectors to benefit from the opportunities of the global information society which can only be fully exploited if based on a framework of trust and security" (2 "Table of contents").

obiettivi vengano perseguiti nel rispetto dei diritti delle persone e dei valori europei. La già citata COM(2018) 795 della Commissione europea sottolinea la necessità di realizzare uno "spazio dei dati europeo"[19], affermando espressamente che "affinché l'IA possa svilupparsi ulteriormente è necessario un valido ecosistema dei dati basato sulla fiducia, sulla disponibilità dei dati e sull'infrastruttura" e che l'accesso ai dati "è un elemento fondamentale per un panorama di IA competitivo"[20]. Si specifica però che l'Unione europea dovrebbe agevolare tale accesso ai dati "nel pieno rispetto delle norme sulla protezione dei dati personali". Analoghi concetti sono espressi anche nell'allegato alla menzionata comunicazione: "l'attuale diffusione dell'IA è alimentata dalla disponibilità di grandi *set* di dati, abbinata all'aumento della potenza di calcolo e della connettività. Mettere dati sicuri, solidi e di qualità a disposizione di una vasta gamma di utenti a livello transfrontaliero è uno dei fondamenti della politica europea. L'apertura ai flussi di dati internazionali continuerà a essere garantita, nel pieno rispetto della normativa dell'UE per la protezione dei dati personali"[21]. Infine, sul punto, nella citata Risoluzione del Parlamento europeo del 12 febbraio 2019 è riconosciuto, da un lato, che lo sviluppo di prodotti e servizi basati sull'intelligenza artificiale necessita del libero flusso di dati e dell'accessibilità ai dati all'interno dell'Unione europea e, dall'altro lato, che occorre garantire un elevato livello di sicurezza, protezione e riservatezza dei dati utilizzati per la comunicazione tra persone e *robot* e intelligenza artificiale, invitando "la Commissione a garantire che qualsiasi futuro quadro normativo dell'Unione europea in materia di intelligenza artificiale garantisca la riservatezza e la confidenzialità delle comunicazioni, la protezione dei dati personali, compresi i principi di legalità, equità e trasparenza, la protezione dei dati fin dalla progettazione e per impostazione predefinita, la limitazione delle finalità, la limitazione della conservazione, la precisione e la minimizzazione di dati, nel pieno rispetto del diritto dell'Unione in materia di protezione dei dati"[22].

Un tentativo di risolvere la tensione fra l'esigenza di utilizzare i dati per lo sviluppo di nuove attività e la protezione delle persone fisiche con riguardo ai loro dati personali, è quello di formulare un nuovo approccio al problema, basato sull'etica[23]. La richiamata Comunicazione della Commissione europea del 25 aprile 2018 pone in primo piano la necessità di promuovere le iniziative in tema di intelligenza artificiale nel rispetto di un "quadro etico basato sui valori dell'Unione e coerente con la Carta dei diritti fondamentali dell'Unione europea". In particolare, nell'ambito della strategia europea volta a rendere l'Europa competitiva sotto il profilo dello sviluppo e dell'adozione di sistemi di intelligenza artificiale, è stata prevista l'elaborazione di "un progetto di orientamenti etici per l'intelligenza artificiale" in cooperazione con il Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie[24].

I principi fondamentali

Pare utile ora passare in rassegna i principi fondamentali del Regolamento europeo per verificare quali siano le eventuali criticità interpretative con riferimento alle applicazioni di intelligenza artificiale.

Dati personali e dati anonimi

Muovendo dalla definizione di dato personale[25], si può constatare che la maggior parte delle informazioni è costituita da dati personali.

Al contrario è assai difficile individuare informazioni che non siano dati personali. Benché l'oggetto del diritto alla protezione dei dati personali sia l'informazione o il dato, dato e informazione sono termini non coincidenti. Più precisamente, il dato è la fonte dell'informazione, nel quale questa è contenuta e dal singolo dato o dall'insieme di dati l'informazione può essere estratta o inferita. Ma l'informazione, a rigore, non coincide con il dato stesso. L'informazione è elaborazione del dato.

Il dato anonimo è solo quello che, in origine o a seguito di trattamento, non può essere collegato a persona fisica. Nella società dell'informazione, in cui raccogliere dati o catalogare informazioni, operando collegamenti non prevedibili dagli interessati, è divenuta attività quanto mai diffusa, la qualificazione del dato anonimo assume una crescente importanza. L'elemento chiave, che segna la distinzione tra dato personale e dato anonimo, è la collegabilità. La collegabilità dipende da numerosi fattori: dal soggetto che opera il collegamento, dal contesto nel quale esso opera e dal dominio di conoscenze che questi ha a sua disposizione. L'anonimato dunque è relativo: si configura in relazione a determinati soggetti o a circostanze specifiche, caso per caso[26].

La definizione di dato anonimo non è nel Regolamento europeo, ma nel considerando n. 26[27], mentre nel D.Lgs.

---

[19] L'espressione era già contenuta nella precedente Comunicazione della Commissione europea, *L'intelligenza artificiale per l'Europa*, COM(2018) 237, 25 aprile 2018, 11.

[20] Così 6 e 7.

[21] Cfr. allegato della Comunicazione della Commissione COM(2018) 795, intitolato *Piano coordinato per lo sviluppo e l'utilizzo dell'intelligenza artificiale "*Made in Europe*"*, 14.

[22] Cfr. Risoluzione del Parlamento europeo del 12 febbraio 2019 su una politica industriale europea globale in materia di robotica e intelligenza artificiale, paragrafo P, 125 e 128.

[23] Un esempio è offerto da *La Carta etica europea sull'uso dell'intelligenza artificiale nei sistemi giudiziari e in ambiti connessi*, adottata dalla *European Commission for the Efficiency of Justice* (organismo del Consiglio d'Europa) il 3-4 dicembre 2018. Si tratta del primo documento con cui vengono espressi alcuni principi etici alla cui osservanza lo sviluppo e l'adozione di sistemi di intelligenza artificiale devono essere subordinati. Tra questi principi vengono indicati, in particolare, il rispetto dei diritti fondamentali dell'uomo, la non discriminazione e il controllo dell'utente sui dati.

[24] "Il progetto affronterà temi quali il futuro del lavoro, l'equità, la sicurezza, l'inclusione sociale e la trasparenza degli algoritmi. Più in generale esso esaminerà l'impatto sui diritti fondamentali, tra cui la vita privata, la dignità, la tutela dei consumatori e la non discriminazione. (...) Saranno invitati a contribuire le imprese, gli istituti accademici e altre organizzazioni della società civile. In parallelo, la Commissione continuerà il proprio lavoro finalizzato al progresso dell'etica a livello internazionale" (16).

[25] Ai sensi dell'art. 4, n. 1 del Regolamento, dato personale è "qualsiasi informazione riguardante una persona fisica identificata o identificabile ('interessato')".

[26] Si rinvia al volume da me curato, *Diritto all'anonimato. Anonimato, nome, identità personale*, in *Trattato di diritto commerciale e di diritto pubblico dell'economia*, Galgano (diretto da), Padova, 2008.

[27] Il considerando n. 26 del Regolamento recita: "I principi di

30 giugno 2003, n. 196 la definizione era contenuta all'art. 4, 1° comma, lett. n)[28], poi abrogato ad opera del D.Lgs. 10 agosto 2018, n. 101 recante le disposizioni per l'adeguamento dell'ordinamento nazionale al Reg. (UE) n. 2016/679[29].

La definizione di pseudonimizzazione[30], invece contenuta nel Regolamento europeo, non è rilevante per individuare i principi fondamentali alla base del trattamento. La pseudonimizzazione è una misura di sicurezza, ma non influenza la base giuridica del trattamento.

Dunque, se le applicazioni di intelligenza artificiale utilizzano dati non anonimi si applica il Regolamento.

Se utilizzano dati anonimi, il Regolamento non si applica, ma occorre ricordare che la qualificazione di dato anonimo è dinamica e soggetta a verifica continua, conseguente all'evoluzione delle tecnologie: dipende fortemente dalle risorse, soprattutto tecnologiche, disponibili.

La qualità dei dati

L'IA si nutre soprattutto di grandi masse di dati.

Dunque, la qualità dei dati diviene essenziale. Da dati qualitativamente non corretti, non possono che scaturire elaborazioni non corrette, secondo il noto principio "garbage in, garbage out". La qualità dei dati è un principio sancito dal Regolamento[31] e già presente nella Dir. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[32]. Sulla base di questo principio il titolare è tenuto a garantire che i dati trattati siano "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati; esatti e, se necessario, aggiornati", dovendo essere "adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati", nonché "conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati"[33].

È evidente il contrasto che emerge, da un lato, tra l'esigenza di disporre di un'ingente mole di dati ai fini dello sviluppo di sistemi di intelligenza artificiale e, dall'altro lato, la necessità di osservare il principio di minimizzazione dettato dal Regolamento secondo cui il trattamento dovrebbe avere ad oggetto soltanto i dati strettamente necessari e pertinenti rispetto alle finalità perseguite. Tale tensione impone necessariamente un bilanciamento di interessi che vede contrapposti il diritto alla protezione dei dati personali e l'esigenza di disporre dei dati personali per sviluppare le applicazioni di intelligenza artificiale.

Ci si è chiesti[34] se il titolare del trattamento possa essere la stessa applicazione di intelligenza artificiale o, se si preferisce, il *robot*. La definizione di titolare[35] contenuta nel Regolamento chiaramente indica che il titolare debba essere persona giuridica o fisica o comunque soggetto giuridico. Se l'applicazione non ha soggettività giuridica, evidentemente, non può essere titolare. Ma l'attribuzione di soggettività giuridica deve corrispondere ad una precisa e consapevole scelta metodologica e fondare un nuovo approccio al tema della responsabilità. Se all'applicazione non viene attribuita una disponibilità economica e se non viene ridisegnato un regime di responsabilità che prescinda da elementi soggettivi, evidentemente non riferibili all'applicazione, l'attribuzione di soggettività giuridica alle applicazioni di intelligenza artificiale e ai *robot* diviene un atto di compiacimento romantico, fine a sé stesso, se non dannoso.

Lo stesso argomento si può svolgere per la designazione del *robot* quale responsabile del trattamento[36]. Anche in questo caso la designazione del responsabile richiede la soggettività giuridica del medesimo, soggettività che non può essere tuttavia fine a sé stessa, ma che si deve inserire in un nuovo modello di responsabilità.

Decisioni automatizzate e diritto di spiegazione

Grandemente sopravvalutato è quanto disposto dal Regolamento con riguardo alle decisioni automatizzate.

L'art. 22 del Regolamento dispone infatti che "l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compre-

---

protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato". Si noti che la definizione di dato anonimo non era presente neppure nella previgente Dir. 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, abrogata ad opera del citato Regolamento a partire dal 25 maggio 2018.

[28] La definizione di dato anonimo era la seguente: "il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile".

[29] D.Lgs. 10 agosto 2018, n. 101, "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Reg. (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 Dir. 95/46/CE (regolamento generale sulla protezione dei dati)", pubblicato in G.U. Serie Generale n. 205 del 4 settembre 2018.

[30] Ai sensi dell'art. 4, n. 5 del Regolamento, per pseudonimizzazione si intende "il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

[31] Cfr. art. 5, Reg.

[32] La direttiva dedicava l'intera Sez. VI a tale principio, rubricandola "Principi relativi alla qualità dei dati".

[33] Completano il quadro dei principi applicabili al trattamento i principi di liceità, correttezza e trasparenza, secondo i quali i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (art. 5, 1° comma, lett. a); di limitazione della finalità, secondo cui i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità (art. 5, 1° comma, lett. b); di integrità e riservatezza, secondo i quali i dati devono essere trattati in maniera da garantire un'adeguata sicurezza mediante misure tecniche e organizzative adeguate (art. 5, 1° comma, lett. f).

[34] Cfr. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, cit.

[35] Il titolare del trattamento 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" (art. 4, n. 7, Reg.).

[36] Ai sensi dell'art. 4, n. 8, Reg., responsabile del trattamento è "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

sa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona" (1º comma).

La norma non vieta le decisioni automatizzate, bensì di assumere decisioni unicamente con sistemi automatizzati[37].

Come è accaduto per il diritto all'oblio, sebbene in questo caso in un ambito più ristretto di commentatori, si è diffusa una convinzione errata, ritenuta vera dai più. Nel caso del diritto all'oblio, infatti, la convinzione e l'aspettativa sociale è che si tratti di un diritto *ad nutum*, esercitabile dall'interessato in qualunque circostanza.

Nel caso delle decisioni automatizzate la convinzione generale è che il Regolamento introduca un divieto generale. Essa, come nel caso del diritto all'oblio, è basata sulla lettura della norma contenuta nelle precedenti versioni del Regolamento[38] che non sono state approvate. La comunicazione che è stata effettuata sulle norme ancora in bozza ha generato il convincimento che il Regolamento, poi diversamente formulato, contenga disposizioni che non sono state approvate nella loro formulazione originaria, ma che invece sono state sottoposte ad una negoziazione serrata.

Parimenti, non esiste un pieno diritto alla spiegazione nell'art. 15 del Regolamento.

Non si tratta, infatti, di un diritto alla spiegazione ma di un diritto ad avere informazioni ai sensi dell'art. 15, 1º comma, lett. h), che limita il diritto dell'interessato ad accedere all'informazione concernente "l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, par. 1 e 4, e, almeno in tali casi, (ad ottenere) informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato".

Qui si legge una mancata sintonia fra il considerando n. 71 e la norma appena citata, disponendo il primo "il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione".

La finalità del trattamento

Un altro problema rilevante è quello che concerne la finalità del trattamento. Come è noto, la legittimità del trattamento si misura non soltanto con riguardo al dato che viene trattato, ma anche con riguardo alla finalità del trattamento di quel dato.

Ora, pur essendo i dati da trattarsi individuati, possono non essere individuate le finalità di trattamento nel caso di dati inferiti, o secondo un'espressione più corretta, informazioni inferite dai dati[39]. La finalità del trattamento in questo caso non è chiara fin dal principio, ma si va definendo con il trattamento stesso e dunque non essendo nota, non può essere comunicata all'interessato.

La responsabilità

Il tema della protezione dei dati personali nel caso di applicazioni di intelligenza artificiale non si può disgiungere da quello della responsabilità[40].

La questione che più frequentemente si pone è chi sia il soggetto responsabile nel caso di danni cagionati da applicazioni di intelligenza artificiale. In particolare l'attenzione si focalizza sui casi in cui l'esito dell'elaborazione effettuata dall'applicazione di intelligenza artificiale non sia del tutto controllabile 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.

Si discute se sia l'autore del programma, il produttore, il

---

[37] Come evidenziato da Pellecchia, *Profilazione e decisioni automatizzate al tempo della* black box society*: qualità dei dati e leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Leggi Civ. Comm.*, 5/2018, 1224-1225, sul punto è emerso un dibattito concernente l'impiego dell'avverbio "unicamente" utilizzato per delimitare l'ambito dei trattamenti vietati dal Regolamento. La dottrina è infatti divisa tra coloro che ravvisano un deficit di protezione degli interessati, sostenendo che l'utilizzo di tale avverbio comporterebbe la sottrazione al divieto di tutte quelle decisioni in cui sia ravvisabile un intervento umano, benché minimo; e coloro che, invece, ritengono – ai fini di tale esonero – che l'intervento umano debba essere significativo. Pare che quest'ultima sia la posizione condivisa dal Comitato europeo per la protezione dei dati che, nelle sue *Guidelines on Automated individual decision-making and Profiling for purposes of Regulation 2016/679* (da ultimo aggiornate il 6 febbraio 2018), esclude che il titolare del trattamento possa eludere il divieto in esame "by fabricating human involvement" (21). Cfr., in senso fra loro opposto, Wachter-Mittelstadt-Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, Volume 7, Issue 2, May 2017, 76-99, *https://doi.org/10.1093/idpl/ipx005* e Malgieri-Comandè, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, in *International Data Privacy Law*, vol. 7, issue 4, 243-265.

[38] Il Parlamento europeo aveva emendato, in prima lettura, il testo del Regolamento proposto dalla Commissione europea, prevedendo all'art. 20 (rubricato in origine "Misure basate sulla profilazione"), che la profilazione idonea a produrre effetti giuridici sull'interessato o a incidere sui suoi interessi, diritti e libertà non potesse essere basata "unicamente o in modo predominante" sul trattamento automatizzato, bensì che dovesse includere obbligatoriamente "una valutazione umana, compresa una spiegazione della decisione conseguita dopo tale valutazione" (5º comma). È dunque evidente che, nella versione non definitiva del Regolamento, era vietata non solo la decisione basata unicamente sul trattamento automatizzato (come oggi previsto), ma anche quella decisione in cui l'apporto umano risultasse minore rispetto all'impiego di sistemi automatizzati. Inoltre era accordato agli interessati il "diritto di ottenere una valutazione umana e una spiegazione della decisione", diritto che – nel testo poi approvato del Regolamento e oggi vigente – è stato limitato al "diritto di ottenere l'intervento umano" (art. 22, 4º comma) e al diritto di accedere ad "informazioni significative sulla logica utilizzata" nell'ambito di un processo decisionale automatizzato (art. 15, 1º comma, lett h).

[39] Se ne è occupato il Consiglio d'Europa, nella dichiarazione del 13 febbraio 2019 intitolata *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*, in cui ha evidenziato l'idoneità dei dati "derivati" di influenzare non solo i comportamenti ma anche le conoscenze, le scelte, le opinioni e, in generale, la capacità di autodeterminazione degli individui: "These data are used to train machine-learning technologies to prioritise search results, to predict and shape personal preferences, to alter information flows, and, sometimes, to subject individuals to behavioural experimentation" (par. 4). Il Consiglio d'Europa prosegue affermando che "computational means make it possible to infer intimate and detailed information about individuals from readily available data. This supports the sorting of individuals into categories, thereby reinforcing different forms of social, cultural, religious, legal and economic segregation and discrimination. It also facilitates the micro-targeting of individuals based on profiles in ways that may profoundly affect their lives" (par. 6).

[40] In tema di responsabilità delle applicazioni di intelligenza artificiale v. Ruffolo, *Intelligenza artificiale e responsabilità*, Milano, Giuffrè, 2018; Santosuosso-Boscarato-Caroleo, Robot *e diritto: una prima ricognizione*, in *Nuova Giur. Comm.*, 28, VII-VIII/2012, 494-516.

venditore o l'utilizzatore che ne trae vantaggio. Si discute altresì, come si è accennato, se sia opportuno introdurre la soggettività giuridica dell'applicazione o se si preferisce, del *robot*[41]. Il dibattito si snoda anche fra la conclamata esigenza di introdurre nuove norme e la asserita possibilità di limitarsi invece ad applicare, con una nuova prospettiva, le norme già esistenti.

Pur ritenendo, come già illustrato, che non ogni fenomeno nuovo richieda una nuova norma, penso che il tema della responsabilità nelle applicazioni di intelligenza artificiale richieda un approccio nuovo e basato su un modello concettuale differente: per rubare un termine alla tecnologia di cui si discute, "disruptive". Occorre superare il paradigma basato sull'errore e sulla colpa e, invece, affrontare il problema sotto il profilo dell'allocazione del rischio. In altri termini, non è rilevante chi sbagli e la ricerca dell'errore è attività costosa e dispendiosa che può essere superata. Occorre invece prevedere meccanismi di allocazione del costo del danno cagionato su quei soggetti che astrattamente potrebbero essere responsabili, ad esempio mediante la costituzione di un fondo al quale attingere, prescindendo dall'individuazione delle modalità dell'incidente o dell'errore. Analogo meccanismo è stato previsto nel circuito delle carte di credito, per il caso di clonazione o furto.

Uno degli obiettivi perseguiti con questo tipo di sistema di allocazione del rischio è immediatamente evidente ed è quello di rassicurare i potenziali utilizzatori sul fatto che, a prescindere dagli esiti di una costosa ricerca sull'errore, otterranno un risarcimento.

Come è noto, il Regolamento ha introdotto un nuovo approccio alla responsabilità. Si tratta del cosiddetto principio di *accountability*. Il termine *accountability* può essere tradotto con responsabilità e, insieme, prova della responsabilità. Il titolare del trattamento deve essere in grado di dimostrare che ha adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi, che per ragioni di sintesi si possono pensare analoghi a quelli utilizzati in Italia nell'applicazione del D.Lgs. 8 giugno 2001, n. 231. Le norme del Regolamento sull'*accountability* hanno dunque lo scopo di promuovere l'adozione di misure concrete e pratiche, trasformando i principi generali della protezione dei dati in politiche e procedure concrete, nel rispetto delle leggi e dei regolamenti applicabili. Il titolare del trattamento deve anche garantire l'efficacia delle misure adottate e dimostrare, su richiesta, di aver intrapreso tali azioni. Quindi, previsione della responsabilità e prova delle misure adottate per fare fronte alla responsabilità. In altre parole, l'*accountability* è un meccanismo a due livelli: da un lato, l'attuazione di misure e procedure, dall'altro lato, la conservazione delle relative prove.

Il principio dell'*accountability* comporta, pertanto, che sia il titolare del trattamento a determinare le misure di sicurezza adeguate al trattamento dei dati personali che effettua, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche"[42].

In questo come in altri casi, il legislatore affida al titolare l'onere di individuare in che modo adempiere alle prescrizioni dettate dalla norma, calandole nella fattispecie concreta, assumendosi la responsabilità non solo dell'implementazione, ma anche della valutazione. Così per le disposizioni in materia di sicurezza l'applicazione del principio di *accountability* sancito dal Regolamento europeo ha comportato l'abrogazione anche del disciplinare tecnico in materia di misure minime di sicurezza previsto dal Codice per la protezione dei dati personali (all. B), dichiarata dal D.Lgs. n. 101/2018. Così, ancora, al principio di *accountability* è necessario riferirsi per una lettura più piena e compiuta della base giuridica del legittimo interesse[43], che impone al titolare una valutazione fra il legittimo interesse al trattamento e gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali.

Con riguardo alle applicazioni di intelligenza artificiale un tentativo di formulare un modello di responsabilità non può prescindere da una combinazione, da un lato, dall'*accountability* del titolare del trattamento e, dall'altro, da una formulazione che prescinda dagli elementi soggettivi, nonché dall'individuazione dell'errore.

Conclusioni

Infine non può tacersi un'ultima considerazione.

Il Regolamento europeo sulla protezione dei dati personali intende superare l'approccio che risale ad almeno venti anni fa con la cosiddetta "Direttiva madre" in materia di trattamento dei dati personali, la già menzionata Dir. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Essa aveva recepito un dibattito culturale e un pensiero dottrinale sviluppatosi nei decenni precedenti e delineato un modello statico di trattamento dei dati personali, ormai superato. Diversa all'epoca anche la tecnologia: era un mondo privo di *smart phone*, *social network* e motori di ricerca. Il modello normativo individuava un unico scambio di dati: dall'interessato al titolare del trattamento. La realtà dei *social network* e dei motori di ricerca, di un modo digitalmente sempre interconnesso, invece, si basa su un modello di condivisione e di cogestione di dati e informazioni, destinati fin dall'origine ad una circolazione globale.

Il Regolamento europeo viene emanato in conseguenza di un cambiamento di scenario tecnologico nell'ambito in particolare delle comunicazioni e con immediate ricadute sociali.

Il Regolamento europeo non tiene conto, però, delle ap-

[41] Cfr. Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)), ove in particolare la Commissione europea è invitata a valutare talune soluzioni giuridiche possibili in relazione al regime di responsabilità dei *robot*, tra cui "l'istituzione di uno *status* giuridico specifico per i *robot* nel lungo termine (...) nonché eventualmente il riconoscimento della personalità elettronica dei *robot*" (par. 59, lett. f).

[42] Così l'art. 32, Reg.

[43] Art. 6, 1° comma, lett. f), Reg.

plicazioni di intelligenza artificiale e dei Big Data, cioè dei trattamenti di dati di massa.

La logica del Regolamento è sempre basata sul dato personale rispetto al cui trattamento una determinazione viene espressa dal singolo individuo: l'interessato controlla e, in taluni casi, gestisce il suo dato seguendone la circolazione. Altre basi giuridiche concorrono a legittimare il trattamento dei dati personali, ma il modello culturale, prima ancora che giuridico, sul quale si base il Regolamento è quello dell'autodeterminazione. Tale logica, benché mitigata dall'*accountability*, non può essere applicata a grandi masse di dati, ai Big data. Non è possibile pensare ad una gestione di tipo individuale dei dati, tanto meno se basata sul consenso. Il consenso, astrattamente il miglior modello possibile, si rivela spesso non adeguato nel fornire una tutela effettiva ed inefficace. Ciò tanto più se ci si confronta con applicazioni di intelligenza artificiale basate sui Big data, nelle quali la determinabilità a priori dei processi di elaborazione non è scontata e nelle quali la finalità del trattamento sovente non è chiara.

Sembra quasi che si tenti di governare le onde del mare goccia a goccia[44], individualmente considerando la goccia. Appare dunque necessario ripensare il modello culturale di riferimento.

Attività contrattuale e Intelligenza Artificiale

Francesco Di Giovanni

L'attitudine delle ''macchine intelligenti'' a sostituire l'uomo in attività implicanti l'impiego di facoltà sensoriali, cognitive ed intellettive comporta che l'attività consistente nel concludere ed eseguire contratti veda l'intervento dell'intelligenza artificiale. Prima di verificare se questi nuovi scenari impongano una revisione delle visioni tradizionali, è utile chiarire il senso dei concetti che applichiamo nel descrivere la vicenda contrattuale, ed il ''nuovo sguardo'' sul contratto sollecitato dai fenomeni in esame aiuta tale chiarimento. È in questa luce che vanno esaminati l'estremo automatismo che caratterizza le attività rivolte ad instaurare ed eseguire contratti mediante i nuovi strumenti dell'era digitale, le nuove opportunità che esse offrono, soprattutto nella gestione delle sopravvenienze, ma anche i rischi legati derivanti dall'affidare alla macchina le scelte negoziali. Soprattutto reclama attenzione la circostanza che le nuove manifestazioni dell'attività contrattuale modificano, spesso in modo surrettizio e con esiti imprevisti, i nostri comportamenti quali ''contraenti'', ed a tale modificazione devono adeguarsi anche gli strumenti di composizione delle controversie.

La sostituzione della macchina all'uomo nell'attività contrattuale: nasce un problema

Da quando gli uomini conducono la propria esistenza in società dotate di una, sia pur minima, organizzazione, essi, per procurarsi ciò che serve alla loro vita (che si tratti di soddisfare bisogni fondamentali ed essenziali, o di dare sfogo a desideri futili o capricciosi), non possono fare a meno di utilizzare quelle forme di relazione alle quali, sotto l'aspetto giuridico, applichiamo la categoria del contratto.

L'attività che consiste nel concludere contratti (e nell'eseguirli) ci appare, perciò, più di altre propria dell'uomo, rivolta com'è ad attuare scelte rispondenti ad esigenze e interessi essenzialmente "umani", e compiute per realizzare finalità economiche, stabilendo rapporti tra uomini (che non cessano di essere tali anche quando ne sono parti soggetti diversi dalle "persone fisiche"), perché umani sono gli interlocutori di tali rapporti e gli interessi economici che in tal modo vengono composti in un assetto condiviso.

Nondimeno, lo sviluppo delle nuove tecnologie ha condotto al sempre più diffuso impiego di "macchine intelligenti", dotate dell'attitudine a sostituire l'uomo in quelle attività nelle quali in passato l'intervento umano era considerato indispensabile, proprio perché implicanti l'impiego di facoltà sensoriali, cognitive ed intellettive. Non è affatto sorprendente, perciò, che l'applicazione dell'intelligenza artificiale si sia estesa anche all'attività contrattuale, producendo nuove manifestazioni di tale attività, accolte ora con atteggiamento ottimistico (preconizzando tutta una serie di benefici effetti), ed ora invece con qualche riserva[1].

In questa sede non interessa formulare giudizi sui costi o sui benefici dell'applicazione dell'intelligenza artificiale all'attività contrattuale[2]. Interessa, piuttosto, esaminare l'impatto che tale applicazione esercita sul diritto dei contratti.

Quali sono i reali termini del problema

Questo esame investe due piani diversi ma tra loro collegati:

Da un lato, viene in questione il quesito se i contratti conclusi mediante intelligenza artificiale (o, se si vuole, conclusi "da" una intelligenza artificiale) impongano di rivedere i concetti, le nozioni o le idee mediante le quali

---

[44] Ho tradotto liberamente l'efficace metafora che riporto: "*Metaphorically, it is as if law of the sea were based on the principle of controlling every drop of water in the oceans according to its origin*": così Bergé-Grumbach-Zeno-Zencovich, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law and Governance*, V/2019, 162.

[1] Cfr., con riguardo ai cc.dd. *"smart contracts"* (dei quali parleremo più oltre) K. Werbach-N. Cornell, *Contracts* ex machina, in *Duke Law Journal*, 2017 [67], 152: *"Proponents of smart contracts argue they will eliminate the fiction of legal disputes. This view is ovely optimistic. While the potential benefits of smart contracts are substantial, the potential problems are significant as well. There is a Frankenstein dimension to a smart contract. An instrument that fuses something innately human, entering into and enforcing agreements, with something mechanical, derived from scientific experiments. Science fiction authors since Mary Shelley have warned of the consequences of such cyborgs"*. Di qui l'affermazione secondo cui *"smart contracts will in some cases merely shift problems rather than eliminate them"*.

[2] Sulla possibilità che gli *smart contracts* consentano di neutralizzare i rischi legati alle sopravvenienze cfr. D. Di Sabato, *Gli* smart contracts: robot *che gestiscono il rischio contrattuale*, in *Contratto e Impresa*, 2017, 378 e segg.