UNIVERSITÀ
DEGLI STUDI
DI BERGAMO

Dottorato di Ricerca in

Economia e diritto dell'impresa (Business & Law)

– XXXIV ciclo –

Settore scientifico disciplinare (SSD): IUS/01 – Diritto Privato

LA *GOVERNANCE* DEI DATI NELLE APPLICAZIONI DI INTELLIGENZA ARTIFICIALE

Relatore

Chiar.mo Prof. Roberto Pucella

Tesi di dottorato

Maria Grazia Peluso

Matricola n. 1021984

ANNO ACCADEMICO 2020 / 2021

INDICE SOMMARIO

Premessa 6

Capitolo 1

Intelligenza Artificiale

1. Quale Intelligenza Artificiale: una possibile definizione 9

1.1. Una macchina è intelligente? 16

2. Come funziona l'Intelligenza Artificiale 24

2.1. Intelligenza Artificiale e Big Data. Quale ruolo dei dati e prime criticità 35

3. Considerazioni conclusive 45

Capitolo 2

Tecnologia e diritto nella *governance* europea

1. I dati quale nuovo asset economico 49

1.1. Il mercato digitale. Caratteristiche e criticità 57

2. La strategia europea: Intelligenza Artificiale e dati, una regolazione necessariamente coordinata 62

3. La strategia dell'Europa sui dati non personali. Il Regolamento 2018/1807 UE e la sua portata applicativa 73

4. La strategia europea sui dati personali: dal pacchetto dati al GDPR 79

5. Considerazioni conclusive 85

Capitolo 3

Il Regolamento generale sulla protezione dei dati personali alla prova dell'Intelligenza Artificiale: prime criticità applicative

1. Non solo un problema di privacy 89

2. Il "dato personale" all'interno della normativa europea: una nozione aperta 99

3. Il principio di limitazione delle finalità nei trattamenti operati mediante tecnologie *data driven* 108
4. I principi di minimizzazione e limitazione della conservazione 114
5. Il principio di integrità e riservatezza alla prova dei fenomeni di *data breach* 121
5.1. Anonimizzazione e Pseudonimizzazione 133
6. Il principio di esattezza 140
7. Possibili profili di una tutela collettiva 143
8. Considerazioni conclusive 146

Capitolo 4

***Black box society* e decisioni automatizzate**

1. Profilazione e decisioni automatizzate 149
2. La Convenzione 108 e le sue recenti modificazioni 160
3. Le decisioni Automatizzate nel GDPR 166
3.1. Le basi di legittimità del trattamento. Quale spazio per il consenso dell'interessato 173
4. Il diritto alla spiegazione, un dibattito ancora acceso 189
4.1. La *black box society* 196
4.2. Quali possibili soluzioni all'opacità intrinseca dei sistemi 203
5. Le previsioni del GDPR a tutela degli interessati: l'*accountability*, la valutazione di impatto e la responsabilità per illecito trattamento dei dati personali 210
5.1. La valutazione preventiva d'impatto 217
5.2. La responsabilità per illecito trattamento dei dati personali 222
6. Possibili prospettive di tutela 240
6.1. La *blockchain* quale possibile alleato nella filiera di dati di qualità 244
7. Considerazioni conclusive 255

Capitolo 5

La regolazione dei dati nella mobilità connessa e autonoma

1. Auto a guida autonoma. Una tassonomia 258

2. Il governo dei dati nelle *smart cars* 269
2.1. Quale base giuridica di legittimità dei trattamenti 274
3. La sicurezza delle vetture, un problema anche di privacy? 284
4. Alcune questioni sui dati generati dalle vetture.....291
4.1. Quale tutela giuridica per i dati grezzi non personali..... 298
5. Considerazioni conclusive 311

Indice Bibliografico..... 316

PREMESSA

Nel 1973 Stefano Rodotà scriveva un testo che per molti versi ancora oggi sorprende per la straordinaria capacità di analizzare lucidamente un fenomeno ancora agli albori e che avrebbe mostrato la sua capacità esplosiva solo dopo qualche decennio. Proprio in apertura della sua prefazione Rodotà sottolinea come in quegli anni si annunciava in Italia la fortuna di un genere letterario che avrebbe fatto «sfiorare i giuristi dal brivido del best-seller»[1]. Faceva riferimento alla difesa della privacy, attaccata dagli elaboratori elettronici capaci di raccogliere e trattare dati di massa.

Da allora il mondo è cambiato, il tema della privacy e della tutela dei dati personali ha interessato – e interessa – gli interpreti che si fanno portatori di una tensione sempre crescente tra tutela della persona e sviluppo economico e sociale. Oggi, tuttavia, si scorge all'orizzonte un nuovo fenomeno con cui i giuristi sono chiamati a confrontarsi: l'Intelligenza Artificiale. Si assiste attualmente a una grande produzione scientifica sul tema, da più parti ci si interroga sulle sfide che gli algoritmi pongono alla tenuta del sistema giuridico; alla produzione dottrinale si accompagnano carte etiche, dichiarazioni di principi, normative tecniche e risoluzioni provenienti dalle Istituzioni.

La diffusione sempre più pervasiva di queste tecnologie *data driven* sta facendo, dunque, emergere la necessità di un'attenta analisi in merito alla compatibilità delle normative oggi vigenti con il nuovo fenomeno digitale. Alcune prime tensioni sono state riscontrate nel contesto della responsabilità civile applicabile in caso di danni derivanti dall'utilizzo di sistemi algoritmici, come dimostra il testo della risoluzione del Parlamento del 2017, recante "raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica".

Oltre a questo fondamentale aspetto, si mostra parimenti necessaria una ponderazione in merito alla *governance* dei dati analizzati e prodotti dai sistemi algoritmici. Essi difatti richiedono un numero molto elevato di dati, non solamente per permetterne un adeguato "addestramento", ma anche per il loro stesso funzionamento,

[1] RODOTÀ, *Elaboratori elettronici e controllo sociale* (1973), Ristampa anastatica, a cura di ALPA, Napoli, 2018, 7 s.

ciò in quanto la macchina funziona proprio mediante un'analisi dei dati a questa sottoposti.

Se dunque l'Intelligenza Artificiale rappresenta il motore di questa nuova rivoluzione tecnologica, i dati ne rappresentano il carburante. Alla luce di questa considerazione appare allora evidente come un'analisi esaustiva del fenomeno non possa prescindere da una lettura critica anche delle normative che regolano la circolazione e il trattamento dei dati di natura personale e non.

Prima di procedere è però necessaria una premessa di stampo metodologico. Di fronte alle evoluzioni della tecnica, anche per il giurista diviene fondamentale comprendere, almeno in modo rudimentale, il funzionamento delle tecnologie. Solo in questo modo sarà possibile avere un'effettiva cognizione dei profili particolarmente critici, dove le tensioni con i testi normativi si fanno più intense; ciò è vero in particolar modo per il settore dell'Intelligenza Artificiale, in quanto proprio la complessità tecnica sembra essere di ostacolo a una piena applicazione degli schemi giuridici oggi vigenti. Un'analisi circa l'efficacia delle norme non potrà dunque prescindere dal confronto con il funzionamento dei sistemi *data driven* al fine di verificarne nel concreto la portata applicativa e l'adeguatezza rispetto agli scopi perseguiti.

Questa la strada che si è cercato di percorrere con il presente lavoro, ove, dunque, allo studio delle normative europee e nazionali si è affiancato un confronto con la tecnica, al fine di far emergere le possibili tensioni con essa nascenti. Un approccio alla materia nel suo complesso potrà premettere una valutazione critica circa l'efficacia di una regolazione che sia idonea a tutelare gli utenti dalle inevitabili esternalità negative derivanti dall'utilizzo di questi applicativi, ma che al contempo non scoraggi lo sviluppo della tecnologia, di per sé foriera di grandi benefici sia economici che sociali.

Per ricordare le celebri parole di Guido Calabresi, si tratta di una "scelta tragica"[2]. Di fronte a una percentuale inevitabile di eventi dannosi, al divieto *tout court* di utilizzo pare preferibile assumersene il rischio e permetterne invece la diffusione. Ciò sia perché il progresso sembra difficile da arrestare, sia perché il rapporto rischi/benefici, per la società nel suo complesso, depone a favore della tecnologia. Si mostra allora evidente la necessità di una comprensione del funzionamento dei dispositivi algoritmici, così da permetterne una regolazione *ex ante* che sia attenta a tutte le fasi di progettazione e

[2] CALABRESI, BOBBIT, *Scelte Tragiche*, Milano, 2006.

sviluppo e che coinvolga tutti gli *stakeholders*, dunque non solamente i giuristi, ma anche i tecnici, così da poter prevedere soluzioni giuridiche che siano al contempo concretamente implementabili ed efficaci.

CAPITOLO 1

Intelligenza Artificiale

SOMMARIO: 1. Quale Intelligenza Artificiale: una possibile definizione. – 1.1. Una macchina è intelligente? – 2. Come funziona l'Intelligenza Artificiale. – 2.1. Intelligenza Artificiale e Big Data. Quale ruolo dei dati e prime criticità. – 3. Considerazioni conclusive.

1. Quale Intelligenza Artificiale: una possibile definizione

Cosa debba intendersi per Intelligenza Artificiale (AI) è ancora oggi oggetto di dibattito tra gli studiosi della materia.

Il termine fu coniato da John McCarthy nel 1955[3], per definire ciò che prima veniva chiamato simulazione computazionale[4], in occasione di un seminario estivo interdisciplinare tenutosi al Dartmouth College di Hannover, nel New Hampshire, organizzato allo scopo di riunire i maggiori esponenti della disciplina[5].

La difficoltà di elaborare una definizione universalmente accettata dalla comunità scientifica trova origine nell'ampiezza del campo di ricerca e nella diversità delle prospettive adottate; contrapposizioni emersero infatti fin dagli albori della materia. A coloro che ritenevano necessario lo sviluppo di macchine che fossero capaci di imitare il funzionamento del cervello umano, si contrapponevano infatti coloro i quali reputavano

[3] MCCARTHY *et al*., *A proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, *31 August 1955* (2006) 27 *AI magazine* 12.
[4] BODEN, *L'intelligenza Artificiale*, Bologna, 2019, 22.
[5] Cfr. sul punto SANTOSUOSSO, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Firenze, 2020, 4. L'Autore riporta uno stralcio della proposta di McCarthy *et al.* introduttiva del seminario estivo al Dartmouth College: «Proponiamo di svolgere uno studio sull'intelligenza artificiale per due mesi, con dieci persone, durante l'estate del 1956 al Dartmouth College di Hannover, nel New Hampshire. Lo studio procederà sulla base della congettura che ogni aspetto dell'apprendimento, o qualsiasi altra caratteristica dell'intelligenza, possa in linea di principio essere descritto con precisione tale che sia possibile costruire una macchina per simularlo. Si tenterà di scoprire come costruire macchine in grado di utilizzare il linguaggio, formare astrazioni e concetti, risolvere tipi di problemi che oggi sono di esclusiva competenza degli uomini, migliorare sé stesse. Riteniamo che sia possibile ottenere un significativo progresso in uno o più di questi problemi dedicando un'intera estate al lavoro collettivo di un gruppo di scienziati selezionati».

piuttosto obiettivo primario della ricerca la creazione di macchine in grado di risolvere i problemi in modo efficiente, prescindendo dunque da una simulazione dei processi cerebrali[6].

Nello sforzo di chiarire il campo di indagine, una prima definizione venne coniata nel 1968 da Marvin Minsky[7], uno dei padri fondatori della disciplina, il quale sostenne che l'Intelligenza Artificiale fosse «*the science of making machines do things that would require intelligence if done by men*»[8]. A questa seguirono diverse definizioni più o meno ampie, in ragione degli scopi perseguiti e delle prospettive teoriche considerate[9]. Seguendo una concezione attenta ai processi del pensiero e al ragionamento, misurando il successo dei sistemi in ragione della somiglianza all'agire umano[10], Haugeland, per esempio, definiva la materia come un nuovo tentativo diretto alla creazione di computer in grado di pensare, macchine dotate di mente[11]. Altre definizioni paiono invece espressione di una maggiore attenzione dedicata al pensiero

[6] Tra coloro che ritenevano non direttamente rilevante il funzionamento del cervello umano lo stesso McCarthy, all'epoca voce fuori dal coro, secondo cui le macchine create allo scopo di risolvere problemi non dovevano necessariamente essere capaci di pensare nello stesso modo degli essere umani. Tra gli oppositori Marvin Minsky, secondo cui invece una corretta comprensione degli oggetti avrebbe richiesto un computer capace di pensare come una persona. V. sul punto WARWICK, *Intelligenza Artificiale. Le basi*, Palermo, 2012 (trad. 2015), 26.

[7] Minsky viene ricordato come uno dei padri fondatori dell'Intelligenza Artificiale. Egli, insieme al collega Edmonds, nel 1951 costruì la prima macchina computazionale basata su una rete di modelli neurali, così come descritti da McCulloch e Pitts. WARWICK, *op. cit.*, 21 s.

[8] La definizione coniata da Minsky viene riportata in molti testi dedicati allo studio dell'AI. Si vedano tra gli altri WARWICK, *op. cit.*, 66; LEXCELLENT, *Artificial intelligence versus human intelligence: are humans going to be hacked?*, Switzerland, 2019, 5.

[9] La definizione di Minsky evidenzia un approccio alla materia diretto alla creazione di sistemi che mimino l'agire umano, che quindi si comportino come gli esseri umani. Lungi dall'essere una voce isolata, nel corso degli anni tale approccio di ricerca venne sviluppato, ma anche aspramente contestato da coloro che invece si affidavano a un approccio maggiormente razionalista.
Nel corso degli anni molteplici sono, dunque, stati i tentativi definitori. Senza alcuna pretesa di esaustività possiamo ricordare alcune definizioni tra cui quella di Rich e Khight secondo cui l'IA è «Lo studio di come far eseguire ai computer le attività in cui, al momento, le persone sono più brave», si v. RUSSELL, NORVIG, *Intelligenza Artificiale. Un approccio moderno*, II, 1, Milano, 2005, 4. Tra le più recenti possiamo citare: «Il campo dell'intelligenza artificiale (IA) si occupa della scienza e dell'ingegneria delle macchine che agiscono in modo intelligente», AA. VV., *Macchine che pensano*, Bari, 2018, 9. Di particolare interesse anche la definizione coniata da Boden: «L'intelligenza Artificiale (IA) cerca di mettere in grado i computer di fare il genere di cose che sanno fare le menti». BODEN, *op. cit.*, 7.

[10] Sul punto anche Bellman forniva una definizione di AI come espressiva dei processi di automazione di attività che vengono associate al pensiero umano, quali il processo decisionale, la risoluzione dei problemi e l'apprendimento. V. RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 4. Recentemente BUTTOLO, *Introduzione alla Robotica*, Albino, 2017, 69, nel tentativo di chiarire l'oggetto della materia, ha specificato come l'AI «altro non è che un ramo dell'informatica che si occupa di progettare e sviluppare algoritmi che permettono ai computer di svolgere ragionamenti simili all'uomo».

[11] RUSSELL, NORVIG, *Intelligenza Artificiale*, *ibidem*.

razionale[12]; tra queste quella coniata da Winstone, il quale riteneva l'Intelligenza Artificiale lo studio dei processi computazionali che rendono possibile percepire, ragionare e agire[13]. Oltre che sui processi del pensiero, parte delle ricerche in materia si è nel tempo concentrato sullo studio del comportamento razionale delle macchine[14], introducendo così il concetto di agente[15]; a tale corrente possiamo ricondurre la definizione elaborata da Poole secondo cui l'intelligenza computazionale è lo studio della progettazione di agenti intelligenti[16].

Dalla lettura delle definizioni sopra richiamate, ciascuna espressione di differenti concezioni teoriche, possiamo notare come esse presentino quale elemento unificatore il riferimento al concetto di intelligenza umana, e al conseguente processo imitativo della macchina, senza tuttavia mai chiarire cosa si debba intendere per "intelligenza". Sebbene sia oggetto di indagine in diverse discipline scientifiche, ad oggi non pare esservi una concezione univoca del termine. Questo piuttosto si rivela essere un'entità complessa, che si compone di differenti aspetti, avente una valenza soggettiva legata al contesto sociale, alle considerazioni del gruppo che osserva e di quello preso in osservazione[17]. A mero titolo di esempio si noti come nel 1932 il New English Dictionary considerava l'intelligenza come esercizio della comprensione, potere intellettuale, conoscenza acquisita e prontezza di intelletto. Nel 1995 la Macmillan Encyclopedia specificava invece come questa fosse espressione della capacità di ragionare e di trarre profitto dall'esperienza; il livello di intelligenza di un individuo veniva fatto discendere da una complessa interazione tra caratteri ereditari e ambiente. Nei primi anni del Novecento Alfred Binet, inventore del test del QI, riteneva elementi essenziali il giudizio, il buonsenso, l'iniziativa e la capacità di adattamento.

[12] Sul punto cfr. la definizione proposta da Charniak e McDermott, il cui approccio risulta maggiormente diretto alla comprensione dei meccanismi di elaborazione del pensiero, secondo cui l'AI consiste nello studio delle facoltà mentali attraverso l'uso di modelli computazionali. RUSSELL, NORVIG, *Intelligenza Artificiale*, *ibidem*.

[13] RUSSELL, NORVIG, *Intelligenza Artificiale*, *ibidem*.

[14] RUSSELL, NORVIG, *Intelligenza Artificiale*, *ibidem*, riportano un'interessante definizione proposta da Nilsson, secondo cui: «L'IA… riguarda il comportamento intelligente negli artefatti».

[15] Per meglio chiarire cosa debba intendersi con detto termine si riporta la spiegazione data da RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 46, in merito a cosa debba intendersi con il termine "agente": «Un agente è qualsiasi cosa possa essere vista come un sistema che percepisce il suo ambiente attraverso dei sensori e agisce su di esso mediante attuatori».

[16] RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 4.

[17] Una volta ampliata la discussione, una definizione più generale di "intelligenza" potrebbe essere: «La varietà di processi di elaborazione delle informazioni che, nel loro insieme, consentono a un essere di perseguire in modo autonomo la propria sopravvivenza», WARWICK, *op. cit.*, 43 ss.

Recentemente l'intelligenza è stata messa in correlazione anche con la consapevolezza spirituale o le emozioni[18].

Pertanto, presa coscienza delle difficoltà derivate dall'utilizzo di un termine connotato anch'esso da una ineliminabile componente di vaghezza, parte dei ricercatori preferirono fare riferimento al concetto di razionalità per riferirsi all'operato di un sistema meccanico. Tale espressione si riferisce all'abilità di scegliere la migliore azione volta al raggiungimento di un certo obiettivo, ottimizzando determinati criteri e utilizzando le risorse disponibili. Dunque, in un dato momento, la razionalità di un sistema dipende dalla misurazione delle prestazioni[19], dalla conoscenza pregressa dell'ambiente, dalle azioni che si possono effettuare e dalla sequenza percettiva fino all'istante dell'azione. Da ciò ne discende che affinché una macchina possa essere definita un agente razionale questa dovrebbe essere in grado di scegliere la migliore azione, cioè quella che massimizzi la misura della prestazione attesa, date le informazioni fornite dai sensori e data ogni ulteriore conoscenza dell'ambiente[20].

Alla luce delle considerazioni sopra svolte, merita una particolare menzione la definizione coniata da Russell e Norvig, tra i maggiori studiosi della materia, secondo cui «l'IA è la ricerca del miglior programma agente per una specifica architettura»[21]. Sebbene particolarmente ampia, questa definizione mostra di cogliere l'essenza della disciplina, prestandosi al contempo a una interpretazione capace di adattarsi ai differenti angoli visuali che caratterizzano un campo di indagine così ampio.

Con la diffusione della tecnologia, alle riflessioni degli scienziati si sono accompagnate quelle di esponenti di diverse branche della ricerca scientifica. La necessità di una definizione univoca, infatti, lungi dall'essere un'esigenza sentita solamente tra gli esperti, si è andata avvertendosi negli anni in diversi ambiti di studi, tra cui anche quello giuridico[22]. La sempre maggiore pervasività nel mercato di artefatti

---

[18] Si rimanda a WARWICK, *op. cit.*, 38, ove l'Autore riporta un confronto tra diverse definizioni di "intelligenza".

[19] Una misura di prestazione rappresenta il criterio in base al quale valutare il successo del comportamento di un agente. Quando si lascia libero un agente in un dato ambiente, esso genererà una sequenza di azioni in base alle percezioni ricevute. Questa sequenza di azioni farà sì che l'ambiente attraversi una sequenza di stati: se tale sequenza è desiderabile, allora l'agente si è comportato bene. V. RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 49.

[20] RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 48.

[21] RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 588 ss.

[22] Lo stesso Parlamento Europeo nella Risoluzione alla Commissione europea, nella parte introduttiva, espressamente riporta la necessità di elaborare una definizione universalmente accettata di Intelligenza Artificiale e di Robot. Pur non cimentandosi nell'impresa, nell'allegato l'Istituzione europea pone

e sistemi guidati da algoritmi variamente catalogati quali Intelligenza Artificiale ha comportato l'emersione da più parti di istanze di regolazione unitaria del fenomeno; soprattutto alla luce delle esigenze di tutela dei diritti fondamentali che si teme vengano minacciati da un utilizzo incontrollato delle nuove tecnologie[23].

Diverse sono state le definizioni proposte dalla più attenta dottrina[24] e dalle stesse Istituzioni europee. La cornice necessariamente sovranazionale del fenomeno ha difatti spinto queste ultime a porre l'attenzione sulla necessità di una riflessione in merito alla effettività dei mezzi di tutela offerti dalla normativa vigente; le stesse modalità di funzionamento degli algoritmi sembrano infatti comportare incertezze in merito alla compatibilità con le categorie classiche del diritto.

Abbracciando dunque una concezione volta a sottolineare le razionalità dei sistemi agenti[25], discostandosi in parte da quanto affermato dalla Commissione Europea[26],

---

l'attenzione su alcune caratteristiche che un robot deve necessariamente possedere per essere ritenuto autonomo. Nello specifico si ritengono necessarie: «*la capacità di acquisire autonomia grazie a sensori e/o mediante lo scambio di dati con il proprio ambiente (interconnettività) e l'analisi di tali dati; la capacità di apprendimento attraverso l'esperienza e l'interazione; la forma del supporto fisico del robot e la capacità di adeguare il suo comportamento e le sue azioni all'ambiente*». V. Risoluzione del Parlamento europeo, Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2015/2103(INL)).

[23] ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale: la costruzione di uno schema di regolamentazione europeo tra mercato unico digitale e tutela dei diritti fondamentali*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di DORIGO, Pisa, 2020, 14 s.

[24] Tra gli altri SANTOSUOSSO, *Questioni definitorie*, in *Biolaw Journal – Rivista di BioDiritto*, 2020, 469 s., ritiene che ciò che viene chiamato AI sia il sofisticato sviluppo di capacità computazionali settoriali; estraneo dunque a ciò a cui normalmente connettiamo l'attributo di intelligente. Sul punto interessante anche COMANDÈ, *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giur. econ.*, 2019, 169 s., in cui l'Autore riporta due definizioni, una più generale, l'altra dal risvolto maggiormente "operativo". Crisci, ritenendola tra le definizioni maggiormente comprensibili, riporta quella data nel dizionario De Mauro secondo cui l'IA è «l'insieme di studi e tecniche che tendono alla realizzazione di macchine, specialmente calcolatori elettronici, in grado di risolvere problemi e di riprodurre attività proprie dell'intelligenza umana». CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm*., 2018, 1792. Per Pagallo, invece, con il termine può intendersi «la scienza della produzione di macchine e sistemi volti all'esecuzione di compiti che, qualora realizzati da esseri umani, richiederebbero l'uso dell'intelligenza per risolvere problemi di apprendimento e conoscenza, di ragionamento e pianificazione». PAGALLO, *Intelligenza artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sistemi int.*, 2017, 615.

[25] Ad oggi l'elemento cardine su cui paiono ruotare le definizioni più recenti risulta essere, infatti, la capacità di raggiungere un risultato. Cfr. sul punto ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 108. Secondo l'autore questa tipologia di definizioni sarebbero comunque foriere di dubbi dal punto di vista giuridico, dal momento che opererebbero unicamente una sostituzione del termine "intelligenza" con il termine "obiettivo"; ciò potrebbe portare l'attenzione degli interpreti su aspetti filosofici di poco ausilio nel campo legislativo.

[26] La Commissione europea, nella raccomandazione al Parlamento emanata nel 2018, aveva elaborato una prima definizione di Intelligenza Artificiale da cui emerge con chiarezza il riferimento a capacità delle macchine che potessero dirsi "intelligenti": «*Artificial intelligence (AI) refers to systems that display*

recentemente l'High-Level Expert Group on AI ha elaborato una definizione molto particolareggiata di Intelligenza Artificiale. Col dichiarato scopo di rendere maggiormente compresibile l'oggetto della materia, il Gruppo di Esperti ha chiarito come detta espressione debba ricomprendere: «*software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions. As a scientific discipline, AI includes several approaches and techniques, such as machine learning (of which deep learning and reinforcement learning are specific examples), machine reasoning (which includes planning, scheduling, knowledge representation and reasoning, search, and optimization), and robotics (which includes control, perception, sensors and actuators, as well as the integration of all other techniques into cyber-physical systems)*» [27].

La particolare specificità che emerge dalla lettura della sopra richiamata definizione consta forse di una preoccupazione, tutta giuridica, di ricomprendere al proprio interno non solamente tutti gli artefatti, siano essi software o hardware, ma altresì tutte le discipline tecniche entro cui si è variamente specializzata la ricerca in materia. Ciò che sembra aver mosso il Gruppo di Esperti pare, infatti, essere il timore di eventuali vuoti di tutela, preoccupazione che tuttavia avrebbe potuto trovare conforto anche in una definizione elastica e forse maggiormente in linea con la veloce evoluzione degli scenari tecnologici. Come tutte le definizioni legate a campi della ricerca aventi un rapido sviluppo, il maggior rischio è proprio quello dell'eccessiva rigidità e, di conseguenza, di una rapida obsolescenza che costringa a continui rimaneggiamenti in un'eterna rincorsa

---

intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications)». Comunicazione della Commissione, *Un'intelligenza artificiale per l'Europa*, COM (2018) 237 final.

[27] High Level Expert Group, *Definition of AI. Main capabilities and disciplines*, 8 aprile 2019, consultabile all'indirizzo: *www. ec.europa.eu*.

all'evoluzione tecnologica. Una definizione che sia al contempo chiarificatrice e operativamente utile dunque non può che essere altresì flessibile[28].

Nella consapevolezza che una nozione universalmente condivisa di Intelligenza Artificiale ad oggi non esiste, una buona definizione potrebbe allora essere quella secondo cui l'AI è una disciplina che studia le modalità di addestramento di algoritmi che siano in grado, secondo diversi gradi di autonomia, di gestire ed elaborare dati e fornire statisticamente delle risposte, indipendentemente dalla fisicità della macchina[29]. Sul punto è stato difatti osservato come non sia il «*corpus mechanicum* a definire e qualificare l'AI bensì un processo totalmente automatizzato basato sull'acquisizione e l'elaborazione di informazioni in grado di fornire un risultato, di correggerlo e implementarlo. L'input resta quello umano: è quest'ultimo che sceglie l'obiettivo che l'applicazione di AI deve perseguire»[30].

Ad oggi, dunque, il fattore chiave su cui ruotano le recenti costruzioni concettuali dell'Intelligenza Artificiale è il raggiungimento di un dato obiettivo[31]. Tuttavia, sebbene pregevole si dimostri il tentativo di abbandono del concetto di "intelligenza", che come visto presenta un carattere fin troppo vago, il dibattito sulla possibilità di qualificare una macchina come intelligente non è mai cessato. Basti pensare alle considerazioni in merito agli esiti dello sviluppo tecnologico, fino ad arrivare alle posizioni di chi si interroga, alcuni con grande preoccupazione, altri con serena attesa, di un'evoluzione delle macchine tale da portare alla c.d. Singolarità. Con detta espressione si intende comunemente il (presunto) momento in cui i computer avranno raggiunto un livello di intelligenza tale da superare quella umana, finendo col "ribellarsi" ai propri creatori[32].

---

[28] Cfr. ANGELINI, *Intelligenza Artificiale e* governance*. Alcune riflessioni di sistema*, in *Intelligenza Artificiale e protezione dei dati*, a cura di PIZZETTI, Torino, 2018, 293 s. L'Autrice riporta anche una definizione di Intelligenza Artificiale secondo cui essa sarebbe «*a science and a set of computational technologies that are inspired by – but typically operate quite differently from – the ways people use their nervous systems and bodies to sense, learn, reason, and take action*». Interessante sul punto ROMANO, *ibidem*.

[29] GIUSTI, *Intelligenza artificiale e sistema sanitario*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., 310; si veda anche ROMANO, *op. cit.*, 107 s.

[30] TREVISI, *La regolamentazione in materia di intelligenza artificiale, robot, automazione: a che punto siamo*, in *Medialaws – riv. dir. media*, 2018, 447.

[31] ROMANO, *op. cit.*, 108.

[32] Rer i sostenitori della Singolarità la "ribellione" delle macchine appare inevitabile. Ciò in quanto una volta raggiunta l'intelligenza umana i sistemi saranno abbastanza intelligenti da potersi "copiare"; divenendo quindi più numerosi degli esseri umani. Saranno inoltre anche in grado di migliorare sé stessi tanto da superare l'uomo. Arrivati a quel punto si ritiene che saranno i computare a occuparsi dei problemi e delle decisioni più importanti. Per un approfondimento del tema si rimanda a BODEN, *op. cit.*, 143 ss.

Al di là di scenari futuribili, dal sapore fantascientifico, le ricadute giuridiche legate alla concezione di macchine intelligenti, in particolare in ragione della dichiarata loro autonomia di decisione, necessitano oggi di un'attenta riflessione. Pertanto, pare necessario chiarire preliminarmente cosa debba intendersi con l'espressione "macchina intelligente".

1.1 Una macchina è intelligente?

La domanda se una macchina possa essere definita intelligente è tuttora oggetto di indagine, più che tra matematici e ingegneri, tra filosofi e giuristi. Dal punto di vista tecnico la questione non ha avuto grande rilievo; non viene infatti ritenuta importante la qualificazione data al sistema agente, purché questo porti a termine correttamente il compito affidatogli.

Lo stesso Alan Turing, comunemente annoverato tra i padri dell'Intelligenza Artificiale e dello studio computazionale della mente[33], riteneva il dibattito sul punto sterile. Consapevole delle difficoltà di simulare in una macchina la complessità del cervello umano, egli reputava quali requisiti indispensabili dell'intelligenza la coscienza e la comprensione alla base delle scelte operazionali. Nell'elaborare il gioco dell'imitazione (anche conosciuto come test di Turing)[34], seppure creato più per una provocazione che non per stimolare un'effettiva critica[35], il matematico proponeva infatti di considerarne il superamento quale certificazione di una macchina che

[33] Alan Turing viene comunemente annoverato tra i padri fondatori della Intelligenza Artificiale grazie al suo lavoro dedicato alle macchine di Turing, (antenati dei nostri moderni computer) e allo studio computazionale della mente. Il matematico, infatti, comprese che per riprodurre il pensiero in una macchina fosse necessario rappresentare i processi di ragionamento attraverso liste di istruzioni che seguono le leggi della logica deduttiva classica; gli algoritmi appunto. DE ANNA, *Automi, responsabilità e diritto*, in *Rivista fil. dir*., 2019, 128 ss.

[34] In tal senso si fa spesso riferimento all'articolo "*Computing machinery and intelligence*", in cui Turing propose che la domanda se le macchine possano pensare venisse riformulata nei termini del cosiddetto gioco dell'imitazione, oggi noto anche come Test di Turing. FRIXIONE, *Il ruolo delle macchine di Turing nelle scienze cognitive*, in *L'eredità di Alan Turing. 50 anni di Intelligenza Artificiale*, a cura di CAPPUCCIO, Milano, 2005, 162.

[35] Il matematico non propose mai di condurre davvero il "test"; l'intento principale doveva essere una propaganda per un'AI futura. Lo scopo era, dunque, quello di convincere le persone che le macchine avrebbero potuto avere capacità di tipo umano, piuttosto che essere oggetto di una seria critica. Così venne descritto dallo stesso Turing al suo studente e amico Robin Gandy. BODEN, *op. cit.*, 120 e AA. VV., *Macchine che pensano*, cit., 167.

sembrasse essere intelligente, non che lo fosse effettivamente[36]. Pertanto, invece di chiedersi se le macchine possano pensare, Turing riteneva più corretto chiedersi se queste avrebbero potuto battere un uomo nel gioco dell'imitazione o, comunque, quanto a lungo avrebbero potuto resistergli[37].

Il gioco, nella sua versione originale, si compone di due partecipanti, un essere umano e una macchina calcolatrice, e di un giudice. Quest'ultimo non conosce la natura fisica dei suoi interlocutori e può comunicare con loro solo in maniera indiretta, convenzionalmente attraverso uno schermo e una tastiera. L'interrogante può fare domande a entrambi e il suo scopo è scoprire nel più breve tempo possibile quale dei due sia l'uomo e quale la macchina. Sono fissate alcune condizioni tra cui il divieto di mentire, salvo quando le domande vertono direttamente su questioni di tipo personale[38]. L'uomo evidentemente si comporterà in modo da agevolare il giudice, mentre la macchina dovrà rispondere in modo da ingannarlo il più a lungo possibile[39].

Dalla descrizione del gioco emerge dunque con chiarezza come questo non sia proposto quale criterio discriminante o definitorio di intelligenza. Il problema appare infatti centrato sulle difficoltà che ha l'interrogante nel riconoscere la natura dei due partecipanti. Non sembra dunque esserci un vero e proprio test; lo stesso Turing non usa detta espressione se non in occasione di un dibattito radiofonico nel 1952[40]. Quanto alle prestazioni delle macchine calcolatrici il matematico si dimostrò particolarmente ottimista. Possiamo ricordare una sua celebre dichiarazione sul punto: «credo che tra circa 50 anni sarà possibile programmare calcolatori con una capacità di memoria di circa 10^9 in modo da far loro giocare il gioco dell'imitazione così bene che un interrogatore medio non avrà più del 70% di probabilità di fare l'identificazione giusta in 5 minuti di interrogatorio. La questione originale 'Possono pensare le macchine?'

[36] Il gioco non mostra, infatti, di affrontare questioni quali la coscienza o la consapevolezza di sé, se non nei limiti in cui queste possano emergere dalle interrogazioni dei giudici. L'esito positivo del test, secondo l'intento dello stesso Turing, dunque, è di certificare unicamente come una macchina sembri pensare allo stesso modo di un essere umano, tanto da ingannarlo. WARWICK, *op. cit.*, 133.
[37] CORDESCHI, *L'intelligenza artificiale. Logica, paradossi e intelligenza artificiale*, in *La Scienza*, 5, Milano, 2005, 677.
[38] LOLLI, *Turing: il coraggio dell'ingenuità*, in *L'eredità di Alan Turing*, cit., 26.
[39] TURING, *Computing Machinery and intelligence* (1950) 59 *Mind* 433 ss., consultabile all'indirizzo: *www.academic.oup.com*. Traduzione italiana in SOMENZI e CORDESCHI, *La filosofia degli automi. Origini dell'intelligenza artificiale*, Torino, 1994; Senza alcuna pretesa di completezza, possiamo trovare una descrizione del famoso Test anche in FRIXIONE, *op. cit.*, 162; BODEN, *ibidem*; BALLO, *Dalla macchina di Turing ai calcolatori digitali*, in *L'eredità di Alan Turing*, cit., 20; ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *Analisi giur. econ.*, 2019, 10 s.
[40] LOLLI, *op. cit.*, 27.

credo sia troppo priva di senso per meritare una discussione. Tuttavia credo che alla fine del secolo l'uso delle parole e l'opinione corrente saranno talmente cambiate che si potrà parlare di macchine pensanti senza aspettarsi di essere contraddetti»[41].

Nonostante l'innegabile fortuna avuta nel corso degli anni, le critiche in merito alla valenza di detto test sono state varie[42]; tra le maggiori quelle volte a sottolinearne la limitatezza. Infatti, seppure il gioco si cimenti in una delle maggiori difficoltà di addestramento dei sistemi agenti, e cioè il riconoscimento del linguaggio naturale, questo viene basato su delle risposte scritte, escludendo quindi dall'indagine tutte le facoltà di reazione fisica all'ambiente esterno.

Nel corso degli anni sono state pertanto messe a punto diverse competizioni, sulla falsariga del gioco dell'imitazione, tutte volte a testare differenti capacità delle macchine tali per cui queste possano essere definite come intelligenti. Tra quelle maggiormente similari a quanto proposto da Turing vi è la Loebner Competition, che si tiene annualmente a Bletchley Park. Attualmente, le regole della competizione prevedono interazioni di venticinque minuti, con venti domande scelte preventivamente al fine di valutare la memoria, il ragionamento, la conoscenza generale e la personalità. I criteri che guidano le valutazioni delle risposte da parte dei giudici sono la pertinenza, la correttezza, la chiarezza e la plausibilità dell'espressione e della grammatica.

Fino ad ora nessun programma è riuscito ad ingannare il 30% delle volte i giudici, con l'unica eccezione di un programma presentato come un ragazzo ucraino di 13 anni che nel 2014 ingannò il 33% degli interroganti. Tuttavia è possibile obiettare come le caratteristiche dichiarate abbiano potuto influenzare nella valutazione i giudici. É facile infatti che gli errori vengano perdonati ai parlanti non madrelingua, ancora di più se questi vengono presentati come dei ragazzi[43].

Esiste poi un test di Turing c.d. totale che include sia un segnale video, in modo che l'esaminatore possa verificare le capacità percettive del soggetto, che la possibilità di passare oggetti fisici attraverso una finestra. Per superare il test, il sistema dovrà

[41] LOLLI, *ibidem*; FRIXIONE, *op. cit.*, 162 s.; TURING, *ibidem*. Traduzione italiana in SOMENZI e CORDESCHI, *op. cit.*, 176.

[42] Sul punto si veda CORDESCHI, *ibidem*, il quale riporta una prima critica alla stessa metodologia utilizzata nel gioco dell'imitazione a opera di Zenon Pylyshyn e Philip Johnson-Liard. Questi ultimi, sostenitori dell'idea generale della cognizione come computazione di strutture di simboli, ritenevano che il Test di Turing non fosse realmente indicativo delle capacità intellettive delle macchine, dal momento che questo si limita a considerare la prestazione senza però tenere conto dei processi cognitivi sottostanti.

[43] BODEN, *op. cit.*, 121.

possedere una visione artificiale, indispensabile per la percezione degli oggetti, e la robotica necessaria alla manipolazione e per potersi fisicamente muovere[44].

Ancora, ritenendo la creatività quale carattere maggiormente rappresentativo dell'intelligenza umana, nel 2001 Mark Riedl[45] ha ideato il test Lovelace 2.0, così chiamato in onore di Ada Lovelace. Questo test prevede che venga chiesto alla macchina di elaborare un prodotto creativo, quale per esempio una storia. A differenza del test di Turing in questa versione il giudice umano, seduto davanti a un computer, sa di interagire con un'intelligenza artificiale e le assegna un compito in due parti. Per prima cosa le chiede un'opera creativa, poi, come secondo compito, indica un criterio che il sistema deve rispettare nella sua elaborazione. Il test si considera superato solo se il programmatore non è in grado di spiegare come il software abbia elaborato la riposta. Sul punto lo stesso Riedl tuttavia ha dichiarato di non essere convinto che il test possa in effetti funzionare dal momento che è improbabile che un programmatore non riesca a capire come la sua macchina sia giunta a un determinato elaborato[46].

Nonostante la diversità tra le competizioni sopra riportate, possiamo notare come l'esito positivo o meno dei test possa solo provare in che misura le macchine posseggano delle capacità similari a quelle degli uomini. Nulla ci dicono in merito al funzionamento delle stesse, a come siano arrivate a un determinato output e, pertanto, se possano o meno essere qualificate come intelligenti.

Ci si domanda allora se un sistema agente possa essere effettivamente in grado di funzionare allo stesso modo in cui funziona un cervello umano. Le modalità di addestramento tramite algoritmi di *deep learning*, per esempio attraverso reti neurali artificiali, possono essere forse considerate un primo passo verso questo obiettivo[47]. Tuttavia le difficoltà tecniche di replicare interamente un sistema nervoso cerebrale sono cosa notoria; ciò non solamente con riferimento al numero di connessioni esistenti tra i neuroni biologici, infinitamente superiori alle simulazioni delle reti neurali oggi più

[44] RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 6.
[45] Mark Riedl è Professore associato e direttore dell'Entertainment lntelligence Lab al Georgia lnstitute of Technology di Atlanta. Ritenendo che il test di Turing fosse troppo facile ne ha proposto una rielaborazione in una nuova forma, avente come parametro di riferimento la creatività. AA. VV., *Macchine che pensano*, cit., 167.
[46] AA. VV., *Macchine che pensano*, *ibidem*.
[47] Sul punto si veda l'interessante contributo di GIOLITO, *Turing e la filosofia della mente*, in *L'eredità di Alan Turing*, cit., 153 ss., nel quale l'Autore riporta alcune argomentazioni a confutazione della possibilità di creare macchine pensanti che siano un duplicato della mente umana, tra cui un'applicazione dello stesso teorema di Gödel. Ciò in quanto il pensiero umano non può essere considerato come unicamente computazione, quale invece appare essere il funzionamento delle macchine.

estese, ma anche in merito al consumo di energia necessario a sostenere i processi computazionali e statistici delle stesse macchine[48]. Inoltre, se anche in futuro fosse possibile ricreare un sistema che presenti la stessa estensione di collegamenti tra neuroni, e consumi un'energia comparabile a quella del cervello umano, non saremmo comunque in grado di dire con certezza se quella macchina sia capace di pensare, sia intelligente, nello stesso modo in cui lo sono gli esseri umani[49].

Diversi sono stati gli argomenti posti a fondamento dell'assunto per cui una macchina – per quanto evoluta – non potrà mai essere considerata un essere senziente. Queste posizioni si fondano per la maggior parte sulla convinzione che il pensiero umano non sia riducibile al solo ragionamento computazionale, così come è per un algoritmo[50]. Le decisioni che guidano l'operato dell'uomo – si dice – non rispondono

[48] Il cervello umano si è evoluto per essere efficiente consumando una quantità di energia sensibilmente inferiore a quella già oggi consumata dai computer, e infinitamente inferiore rispetto a quella che verrà consumata in futuro dai super computer, o dai computer quantistici. Il problema delle risorse energetiche ad oggi viene considerato quale una possibile limitazione alle simulazioni neurali. WARWICK, *Intelligenza Artificiale*, cit., 42; AA. VV., *Macchine che pensano*, cit., 58 ss.; DRIGO, *Sistemi emergenti di intelligenza artificiale e personalità giuridica: un contributo interdisciplinare alla tematica*, in *Il ragionamento giudico nell'era dell'intelligenza artificiale*, a cura di DORIGO, Pisa, 2020, 182; Sul punto si rimanda anche a CINGOLANI, *L'altra specie. Otto domande su noi e loro*, Bologna, 2019, 14 e 27 ss. L'Autore sottolinea come se pure oggi le prestazioni dei super computer si avvicinino a quelle cerebrali, con operazioni nell'ordine di 10^{16} al secondo, il consumo di energia necessario rimane incomparabile, 10 Megawatt contro le 40 Watt necessarie all'uomo. A ciò deve aggiungersi – chiarisce l'Autore – come debba essere tenuto in considerazione anche il problema del raffreddamento, che nel funzionamento delle macchine consuma una parte considerevole dell'energia assorbita.

[49] Sul punto si rimanda a D'ALESSANDRO, *Dal miraggio dell'Intelligenza Artificiale alla simulazione di un sistema vivente*, in *L'eredità di Alan Turing*, cit., 245 ss. Secondo l'Autore il pensiero umano, seppure frutto di dati immagazzinati e richiamati, è il risultato di diversi fattori anche biochimici. Il pensiero, le scelte, sono, infatti, influenzate dalle emozioni e dalle reazioni al mondo esterno, che in ogni momento modificano il sistema; sistema che si compone di un enorme numero di connessioni neurali che in ogni momento mutano non solo di quantità ma anche di forma. L'A. sottolinea come ad oggi non sia possibile comparare le capacità di una singola macchina con quelle di un essere umano. Sul punto, infatti, si precisa come il cervello umano sia frutto di un'evoluzione durata milioni di anni e diretta non al perfezionamento delle abilità di calcolo, ma soprattutto alle navigazione e alla comunicazione. Parrebbe essere pertanto più vicina al pensiero umano la rete internet quale insieme di connessioni. Ciò non in ragione della quantità di computer connessi, ma in quanto la rete stessa si dimostra in grado di interagire con il mondo esterno mutando in risposta ai diversi stimoli a cui è sottoposta.
Sul tema interessanti anche le considerazioni di Cingolani, il quale ritiene che con gli attuali standard tecnologici i robot, singolarmente, avranno una capacità computazionale limitata a quanto necessario per muoversi con abilità e interagire fisicamente col mondo. Per quanto invece riguarda la parte "cognitiva", questa dovrà essere gestita «probabilmente con l'ausilio di una mente unica a cui tutti i robot saranno collegati, una sorta di repositorio globale dell'intelligenza delle macchine, che utilizzerà il *Cloud* per conservare tutte le informazioni e le "cose da imparare" dai robot in cui ciascuna macchia potrà fare l'*upload* e il *download* delle proprie esperienze». CINGOLANI, *op. cit.*, 14 s.

[50] GIOLITO, *op. cit.*, 153 ss. Interessante sul punto anche il riferimento di De Anna a Platone. Il filosofo greco aveva già distinto l'intelligenza (*nous*), ossia la capacità di comprendere l'essenza delle cose, dalla capacità di ragionare (*dianoia*), ossia di inferire conseguenze a partire da verità colte con l'intelligenza. Sebbene dunque per Platone fosse chiaro che lo studio della logica formale classica – deduttiva – non esauriva la conoscenza del pensiero, la sua teoria del sillogismo venne posta alla base della creazione di

unicamente ad una logica deduttiva; esiste infatti anche una logica induttiva, per cui l'essere umano riesce a giungere a determinate conclusioni proiettando informazioni originali che non sono completamente contenute nelle premesse[51] e che quindi dipendono da differenti fattori. Le azioni sono guidate anche da momenti istintuali, da *input* o da sensazioni percepite, e non legate unicamente a un ragionamento razionale. La stessa crescita emotiva e cerebrale appare connessa alle esperienze fatte durante lo sviluppo dei soggetti, elementi questi che difficilmente possono essere simulati.

Tra i più noti argomenti in opposizione alla concezione di macchine intelligenti vi è la teoria dell'intenzionalità, secondo cui non sarebbe possibile parlare di una effettiva intelligenza in quanto alle macchine mancherebbe ogni forma di comprensione, di intenzionalità nell'azione[52]. Uno dei maggiori sostenitori di detta corrente di pensiero è certamente John Searle, il quale sul punto elabora il suo esperimento mentale più famoso e controverso, quello della stanza cinese. In questo esperimento un uomo si trova in una stanza senza finestre ma provvista di una fessura attraverso cui vengono inserti dei foglietti su cui sono riportati dei simboli. C'è poi una scatola contenente foglietti con altri simboli dello stesso genere e un libro di regole in cui si dice che, quando un certo simbolo viene inserito nella stanza, l'uomo ne deve trasmettere un altro, o eseguire una serie di accoppiamenti tra simboli prima di passare un foglietto al di fuori della stanza. All'insaputa dell'operatore i simboli sono ideogrammi cinesi, il libro di regole è un programma NLP (*Natural Language Processing*) per il cinese, e i cinesi fuori dalla stanza lo stanno utilizzando per rispondere alle loro domande. Tuttavia, l'uomo che è entrato nella stanza non conosceva il cinese, e quando esce dalla stanza ancora non lo conosce. La conclusione a cui giunge Searle è dunque che la

---

un linguaggio artificiale rigoroso, quale quello proposto da Boole e Frege. Questi ultimi, difatti, volevano costruire un linguaggio artificiale da adoperare nelle dimostrazioni matematiche. Dal lavoro dei due matematici nacque la logica formale classica, la quale studia inferenze che permettono di ricavare la conclusione con certezza, esplicitando in essa informazioni già completamente contenute nelle premesse. DE ANNA, *op. cit.*, 128 ss.

[51] DE ANNA, *op. cit.*, 129.

[52] Sul punto si rimanda a SANTOSUOSSO, *Questioni definitorie*, *ibidem*, ove l'A. riporta una riflessione dello stesso Roger Penrose, il quale «è molto chiaro nel porre la distinzione tra "agire sulla base dell'esperienza", che è quella che può portare una macchina a vincere persino nel Go contro l'umano più esperto (come già accaduto per gli scacchi con Kasparov), e la "comprensione di quello che sta facendo". Così le macchine sviluppano abilità senza avere la conoscenza teorica di quale sia il fondamento di quelle azioni". L'Autore sottolinea come l'utilizzo pervasivo della parola "intelligenza" sia, dunque, imputabile a un "gioco di etichette". Sarebbe, pertanto, semanticamente corretto parlare di "intelligenza" solo qualora le macchine effettivamente possedessero quella che gli esperti di AI chiamano *general purpose intelligence*; in pratica macchine che siano in grado operare bene in qualsiasi campo e, dunque, a prescindere dall'obiettivo del loro addestramento.

computazione formale (ciò che avviene nella stanza), da sola, non può generare intenzionalità. Pertanto, anche qualora fosse possibile creare sistemi di AI "forte", cioè sistemi di AI generale, questi non sarebbero comunque intelligenti, dal momento che è improbabile che si riesca a generare autentica comprensione[53].

All'esperimento di Searle vennero fornite differenti risposte[54], in particolare quella per cui, sebbene non si possa affermare con certezza che l'operatore abbia imparato il cinese, dall'esperimento si deve concludere che il sistema stesso – quindi la stanza, l'operatore e le regole – ha dimostrato di conoscere il cinese[55].

Nel tempo la discussione filosofica intorno a questi temi ha accompagnato l'evoluzione degli studi dedicati all'indagine del modo in cui gli stati e i processi mentali sono correlati agli stati e ai processi del corpo[56]. Basti pensare alla teoria monista (o anche detta materialista) corpo mente, alla quale si contrappongono coloro che ritengono che le modalità di elaborazione del pensiero non siano unicamente ricomprese nei collegamenti neuronali ma che ci sia qualcosa di più – i c.d. *qualia* – che ancora non è stato di preciso individuato; insomma, il tutto è più della somma delle singole parti. Sul punto, vennero ideati esperimenti mentali quali quelli del cervello in una vasca[57] o della protesi cerebrale[58].

---

[53] La tesi di Searle si sviluppava sulla concezione per cui i "significati" attribuiti ai programmi di AI derivano completamente dai programmatori/utilizzatori umani; essi sono arbitrari rispetto al programma stesso, che pertanto è semanticamente inerte. Questi sono dunque "tutta sintassi e niente semantica", e come tali incapaci di comprendere il significato dei simboli utilizzati. Questo argomento, sebbene diretto originariamente contro l'AI simbolica, venne successivamente rivolto anche al connessionismo e alla robotica. Cfr. Sul punto BODEN, *op. cit.*, 132 ss.; RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 601 ss.

[54] Si veda Boden, la quale ricorda come le tesi sostenute da Searle e dai sostenitori dell'intenzionalità non trovino pieno riconoscimento. L'Autrice dà conto, tra gli altri, del pensiero di Newell e Simon secondo cui ogni PSS (*Physical Symbol System*) che esegue le giuste computazioni è realmente intelligente, ossia ha «i mezzi necessari e sufficienti per l'azione intelligente». BODEN, *op. cit.*, 132.

[55] Interessante sul punto Lolli, il quale sottolinea come anche la conclusione a cui giunge Searle – l'uomo non conosce il cinese – non sia dimostrata; l'uomo, infatti, potrebbe anche arrivare a imparare il cinese operando solamente con i simboli. Evocativa anche la risposta che secondo l'A. Turing avrebbe dato al filosofo per cui: «la possibilità di giocare il gioco del cinese sarebbe soltanto una prova che chi ha tradotto in regole il cinese ha fatto un lavoro completo, e che il cinese è traducibile in regole». LOLLI, *op. cit.*, 28.

[56] RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 597.

[57] Questo famoso esperimento mentale si basa sull'ipotesi che la tecnologia possa arrivare a un punto di evoluzione tale per cui sia possibile estrarre un cervello umano e farlo sviluppare immerso in una vasca ingegnerizzata. Contemporaneamente verrebbero inviati dei segnali elettrochimici al cervello grazie a una simulazione computerizzata del mondo; i segnali motori provenienti dal cervello verrebbero intercettati e utilizzati per la simulazione stessa. Se adottassimo la teoria monista dovremmo arrivare alla conclusione che il cervello fatto crescere e sviluppare in una realtà simulata potrebbe sperimentare stati mentali identici a quelli provati da qualunque persona nella realtà. Secondo un'altra concezione, invece, si ritiene che le esperienze umane, sebbene apparentemente uguali, vengano in realtà esperite in modo diverso da

Appare dunque evidente come la risposta alla domanda postaci in principio – una macchina è intelligente? – non sia univoca ma piuttosto legata a concezioni teorico-ideologiche di volta in volta assunte; così come per le difficoltà riscontrate nell'individuazione di una definizione universalmente accettata di Intelligenza Artificiale. La domanda tuttavia pare frutto di un fraintendimento legato a una visione antropomorfica delle macchine[59]. Se dovessimo eleggere come metro di paragone l'intelligenza umana, dovremmo concordare con l'assunto per cui anche qualora un sistema superasse uno tra i differenti test elaborati non potrebbe comunque considerarsi intelligente, dal momento che questo si limita a manipolare dei simboli senza comprenderne il significato semantico[60]. Ciò che fa la macchina è infatti rispondere ad un determinato *input* secondo quanto è stata programmata a fare.

Sebbene l'introduzione della statistica abbia permesso di imitare il pensiero umano in modo più accurato che non grazie alla logica deduttiva[61], potremmo parlare di macchina realmente intelligente solo nella misura in cui questa sia effettivamente in grado di comprendere quello che fa, se fosse capace di deliberazione e di autoriflessione, se potesse generare nuove idee e valutarle[62]. Ad oggi non abbiamo ancora avuto esperienza, e si dubita di averne effettivamente possibilità in futuro, di un sistema avente tali caratteristiche, le maggiori preoccupazioni sul punto muovono proprio da

---

persona a persona; ciò in quanto le sensazioni hanno natura intrinseca e quindi differente da soggetto a soggetto, anche se non si è ancora in grado di definire in che modo lo siano. Si tratta, appunto, dei c.d. *qualia*. Vedi sul punto RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 598.

[58] Anche questo esperimento mentale è volto all'indagine circa le modalità di pensiero umano. Qui si immagina un avanzamento della tecnologia tale che sia possibile sostituire singolarmente e ad uno ad uno tutti i neuroni biologici con dei neuroni artificiali e poi compiere il processo inverso, assumendo di poter mantenere in vita i neuroni biologici espiantati. Se si abbraccia una concezione secondo cui il pensiero umano è legato unicamente alle connessioni neuronali si dovrebbe concludere che anche qualora un cervello risultasse completamente composto da neuroni meccanici non ne muterebbe il funzionamento e ciò che noi intendiamo come coscienza permarrebbe; questa l'opinione di Moravec, un ricercatore di robotica e un funzionalista. Secondo Searle invece la coscienza svanirebbe, pur assumendo che il comportamento esterno potrebbe rimanere invariato. Sul punto si rimanda all'interessante critica a tale esperimento esposta da RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 2005, 599 ss.

[59] SANTOSUOSSO, *Questioni definitorie*, cit., 469 s.

[60] WARWICK, *op. cit.*, 25.

[61] Basandosi sulla statistica si può infatti studiare la probabilità con cui certe variabili co-variano senza dover tenere in considerazione il processo sottostante che le lega. In tal modo è possibile verificare come in un ragionamento induttivo premesse di certi tipi rendono altamente probabili determinate conclusioni, senza tuttavia sapere qual è il meccanismo sottostante o quali processi mentali utilizzano gli esseri umani per ragionare in modo induttivo. Utilizzando, dunque, queste metodologie si può imitare il pensiero umano, nel senso che si ottengono risultati simili, senza imitare tuttavia i processi che portano a quei risultati. DE ANNA, *op. cit.*, 130.

[62] Un sistema avente dette caratteristiche viene denominato tra gli esperti come AI forte (*strong* AI). Ad oggi tuttavia sono stati creati solamente sistemi aventi una AI debole (*week* AI) e si dubita che in futuro sia effettivamente possibile sperimentare una forma di AI forte. V. BODEN, *op. cit.*, 122.

una tale rappresentazione delle macchine quasi fossero esseri umani. Si assume infatti che il comportamento delle stesse – qualificato come intelligente – sia espressivo di un'autonomia decisionale; con tutte le derive in merito all'assegnazione ai sistemi agenti di una più o meno estesa personalità giuridica o elettronica.

Operare un confronto tra specie diverse appare però relativamente privo di significato, così come viziata appare la considerazione per cui l'unica forma di intelligenza e di coscienza sia quella umana, metro di paragone di ogni altra specie. Il dato fondamentale infatti è piuttosto il risultato espresso dalla macchina, e non se questa sia o meno un duplicato della mente umana[63].

Allo stato attuale della tecnica pertanto, oggetto di indagine dovrebbero essere le modalità di funzionamento delle macchine, la loro utilità e l'accuratezza del calcolo statistico, piuttosto che la possibilità o meno di considerarle intelligenti e autonome; ciò in ragione della necessità sempre più avvertita di una spiegazione circa i risultati conseguiti dalle stesse.

Pertanto, al fine di poter rispondere compiutamente all'esigenza di trasparenza in merito al funzionamento delle macchine, pare opportuno, seppur per brevi cenni, indagare l'evoluzione delle tecniche di addestramento dei sistemi di AI.

2. Come funziona l'Intelligenza Artificiale

Pensare all'intelligenza artificiale come ad una conquista moderna è un fraintendimento comune; la sua storia affonda le radici nel tempo. La prima macchina a controllo autonomo può essere attribuita a Ctesibio di Alessandria che nel 250 a.C. circa realizzò un orologio ad acqua dotato di un regolatore che ne manteneva il flusso costante e predicibile[64]. La spinta alla creazione di artefatti sempre più autonomi, da allora, non si è mai fermata. Le prime teorizzazioni della materia, come oggi la

[63] Sul punto interessante la considerazione di Giolito secondo cui più che un'indagine in merito all'effettiva capacità delle macchine di pensare sarebbe più utile sfruttare le nuove tecniche di addestramento, quali le reti neurali e la vita artificiale simulata, per lo studio di particolari proprietà della mente umana. Lo sviluppo della tecnologia sarebbe, infatti, di particolare rilevanza proprio perché diretto all'indagine di particolari proprietà del cervello. GIOLITO, *op. cit.*, 153 ss. Si v. anche WARWICK, *op. cit.*, 60 s.; SANTOSUOSSO, *Questioni definitorie*, *ibidem*.

[64] L'invenzione di tale macchina cambiò la concezione stessa degli artefatti. Prima si pensava che solo gli esseri viventi possedessero la capacità di modificare il proprio comportamento per reagire ai cambiamenti generati nell'ambiente. RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 22.

conosciamo, possono tuttavia essere datate intorno al 1840, quando Ada Lovelance descrisse alcuni elementi di base della programmazione moderna[65]. Si dovrà attendere ancora qualche anno perché si senta parlare di Intelligenza Artificiale, quando grazie ai lavori di Turing e alle teorizzazioni di McCulloch e Pitts il settore vide nascere un grande interesse e i risultati raggiunti portarono un periodo di forte crescita e di sostanziosi finanziamenti governativi[66]. Le prime conquiste degli anni '60 fecero però nascere aspettative irrealistiche tali per cui quando i risultati tanto proclamati non si materializzarono gran parte dei finanziamenti per la ricerca vennero meno.

Lo sviluppo del settore, contrariamente a quanto potrebbe pensarsi, non ha dunque avuto una crescita lineare ma piuttosto ha alternato periodi di forte sviluppo, guidati da grandi investimenti pubblici e oggi anche privati, e c.d. inverni in cui la ricerca pareva invece essere stata congelata. Nemmeno le ricerche nel campo delle reti neurali, attualmente le più promettenti, poterono sempre godere di riconoscimenti, così come fu per l'AI simbolica[67].

Tuttavia, nonostante periodi di crisi, la ricerca in materia non si arrestò mai definitamente ma continuò a muoversi lungo due direttrici. Da una parte un approccio "classico" basato sulla ricerca di programmi che rispondessero alla logica formale, IF/THEN, portarono alla nascita dei c.d. sistemi esperti[68]; sistemi autonomi nel portare

[65] BODEN, *op. cit.*, 12.

[66] L'interesse intorno alla materia comportò lo stanziamento, nella prima metà del Novecento, di finanziamenti governativa, in particolare dalla DARPA. Tuttavia, il settore si presentava diviso in diverse sotto-discipline; ciò può essere in parte dovuto alla diversità di approcci e di concezioni teoriche. Nel 1956 venne, dunque, istituito il famoso seminario ad Hannover, ove vennero riuniti gli allora maggiori esponenti del settore. L'obiettivo del seminario estivo era proprio quello di far avvicinare gli studiosi e facilitarne la condivisione delle conoscenze, così da unificare l'intera disciplina, allora spezzettata, in un unico campo, a cui venne dato il nome di Intelligenza Artificiale. Fu in tale occasione che si gettarono le basi di molte di quelle che in seguito sarebbero diventate le fondamenta classiche della materia. Cfr. WARWIK, *op. cit*., 22.

[67] Sempre sul finire degli anni '60 anche questo campo subì un brusco arresto a seguito delle feroci critiche mosse da Marvin Minsky e Seymour Papert. I matematici, infatti, sottolinearono i limiti e l'incapacità dei percettroni di generalizzare per affrontare determinati tipi di problemi relativamente semplici per i sistemi formali. La grande influenza che i due studiosi avevano in tutta la comunità scientifica comportò quasi immediatamente il taglio dei finanziamenti, per lo più di origine governativa, alla ricerca, comportando un'inevitabile stasi del settore. Cfr. WARWIK, *op. cit*., 24; AA. VV., *Macchine che pensano*, *ibidem*.

[68] I sistemi esperti si basano sull'utilizzo della logica classica che, in un dominio finito e conosciuto, grazie a una serie di condizioni (IF), conclusioni (THEN) e regole di risoluzioni dei conflitti, permettono alla macchina di portare a termine compiti prestabiliti in modo autonomo, come se a operare fosse un esperto nella materia. Uno dei primi sistemi testati con successo, sebbene non venne mai utilizzato sul campo, fu MYCIN. Creato nel 1975, questo software era adoperato in medicina per diagnosticare le infezioni del sangue abbinando sintomi e condizioni fisiche (condizioni) con conclusioni diagnostiche, suggerimenti di ulteriori test o prescrizioni di farmaci (azioni). Contente circa 450 regole elaborate grazie

a termine un compito specifico[69]. Dall'altra parte le ricerche si concentrarono sul funzionamento del cervello umano, e conseguentemente sul tentativo di riprodurne il funzionamento, portando a un approccio che potremmo definire "moderno" con lo sviluppo di algoritmi di *machine learning*, tra i quali possiamo ricordare le reti neurali artificiali e gli algoritmi c.d. evolutivi. Quest'ultimo approccio, complice anche la diffusione avuta nei media, è quello che oggi torna maggiormente alla mente quando si sente parlare di Intelligenza Artificiale. Prima però di procedere ad approfondire il funzionamento degli algoritmi di *machine learning* è necessario chiarire il funzionamento della metodologia classica dal momento che essa non è in disuso. Entrambi gli approcci si rivelano efficienti nella soluzione di differenti compiti, difatti le ultime ricerche in materia sembrano volte alla creazione di sistemi c.d. misti, che possano dunque sfruttare le potenzialità di entrambi e al contempo far fronte alle rispettive fragilità.

L'approccio classico all'IA, detto anche simbolico, si basa su di una logica formale IF/THEN. Ne discende che per il funzionamento della macchina è necessaria la previsione di stringhe di regole in cui debbono essere descritte le possibili condizioni (IF), in cui essa si trova ad operate, e le conseguenti risposte (THEN). Se quest'approccio funziona abbastanza bene in ambienti ristretti, emersero fin da subito i limiti a cui sarebbe andato incontro nella risoluzione di problemi nel mondo reale. Infatti, per poter gestire la complessità della realtà i progettisti avrebbero dovuto ipotizzare ogni possibile scenario a cui il sistema avrebbe potuto andare incontro, finendo così per aumentare infinitamente le condizioni (IF) memorizzate nella macchina e rendendo semplicemente impossibile la computazione; si tratta del c.d. fenomeno dell'esplosione combinatoria[70]. A ciò si aggiunga la grande difficoltà di poter prevedere

---

alle interviste fatte agli esperti del settore, MYCIN veniva considerato più affidabile di molti giovani medici e valido come alcuni dei più competenti. La particolarità di questo sistema era legata alla necessità che le regole su cui esso si basava dovessero rispecchiare le incertezze intrinsecamente associate alla conoscenza medica; a questo fine venne implementato un metodo di calcolo di incertezza denominato "fattori di certezza".
Ad oggi i moderni sistemi esperti spaziano dai programmi utilizzati nella ricerca scientifica e nel commercio, alle semplici applicazioni per i telefoni. La grande utilità di questi programmi è, dunque, rappresentata dalla loro capacità di sostituire gli esperti umani in campi ben determinati. Per un'analisi più approfondita del funzionamento dei sistemi esperti si rimanda a WARWIK, *op. cit*., 67 ss.; RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 1, 32 ss.; BODEN, *op. cit*., 34 ss.

[69] BUTTOLO, *op. cit*., 81.

[70] Con il termine "esplosione combinatoria" si intende quel fenomeno generato dal moltiplicarsi delle condizioni implementate in un sistema, tale per cui esse richiedano più computazioni di quante possano essere in effetti supportate. Uno degli obiettivi principali degli agenti aventi AI è quello di affrontare

ogni possibile scenario e conseguentemente le possibili conclusioni a cui dovrebbe rispondere il sistema agente. Se anche, in linea teorica, potessimo immaginare di "mappare" tutto il possibile, va tuttavia tenuto in considerazione che lo stesso agire della macchina potrebbe comportare un mutamento dell'ambiente in cui essa opera, generando così nuove variabili capaci di influenzarne l'agire e di cui sarebbe dunque necessario "istruire" il sistema. Inoltre, queste modalità di funzionamento potrebbero comportare ridondanze tali da rallentare l'operato della macchina, trovandosi questa nella condizione di dover ogni volta vagliare dal principio anche le condizioni già in precedenza analizzate. Possiamo dunque vedere le difficoltà dell'approccio classico quando questo si trovi a operare in ambienti dove ci siano molte variabili.

Per ovviare a tale problema si introdussero dei condizionamenti – delle euristiche[71] – e dei *frame*[72]. Con tale ultimo termine si intende una rappresentazione della conoscenza mediante strutture dati a carattere gerarchico che rappresentino singoli concetti. Attraverso queste strutture dati i computer possono rintracciare in modo più efficiente

---

problemi e ricavare conclusioni, indipendentemente dalla situazione in cui si trovano a operare. Tuttavia, per poter far fronte a qualsiasi evenienza, bisognerebbe aggiungere continuamente delle regole in grado di coprire ogni situazione possibile, non importa quanto improbabile. La presenza di numerose regole può comportare un rallentamento del sistema, tale per cui esso risulti molto più lento di un essere umano nel prendere una decisione. Anche il *debug*, effettuato allo scopo di garantirne il corretto operare, può rivelarsi difficile a causa della molteplicità di regole che interagiscono rischiando di invalidarsi a vicenda. WARWIK, *op. cit*., 75.; BODEN, *op. cit*., 26.

[71] Il termine non ha avuto origine con la programmazione; è molto più familiare tra i logici e i matematici che lo usano da molto tempo. Sia negli esseri umani che nelle macchine le euristiche facilitano la soluzione dei problemi. Nell'ambito dell'AI lo fanno orientando il programma verso certe parti dello spazio di ricerca e allontanandolo da altre. Molte euristiche, tra cui la maggior parte di quelle usate agli albori dell'AI, sono regole empiriche che non garantiscono il successo. Indipendentemente dal grado di affidabilità, le euristiche sono oggi un aspetto essenziale della ricerca nell'ambito dell'Intelligenza Artificiale. Ciò in quanto il crescente specialismo a cui si assiste dipende in parte dalla definizione di nuove euristiche che possono migliorare grandemente l'efficienza dei sistemi, ma solo in un genere di problema o di spazio di ricerca molto ristretto. Per esempio, il programma IBM per gli scacchi Deep Blue, che fece grande scalpore battendo il campione del mondo Gary Kasparov nel 1997, utilizzava *chip hardware* dedicati, che elaboravano 200 milioni di posizioni al secondo, generando ogni possibile mossa fino a otto mosse in avanti. Tuttavia, esso doveva utilizzare le euristiche per selezionare la mossa "migliore" tra quelle elaborate. Poiché le sue euristiche non erano affidabili, neanche Deep Blue riuscì a battere Kasparov tutte le volte. BODEN, *op. cit.*, 28 ss.

[72] Oltre a queste, per ovviare al problema dell'esplosione combinatoria, sono state utilizzate nel corso degli anni differenti tecniche. Si pensi: agli alberi di decisione; alle tecniche di risoluzione dei conflitti; alle ricerche *depht-first* o *breadth-first*. Tra i vari approcci di particolare interesse, anche per le prospettive di applicazione futura, è la logica *fuzzy*, grazie alla quale è possibile operare con un concetto "sfumato". A differenza della logica formale, ove si hanno solamente due possibilità, pieno o vuoto, vero o falso, 0 o 1, grazie alla funzione *fuzzy* è invece possibile operare nell'incertezza. Sebbene le regole siano sempre IF/THEN, in questo caso abbiamo a che fare con delle condizioni che possono anche essere vere solo in parte. Un sistema *fuzzy*, infatti, permette di contemplare le funzioni come percentuale di un dato valore di riferimento. Per un approfondimento in merito al funzionamento dei sistemi *fuzzy* si rimanda a WARWIK, *op. cit*., 76 ss.; BODEN, *ibidem*.

analogie necessarie per conoscere l'ambiente in cui operano e selezionare le possibili azioni[73]. L'uso di queste tecniche permetterebbe dunque una selezione delle condizioni, tra tutte quelle possibili, che in un dato momento debbano essere vagliate per poter arrivare al risultato voluto. Ciò comporta un notevole risparmio di tempo e di energia da parte del sistema, che non dovrebbe ripetere operazioni ridondati né verebbe influenzato da ogni minimo cambiamento dell'ambiente. L'intuizione dei *frame* nacque proprio osservando il modo di agire umano; gli esseri umani, infatti, nella scelta delle proprie azioni operano anche grazie a una conoscenza del mondo che permette di poter dare per assodate alcune nozioni, dedicando l'attenzione in modo più specifico al compito da dover svolgere, senza dunque essere costretti a valutare nuovamente il proprio ambiente a ogni minimo mutamento.

Sebbene siano per alcuni aspetti simili, i sistemi esperti basati sulle regole e quelli basati sui *frame* funzionano in maniera differente. Come è possibile intuire i sistemi esperti basati sulla logica IF/THEN sono maggiormente *data driven*. Ne discende che il cambiamento anche di un piccolo parametro potrebbe comportare un rallentamento del sistema, dovendo esso vagliare tutta la catena di eventi che possono derivare dal tale cambiamento. Nei sistemi basati sui *frame*, invece, se tale cambiamento non interessa lo specifico *frame* preso in considerazione esso non avrà alcun impatto nella decisione finale della macchina, non rallentandone quindi l'opera.

Da quanto sopra brevemente riportato potremmo concludere definendo l'approccio classico come funzionale. Questo, adottando una prospettiva top-down[74], mira infatti all'osservazione e alla replica del comportamento umano in determinate situazioni al

---

[73] Un *frame* rappresenta, dunque, la conoscenza-tipo su di una determinata entità. Semplificando, si tratta di un file compreso nel computer contenente un certo numero di informazioni memorizzate nei suoi *slot*. Ognuno di questi *slot* è di per sé un *sub-frame* con ulteriori livelli di informazioni. Un esempio potrà forse meglio chiarirne il funzionamento. Si assuma di avere un sistema AI basato su *frame* che si utilizza per operare in una casa. È possibile dire al computer che cosa è una stanza, specificando una struttura dati a carattere gerarchico (appunto un *frame*) che rappresenta una stanza come avente: un pavimento; un soffitto; dei muri; delle porte; delle finestre e un arredamento. Le stanze reali hanno un numero variabile di muri, porte e finestre, pertanto il *frame* possiede degli *slot* in cui è possibile specificare il numero effettivo di questi elementi; è anche possibile assegnare valori di *default*. BODEN, *op. cit*., 30 ss.; WARWIK, *op. cit*., 92.
Interessante sul punto la considerazione di Boden secondo cui «I *frame* possono essere ingannevoli. Le assunzioni di *default*, per esempio, sono problematiche (qualche stanza non ha finestre e gli *open space* non hanno porte). Oppure si pensi ai concetti di uso quotidiano quali cadere o versare. Pertanto in alcune applicazioni che utilizzano tecniche recenti per trattare i Big Data, un singolo concetto può essere rappresentato come un *cluster* (grappolo), o un *cloud* (nuvola), composta da centinaia o migliaia di concetti talvolta associati, in cui le probabilità delle molte associazioni tra le coppie sono distinte». BODEN, *op. cit*., 36.
[74] WARWIK, *op. cit*., 66.

fine di poter individuare delle soluzioni efficienti che permettano il raggiungimento del compito affidato al sistema. Tuttavia il grande successo mediatico che gira attorno all'Intelligenza Artificiale oggi, si basa su un diverso paradigma. L'approccio moderno è infatti orientato in una prospettiva opposta, bottom-up. Si procede dallo studio di alcune caratteristiche del cervello umano per poi creare dei modelli semplificati dello stesso e, dunque, studiarne i risultati. A questa branca possiamo ricondurre il *machine learning* (che potremmo tradurre come apprendimento automatico), all'interno del quale una tra le tecniche forse più nota è il *deep learning*, che permette il riconoscimento dei *pattern* presenti nei dati a vari livelli gerarchici[75]. Le reti neuronali, di cui si stente molto parlare, sono implementate proprio mediante algoritmi di *deep learning*, queste tutta via non esauriscono il campo di ricerca. Per esempio grande interesse negli ultimi anni hanno avuto gli algoritmi genetici[76].

Con il termine *machine learning*, dunque, si intendono quelle tecniche che permettono a una macchina di apprendere in maniera automatica, senza cioè essere specificamente programmate con singole strisce di comando. Come visto poc'anzi, vi sono diverse tecniche e algoritmi che permettono questo tipo di apprendimento, tuttavia per necessità espositive il presente lavoro si concentrerà sul *deep learning* e sulle reti neurali, in quanto gran parte dell'interesse giuridico sul tema dell'Intelligenza Artificiale oggi è dedicato proprio a detti algoritmi, in parte grazie anche all'attenzione mediatica che ha accompagnato i primi successi ottenuti e i recenti investimenti nel settore.

---

[75] In altri termini il *deep learning* scopre una rappresentazione della conoscenza multilivello – per esempio, dai *pixel* ai rilevatori di contrasto, ai rilevatori di contorni, ai rilevatori di forma, alle parti degli oggetti, agli oggetti. V. sul punto BODEN, *op. cit.*, 49 s. Interessante anche la definizione data da GOODFELLOW, BENGIO, COURVILLE, *Deep Learning*, Cambridge, 2016, 8 ss., secondo cui il *deep learning* è un tipo di *machine learning*, una tecnica che permette a un sistema di migliorare con l'esperienza e con i dati. Secondo gli Autori questa tecnica sarebbe quella maggiormente idonea alla creazione di sistemi di AI che possano operare nella complessità dell'ambiente reale.

[76] Questa tipologia di algoritmi, noti anche come algoritmi evolutivi, imita i processi di selezione naturale al fine di poter arrivare alla migliore soluzione possibile, partendo da una serie di soluzioni potenziali. In questo approccio ciascun membro della popolazione è definito secondo un corredo genetico che lo descrive in maniera univoca. Tale composizione può essere descritta in codice binario, in termini di 1 e 0. Per passare da una generazione all'altra, i cromosomi di un individuo si mescolano/accoppiano a quelli di un altro, tramite processi di *cross-over* o di mutazione, che traggono ispirazione dai corrispettivi biologici. Vi sarà dunque una nuova popolazione, composta da nuovi cromosomi e nuovi individui. Ciascun individuo verrà valutato in base alla funzione di *fitness* – che definisce l'idoneità dei nuovi soggetti a seconda del problema per il quale si applica l'algoritmo genetico – e la popolazione ridotta eliminando i cromosomi meno idonei. L'intero processo è ripetuto selezionando gli individui più efficienti fino a che la funzione di *fitness* non produce nessuna, o pochissime, variazioni. Solo a quel punto si può assumere di aver trovato una soluzione. WARWIK, *op. cit.*, 167 ss. Per un approfondimento si v. anche BODEN, *op. cit.*, 108 ss.; AA. VV., *Macchine che pensano*, *op. cit.*, 137.

A mero titolo di esempio, basta guardare al grande interesse suscitato da Deep Blue, che nel 1997 ha battuto il campione di scacchi Kasparov, da Watson, un software IBM che dopo aver vinto al gioco Jeopary! nel 2011 oggi viene utilizzato per le diagnosi mediche[77], o ancor più di recente ad AlphaGo, che nel 2016 ha battuto Lee Sedol, uno dei più grandi campioni mondiali di Go[78]. Oltre a queste dimostrazioni di abilità, si pensi al dibattito in merito alla circolazione delle auto a guida autonoma o all'utilizzo di robot medicali; compiti che fino a pochi anni fa venivano ritenuti troppo complessi per un sistema meccanico[79]. Tutti questi software, sempre più abili nel compiere azioni complesse, si basano su sistemi algoritmici che prevedono l'utilizzo di diverse reti neurali artificiali (*Artificial Neural Network*) che permettono alle macchine non solamente di processare numerose variabili ma anche di "imparare" dall'esperienza.

Per meglio comprendere come funzionino tali macchine, e come esse possano "imparare", è necessario fare un passo indietro. La prima teorizzazione delle reti neurali è nata anch'essa nella prima metà del secolo scorso grazie al lavoro di McCulloch e Pitts, i quali nel 1943 descrissero modelli matematici di neuroni che chiamarono

[77] Per un approfondimento in merito al funzionamento di Watson si rimanda a BODEN, *op. cit.*, 66 ss.

[78] Il Go fino al 2016 veniva ritenuto un gioco troppo complesso per una macchina. In questo gioco due avversari si affrontano posizionando sul tavolo da gioco delle pedine bianche e nere con l'obiettivo di conquistare più territorio possibile. Si gioca su una scacchiera 19x19, che permette circa 10^{171} combinazioni possibili, contro le circa 10^{50} di una normale scacchiera 8x8. Il software sviluppato da DeepMind, che proprio nel 2016 riuscì a battere uno dei migliori giocatori a livello mondiale, utilizza diverse reti neurali. Innanzitutto l'algoritmo imparò il gioco attingendo a un *database* contente quasi 30 milioni di mosse, costruito da giocatori umani esperti. La rete poi potè migliorare giocando migliaia di partite contro altre versioni di sé stessa. Una diversa rete stima le possibilità di vittoria a partire da una certa configurazione della scacchiera e infine, un algoritmo di ricerca esamina l'intero "albero" di mosse possibili in una partita per determinare quale cammino offra maggiori possibilità di vittoria. L'utilizzo di differenti reti neurali ha dunque permesso ad AlphaGO, non solo di apprendere le regole del gioco e le strategie utilizzate dai campioni mondiali, ma anche di elaborane alcune del tutto inedite. All'esito della competizione con Lee Sedol alcuni commentatori, in particolare dopo una mossa inedita e particolarmente ardita che si è rivelata essere la chiave della vittoria, hanno ritenuto che AlpahaGo sia dotata di quello che noi chiamiamo intuito. AA. VV., *Macchine che pensano*, *op. cit.*, 73 ss.

[79] Le reti neurali, lungi dall'essere utilizzate unicamente nei giochi, hanno diverse possibili applicazioni, dalla finanza alla medicina. Proprio in quest'ultimo campo l'impiego dell'Intelligenza Artificiale pare essere particolarmente attivo. Un gruppo di ricercatori dell'Università di Tel Aviv usa l'apprendimento profondo per analizzare lastre al torace. Il loro sistema è in grado di distinguere tra un cuore ingrossato e l'accumulo di liquido intorno ai polmoni. Un altro gruppo di ricerca, del National Institute of Health Clinical Center di Bethesda, nel Maryland, usa metodi simili per rilevare crescite cancerose a livello della colonna vertebrale; abbiamo già nominato Watson, che in un caso ha impiegato solo qualche minuto per individuare una rara forma di leucemia secondaria in un paziente.
La DeepMind di Google ha in corso diversi progetti in ambito medico e, grazie a una collaborazione con il sistema sanitario nazionale del Regno Unito, ha accesso a grandi quantità di dati sui pazienti. AA. VV., *Macchine che pensano*, *op. cit.*, 124.

percettroni[80]. Sul modello elaborato dai due matematici vennero poi implementate le prime vere reti neurali, seppure aventi una dimensione ridotta, composte da una serie di percettroni tra loro collegati a cui venivano sottoposti dei dati di *input* e a cui seguivano delle risposte, *output*, di natura binaria[81].

Il funzionamento delle reti neurali artificiali si ispira dunque al cervello umano. Queste vengono programmate con diversi livelli di neuroni artificiali, o nodi, tra loro collegati e aventi ognuno un "peso". Le reti oggi maggiormente utilizzate sono quelle multi livello, ove cioè sono presenti oltre all'*input* e all'*output* anche dei livelli "nascosti" composti da nodi che processano i dati raccolti. Ogni livello (*layer*) di neuroni indaga a un diverso livello di astrazione e trasmette l'informazione al livello successivo a cui esso è collegato, fino all'ultimo che corrisponde all'*output* del sistema[82]. Questa tipologia di algoritmi viene utilizzata per esempio nel riconoscimento delle immagini; in questi casi verrà fornita al sistema un'immagine, questa verrà scomposta e indagata a diversi livelli di astrazione – per esempio verranno indagati i *pixels*, i toni dell'immagine, i contorni etc. – allo scopo di ritrovare collegamenti (*patterns*) con i dati di addestramento e poter giungere a catalogare l'immagine come appartenente o meno a una data categoria. Una volta restituito un risultato, solitamente un algoritmo di *back-propagation* confronta il risultato ottenuto dal sistema neurale e modifica di conseguenza i singoli pesi dati ai nodi, così da rinforzare alcuni

[80] I percettroni vennero ideati da McCulloch e Pitts ispirandosi al funzionamento di un neurone biologico. Il neurone biologico, infatti, riceve una serie di segnali attraverso i dendriti (le linee di *input*), ciascuno dei quali può essere più o meno influente. Tutti i segnali ricevuti dal singolo neurone vengono sommati e il risultato viene confrontato con il livello soglia: se la somma totale è uguale o superiore a questo valore, il neurone scarica; se è inferiore non scarica. Similmente opera anche il modello creato dai due matematici. Nel percettrone i valori di ingresso x e y sono moltiplicati per i pesi W_1 e W_2 e poi sommati. Il totale viene confrontato con un valore soglia, cioè un valore negativo che la somma dei valori di *input* pesati deve sorpassare. Se la somma degli *input* pesati è uguale o superiore al dato valore il percettrone scarica, producendo un *output* "1"; se, invece, la somma è inferiore, questo non scarica e produce un *output* "0". L'*output* può essere a sua volta moltiplicato per il proprio peso prima di divenire l'*input* del percettrone successivo. Per una approfondimento si rimanda a WARWIK, *op. cit.*, 153 s.

[81] Minsky ed Edmonds realizzarono il primo computer AI basato su una rete di modelli neurali così come descritti da McCulloch e Pitts. Cfr. WARWIK, *op. cit.*, 21 s. Si trattava, tuttavia, di una rete avente un solo livello nascosto di neuroni. Il grande successo si ebbe però solo recentemente, quando si scoprì un metodo efficiente per consentire alle reti multistrato di scoprire relazioni su multilivelli. Questo fu reso possibile dalle tecniche di *deep learning* che permisero al sistema di apprendere la struttura, raggiungendo in profondità un dominio e non solo *pattern* superficiali. In altri termini grazie a questa tipologia di algoritmi il sistema scopre una rappresentazione della conoscenza a più livelli, anziché a livello unico, come invece accadeva nelle prime applicazioni delle reti neurali. V. BODEN, *op. cit.*, 87 s.

[82] Per un approfondimento tecnico in merito al funzionamento delle diverse tipologie di reti neurali si rimanda a RUSSELL, NORVIG, *Intelligenza Artificiale*, cit., 2, 423 ss. e a GOODFELLOW, BENGIO, COURVILLE, *op. cit.*, 489 ss. È possibile vedere le modalità di funzionamento di una rete neurale all'indirizzo: *https://playground.tensorflow.org*.

collegamenti e indebolirne altri; ciò al fine di giungere in maniera ottimale e più velocemente possibile al risultato corretto[83]. In questo senso è possibile dire che l'algoritmo è autonomo e che "impara", questo in quanto non è il programmatore del software a modificare i singoli pesi dei neuroni appartenenti alla rete. In ragione della sempre maggiore complessità data dall'estensione della rete è un altro algoritmo che compie quest'ultimo passaggio a partire dei risultati ottenuti dal sistema. Potremmo dunque dire che l'algoritmo impara dall'esperienza modificando la stessa rete neurale. Infatti, se un dato collegamento porta a una risposta giusta allora verranno aumentati i pesi di quella "catena"; ciò comporterà collegamenti più "forti" che porteranno più velocemente a quel risultato corretto. Se invece il risultato ottenuto non è corretto, allora i pesi dei singoli neuroni verranno diminuiti finendo così con rendere sempre meno possibili quei collegamenti che hanno portato a una risposta errata.

Evidentemente, per fare ciò è necessario un lungo periodo di addestramento delle reti neurali, addestramento che viene compiuto sottoponendo le stesse a una grande quantità di dati che possono essere o meno catalogati. Tra le diverse tipologie di addestramento, quelle maggiormente utilizzare sono: l'apprendimento per rinforzo, l'apprendimento supervisionato e quello non supervisionato[84]. Brevemente, nell'apprendimento supervisionato vengono fornite alla rete neurale una grande serie di dati (*input*) classificati[85]. A questa vengono poi sottoposti nuovi dati, questa volta non catalogati, che la macchina deve riconoscere nel senso di riportarne l'appartenenza o meno ad una data categoria, generando dunque ipotesi sui tratti rilevanti. L'addestramento termina con una validazione compiuta da chi addestra il sistema, il quale dovrà verificare che la risposta data dalla macchina sia o meno corretta.

---

[83] GOODFELLOW, BENGIO, COURVILLE, *op. cit.*, 18 e 203 ss.; DENG, YU, *Deep Learning: Methods and Applications* (2014) 7 *Foundations and Trends in Signal Processing* 203 ss.; LECUN, BENGIO, HINTON, *Deep Learning* (2015) *Nature* 436 ss.; BENGIO, *Learning Deep Architectures for AI* (2009) 2 *Foundations and Trends® in Machine Learning* 10 ss.; LEXCELLENT, *op. cit.*, 10 ss.

[84] Per un approfondimento in merito alle tecniche di addestramento delle reti neurali si rimanda a GOODFELLOW, BENGIO, COURVILLE, *op. cit.*, 105 ss.; DENG, YU, *op. cit.*, 197 ss.; LECUN, BENGIO, HINTON, *ibidem*.

[85] Per il riconoscimento delle immagini viene oggi grandemente utilizzato un *dataset* chiamato ImageNet, il quale comprende un grandissimo numero di immagini di varia natura già etichettate. É possibile usufruire di diverse tipologie e grandezze di *dataset* per addestrare le Intelligenze Artificiali al riconoscimento delle immagini; per esempio Labeled Faces in the Wild contiene una collezione di oltre 13.000 immagini di volti presi dal web. L'utilizzo di tali *dataset* comporta evidentemente un notevole risparmio di tempo per gli addestratori, i quali non dovranno catalogare ogni singola immagine. AA VV., *Macchine che pensano*, *op. cit.*, 70.

Nell'apprendimento per rinforzo, invece, i dati solitamente non vengono già previamente catalogati, ma vengono sottoposti alla macchina in modo che essa riesca a riconoscere dei *patterns* e possa essa stessa suddividerli in categorie. I risultati espressi dal sistema vengono quindi validati dall'addestratore; questo tipo di addestramento risulta quello maggiormente praticato oggi. Infine, l'apprendimento non supervisionato, ad oggi ancora poco utilizzato, permette di sottoporre al sistema una serie di dati senza alcuna catalogazione, lasciando dunque che sia il sistema stesso a imparare le proprietà utili dalla struttura del *dataset*. In partica, l'utilizzatore non fornisce né risultati attesi né messaggi di errore. L'apprendimento è guidato dal principio secondo cui i tratti che concorrono generano aspettative sul fatto che concorreranno anche in futuro, dunque i programmatori non hanno bisogno di sapere quale *pattern* o *cluster* è presente nei dati in quanto sarà il sistema stesso a scoprirlo autonomamente[86]. Sebbene oggi questo approccio sia ancora poco sviluppato, in ragione del comprensibile timore in merito alla possibile perpetrazione di *bias* non riconosciuti come tali dal sistema, appare comunque essere molto promettente, dal momento che si ritiene possa essere utilizzato per scoprire nuove conoscenze, potendo dunque trovare sempre maggiore applicazione in futuro[87].

Chiarito il funzionamento delle reti neurali, a prescindere dalle modalità di addestramento, una tra le maggiori preoccupazioni in merito all'utilizzo delle stesse è legato a una loro intrinseca opacità. Se infatti da una parte è possibile conoscere i dati di addestramento e gli *output* della macchina, difficile è comprenderne le effettive modalità di scelta. Ciò è dovuto alle interazioni tra i nodi che compongono i livelli intermedi "nascosti" in queste reti. É difatti difficile risalire a quale delle possibili variabili, che a loro volta interagiscono con i dati in ingresso, abbia avuto un peso prevalente nella determinazione della scelta della macchina. Questa condizione è stata definita, con una felice espressione, *black box*[88], proprio in ragione della complessità e opacità di funzionamento anche agli occhi degli stessi ideatori. Finché i risultati ottenuti sono corretti *nulla quaestio*. Tuttavia qualora il sistema sbagli, o mostri risultati discriminatori, la difficoltà di arrivare a una spiegazione che sia intellegibile comporta

[86] BODEN, *op. cit.*, 47 s.; GOODFELLOW, BENGIO, COURVILLE, *ibidem*; DENG, YU, *op. cit.*, 214 ss.
[87] LECUN, BENGIO, HINTON, *op. cit.*, 436 ss. Dello stesso parere anche BENGIO, *Learning Deep Architectures for AI*, cit.
[88] Questa espressione viene adoperata con riguardo al funzionamento degli algoritmi di Intelligenza Artificiale da PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, 2015.

l'emergere di preoccupazioni in merito all'utilizzo e, soprattutto, in merito alla questione di chi debba essere ritenuto responsabile di eventuali danni.

La difficoltà di spiegazione circa i risultati ottenuti dai sistemi contenenti algoritmi non lineari ha spinto gli esperti alla creazione di modelli algoritmici che permettano di risalire, in modo maggiormente efficiente in termini di tempi e costi, alle modalità di funzionamento degli stessi. Queste tipologie di modelli, che possiamo definire *interpetrable by design*[89], sono stati ideati sul presupposto per cui debba essere sacrificata in parte la precisione dei risultati ottenuti; questo in quanto la difficoltà di spiegazione nasce proprio dalla complessità del numero di dati processati, che tuttavia permette al contempo una maggiore accuratezza nei risultati. La diminuzione degli *input*, quindi delle variabili, permetterebbe una maggiore controllabilità e di conseguenza una spiegabilità del processo decisionale. Quello a cui si vorrebbe giungere parrebbe essere un giusto mezzo tra efficienza e spiegabilità[90].

Altre proposte furono avanzate in tema, tra cui quelle di progettare gli algoritmi con una sorta di *check point*, cioè dei nodi ove sia possibile controllare la correttezza delle operazioni svolte dall'algoritmo fino a quel momento. Questa metodologia tuttavia comporterebbe un rallentamento nel funzionamento del sistema, andando così ad inficiare una delle maggiori funzionalità dello stesso: la velocità di decisione.

Rimandando al prosieguo l'analisi delle criticità legate alle decisioni algoritmiche, e alla sentita esigenza di una maggiore trasparenza nel funzionamento delle tecnologie digitali nel contesto della materia che qui ci occupa[91], appare opportuno dare conto di un elemento imprescindibile a una completa analisi del fenomeno.

Dalla veloce analisi compiuta è emerso infatti come nonostante le origini dell'IA siano risalenti, i primi successi si ebbero solo sul finire del XX secolo, grazie al grande aumento della potenza di calcolo dei computer e, soprattutto, alla quantità di dati utilizzabili per "addestrare" le macchine. Il c.d. fenomeno dei Big Data rappresenta il fattore fondamentale di crescita e di sviluppo dell'intera Intelligenza Artificiale. Come è

[89] LISBOA, *Interpretability in Machine Learning – Principles and Practice*, in *Fuzzy Logic and Applications 10th International Workshop*, *Genoa, November 19-22*, 2013, 16 ss.
[90] LISBOA, *Interpretability in Machine Learning*, cit., 15; VELLIDO, MARTIN-GUERRERO, LISBOA, *Making machine learning models interpretable*, in *European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning*, Bruges, 2012, 163 ss.
[91] Un'analisi approfondita in merito alle istanze di spiegabilità delle decisioni algoritmiche verrà trattata *infra* nel capitolo 4 del presente lavoro.

stato giustamente osservato, se possiamo concepire l'IA come il motore della nuova rivoluzione tecnologica, certamente i dati ne rappresentano il carburante[92].

2.1 Intelligenza Artificiale e Big Data. Quale ruolo dei dati e prime criticità

Parlare di Intelligenza Artificiale non può prescindere da un'analisi circa i dati, siano essi di addestramento o prodotti dagli stessi artefatti digitali.

Dall'indagine in merito al funzionamento degli algoritmi è difatti emerso come il grande successo degli ultimi anni sia addebitabile in buona parte all'enorme disponibilità di dati che, come visto, sono necessari all'addestramento e in definitiva allo stesso funzionamento dell'IA. I dati prodotti e utilizzabili hanno difatti subito una crescita esponenziale grazie allo sviluppo della rete internet e alla diffusione dell'*Internet of Things* (IoT). Detto termine è stato coniato nel 1999 dal ricercatore britannico Kevin Ashton[93] per indicare il *network* di artefatti che posseggono una connessione a internet, necessaria al fine di conservare e scambiare i dati raccolti tramite sensori, oltre che per avere accesso a diversi contenuti presenti nelle banche dati; si tratta tendenzialmente di oggetti di uso quotidiano quali smartphone, ma anche frigoriferi, sveglie, orologi, termostati etc., che grazie alla connessione internet possono comunicare tra loro e raccogliere dati che poi verranno conservati nel *cloud* e trattati[94]. Grande attenzione all'IoT, data la sua importanza strategica per il mercato digitale, è

[92] ANGELINI, *Intelligenza Artificiale e* governance, cit., 296.

[93] MACERATINI, *Dall'*Internet of Things *alle* Smart Roads*. Riflessioni informatico-giuridiche su strade intelligenti, veicoli automatici e connessi*, in *Riv. elett. dir. eco. man*., 2019, 72; SANTOSUOSSO, *Intelligenza artificiale e diritto*, cit., 180; GAETA, *La protezione dei dati personali nell'*Internet of Things*: l'esempio dei veicoli autonomi*, in *Dir. inform*., 2018, 147 s. L'Autrice, sul punto, sottolinea come sebbene la paternità dell'espressione sia attribuita ad Ashton, così come confermato dalla dottrina maggioritaria, la nascita dell'IoT è stimata intorno agli inizi del XXI secondo, quando il numero di dispositivi connessi in rete ha superato quello della popolazione mondiale.

[94] Particolarmente chiara la definizione riportata da Gaeta secondo cui «L'IoT è un'architettura che facilita lo scambio di beni e servizi e si traduce in un network informatico che collega tra loro oggetti – fisici o virtuali – che si rendono riconoscibili e acquisiscono intelligenza grazie alla possibilità di comunicare dati su se stessi e sull'ambiente che li circonda». GAETA, *ibidem*. Interessanti anche le considerazioni di Maceratini, secondo cui «[…] siamo di fronte al fenomeno di oggetti di uso quotidiano "intelligenti", ovvero, capaci di interagire fra loro e con gli utenti, sviluppando le potenzialità insite nella rete in direzione di innovative applicazioni delle informazioni provenienti dall'ambiente». MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, *ibidem*. Le definizioni di IoT sono molteplici, sul punto si rimanda a D'ACQUISTO, NALDI, *Big Data e Privacy by Design*, Torino, 2017, 20 s.; SANTOSUOSSO, *Diritto, Scienza, Nuove Tecnologie*, Padova, 2016, 318; BENEDETTI, *IA e (in)sicurezza*, in *Intelligenza Artificiale, protezione dei dati personali e regolazione*, a cura di PIZZETTI, Torino, 2018, 239 ss.; SARZANA DI SANT'IPPOLITO, NICOTRA, *Diritto della Blockchain, intelligenza artificiale e IoT*, Milano, 2018, 281 ss.; SANTOSUOSSO, *Intelligenza artificiale e diritto*, cit., 180 s.

dedicata anche dalle Istituzioni europee[95]. Già nel 2015 nel contesto della strategia UE per il mercato unico digitale venivano comprese strategie per accelerare lo sviluppo delle IoT, in particolare evitando la frammentazione e favorendo l'interoperabilità tra i sistemi[96].

Oggi si sente sempre più spesso parlare di *Internet of Everything* in quanto la crescente diffusione e pervasività nell'utilizzo di tali oggetti ha permesso una connessione pressoché generalizzata delle apparecchiature elettroniche, si ritiene infatti che siano più di venti miliardi gli oggetti tra loro connessi[97]. Da quanto riportato appare pertanto evidente come il numero dei dati prodotti abbia avuto negli anni una grande crescita e sia destinato ad aumentare ancora in futuro. La soglia degli zettabyte è stata ormai raggiunta e la crescita non accenna a fermarsi; si stima che entro il 2025 si produrranno circa 163 zettabyte di dati. Per avere un'idea della effettiva grandezza basti considerare che uno zettabyte corrisponde a 10^{12} gigabyte[98].

É facile comprendere come sia possibile arrivare a tali cifre se solo si osserva il cambiamento sociale che ha portato i cittadini a vivere in quella che è stata efficacemente definita Infosfera[99]. Il processo di digitalizzazione, che consente la

---

[95] Una definizione di IoT è presente anche nel sito internet dell'UE dedicato al *digital single market* e all'*Internet of Things* secondo cui: «*Internet of Things (IoT) merges physical and virtual worlds, creating smart environments.* […] *(IoT) represents the next step towards the digitisation of our society and economy, where objects and people are interconnected through communication networks and report about their status and/or the surrounding environment*». Definizione consultabile all'indirizzo: *ec.europa.eu/digital-single-market/en/internet-of-things* (ultimo accesso 3 novembre 2020).

[96] Espressione di tale interesse è dimostrata dalla creazione di un'associazione, l'*Alliance for Internet of Things Innovation*, lanciata dalla Commissione nel 2015 al fine di sostenere la creazione di un ecosistema di IoT innovativo.

[97] Si ritiene, infatti, che la tendenza sia quella di vedere connessi persone, dati e procedure utilizzando sistemi capaci non solo di memorizzare, ma altresì di apprendere e generare informazioni, evidentemente grazie all'utilizzo di tecniche di Intelligenza Artificiale. MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 73; GAETA, *op. cit.*, 148; Interessanti le considerazioni di SANTOSUOSSO, *Intelligenza artificiale e diritto*, cit., 182. L'A. richiama una descrizione analitica del fenomeno ritenendo che esso si componga di quattro elementi: persone; dati; processi e cose. Ne segue, dunque, una valorizzazione non solamente delle persone/cose e dei dati da essi prodotti, ma anche degli stessi processi che permettono i collegamenti tra le varie entità a fondamento del *network* così creato. La necessità di collegamenti con un tempo di latenza sempre più ridotto non viene spesso valorizzata, sebbene essa sia l'obiettivo a fondamento della diffusione della rete 5G. Collegamenti sempre più istantanei, che permettano dunque la trasmissione del comando quasi in tempo reale, difatti è necessaria allo sviluppo di tecnologie di Intelligenza Artificiale, tra cui anche le auto *driverless*, le quali necessitano di collegamenti veloci con l'infrastruttura e con gli altri veicoli per poter correttamente circolare.

[98] Per fare un paragone esplicativo, uno zettabyte corrisponde a una capacità di archiviazione pari a oltre 36.000 anni (in termini di durata) di video in HD, corrispondente a una pila composta da 250 miliardi di DVD. V. DALMASTRO, NICITA, *Big Data. Come stanno cambiando il nostro mondo*, Bologna, 2019, 25.

[99] Il termine è stato coniato da Floridi, il quale specifica come esso denoti «l'intero ambiente informazionale costituito da tutti gli enti informazionali (inclusi gli agenti informazionali), le loro proprietà, interazioni, processi e relazioni reciproche. È un ambiente comparabile a quello del cyberspazio

trasformazione delle informazioni in dati fruibili digitalmente, e la pervasività dell'utilizzo del web, ha difatti creato una vera e propria società dell'informazione ove ogni cosa è a portata di click[100]. I vantaggi, anche in termini di inclusività e di benessere sociale, sono innegabili. Non è tuttavia, come si suol dire, tutto oro quel che luccica. Da una parte infatti si sono acuite le fratture tra ricchi e poveri; già oggi non solo le fasce più povere delle società, ma finanche intere popolazioni si trovano in una posizione di inferiorità tecnologica[101]. I rischi discendenti da una progressiva esclusione dalla

---

(che è in realtà solo una sua sub-regione), dal quale tuttavia differisce, perché include anche lo spazio offline e quello analogico dell'informazione. Si tratta dunque di un ambiente (e di un concetto) che è in rapida evoluzione. […] L'infosfera non sarà un ambiente virtuale sorretto da un soggiacente mondo genuinamente 'materiale'; piuttosto, sarà il mondo stesso a essere sempre più interpretato e compreso in termini informazionali, come parte dell'infosfera. Al fine di tale slittamento, l'infosfera cesserà di essere un modo di riferirsi allo spazio dell'informazione per divenire sinonimo dell'Essere». Interessante anche la considerazione per cui le tecnologie ingegnerizzate stiano modificando il mondo, non solamente nella sua struttura, ma anche nella stessa concezione che di esso ne viene data; ne trasformano, dunque, la natura. L'A. conia un ulteriore ed efficace ideologismo per descrivere questo operare: "Reontologizzare". Con detto termine si fa riferimento «a una forma molto radicale di re-ingegnerizzazione, che non soltanto disegna, costruisce o struttura un sistema (ad esempio, una società, una macchina o un artefatto) in modo nuovo, ma che fondamentalmente trasforma la sua natura intrinseca. In tal senso, nanotecnologie e biotecnologie non stanno solamente costruendo in modo diverso il nostro mondo, ma lo stanno reontologizzando». FLORIDI, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, 2009, 186.

[100] Particolarmente interessante le considerazioni di Floridi in merito alla trasformazione, non solamente della società in società digitale, quanto anche degli essere umani (agenti) in agenti informazionali: «[…] ci siamo assuefatti a pensare la nostra vita online come una mescolanza tra un adattamento evolutivo di agenti umani a un ambiente digitale e una forma di neocolonizzazione postmoderna di questo da parte del primo. Abbiamo visto che in realtà le ICT stanno tanto reontologizzando il nostro mondo quanto creando nuove realtà, eliminando gradualmente la soglia tra il qui (analogico, offline) e il là (digitale, online). […] Tutti noi stiamo diventando organismi informazionali connessi (inforg). Questo non sta accadendo tramite qualche ridicola trasformazione del nostro corpo, bensì, più seriamente e realisticamente, tramite la reontologizzazione del nostro ambiente e di noi stessi. […] Il cambiamento più radicale, determinato dalla reontologicizzazione dell'infosfera, consisterà nell'emergere di agenti umani intesi come organismi informazionali, interconnessi, tra altri organismi e agenti informazionali». FLORIDI, *op. cit.*, 189 ss. Da questa considerazione l'A. fa discendere come diverrà naturale, nel senso di ordinario, per gli esseri umani interagire con le macchine le quali, all'interno dell'infosfera, potranno essere qualificate anch'esse come agenti informazionali. A quanto esposto segue, tuttavia, un avvertimento, che suona particolarmente vicino ai tempi che stiamo vivendo: «Stiamo assistendo, pertanto, a una migrazione epocale e senza precedenti dell'umanità dal proprio *Umwelt* all'infosfera, e ciò anche in ragione del fatto che quest'ultima stia assorbendo il primo. Il risultato è che gli esseri umani saranno inforg tra altri inforg e agenti (potenzialmente digitali) che operano in un ambiente amichevole nei confronti delle creature digitali. […] quando la e-migrazione sarà completa, ci sentiremo sempre più deprivati, esclusi, handicappati o poveri al punto da restare paralizzati o psicologicamente traumatizzati, allorquando saremo sconnessi dall'infosfera, come pesci fuori dall'acqua. Un giorno, essere inforg sarà così naturale che ogni interruzione nel nostro normale flusso di informazioni ci renderà malati». FLORIDI, *op. cit.*, 192.

[101] Si parla di un vero e proprio *digital divide*, con tale espressione intendendosi il divario tra chi ha accesso alle tecnologie dell'informazione e invece chi ne è escluso. La recente crisi sanitaria mondiale ha evidenziato ulteriormente le criticità legate all'esclusione di una parte della popolazione dall'accesso alla tecnologia. Le disuguaglianze e la disomogeneità di accesso agli strumenti tecnologici, mostrano altresì un divario culturale, richiedendo interventi mirati anche sul piano dell'educazione e dell'aggiornamento costante, al fine di garantire effettivamente pari opportunità ai cittadini. Cfr. sul punto PALAZZANI, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Roma, 2020, 26 ss. Interessante sul punto anche la panoramica offerta da RODOTÀ, *Il mondo nella rete. Quali diritti, quali*

rappresentatività digitale non possono quindi che essere guardati con sempre maggiore preoccupazione. Oltre alle istanze di giustizia sociale e di parità di accesso alla tecnologia, che per esigenze di brevità espositiva non verranno trattate nel presente lavoro, emergono altresì preoccupazioni in merito alla privacy degli utenti e allo sfruttamento dei dati da questi prodotti.

Prima di approfondire l'analisi di tali profili e di come essi vengano declinati nell'utilizzo nelle tecnologie di IA, appare opportuno chiarire preliminarmente la natura e il ruolo svolto dai dati nella misura che qui interessa.

L'indagine deve necessariamente prendere le mosse da un ulteriore tentativo definitorio, in prima istanza del concetto stesso di dato. Pare utile adottare una definizione orientata alle finalità di utilizzo da parte dei sistemi di Intelligenza Artificiale. Pertanto, per "dato" deve intendersi qualsiasi entità osservabile digitalmente. La scelta di espungere ogni accezione semantica al termine risponde all'esigenza di non limitare eccessivamente lo studio del fenomeno. Ne deriva come non sia possibile qualificare il dato come "informazione". Ciò in quanto il termine "informazione" denota entità già dotate di un significato per l'osservatore. Non così invece per quanto oggetto delle operazioni computazionali delle tecnologie di AI[102].

Così chiarito cosa debba intendersi per "dati", e come detto termine vada a ricomprendere, in modo necessariamente ampio, tutto ciò che possa essere osservato da una macchina, si coglie con maggior chiarezza la portata espansiva e il ruolo cardine da essi ricoperto nell'attuale contesto tecnologico. I cosiddetti Big Data rappresentano infatti il carburante delle Intelligenze Artificiali. Pur non essendoci accordo nella comunità scientifica in merito a cosa vada ricompreso sotto il termine "Big Data", pare utile ai fini del presente lavoro adottare una definizione che faccia perno sulle tre principali caratteristiche convenzionalmente attribuite al fenomeno; le famose "3 V": Volume, Velocità e Varietà[103]. A queste è stata poi successivamente aggiunta prima una

---

vincoli, Roma-Bari, 2014. Le stesse Istituzioni europee si sono mostrate consapevoli dell'urgenza di rendere la tecnologia accessibile paritariamente proponendo nella agenda digitale lo stanziamento di fondi a ciò specificamente destinati. Sul punto si rimanda alle comunicazioni consultabili all'indirizzo: *www.europarl.europa.eu*. Per un approfondimento sul tema si rimanda a JORGENSEN, *Human rights in the global information society*, Cambridge, 2019.

[102] OTTOLIA, *Big Data e innovazione computazionale*, Torino, 2017.

[103] RUOTOLO, *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018, 97 s.; PERRUCCI, *Dai "Big Data" all'ecosistema digitale. Dinamiche tecnologiche e di mercato e ruolo delle politiche pubbliche*, in *Analisi giur. econ.*, 2019, 69 s.; RABAI, *I «big data» nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in

quarta "V", la Veridicità (*Veracity*), e infine una quinta indicante il Valore, allo scopo di rendere la definizione più precisa[104].

Procedendo con ordine, con il termine "Volume" si intende fare riferimento alla grande quantità di dispositivi che, mediante la connessione alla rete, generano una enorme mole di dati eterogenei (file di testo, pdf, formati video, immagini, etc.)[105]. La quantità di dati prodotti, oltre che la facilità ed economicità della loro raccolta, permette ai *data scientist* di analizzare un fenomeno, non solo economico ma anche sociale, non più per campioni di popolazione[106] – come accadeva un tempo – ma avvicinandosi alla sua dimensione globale[107]. Ciò evidentemente permette di creare modelli che, descrivendo compiutamente un determinato fenomeno, possano essere sfruttati per analisi predittive sempre più affidabili. Grande interesse viene riservato a detta metodologia di analisi, è difatti possibile simulare realisticamente diversi scenari e come essi possano impattare sulla realtà sociale. Grazie alla creazione di modelli completi

---

Amministrare, 2017, 407 s.; FARINA, *Il* cloud computing *e i Big Data*, in *Tecnologia e Diritto*, I, a cura di ZICCARDI e PERRI, Milano, 2019, 55 ss. Interessante la definizione proposta da De Gregorio e Torino. Gli A. accanto all'indicazione circa le caratteristiche quantitative e qualitative, che identificano i Big Dati quali grandi moli di dati di diversa provenienza, intendono ricomprendere nella definzione, in una prospettiva omnicomprensiva, anche l'insieme dei processi e delle tecniche finalizzate a ottenere "informazioni da informazioni". V. DE GREGORIO, TORINO, *Privacy, tutela dei dati personali e Big Data*, in *Privacy digitale, Riservatezza e protezione dei dati e nuovo Codice Privacy*, a cura di TOSI, Milano, 2019, 454 s.

Interessante sul punto anche le considerazioni di VESPIGNANI, RIJTANO, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, Milano, 2019, 46 ss. Secondo gli Autori le definizioni basate sulle 3 V risulterebbero asfittiche, in quanto per comprendere pienamente il valore dei Big Data non sarebbe sufficiente concentrarsi sulla quantità. Il valore risiederebbe, invece, nel fattore di novità che essi hanno portato; la grandezza quindi andrebbe considerata relativamente alle informazioni in più disponibili rispetto al passato, e infine alla loro finalità quale carburante per le AI.

[104] Diverse sono state le proposte di definizione del termine, così come diverse sono state le "V" identificate, fino a 70. Si è, per esempio, fatto riferimento alla "valenza" quale caratteristica legata alla connessioni tra i dati; alla "visualizzazione", che indicherebbe il modo in cui gli analisti riescono a rappresentarli; infine, al "valore", caratteristica che deriva da tutte la altre, evidentemente legato alla capacità di estrarre valore dai Big Data. V. sul punto DALMASTRO, NICITA, *op. cit.*, 26. Interessanti anche le considerazioni di PALAZZANI, *op. cit.*, 37 ss.

[105] Proprio lo sviluppo e la diffusione degli *Internet of Things* ha comportato la raccolta di un numero sempre maggiore di dati degli utenti; dati che vengono più raccolti e conservati in *data storage* accentrati (quali possono essere i *cluod*), essendo la disponibilità di memoria di archiviazione di tali apparecchi necessariamente ridotta.

[106] Basti pensare alle analisi compiute dall'ISTAT, necessariamente a campione, o – meglio – quelle che ancora oggi vengono fatte in occasione dei risultati elettorali. Dalla recente esperienza americana è emerso con chiarezza come le predizioni svolte su una campionatura di elettori non sono sempre affidabili; ciò è addebitale a diversi fattori, di natura oltre che sociologici, tra cui certamente anche quello dell'effettiva rappresentatività del campione raccolto.

[107] D'ACQUISTO, NALDI, *op. cit.*, 5 s.

oggi è possibile verificare per esempio i piani di evacuazione delle città in caso di calamità[108].

Il secondo attributo, la "Velocità", indica le modalità di produzione dei dati e in particolare la capacità delle tecnologie di generare questi ultimi in modo continuativo, in luogo di una produzione discreta[109]. Per meglio comprendere, si prendano per esempio in considerazione le autovetture. Queste sono provviste di diversi sensori che monitorano e trasmettono continuativamente dati tecnici di funzionamento, i quali verranno conservati e trattati per diverse finalità. Evidentemente la fornitura di questo flusso continuo (*stream*) di dati richiede un costante aggiornamento da parte delle applicazioni di analisi; dati non aggiornati o incompleti, infatti, potrebbero generare errori nei risultati.

Tra i più noti esempi di applicazioni che sfruttando algoritmi possono processare questa grande mole di dati possiamo ricordare Google Flu Trends (GFT), un servizio di Google deputato a predire la diffusione di casi di influenza analizzando le ricerche effettuate dagli utenti nel proprio motore di ricerca. Nel 2009 venne individuato un nuovo ceppo influenzale derivato dalla Aviaria; la grande carica virulenta fece emergere la necessità di indagare la dinamica della sua diffusione e la possibilità di verificazione di una pandemia. Le analisi compiute, fino a quel momento, venivano condotte sulla scorta dei dati raccolti dalla CDC in merito alle diagnosi svolte dal personale sanitario. Chiaramente questa metodologia, oltre che necessitare di molto tempo per la raccolta di dati, non avrebbe potuto tenere in considerazione diverse variabili tra cui la mobilità dei cittadini. Il successo di Google Flu nell'individuare il picco influenzale nel 2009, grazie

[108] L'evoluzione di modelli sempre più reali, capaci dunque di processare un gran numero di variabili, ne ha permesso l'uso per simulare anche situazioni emergenziali. Si pensi al modello, creato originariamente a Los Alamos, e oggi divenuto il riferimento predittivo per il National Planning Scenario 1 degli Stati Uniti. Questo modello viene utilizzato per simulare cosa accadrebbe nella città di Washington nel caso di un attacco nucleare. Le grandi capacità di elaborazione di questo modello, creato mediante l'uso di diversi algoritmi, hanno permesso la simulazione di tutta l'area metropolitana di Washington e dei suoi 730.000 abitanti. Il modello permette la simulazione di agenti che rispondono attraverso modalità di comportamento, come l'evacuazione dell'area o la ricerca di famigliari. Ciò consente di identificare anche fenomeni controintuitivi, quali la congestione delle strade che portano verso il *Ground Zero* dovuta a coloro che cercano di raggiungere i propri famigliari con cui non possono comunicare. Chiaramente lo scopo di queste simulazioni è quello di creare uno strumento predittivo che sia di ausilio ai governi durante la gestione di eventi di crisi. V. VESPIGNANI, RIJTANO, *op. cit.*, 120 ss.

[109] Interessante sul punto la considerazione critica di OTTOLIA, *op. cit.*, 59 ss., secondo cui detta caratteristica sarebbe indicativa della capacità non solamente di creazione, ma in particolare della rapidità dell'intero processo di raccolta e analisi da parte degli algoritmi. In questa accezione l'A. sottolinea come detta capacità non debba essere considerata dirimente ed essenziale a qualificare i Big Data, dal momento che operativamente i dati possono altresì essere raccolti e poi sottoposti ad analisi successivamente quali dati storici.

alla sua velocità di raccolta e analisi, ha reso evidente come l'elaborazione di modelli descrittivi di un fenomeno nella sua dimensione globale avrebbe permesso una maggiore affidabilità delle previsioni. Sulla scorta di tale consapevolezza vennero dunque elaborati modelli predittivi che potessero essere compresivi di diverse variabili tra cui lo spostamento, non solo degli uomini, ma anche degli animali vettori dei virus; come avvenuto per Zika[110].

La terza "V" indica la "Varietà", intendendosi con tale termine l'eterogeneità dei dati prodotti. Il flusso dei dati, come evidenziato, cresce grazie al numero sempre maggiore di tecnologie deputate alla loro raccolta in diversi formati. Se da una parte ciò permette una maggiore estrapolazione di informazioni, dall'altra proprio la conformazione dei dati raccolti ne rende complessa la gestione, sia in termini di organizzazione e di spazio di conservazione, che di analisi degli stessi.

La quarta "V" rappresenta la "Veridicità". A differenza dei precedenti, questo attributo non è descrittivo di una qualità intrinseca del fenomeno; pare piuttosto essere funzionale alle istanze sempre più sentite di una regolazione in merito alla qualità dei dati. Difatti, proprio la velocità di generazione e di raccolta da fonti eterogenee rende complessa la verifica circa la loro correttezza, finendo così per comportare anche un aumento dell'incertezza dei risultati degli algoritmi di *data analysis*. La difficoltà di controllo e di selezione dei dati raccolti, infatti, può inevitabilmente comportare che alcuni di essi risultino errati o incompleti, da ciò discendendo possibili errori nella risposte degli algoritmi che su questi generano previsioni[111].

---

[110] Modelli computazioni sono stati utilizzati per simulare la diffusione di Ebola e più tardi di Zika. Sul punto interessante la testimonianza resa da Vespignani in merito alla creazione di un modello predittivo della diffusione di Zika. V. VESPIGNANI, RIJTANO, *op. cit.*, 116 ss. Come è noto, nel 2016, a pochi mesi dall'inizio delle Olimpiadi in Brasile, il virus Zika generò un'epidemia con milioni di casi in America Latina e nei Caraibi. Le gravi patologie, tra cui anche malformazioni neonatali, di stampo neurologico, fecero emergere l'esigenza di monitorare e contenere la diffusione del contagio. A differenza di Ebola, il quale si trasmette quasi esclusivamente da uomo a uomo, Zika viene trasmesso per lo più tramite le punture di zanzare. Questa metodologia di diffusione comportava, evidentemente, delle difficoltà maggiori in quanto i modelli avrebbero dovuto tenere in considerazione, non solamente i dati sul comportamento umano, ma anche le popolazioni di zanzare, il loro ciclo di vita e le migrazioni delle stesse. Grazie allo studio compiuto dagli entomologi e a un algoritmo di *machine learning* fu possibile generare gli *input* necessari ai modelli di simulazione della diffusione del virus. Grazie ai dati emersi dalle analisi numeriche fu, per esempio, scoperto che l'introduzione di Zika in Brasile era avvenuta al più tardi nei primi mesi del 2014, quindi circa due anni prima della grande ondata di casi osservata nel 2016.

[111] D'ACQUISTO, NALDI, *op. cit.*, 6 s.; DALMASTRO, NICITA, *op. cit.*, 25 ss. Vi sono diverse esperienze di algoritmi che hanno generato previsioni errate proprio in ragione della difficoltà di selezionare tra l'enorme volume dei dati raccolti quelli che fossero coerenti con lo scopo dell'analisi e al contempo veritieri. Basti pensare alla parabola discendente di Google Flu Trends (GFT), di cui si è già richiamato il successo raggiunto nel 2009. Nel febbraio 2013 un articolo sulla rivista Nature riportava che GFT

Da ultimo è stato poi introdotto come attributo il "Valore". Così come per la veridicità, anche questa caratteristica non è descrittiva di una qualità delle informazioni generate o raccolte. Con detto termine viene indicata la capacità dei dati di produrre valore, inteso come la rilevanza nell'attuale contesto economico-sociale sia in relazione all'utente che alle compagnie che li raccolgono[112]. Sebbene possa sembrare una caratteristica "minore" rispetto a quanto sopra riportato, la crescita di valore oggi acquisito dai dati ha comportato l'emersione di un esteso mercato digitale e l'affermazione di grandi top player, quali Amazon, Facebook, Google etc., la cui posizione dominante rischia di rendere sempre più difficoltosa l'instaurazione di una effettiva concorrenza. Le stesse Istituzioni europee hanno invitato i soggetti privati, oggi tra i maggiori protagonisti del mercato, a rendere i dati raccolti liberamente accessibili, così come avviene per i dati raccolti dalle pubbliche amministrazioni, al fine di non ostacolare l'ingresso nel mercato alle nuove imprese. Dette preoccupazioni sorgono in ragione dell'evidenza che il mercato digitale rischia di essere guidato appunto da poche grandi imprese, detentrici delle maggiori collezioni di dati, i cosiddetti Over the Top[113].

---

prevedeva più del doppio della percentuale di visite mediche per influenza rispetto ai dati provenienti dai rapporti di sorveglianza dei laboratori del *Centers for Disease Control and Prevention* (CDC) statunitense. Confrontando le prestazioni di GFT con modelli molto semplici basati sui dati del CDC emerse come l'algoritmo di Google aveva iniziato a fallire in modo significativo e richiedeva una revisione sostanziale. Il sistema, difatti, era stato sin dai primi tempi anche foriero di alcuni degli inconvenienti insiti nell'uso di algoritmi e Big Data. Essenzialmente, la metodologia usata consisteva nel trovare tra 50 milioni di termini di ricerca quelli che descrivevano meglio i dati storici dell'influenza. Le probabilità di trovare termini di ricerca che descrivono l'andamento dell'influenza, ma non sono causalmente correlati e non prevedono il futuro è evidentemente piuttosto elevata. Gli sviluppatori GFT, infatti, avvertirono subito la necessità di eliminare termini di ricerca stagionali non connessi all'influenza, ma fortemente correlati nel tempo ai dati del CDC. Questo metodo *ad hoc* di selezione di termini di ricerca particolari è però fallito quando GFT ha completamente perso la pandemia di influenza non stagionale 2009, chiamata A-HLNL o "febbre suina", che ha causato centinaia di morti e migliaia di contagi nel mondo. Per questo motivo, nel 2009 gli ingegneri di Google aggiornarono l'algoritmo, annunciando poi ulteriori modifiche nell'ottobre 2013. Tuttavia, nonostante i vari aggiustamenti algoritmici e di analisi dei dati, il nuovo GFT continuava a sopravvalutare l'incidenza dell'influenza con errori rilevanti, fino a delle stime per eccesso di oltre il 100% nelle stagioni 2011/2012 e 2012/2013. Nel 2015 il sistema è stato chiuso e Google ha interrotto la ricerca a supporto e sviluppo dei sistemi di predizione dell'influenza stagionale. La parabola di Google Flu Trends è stata da molti presa ad esempio come uno dei fallimenti più clamorosi dell'Intelligenza Artificiale e delle predizioni basate su Big Data. VESPIGNANI, RIJTANO, *op. cit.*, 96 ss.

[112] PALAZZANI, *op. cit.*, 37 ss.

[113] Un ruolo preminente, nel capitalismo digitale, lo hanno le grandi piattaforme digitali che hanno sviluppato una rete globale di infrastrutture per la *data economy*. Anche qui occorre, tuttavia, chiarire il quadro: le piattaforme digitali sono moltissime, svolgono compiti diversi e hanno diversi criteri di interoperabilità, standardizzazione, apertura, investimenti etc. Per quanto sia facile accomunarle, le piattaforme globali hanno non solo modelli di business diversi, ma anche un modo differente di sfruttare il dato. Le piattaforme digitali spesso sono denominate *Over the top* per il fatto che sviluppano servizi che si trovano gerarchicamente al di sopra delle infrastrutture fisiche di telecomunicazione fisse e mobili grazie alle quali accediamo alla rete. Un recente rapporto OCSE, *Data-Driven Innovation far Growth and*

Proprio la regolazione del mercato digitale, l'accesso ai dati e le istanze di tutale dei cittadini rappresentano una delle maggiori sfide giuridiche del nostro tempo.

Chiarito il perimetro del fenomeno, è necessaria una considerazione di natura tecnica in merito alla raccolta delle informazioni e al loro trattamento. La maggior parte dei dati raccolti non sono infatti strutturati, bensì grezzi (*data exhaust*), acquisiti a grandi velocità e composti da differenti formati[114]. L'uso di dati eterogenei, pur permettendo l'estrapolazione di molte informazioni, può tuttavia portare a un fenomeno di *over-collection*, cioè di ridondanza; per tale motivo si opera spesso una seconda fase di lavorazione diretta alla preparazione e alla conservazione dei dati per gli usi successivi. Tuttavia, oggi sul mercato si predilige la condivisione di dati grezzi, nel loro formato originario, così da permettere un'analisi che possa estrapolarne maggiore valore[115]. Infatti, essendo questi immagazzinati in modo diverso dai tradizionali *database*, i quali sono generalmente organizzati secondo criteri relazionali, ciò che viene ritenuto rilevante è proprio il processo di lavorazione e aggregazione delle informazioni. Il grande valore degli algoritmi risiede dunque proprio nella loro capacità di rivelare relazioni (*correlation insights*) tra la massa di dati grezzi, *pattern* questi che sono a fondamento dei modelli di analisi predittiva[116].

Da tutto quanto sopra esposto appare evidente come il volume e l'eterogeneità dei dati generati e raccolti renda difficoltosa la verifica in merito alla qualità degli stessi, sia in termini di esattezza delle informazioni che di rimozione di possibili *bias*. Il problema si avverte particolarmente proprio nel momento in cui le informazioni raccolte fungono da *dataset* per l'addestramento degli algoritmi[117]. La loro capacità di trovare

---

Well-Being, mostra come l'acquisizione, l'analisi e la gestione dei Big Data necessitino di notevoli investimenti infrastrutturali. La mancanza di infrastrutture di reti tradizionali che caratterizza gli *Over the top* non comporta, infatti, anche assenza di investimenti. Anzi. I "giganti dei dati" presentano un elevatissimo livello di capitale investito in immobilizzazioni tecnologiche e, quindi, una struttura dei costi caratterizzata da elevati oneri fissi e irrecuperabili (*sunks*) e bassi costi marginali, assieme a una scala mondiale di copertura della rete (e quindi dei relativi servizi). DALMASTRO, NICITA, *op. cit.*, 51.

[114] La mole di dati generati e raccolti, così come sopra indicato, pare destinata a crescere, in ragione della sempre maggiore diffusione nell'utilizzo di prodotti IoT capaci non solamente di raccogliere i dati, ma di generarli. Come sopra ricordato, la maggior parte dei dati prodotti oggi sono non strutturati, tuttavia i dati raccolti possono essere altresì strutturati, raccolti in *database* e quindi aventi già di per sé un valore, o semi-strutturati; tra questi ultimi possono essere fatte rientrare le comunicazioni e-mail nelle quali, infatti, possiamo trovare dati di diverso formato, ma comunque tra loro legati dall'appartenenza ad uno stesso ID.

[115] DALMASTRO, NICITA, *op. cit.*, 28.

[116] MESSINA, *Le linee guida in materia di Intelligenza Artificiale: alla ricerca di un'"etica by design" nel nuovo scenario digitale*, in *De Iustitia – riv. giur.*, 2019, 89 s.

[117] La necessità sempre più sentita in merito alla trasparenza di funzionamento degli algoritmi, alla luce del rischio di possibili violazione dei diritti degli interessati, vede come contraltare l'utilizzo di tecnologie

collegamenti e ricorrenze statistiche potrebbe difatti portare a risultati di scarsa qualità, secondo un effetto *garbage in-garbage out*[118]. Sul punto è interessante notare come i possibili *output* discriminatori generati delle macchine possano essere dovuti anche a una sotto rappresentazione di determinate categorie di soggetti; problema che potrebbe acuirsi in considerazione del divario tecnologico, che pare essere in forte crescita. A ciò deve aggiungersi come spesso venga incoraggiato l'utilizzo delle tecnologie di Intelligenza Artificiale sull'assunto per cui i risultati da esse generati siano "neutrali". Tuttavia detta affermazione appare frutto di un fraintendimento, si ritiene difatti che le scelte operate dagli algoritmi siano neutrali perché essi non sono condizionati da costrutti valoriali o da esperienze personali, come invece sarebbero gli esseri umani chiamati a decidere nelle medesime situazioni. Ciò non è del tutto corretto, gli *output* infatti sono generati proprio processando i dati raccolti nella società, e di questa quindi sono espressione. Difficilmente i *dataset* verranno creati con dati volutamente discriminatori, tuttavia proprio la capacità degli algoritmi di trovare correlazioni può portare alla luce eventuali discriminazioni latenti[119]. Ed è qui che emerge come gli *output* delle macchine non siano neutrali, e ciò semplicemente perché non lo sono i dati su cui esse operano[120]. Nemmeno neutrale risulta essere la scelta operata dal

---

di AI quali mezzi idonei a migliorare e rendere più efficiente la stessa società. Sul punto interessanti le considerazioni critiche di Maceratini in merito all'utilizzo degli algoritmi, che verrebbe presentato quale "rassicurante". Le modalità stesse di funzionamento, mediante correlazioni statistiche, permetterebbero, infatti, di affrancarsi dalla necessità di ricostruzione delle cause degli eventi; così facendo sarebbe possibile governare meglio la complessità, definita "liquida", della società moderna e ciò grazie a previsioni generalizzanti, in quanto calcolate matematicamente. Le tecnologie di AI consentirebbero il raggiungimento di alcuni obiettivi ritenuti decisivi dalla società: la sicurezza, la velocità e l'economicità. MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. e impr.*, 2019, 863 ss.

[118] Prendendo dati sporchi e imprecisi o di cattiva qualità in ingresso, le AI producono modelli sbagliati e quindi inutili. Cfr. ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, cit., 13. Appare chiaro come le possibili esternalità negative, legate a una cattiva rappresentazione degli stessi dati in ingresso, abbiano portato a istanze di regolazione e valutazione della qualità dei dati. Una possibile soluzione prospettata potrebbe essere l'utilizzo della tecnologia *blockchain* proprio al servizio di un controllo di qualità dei *dataset* di addestramento degli algoritmi. Le difficoltà legate alla quantità e alla varietà dei dati da contrallere potrebbero, dunque, essere superate proprio grazie all'utilizzo delle tecnologie di Intelligenza Artificiale per il controllo e la verifica delle informazioni. V. PALAZZANI, *op. cit.*, 40 ss.

[119] SCALZINI, *Alcune questioni a proposito di algoritmi, dati, etica e ricerca*, in *Riv. it. med. leg.*, 2019, 172 ss.; PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della* Black Box Society*: quale leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Nuove leg. civ. comm.*, 2018, 1210 ss.

[120] Le distorsioni e le discriminazioni possono essere considerate rischi intrinsechi a ogni attività economica o sociale. Tuttavia particolari preoccupazioni destano dette distorsioni qualora siano operare all'interno delle AI, ciò in quanto gli effetti negativi generati potrebbero colpire una platea più vasta di destinatari in assenza dei meccanismi di controllo sociale che disciplinano il comportamento umano. In

programmatore sia in merito alla scelta dei *dataset* di addestramento, che in merito alla stessa creazione dell'algoritmo di AI. Ma andando ancora più a ritroso nemmeno il dato considerato singolarmente può essere considerato neutrale; esso difatti essendo espressione del reale ne è una necessaria semplificazione, frutto della scelta operata da coloro che hanno determinato gli *script* – i comandi – idonei a rendere computabile il fenomeno. Al fine di ovviare a tali problemi sono state da più parti avanzate istanze di verifica della qualità dei dati raccolti; sul punto le normative ISO, volte a dettare criteri di qualità per i dati utilizzati dai software, paiono particolarmente interessanti[121].

3. Considerazioni conclusive

L'innovazione tecnologica e digitale ha comportato l'emersione di differenti criticità non solamente sul piano giuridico ma anche su quello etico e sociale; il fenomeno che qui interessa ne è una tra le più evidenti espressioni. Le prime difficoltà emergono fin dalla scelta di una definizione in merito a cosa debba intendersi con l'espressione "Intelligenza Artificiale" che, come visto, non ha ancora trovato una comune visione tra gli esperti della materia.

Lungi dall'essere una mera questione semantica, la mancanza di una definizione condivisa nel panorama scientifico dimostra la complessità di determinare un perimetro della materia, a cui non possono che accompagnarsi incertezze regolatorie.

---

particolare si pensi al caso in cui i sistemi di AI "apprendano" durante il loro funzionamento; evidentemente in questi i rischi di discriminazioni non discendono più unicamente da possibili difetti di progettazione, ma da correlazioni che il sistema individua processando l'ampio set di dati a propria disposizione. V. sul punto CORONA, DEL PIZZO, *IA: l'approccio europeo è basato sull'eccellenza e la fiducia*, 5 giugno 2020, consultabile all'indirizzo: *www.dirittodiinternet.it* (ultimo accesso 20 settembre 2020).

Interessante anche la posizione di Amato Mangiameli, il quale sottolinea come la non neutralità degli algoritmi sia legata ad alcuni fattori tra cui: l'asimmetria informativa tra una società che offre un servizio e l'utente; l'assenza di trasparenza relativa al funzionamento dell'algoritmo e la creazione di una *filter bubble* che mostrerebbe all'utente solamente le informazioni che l'algoritmo ha calcolato possano interessargli. Da ciò ne discende – chiarisce l'Autore – come non vi siano algoritmi neutrali, questi non si limiterebbero a riflettere la realtà, ma ne proporrebbero una loro versione «fatta di formule classificanti, dal peso attribuito ai singoli parametri inseriti, dalle procedure che determinano il risultato». AMATO MANGIAMELI, *Algoritmi e "big data". Dalla carta sulla robotica*, in *Riv. fil. dir.*, 2019, 109.

[121] Si tratta dello Standard ISO/IEC 25012 che definisce le caratteristiche di qualità dei dati, pubblicato nel 2008 e successivamente riconfermato ed esteso con lo Standard ISO/IEC 25024. Complementare è il modello di qualità dei software compreso nello Standard ISO/IEC 25010. La prima certificazione relativa all'ISO/IEC 25012 è stata rilasciata nel 2020 a Infocamere dall'Ente di certificazione AENOR, relativamente alla qualità dei dati nel Registro delle Imprese. Sul punto si rimanda al comunicato stampa di Infocamere reperibile all'indirizzo: *www.infocamere.it* (ultimo accesso 20 settembre 2020).

La discussione sul punto non è sterile dal momento che la materia sembra essere in parte ancora percorsa da improprietà e fraintendimenti che rischiano di viziare anche il ragionamento giuridico.

Le ricadute del settore nell'economia e nella stessa organizzazione della società moderna, ha spinto, tra gli altri, anche le Istituzioni europee all'elaborazione di un tentativo definitorio quale sintesi del dibattito in materia.

Di particolare spessore la definizione da ultimo elaborata dal Gruppo di esperti in Intelligenza Artificiale (AI HLEG) nel testo "*Definition of AI. Main capabilities and disciplines*". Nel documento si trova una definizione molto articolata e diretta allo scopo di estenderne il più possibile la portata applicativa, così da ricomprendere al proprio interno tutta l'estrema varietà di applicazioni e fenomeni che possono essere astrattamente qualificati come Intelligenza Artificiale. Se da una parte la disposizione ha certamente il pregio di superare il classico – e spesso sterile – confronto con l'essere umano, eterno metro di misura delle *performance* meccaniche, dall'altra la tecnica normativa adottata presta il fianco al rischio di una veloce cristallizzazione. Proprio in ragione di una necessaria flessibilità e del rispetto del principio di neutralità tecnologica, si ritiene più efficace, ai fini del presente lavoro, una definizione elastica, facente perno sulla capacità "agente" delle applicazioni *data driven*, più che sulle specifiche tecniche di addestramento utilizzate[122].

Chiarito cosa debba intendersi per Intelligenza Artificiale, a fronte del suo innegabile carattere *distruptive*, è parso necessario prestare attenzione alle modalità di funzionamento degli algoritmi, in quanto solamente una effettiva comprensione permette di valutare in modo consapevole l'impatto delle tecnologie e come esse possano essere regolate dalla normativa vigente.

Dall'analisi in merito alle tecniche di addestramento degli algoritmi attualmente più promettenti, quindi al *machine learning* nella specifica declinazione del *deep learning*, emerge con evidenza il ruolo centrale ricoperto dai dati. Essi, infatti, rappresentano un *asset* indispensabile per le stesse applicazioni di AI, permettendone *ab origine* non solamente l'addestramento ma anche un funzionamento efficiente e funzionale al raggiungimento degli obiettivi prefissati. Proprio grazie alla varietà dei dati è possibile per le macchine "imparare" a riconoscere sempre più efficacemente schemi e

[122] Si rimanda *supra* al §1.

correlazioni ricorrenti, al fine di poter rispondere correttamente e velocemente allo scopo per cui sono programmate. Questo tipo di funzionamento, si ricorda, è alla base anche delle analisi predittive, permettendo la creazione di *cluster* di utenti legati da caratteristiche simili che, statisticamente, ci si aspetta si comportino nel medesimo modo se sottoposti ai medesimi stimoli.

É evidente, allora, come la qualità dei dati raccolti e trattati dalle AI assuma una basilare rilevanza. La produzione sempre più estesa di dati provenienti da differenti fonti, elementi questi che qualificano i Big Data, permette certamente una rappresentazione più particolareggiata del reale. Tuttavia, proprio a fronte delle modalità di funzionamento degli algoritmi appare evidente la necessità di controllo circa la qualità dei dati raccolti. Fondamentale si dimostra il controllo degli attributi quali esattezza, completezza e aggiornamento, in quanto dati errati o incompleti possono comportare risultati errati o discriminatori; rischio questo particolarmente sentito per le tecnologie *data driven*[123].

Assodato come il concetto di Intelligenza Artificiale debba essere tenuto distinto da quello di intelligenza umana e, dunque, come anche il concetto di autonomia non possa essere considerabile alla stregua di una sorta di autodeterminazione e coscienza della macchine, l'analisi effettuata ha fatto emergere ulteriori criticità in relazione alla trasparenza e alla spiegabilità degli *output*. L'indagine si è concentrata, per esigenze di brevità espositiva, in particolare sulle ANN, in quanto tra le tecniche maggiormente opache. Se è vero che l'architettura dell'algoritmo è progettata da un ingegnere, il quale elabora le formule ritenute più idonee a raggiungere un obiettivo dato, dall'altro esse non solo si compongono di molti "strati" collegati tra loro, ma mostrano avere un carattere di autonomia nella misura in cui vengono regolate da altri algoritmi – quali per esempio quelli di *back propagation* – al fine di rendere più efficiente il raggiungimento dell'obiettivo. Come visto, proprio la complessità dell'architettura comporta un'estrema difficoltà di comprensione e di spiegazione delle scelte operate dalla macchina[124].

L'esigenza di trasparenza è certamente sentita in relazione al regime di responsabilità civile applicabile, ma riveste importanza anche nell'ambito del trattamento dei dati. La comprensibilità dei processi decisionali è infatti al centro del dibattito sul tema del diritto alla spiegazione, che parte dei commentatori fa discendere dalle disposizioni del

[123] Si rimanda *supra* al § 2.1.
[124] Si rimanda *supra* al § 2.

GDPR; è tuttavia ancora controverso se il Regolamento 2016/679 UE abbia effettivamente introdotto tale diritto per gli interessati. Alla luce delle analisi sopra compiute, ci si domanda finanche se sia possibile fornire una spiegazione comprensibile in merito allo specifico *output* del sistema. Difatti, dato il carattere estremamente tecnico della materia, è evidente come divenga difficoltoso confezionare una spiegazione che sia comprensibile anche per gli interessati, i quali non sempre posseggono le conoscenze specialistiche necessarie.

Dette considerazioni si intrecciano con il profilo della tutela dei dati personali degli utenti. Il tema acquista particolare rilievo in ragione della abilità sempre maggiore delle tecniche di *data analysis* di inferire dati personali anche da quelli di natura non personale, oltre che della capacità di re-identificare i dati pseudonimi e anonimi. Ciò è possibile proprio grazie alla raccolta massiva e variegata di dati che permette di creare *dataset* sempre più estesi, grazie anche alla possibilità di acquisto da terzi soggetti, quali per esempio i c.d. *databroker*, nel mercato digitale.

Nel panorama europeo sono attualmente vigenti delle normative a tutela dei dati dei cittadini, appare allora opportuno vagliarne l'effettiva applicabilità nel contesto delle applicazioni digitali. Ciò è reso necessario dall'esigenza di bilanciare il diritto alla tutela dei dati, nelle sue molteplici accezioni, con altri diritti ritenuti parimenti meritevoli di tutela, tra cui la libertà di iniziativa economica.

Ulteriori incertezze emergono anche in relazione ai dati creati dalle applicazioni digitali, in special modo dagli IoT. L'esigenza di una libera circolazione, elemento indispensabile al consolidamento del mercato digitale, poterebbe trovare un ostacolo nell'applicazione ai dati di un regime proprietario. La questione merita un approfondimento in quanto si mostra già attuale in ragione della concentrazione dei dati in capo a poche grandi imprese all'interno del mercato[125].

Chiarita dunque l'importanza dei dati nel contesto tecnologico, come essi vengano raccolti ed utilizzati, e le criticità a essi legate, nel prosieguo l'indagine partirà dall'analisi delle normative di settore, quali primi strumenti di regolazione del trattamento e della circolazione dei dati personali e non, e degli efficacia delle stesse nelle tecnologie di AI.

[125] Un approfondimento verrà dedicato *infra* nel capitolo 5.

CAPITOLO 2

Tecnologia e diritto nella *governance* europea

SOMMARIO: 1. I dati quale nuovo asset economico. – 1.1. Il mercato digitale. Caratteristiche e criticità. – 2. La strategia europea: Intelligenza Artificiale e dati, una regolazione necessariamente coordinata. – 3. La strategia dell'Europa sui dati non personali. Il Regolamento 2018/1807 UE e la sua portata applicativa. – 4. La strategia europea sui dati personali: dal pacchetto dati al GDPR. – 5. Considerazioni conclusive.

1. I dati quale nuovo asset economico

Le criticità nascenti dal trattamento dei dati degli utenti da parte di algoritmi e di tecniche di *data mining* vengono abitualmente ricollegate alla dimensione della tutela della riservatezza e del controllo dei propri dati, trascurando spesso l'analisi del fenomeno nella sua dimensione anche economica. Si riscontra infatti, secondo una posizione tradizionalmente dominante, una tendenziale ritrosia a ritenere il dato personale oggetto di una prestazione in un contratto di scambio. Tale orientamento, supportato anche da alcune Istituzioni, quali il Garante per la Protezione dei dati personali e l'*European Data Protection Supervisor*, muove dall'assunto per cui il dato personale rappresenta l'estrinsecazione dell'identità e della personalità degli individui[126]. Così delineatane la natura, il diritto alla protezione dei dati personali, in quanto diritto della personalità, è stato ricompreso nel novero dei diritti fondamentali e dunque ritenuto assoluto, indisponibile, intrasmissibile e imprescrittibile[127]; ne discende

[126] Per quanto riguarda la posizione espressa dalle Istituzioni si rimanda al Discorso del Presidente dell'Autorità Garante per la Protezione dei Dati Personali Antonello Soro, Relazione annuale per il 2018, Roma, 7.5.2019, consultabile all'indirizzo: *www.garanteprivacy.it* (ultimo accesso 10 dicembre 2020); European Data Protection Supervisor, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 2017, consultabile all'indirizzo: *https://edps.europa.eu/sites/edp/files/publication/17-03-14_opinion_digital_content_en_0.pdf* (ultimo accesso 15 dicembre 2020).

[127] Per un'interessante analisi evolutiva dei diritti della personalità si rimanda a G. RESTA, *I diritti della personalità*, nel *Trattato Sacco*, II, *Le persone fisiche e i diritti della personalità*, a cura di Alpa e G.

l'impossibilità di ogni commercializzazione dei dati, essendo questi espressione di attributi fondamentali del proprio essere[128]. Queste considerazioni, tuttavia, si scontrano con la prassi commerciale ove l'offerta di contenuti digitali, ricalcando chiaramente schemi negoziali sinallagmatici[129], ha fatto emergere il tema della patrimonializzazione dei dati degli utenti, ossia la possibilità di attribuire a questi un valore economico in quanto beni di scambio[130].

Grazie alla grande diffusione delle tecnologie dell'informazione e della comunicazione (ICT), la creazione di un'infrastruttura globale[131] e lo sviluppo di un

---

RESTA, Torino, 2006, 361 ss.; ZENO ZENCOVICH, voce «personalità (diritti della)», nel *Digesto, Disc. priv., sez. civ.*, XIII, Torino, 1995, 430 ss.

[128] La dimensione economica si mostra evidente nel caso, sempre più frequente, di una fruizione di servizi aventi come corrispettivo la cessione dei propri dati. Ciò dimostra evidentemente come la cessione del dato personale venga oggi, nelle pratiche commerciali, ritenuta una controprestazione a un servizio. Tuttavia, secondo una posizione tradizionalmente dominante, le stesse caratteristiche dei dati personali osterebbero al loro riconoscimento quale oggetto di una prestazione in un contratto di scambio. In merito alle criticità nascenti dal permettere la commercializzazione dei dati personali si rimanda alla riflessione di ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessioni*, in *Contr. e imp*., 2017, 723 ss. Secondo alcuni commentatori non sarebbe accettabile l'idea che la persona eserciti un diritto di proprietà sui propri dati, potendone disporre liberamente. Ciò in quanto si ritiene che il dato, quale espressione della propria personalità, concorrerebbe a creare una dimensione digitale, la quale tuttavia non sarebbe che un prolungamento della dimensione umana. Da ciò ne discende la considerazione per cui come alla persona non si consente di alienare parti del corpo che potrebbero comprometterne la funzionalità, allo stesso modo si dovrebbe proibire la cessione volontaria dei dati personali, e in particolare quelli sensibili. Pertanto «la preoccupazione della 'vendita' di dati personali non sarebbe diretta solo a tutelare una parte considerata debole e riequilibrare la disparità di potere tra titolare e interessato, ma guarderebbe ad una platea più ampia tutelando non tanto il singolo ma lo stesso in un'ottica collettiva: si esprime così l'esigenza di evitare la commercializzazione della persona come parte della società». D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inform*., 2020, 670.

[129] V. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 41. L'A. sottolinea che la cessione dei dati personali, come corrispettivo alla prestazione di un servizio, configuri un fenomeno negoziale. Il rapporto vede contrapporsi, da un lato, il titolare del trattamento che necessita dei dati personali e, dall'altro, il soggetto a cui questi dati si riferiscono, essendo colui che solo è in grado di fornire quella "particolare" ricchezza, patrimonialmente valutabile.

[130] V. sul punto anche AA. VV., *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di ZORZI GALGANO, Milano, 2019; DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, 12; THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws – riv. dir. med.*, 2019, 131; ID., *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv*., 2016, 540 ss.; RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, cit., 23 ss.; ID., *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inform*., 2018, 690 ss.; G. RESTA, voce «Autonomia contrattuale e diritti della personalità nel diritto UE», nel *Digesto, Disc. priv., sez. civ.*, IX, Torino, 2013, 92 ss.; PRINS, *Property and Privacy: European Perspectives and the Commodification of our Identity*, in *The Future of the Public Domain, Identifying the Commons in Information Law*, 2006, 223 ss.

[131] Negli anni, in parallelo con lo sviluppo delle tecniche di Intelligenza Artificiale, è stata sviluppata una vera e propria infrastruttura di dati globale. Interagiamo con essa ogni volta che accediamo alla rete internet; non si tratta, difatti, unicamente di un'infrastruttura fisica, ma comprende software, *social network*, siti internet, etc. L'Intelligenza Artificiale si "nutre" di essa e contemporaneamente la alimenta

mercato digitale, ove le imprese acquistano/vendono dati spesso grezzi, strutturati e non[132], si è infatti assistito a un incremento esponenziale della rilevanza dei dati nell'attuale società, non a caso definita dell'informazione[133]. L'aumento non solo della quantità, ma anche della qualità e diversità dei trattamenti, ha fatto emergere con evidenza l'importanza strategica dei Big Data per l'economia mondiale[134]. Questi si dimostrano essere un *input* fondamentale dell'intero sistema economico, strumento di indagine ma anche di continuo addestramento dell'algoritmo, e al contempo un prodotto in sé, capace di generare valore autonomo[135] proprio in ragione dell'estrema versatilità di utilizzo. L'economia digitale ha comportato pertanto lo sviluppo di un sistema sempre più assetato di informazioni, rendendo così il dato una preziosa risorsa, oltre che una moneta di scambio, riconoscendone un valore eminentemente patrimoniale.

Alla tradizionale concezione di dato personale quale esplicazione della personalità del soggetto, approccio questo che potremmo definire morale, deve dunque affiancarsi un approccio negoziale, che discende dalla considerazione del dato quale suscettibile di scambi aventi rilievo economico[136]. I dati rappresentano difatti un asset fondamentale

---

grazie alla produzione di dati generati dagli artefatti; difficilmente le due dimensioni oggi potrebbero essere completamente distinte. Cfr. AA. VV., *Macchine che pensano*, cit., 37.

[132] La differenza tra dati strutturati e non assume rilievo non solamente nella prospettiva della tutela degli utenti che generano i dati, ma anche sotto un profilo di analisi economica. Come è noto, si fa riferimento a un dato strutturato quando esso è associato a un'identità e ordinato secondo alcune variabili; solitamente sono questa tipologia di dati a essere acquisiti mediante il consenso dell'interessato. Il dato non strutturato, invece, si riferisce a dati grezzi, a frammenti di informazioni, per i quali è possibile un'associazione a un'identità solo *ex post* e mediante le inferenze con altri dati raccolti; tendenzialmente questi dati vengono acquisiti fuori da una relazione contrattuale, quindi senza che sia richiesto un esplicito consenso per il loro utilizzo. Cfr. NICITA, *Il dato profilato nella prospettiva economica tra* privacy*,* propertization*,* secrecy, in *I dati personali nel diritto europeo*, cit., 1171.

[133] DE GREGORIO, TORINO, *op. cit.*, 449 s.; FARINA, *op. cit.*, 55 ss.

[134] Negli anni '90 del secolo scorso il processo di digitalizzazione della società ha avuto un nuovo stimolo proprio grazie al progresso tecnologico, tanto che il fenomeno è stato efficacemente descritto come "spostamento dal modo degli atomi ai bit", v. NEGROPONTE, *Being Digital*, New York, 1995. Difatti la crescita della sfera digitale ha condotto a un cambio di paradigma: dalla proprietà sulle cose a quella sulle informazioni. La rete, in particolare, costituisce una nuova miniera di dati – personali e non – la cui estrazione permette di generare valore e nuovi livelli di conoscenza.

[135] DALMASTRO, NICITA, *op. cit.*, 10 s.

[136] Anche la Commissione europea ha fatto proprio l'orientamento volto a riconoscere ai dati personali un valore economico *de facto*. V. Commissione europea, *Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali*, 2016, n. 28, consultabile all'indirizzo: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52016SC0163* (ultimo accesso 3 settembre 2020). Interessante sul punto la posizione di D'Ippolito, il quale sottolinea la vicinanza della materia con la disciplina sul diritto d'autore. L'A. ritiene, infatti, che così come il diritto d'autore si compone di un diritto morale, quale il riconoscimento della paternità dell'opera, e un diritto di "sfruttamento economico", quale la possibilità di riprodurre l'opera stessa, anche in materia di protezione dati si potrebbe configurare un diritto morale e uno negoziale (o di sfruttamento economico). Ciò permetterebbe di compiere un'analisi giuridico-economica del fenomeno più coerente, ma avrebbe anche il pregio di permettere una tutela più intensa al cittadino nel contesto digitale; infatti ai tradizionali

nelle imprese[137] – soprattutto per le piattaforme digitali – tanto da essere stati definiti il nuovo petrolio[138].

Il paragone con il petrolio, pur se evocativo, e ciò ne giustifica il successo, pare tuttavia impreciso. Il petrolio, come è noto, è un bene avente un valore di mercato generato dalla tensione tra la sua scarsità e la richiesta. Diverse invece le considerazioni che valgono per i dati prodotti, in quanto essi – come visto – di per sé non sono un bene

---

strumenti di tutela dei diritti fondamentali poterebbero essere affiancati anche quelli di stampo negoziale e di tutela del consumatore. D'IPPOLITO, *op. cit.*, 635 s. Del medesimo parere si mostra il TAR Lazio nelle recenti sentenze contro la piattaforma Facebook, sebbene poi faccia un esplicito riferimento al regime della compravendita quale categoria ove racchiudere i rapporti tra utenti e fornitori di servizi. I giudici chiariscono come: «*Le tesi di parte ricorrente presuppongono che l'unica tutela del dato personale sia quella rinvenibile nella sua accezione di diritto fondamentale dell'individuo, e per tale motivo Facebook era tenuta esclusivamente al corretto trattamento dei dati dell'utente ai fini dell'iscrizione e dell'utilizzo del "*social network*". Tuttavia, tale approccio sconta una visione parziale delle potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un "*asset*" disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto. A fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili forme di protezione, quali il diritto di revoca del consenso, di accesso, rettifica, oblio, sussiste pure un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati. Il fenomeno della "patrimonializzazione" del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un* "social network"». T.A.R. Lazio, 10.1.2020, n. 260, in *Foro Amm*., I, 2020, 99 ss.; in *Dir. int*., 2020, 521, con nota di BRAVO, *La «compravendita» di dati personali?*.

[137] Oltre al settore del marketing, le potenzialità legate allo sfruttamento dei Big Data interessano in modo trasversale l'intera società. Non solo le imprese private, con la c.d. Industria 4.0, ma anche le Istituzioni pubbliche possono generare valore dall'analisi dei dati. Si pensi agli algoritmi, già in uso in alcuni Stati, che permettono di razionalizzare il trasporto pubblico, oppure alle modellizzazioni dirette a testare i piani di evacuazione delle grandi città. I possibili vantaggi, non solo in termini di competitività economica, generati dalle tecnologie *data driven* sono enormi.

[138] L'espressione, coniata nel 2017 in un articolo pubblicato su The Economist, ha il merito di mettere in luce la crescente importanza dei dati, non solo nello sviluppo tecnologico, rappresentando essi di per sé un mercato in forte crescita. Mano a mano che le tecnologie informatiche divengono più pervasive il valore stesso dei dati da queste raccolti aumenta esponenzialmente, grazie alla creazione di veri e propri "giacimenti" di dati da cui estrarre informazioni e di conseguenza ricchezza. The Economist, *The world's most valuable resource is no longer oil, but data*, pubblicato il 6.5.2017, consultabile all'indirizzo: *https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data* (ultimo accesso 20 dicembre 2020). L'articolo mette in luce un'ulteriore e interessante criticità legata all'espansione pervasiva della *digital economy*. La conquista del mercato da parte dei "giganti di internet" (si tratta di Alphabet, affiliata Google, Apple, Amazon, Facebook, Alibaba e Microsoft), avendo accesso a una grande mole di dati detengono pressoché la totalità delle quote di mercato, divenendo inoltre tra i primi sviluppatori di tecnologie di AI. Ciò origina – si sottolinea – una possibile barriera all'ingresso nel mercato delle PMI. Il tema del dato quale bene economico e l'indagine circa il regime normativo a esso applicabile verrà approfondito *infra* al capitolo 5, a cui si rimanda. Si v. DEL FEDERICO, POPOLI, *Disposizioni generali*, in *Il nuovo regolamento europeo sulla privacy e sulla tutela dei dati personali*, diretto da FINOCCHIARO, Torino, 2017, 61.

esauribile, né scarso[139]. Questi possono essere riprodotti, riutilizzati e riorganizzati senza che ciò ne comporti un esaurimento, potendo di fatto essere conservati per un tempo potenzialmente indefinito, mantenendo intatte le proprie caratteristiche[140]. A ciò deve aggiungersi come risulti complessa la stessa attribuzione al singolo dato di un preciso valore economico, proprio a causa di dette caratteristiche e dell'utilizzo che ne viene fatto. Il tema è stato oggetto negli ultimi tempi di attenta riflessione, soprattutto in un'ottica di protezione degli utenti che spesso cedono i propri dati non pienamente consapevoli del valore degli stessi[141]. Le considerazioni nascono in particolare in merito a quelle transazioni, ormai quotidiane, poste in essere con i *Tech Giants* e dirette a usufruire di una applicazione o di un servizio dichiarati gratuiti; in relazione a questa prassi di mercato si è parlato di "*internet cost trap*"[142] per indicare come il cittadino sia tratto in "inganno" da un servizio solo apparentemente gratuito, erogato invece come corrispettivo alla cessione dei propri dati personali[143].

---

[139] Basti pensare come i dati, a differenza del petrolio, non si consumano con il loro utilizzo; inoltre il loro valore aggiunto è dato specificamente dalla capacità di analisi e di sfruttamento di *dataset* in continua crescita e tendenzialmente sempre disponibili. MAGGIANO, CICERCHIA, *Algoritmi, etica e diritto*, in *Dir. inform*., 2019, 1161 s.

[140] Le "informazioni" mostrano avere caratteristiche simili a quelle dei beni pubblici. Si tratta, infatti, di beni non escludibili, ciò in quanto una volta rivelate queste sono immediatamente acquisite da chi le riceve. Esse inoltre non presentano una rivalità nel consumo, infatti è possibile condividerle con un numero illimitato di soggetti. Le criticità legate alla considerazione dei dati quali beni pubblici saranno oggetto di approfondimento nell'ultima parte del presente lavoro. Basti qui ricordare che per non scoraggiare gli investimenti nel settore sarebbe necessario tenere in considerazione anche la possibilità di introdurre delle privatizzazioni dei dati per i casi in cui questi non sarebbero stati prodotti per l'impossibilità del produttore di valorizzarli sul mercato. V. sul punto, in merito al valore dell'informazioni all'interno dei mercati digitali, NICITA, *op. cit.*, 1165 s.

[141] DE FRANCESCHI, *Il "pagamento" mediante dati personali*, in *I dati personali nel diritto europeo*, cit., 1389; Organisation for Economic Co-Operation and Development, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OEDC Digital Economy Papers No. 220, 2013; MALGIERI, CUSTERS, *Pricing privacy: the right to know the value of your personal data* (2018) 34 *Computer Law & Security Review* 289 ss.; PROIETTI, *La responsabilità nell'Intelligenza Artificiale e nella robotica*, Milano, 2020, 88 ss. Si veda anche la sentenza del T.A.R. Lazio, 10.1.2020, n. 260, cit.

[142] Si tratta della c.d. "trappola del dono", indicandosi con tale espressione la considerazione per cui se il servizio o il bene offerto è dichiarato gratuito, allora il prodotto "venduto" sarebbe l'utente stesso. Il vero prodotto dei fornitori di servizi sarebbe, infatti, la raccolta e lo sfruttamento dei dati degli utenti, al fine di permettere la realizzazione di una pubblicità mirata o targettizzata, sempre più possibile grazie alle attività di profilazione mediante algoritmi. Cfr. D'IPPOLITO, *ibidem*; DE FRANCESCHI, *Il "pagamento" mediante dati personali*, cit., 1397; LANIER, *You are not a gadget: a manifesto*, London, 2011.

[143] RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inform*., cit., 709. Interessante notare come proprio su questa tesi si fondi la *class action* promossa da alcune associazioni a tutela dei consumatori in Europa contro Facebook, oltre che la sanzione comminata dall'Autorità Garante della Concorrenza e del Mercato alla stessa piattaforma per partiche commerciali scorrette; laddove Facebook non avrebbe adeguatamente informato gli utenti dell'attività di raccolta, con finalità commerciali, dei propri dati, ingannandoli enfatizzando la sola

Al fine di rendere maggiormente consapevoli gli utenti sono stati dunque elaborati servizi e applicazioni di varia natura[144]. Tra questi, per esempio, l'algoritmo messo a disposizione dal Financial Times[145] che indica un valore economico dei dati del singolo individuo tenendo in considerazione molte variabili, oltre che effettuando una comparazione tra classi di persone aventi redditi differenti. Testando l'algoritmo è emerso un differenziale nel valore dei dati di solo qualche decina di centesimi di dollaro, ciò a dimostrazione della impossibilità di ricondurre la stima del valore delle informazioni alla semplice valutazione dei classici parametri reddituali.

Il panorama dei modelli di monetizzazione dei dati personali, che permettono alle imprese di acquistare i dati direttamente dai consumatori, è oggi molto vasto. Tra essi si possono annoverare: i *data-insight models*, in cui aziende offrono agli utenti delle piattaforme in cui raccogliere, gestire e commerciare i propri dati[146]; i *data-tranfer models*, in cui le società acquistano, a fronte di un corrispettivo, le informazioni dagli utenti e, dopo averle catalogate e assegnato loro un valore, le trasferiscono sul mercato dove terzi possono acquistarle[147]. Tra questi, per fare un esempio, l'*App* "Weople" che dichiara di agire come una banca per investire i dati personali. L'applicazione, su delega degli interessati, esercita i diritti messi a disposizione dal GDPR, individuando e monitorando l'utilizzo dei dati personali, impegnandosi a restituire agli utenti parte del valore economico prodotto dal loro sfruttamento[148].

---

gratuità del servizio. V. provvedimento AGCM, PS11112, del 29 novembre 2018. Per un approfondimento della vicenda si rimanda a D'IPPOLITO, *op. cit.*, 650 ss.

[144] Interessante anche un'*App* (ErnieApp), frutto di una *startup* italiana, la quale rivela quanto valore le piattaforme digitali stanno estraendo dall'uso dei dati personali dell'utente. Tutto ciò mostra, concretamente, l'esistenza di un potenziale mercato che caratterizza l'ecosistema dei Big Data e ne spiega il funzionamento. Nel panorama economico si parla, infatti, di *Personal Data Economy*, a indicare il fenomeno per cui, per mezzo della cessione di dati personali, si realizzano trasferimenti di ricchezza. Si assiste oggi alla costruzione di un sistema economico "*user-centric*" che concepisce l'individuo quale proprietario di una ricchezza che può essere oggetto di operazioni economiche. Cfr. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, cit., 51; ELVY, *Paying for privacy and the personal data economy* (2017) *Columbia Law Review* 1369 ss.; DALMASTRO, NICITA, *op. cit.*, 29.

[145] É possibile stimare il proprio pacchetto dati al seguente indirizzo: *https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2WDzN1Z8V* (ultimo accesso 3 dicembre 2020).

[146] Questi modelli di business trovano spazio per lo più nel contesto economico americano. In Italia Tim ha avviato un progetto chiamato "*My data store*" nell'ambito del quale viene messa a disposizione degli utenti una piattaforma digitale che consente ad essi di conservare e gestire i propri dati, anche mediante un confronto con quelli degli altri utenti. Cfr. RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, cit., 50 s.

[147] RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, *ibidem*.

[148] La rilevanza di tale servizio è confermata dal fatto che su di essa il Garante ha avviato un'indagine chiedendo l'intervento del Comitato Europeo per la Protezione dei Dati Personali (EDPB). Dalle

É necessario comunque chiarire come questi strumenti, sebbene utili, siano necessariamente imprecisi; molti sono i fattori da dover tenere in considerazione e spesso non è dunque possibile avere una valutazione economica affidabile. Per meglio comprendere si pensi agli algoritmi di previsione dei risultati elettorali. Il valore degli elettori non è uguale per le società – soprattutto americane – che si occupano di campagna elettorale, oggi sempre più diretta a tecniche di micro-targetizzazione[149]. Il dato di un elettore indeciso ha evidentemente più valore di quello di uno politicamente schierato; anche tra elettori indecisi il valore del dato sarà più elevato per quelli che si trovano in fasce geografiche che non siano tradizionalmente indirizzate verso un determinato schieramento politico. La ragione della diversità di valutazione qui è lampante ed è strettamente legata alla maggiore possibilità di orientare il voto. Ciò fa comprendere tuttavia come siano molti i fattori che possono influenzare la valutazione economica, anche in ragione delle differenti finalità di utilizzo dei dati. Inoltre, è necessario aggiungere che oggi per le imprese è l'insieme dei dati ad acquistare valore, a seguito dell'analisi che ne viene fatta, più che il dato grezzo facente capo al singolo individuo[150].

Da quanto sopra esposto emerge quindi come nell'attuale contesto di trasformazione dell'intera società il potenziale economico rappresentato dallo sfruttamento dei dati si dimostra essere enorme, e ciò soprattutto grazie alla mole considerevole di informazioni

---

risultanze di tale istruttoria potranno sicuramente giungere indicazioni e chiarimenti utili in merito all'attività di Weople, nonché sulla possibilità di utilizzare il diritto alla portabilità dei dati *ex* art. 20 del Regolamento tramite deleghe su "larga scala". Cfr. D'IPPOLITO, *op. cit.*, 649 s.

[149] Interessante l'analisi compiuta da BONAVITA, *La profilazione e il micro-targeting*, in *Il diritto di internet nell'era digitale*, a cura di CASSANO e PREVITI, Milano, 2020, 391 ss. Nel saggio l'Autore analizza le finalità a cui viene diretta la profilazione, in particolare nel settore marketing. Attenzione viene prestata alle tecniche di *microtargeting* e alle prospettive evolutive che esse veicolano, grazie allo sviluppo dei processi di *data mining* in grado di segmentare sempre più il mercato. Viene fatto un interessante riferimento anche ad attività di *Hyper-targeting* e di *micro-targeting*. In argomento v. anche ID., *La profilazione*, cambridge analytica *e il* micro-targeting, in *Tecnologia e Diritto*, III, cit., 65 ss. Per un approfondimento, anche in tema di marketing politico, si rimanda a GUGGINO, BANORRI, *L'*advertising *ai tempi dell'Intelligenza Artificiale: algoritmi e* marketing *personalizzato*, in *Intelligenza Artificiale. Il diritto, i diritti, l'etica*, a cura di RUFFOLO, 2020, Milano, 625 ss.

[150] Negli Stati Uniti sono state presentate alcune interessanti proposte legislative dirette a obbligare i titolari del trattamento a informare gli utenti del valore attribuito ai loro dati; così che questi possano effettuare una scelta effettivamente consapevole. Si pensi al progetto di legge: *Designing Accounting Safeguards to Help Broaden Oversight and Regulations on Data Act (Dashboard Act)*. Cfr. SPERANDIO, *Ecco come il Senato Usa vuole indagare sul valore dei dati di Amazon, Facebook e Google*, in *Smart Magazine*, 24.6.2019, consultabile all'indirizzo: *www.startmag.it/innovazione/amazon-facebook-google-dati-valore/* (ultimo accesso 30 gennaio 2021). Sull'importanza di informare gli interessati del valore economico attribuito ai loro dati si veda MALGIERI, CUSTERS, *ibidem*.

estratte e raccolte da dispositivi di uso sempre più comune[151]. I dati, lungi dall'essere unicamente espressione di attributi del singolo individuo, assumono dunque rilevanza proprio in ragione della loro capacità di generare ricchezza. La tradizionale dicotomia tra mercato e persona viene così a sfumare, al pari dell'assunto circa l'indisponibilità e non commerciabilità degli attributi della persona, di fronte alla consapevolezza che nella prassi di mercato di un'economia complessa – quale è quella dei dati – le informazioni ricoprono un ruolo fondamentale in termini economici[152]. La disponibilità sempre maggiore e l'evoluzione delle tecniche di analisi hanno infatti comportato una profonda trasformazione di ogni settore di mercato; grazie allo sfruttamento dei Big Data vengono creati nuovi modelli di business – *data driven* – in grado di cogliere, pur con un investimento contenuto, vantaggi in termini di produttività ed efficienza[153]. Si è così assistito alla creazione di un mercato ove, grazie all'irrefrenabile diffusione delle tecniche di *data mining*, le società che raccolgono dati hanno raggiunto un enorme potere, potendo sia vendere i *dataset* o, come sempre più spesso accade, acquisendo un ruolo rilevante anche nel settore delle tecnologie, in particolare nell'Intelligenza Artificiale. Per comprendere l'importanza del fenomeno basti pensare che si è stimato l'economia digitale possa contribuire alla crescita del PIL europeo di circa cinquecento

[151] Il riferimento è, ovviamente, alla diffusione sempre più pervasiva degli *Internet of Things*. La capacità di questi oggetti di raccogliere a livello locale le informazioni degli utenti permette di avere accesso a dati quasi ininterrottamente; anche quando l'utilizzatore non ne sia a conoscenza. Particolari criticità sorgono poi per quei dispositivi che raccolgono dati sanitari degli utenti. Il settore della *smart health* è oggi in forte crescita, molteplici sono le società che progettano applicazioni e dispositivi in grado di analizzare le condizioni di salute dei propri utilizzatori e, alcune, finanche di proporre diagnosi. Per un approfondimento in merito all'utilizzo dei dati nel settore medico, e delle criticità correlate, senza pretesa di esaustività si rimanda a: SCALZINI, *Alcune questioni a proposito di algoritmi, dati, etica e ricerca*, in *Riv. it. med. leg*., 2019, 169 ss.; AMRAM, *L'Ulisse* Accountable. *Ricerca e protezione dei dati personali concernenti la salute: il tentativo di armonizzazione a livello europeo post GDPR e le interpretazioni offerte dai sistemi irlandese, belga, spagnolo e italiano*, *ivi*, 209 ss.; COMANDÈ, *Ricerca in sanità e* data protection *un puzzle… risolvibile*, *ivi*, 187 ss.; RICOTTI, *Dati sanitari e gli altri profili etici nella bioingegneri*a, *ivi*, 251 ss.; COMANDÈ, *Intelligenza artificiale e responsabilità tra* liability *e* accountability, cit., 169 ss.; MASTRELIA, *Gestione dei* Big Data *in una prospettiva orientata alla tutela della* privacy *degli individui*, in *Dir. ind*., 2018, 364 ss.; ASCIONE, *Il futuro della salute. Come la tecnologia digitale sta rivoluzionando la medicina (e la nostra vita)*, Milano, 2018; CAPPELLETTI, GOLATO, *Medicina di Laboratorio 4.0*, in *Riv. it. med. leg*., 2018, 192 ss. Interessante anche il documento elaborato dal Comitato etico nazionale per la bioetica, in concerto con il Comitato nazionale per la biosicurezza, le biotecnologie e le scienze della vita, dal titolo *Intelligenza artificiale e medicina: aspetti etici*, pubblicato il 29.5.2020, consultabile all'indirizzo: *federalismi.it* (ultimo accesso 26 gennaio 2021).

[152] RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, *ibidem*.

[153] PRETA, ZOBOLI, *Intelligenza Artificiale ed economia dei dati. Profili regolatori e concorrenziali in tema di accesso e condivisione dei dati*, in *Analsi giur. econ*., 2019, 213 ss.

miliardi di euro[154]; appare dunque evidente l'esigenza di una regolazione che, permettendo il potenziamento del mercato unico digitale, sia in grado di sfruttare questo enorme potenziale[155].

1.1 Il mercato digitale. Caratteristiche e criticità

Prima di procedere con l'analisi della strategia europea di settore è necessario chiarire preliminarmente le caratteristiche del mercato digitale, le cui particolarità necessitano di una attenta riflessione diretta a vagliare l'efficacia delle differenti proposte regolative.

L'avvento e la diffusione delle applicazioni digitali sono – come è noto – alla base del fenomeno della convergenza delle tecnologie e dei mercati dell'informazione e della comunicazione[156]. Questo fenomeno, in corso già da trent'anni, ha indotto le Istituzioni sovranazionali a studiarne le evoluzioni con una specifica attenzione alle industrie dell'informatica e delle telecomunicazioni. Nel corso degli anni si è assistito infatti ad un'espansione, quasi a macchia d'olio, delle tecnologie in ogni settore produttivo, comportando il passaggio a un sistema di mercato sempre più complesso. Tra i maggiori esperti si ritiene finanche che sarebbe più appropriato parlare oggi di ecosistema digitale, più che di mercato[157]. La metafora, introdotta da Fransman, fa perno sulla molteplicità degli attori coinvolti, che a rigore poteremmo definire "specie"[158], e sulla

[154] ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679/UE*, in *Eurojus*, 31.5.2018, consultabile all'indirizzo: *http://rivista.eurojus.it/alcune-riflessioni-a-margine-della-nuova-disciplina-in-materia-di-protezione-dei-dati-personali-di-cui-al-regolamento-ue-2016679ue/* (ultimo accesso 26 gennaio 2021).

[155] Presa coscienza delle potenzialità del settore la Commissione, presieduta da Juncker, nel 2015 ha presentato un'agenda per il mercato unico digitale corredata da un piano composto da sedici azioni dirette a gettare le basi per un quadro giuridico unitario della materia. Cfr. ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina*, *ibidem*.

[156] Si parla di convergenza tra tecnologie già nel *report* pubblicato dall'OECD nel 1992. L'organizzazione per la cooperazione e lo sviluppo economico fu tra i primi organismi a osservare il fenomeno in ragione delle potenzialità dirompenti sui mercati, e in particolare su quelli delle telecomunicazioni e informatici. V. OECD, *Convergence between Communications Technologies*: *Case Studies from North America and Western Europe*, Parigi, 1992; OECD, *Telecommunications and Broadcasting: Convergence or Collision? No. 29*, OECD Digital Economy Papers(5), 1992, consultabile all'indirizzo: *https://www.oecd-ilibrary.org/science-and-technology/telecommunications-and-broadcasting_237416285388* (ultimo accesso 5 novembre 2020).

[157] V. sul punto l'interessante analisi compiuta da PERRUCCI, *op. cit.*, 61 ss.

[158] A ciò è necessario aggiungere come vi siano altresì una pluralità di attori, oltre ai soggetti che generano i dati, tra cui: fornitori della strumentazione tecnologica (comprese le piattaforme digitali);

complessità dell'ambiente in cui essi agiscono[159]. Analizzando l'ambiente digitale, difatti, possono essere individuati differenti livelli funzionali che interagiscono e influenzano il sistema; si pensi agli elementi hardware e software, all'operatività e connettività delle reti, alle applicazioni e servizi e, infine, al consumo dei prodotti. Inoltre, recentemente, una fondamentale importanza stanno rivestendo le tecnologie ad alta pervasività (*general purpose technologies*), per lo più software, che sono sviluppate mediante l'utilizzo di algoritmi di Intelligenza Artificiale[160]. É evidente che ogni livello potrebbe rappresentare un mercato a sé stante, nel quale possono essere individuati *competitors*, prodotti e utenti a cui destinare l'offerta. Tuttavia, un'attenta analisi, che sia diretta a valutare il ruolo dei Big Data, non può prescindere dall'esame di tutti questi elementi e delle modalità di interazione tra di essi.

Oltre alle considerazioni in merito alla complessità delle dinamiche di mercato è necessario ricordare come il *Digital Single Market* si differenzi dai mercati "tradizionali" anche per i beni in esso oggetto di scambio. Nei mercati "tradizionali", difatti, il valore economico è prodotto dallo scambio di beni e servizi; nel mercato

---

coloro che utilizzano i Big Data per creare valore aggiunto; i *data brokers*; le imprese e organizzazioni per la ricerca e sviluppo di nuove tecnologie e gli stessi enti pubblici.

[159] FRANSMAN, *The New ICT Ecosystem: Implications for Policy and Regulation* (2010) *Cambridge University Press* 21 ss.

[160] Interessante sul punto l'*interim report* dell'AGCom ove viene descritto l'ecosistema dei Big Data. Nel documento si riporta come dall'analisi del sistema emergano differenti criticità legate alla concorrenza e alla trasparenza del mercato, con ciò sottolineando la presenza di evidenti situazioni di fallimento del mercato. Viene in particolare evidenziato come «i fallimenti di mercato si ripercuotono su tutto il contesto sociale, compreso il sistema dell'informazione, il pluralismo delle fonti, e le stesse modalità di aggregazione sociale e di formazione dell'opinione pubblica. In conseguenza dell'esistenza di strutturali e duraturi fallimenti di mercato, è necessario, soprattutto laddove sono in discussione diritti sociali e politici, adottare un approccio *ex ante* alla regolamentazione del dato (e ai connessi algoritmi). Peraltro, questo nuovo paradigma deve considerare che le asimmetrie informative tra utenti e operatori sono pervasive e strutturali. In questo contesto, è difficile ripristinare condizioni di efficienza attraverso meccanismi di trasparenza e di consenso informato. Infatti, tali strumenti appaiono, in molti casi, insufficienti a garantire un riequilibrio conoscitivo tra operatori e consumatori, in una situazione in cui spesso soggetti quali esperti del settore, istituzioni specializzate, nonché centri di ricerca non hanno a disposizione elementi conoscitivi sufficienti a comprendere l'entità e la natura stessa dei fenomeni. In linea con quanto avviene già in contesti ad alta tecnologia (quali quelli delle comunicazioni elettroniche), appare necessario accompagnare la nuova regolazione verso forme tecniche di regolazione diretta degli operatori che utilizzano i Big Data». V. AGCom, *Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera 217/17/CONS*, 8.6.2018, 7, consultabile all'indirizzo: *https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0* (ultimo accesso 30 dicembre 2020). Nel 2020 l'AGCom, continuando nell'opera di osservazione del mercato, ha pubblicato un nuovo documento in merito all'impatto dei Big Data nel mercato. AGCom, *Indagine conoscitiva sui Big Data di cui alla delibera 458/19/CONS*, 10.2.2020, consultabile all'indirizzo: *https://www.agcom.it/documents/10179/17633816/Documento+generico+10-02-2020+1581346981452/39c08bbe-1c02-43dc-bb8e-6d1cc9ec0fcf?version=1.0* (ultimo accesso 30 dicembre 2020).

digitale, invece, questi ricoprono un ruolo ancillare, in quanto funzionali a generare valore in un mercato più ampio, denominato dell'attenzione. In questo mercato il valore viene dato dal tempo che l'utente dedica alla fruizione e alla ricezione dei messaggi di varia natura a cui viene esposto. In questa prospettiva la scarsità del tempo di attenzione, e le modalità in cui detta variabile può essere allocata in modo ottimale, rappresenta il fulcro attorno a cui operano le piattaforme digitali e dunque l'oggetto stesso degli scambi[161].

Lo studio del funzionamento del mercato digitale non è quindi opera semplice, soprattutto in ragione della complessità delle interazioni tra i diversi attori nei differenti livelli funzionali. Date le grandi potenzialità economiche che esso veicola[162] è opportuna un'attenta valutazione in merito agli effetti derivanti dall'introduzione di normative, e ciò a causa della profonda influenza che una disciplina troppo rigida è in grado di esercitare sulle dinamiche competitive. Già da una prima analisi emergono tuttavia alcuni segnali di una situazione di fallimento di mercato, da cui discende un detrimento non solamente dei diritti dei consumatori ma anche della stessa qualità dell'offerta, essendo limitato enormemente lo sviluppo di prodotti e servizi che un mercato aperto invece permetterebbe.

Parte dei commentatori ha comunque reputato prematura la richiesta di un intervento normativo sul punto, ritenendo piuttosto necessaria una preliminare verifica dell'effettivo fallimento di mercato. Detta posizione può essere fatta discendere dalla prospettiva per cui il mercato digitale, sebbene abbia un innegabile impatto nelle economie mondiali, rimane un fenomeno troppo recente per poter valutare compiutamente la sussistenza in esso di eventuali effetti distorsivi. In parte si ritiene

[161] NICITA, *op. cit.*, 1168. L'A. evidenzia come il tempo di attenzione degli utenti registra un flusso di informazioni sia in interata, da parte delle piattaforme digitali, che in uscita grazie ai dati forniti dagli utenti durante la fruizioni dei servizi. Si ritiene dunque operante un doppio filtro: «da un lato riveliamo alle piattaforme digitali informazioni dettagliate su ciò che preferiamo (prodotti, servizi, amici, visioni politiche, sociali e personali), dall'altro le piattaforme digitali selezionano informazioni (su prodotti, servizi, amici, visioni politiche, sociali e personali) che ci fanno risparmiare tempo di attenzione (e quindi tempo *tout court*, ottimizzando l'allocazione di una risorsa)».

[162] Si registrano, infatti, elevate economie di scala – in particolare dal lato delle imprese che forniscono servizi e raccolgono dati – come conseguenza della crescita del volume di dati e della capacità della tecnologia di trovare correlazioni e di estrarre dunque valore tra *dataset* sempre più eterogenei. Interessanti le considerazioni in merito alle opportunità nascenti dall'uso dei Big Data nella catena di distribuzione in HOBERG, voce «Supply Chain and Big Data», in *Encyclopedia of Big Data*, a cura di SCHINTLER, MCNEELY, Berlin, 2021, consultabile all'indirizzo: *https://www.researchgate.net/publication/338549111_Supply_Chain_and_Big_Data* (ultimo accesso 15 gennaio 2021).

difficile finanche valutare l'efficacia degli attuali strumenti regolativi della concorrenza, essendo complessa la stessa individuazione di un mercato rilevante per i dati[163].

Queste considerazioni tuttavia non convincono pienamente; se è vero che i confini tra i mercati sono divenuti meno chiari e più mutevoli, sarebbe allora maggiormente auspicabile porre l'attenzione sulle teorie del danno e sull'identificazione delle strategie anticoncorrenziali, più che centrare l'analisi sulla definizione di mercato rilevante[164]. Difatti osservando il mercato sotto queste lenti emergono evidenti criticità legate all'assetto concorrenziale dello stesso. Si registrano barriere all'ingresso, in particolare nella fase di raccolta dei dati, dovute al ruolo di assoluta preminenza delle multinazionali digitali. Queste ultime, avendo accesso ad una grande mole di dati, hanno conquistato un forte vantaggio concorrenziale e di conseguenza una posizione dominante, rendendo difficile l'ingresso nel mercato alle piccole e medie imprese che spesso finiscono con l'essere direttamente acquisite delle Big Tech[165].

A ciò deve aggiungersi la presenza di significative e strutturali asimmetrie informative tra le imprese e i consumatori. Questi ultimi si trovano in una posizione di endemica debolezza dal momento che sovente non comprendono a pieno gli aspetti tecnici e i meccanismi a fondamento del funzionamento dell'economia *data driven*; proprio l'ignoranza dei consumatori determina esternalità positive per le società che generano e raccolgono dati[166].

---

[163] Cfr. sul punto PRETA, ZOBOLI, *op. cit.*, 219 ss. Gli Autori ritengono, infatti, che non siano emerse evidenze sufficientemente chiare di un fallimento di mercato e che, dunque, debba essere necessaria una attenta verifica di un suo effettivo avveramento, tale da poter giustificare un intervento regolatorio. Gli Autori reputano piuttosto maggiormente appropriato l'istituzione di un'autorità di concorrenza (e di un unico regolatore digitale) che, pur mantenendo le proprie attribuzioni e competenze, utilizzi strumenti sempre più evoluti, tra cui la stessa Intelligenza Artificiale, al fine di far fronte alle possibili criticità che possano discendere dalla *data driven economy*.

[164] PERRUCCI, *op. cit.*, 81; DI PORTO, *La rivoluzione Big Data. Un'introduzione*, in *Conc. merc*., 2016, 10.

[165] DI PORTO, *op. cit.*, 11 s.; D'ACQUISTO, PIZZETTI, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, in *Analisi giur. econ*., 2019, 94 ss.; PERRUCCI, *op. cit.*, 82. Contra v. PRETA, ZOBOLI, *op. cit.*, 219, secondo cui la valutazione deve essere fatta caso per caso in quanto «i Big Data per ciò stessi non possono garantire un consistente vantaggio competitivo, tuttavia la loro combinazione con altre caratteristiche tipiche di chi opera in mercati digitali potrebbe favorire il crearsi di dinamiche anti-competitive […] non si può arrivare a una conclusione generale per cui i dati di per sé possano conferire un vantaggio competitivo». Sul punto, nel 2016, l'European Data Protection Supervisor (EDPS) ha sottolineato l'incidenza dei Big Data in ambito concorrenziale, evidenziando il rischio di creare forme di posizioni dominanti nel mercato proprio in relazione alla quantità di dati raccolti e analizzati, invitando al dialogo le Autorità competenti. EDPS, *Opinion on coherent enfrorcement of fundamental rights in the age of big data*, 2016.

[166] D'IPPOLITO, *op. cit.*, 650 ss.; PERRUCCI, *op. cit.*, 71. Interessante, sul punto, il recente caso che ha visto l'Autorità Antitrust tedesca, nel febbraio del 2019, imporre importati restrizioni a Facebook, in merito alle modalità con cui l'azienda profila i propri utenti. L'Autorità ha così disposto alla società di chiedere il consenso dei consumatori sia in caso la piattaforma faccia utilizzo dei dati raccolti dalle proprie

A fronte delle criticità riscontrate alcuni interventi possono rappresentare un primo passo nella prospettiva di potenziamento e di sviluppo del mercato. In particolare sarebbero auspicabili sia un libero accesso ai dati, così da dare respiro alla concorrenza[167], sia una circolazione più agevole degli stessi mediante l'uso di protocolli informatici unitari e condizioni generali di contratto; interventi questi che accrescerebbero anche la fiducia dei consumatori.

Quanto alle asimmetrie tra imprese e utenti, a livello europeo si è prestata una particolare attenzione allo strumento dell'informativa sul trattamento dei dati, allo scopo di renderla maggiormente trasparente[168]. Per far fronte al *gap* informativo è stata anche avanzata un'interessante proposta avente ad oggetto l'uso di particolari tecniche informatiche, quali il *web scraping*. Tralasciando i dettagli tecnici di funzionamento, il *web scraping* permette l'estrazione dell'intero contenuto presente in un sito web[169]. Certamente il pregio di tale procedimento risiede evidentemente nella presa di coscienza

---

applicazioni, sia in caso siano impiegati dati raccolti su siti terzi. L'Antitrust aveva, infatti, riscontrato un abuso di posizione dominante dato dalla capacità di Facebook di costruire profili dei propri utenti, potendo questa avere accesso a una grande mole di dati provenienti anche da terze parti. Proprio questa disponibilità di dati, indispensabile per costruire profili accurati, garantirebbe a Facebook un significativo potere di mercato, che non poterebbe essere intaccato da altri *competitor*; questi, infatti, non sarebbero in grado di sfruttare simili capacità di combinazione di dati da diverse fonti. Elemento forse ancora più interessante risiede nella natura del provvedimento emanato. l'Autorità tedesca, al fine di rimuovere una distorsione competitiva, ha utilizzato uno strumento di *data protection*: il consenso degli interessati per l'utilizzo di dati raccolti da siti terzi. Così facendo l'Antitrust mira a ottenere una riallocazione di valore economico in capo agli stessi utenti che generano i dati. Per un approfondimento della vicenda si rimanda a D'ACQUISTO, PIZZETTI, *op. cit.*, 96 ss.

[167] La condivisione dei dati, in astratto, può migliorare la qualità dei prodotti e dei servizi, fornire uno stimolo all'innovazione e, di conseguenza, avere un impatto positivo tanto sul benessere dei consumatori quanto sull'efficienza dei mercati. Ciò detto, i vantaggi competitivi sono radicati nel fatto che i dati sono un *input* che non ammette sostituti e ciò è estremamente raro, poiché i dati sono sovente sostituibili da altri e, al contempo, le società interessate riescono spesso a generare o a ottenere dal mercato i dati in questione. In questo senso, la condivisione dei dati può anche rappresentare un rischio per l'efficienza del mercato e il benessere dei consumatori. In particolare, il fatto che la condivisione dei dati sia gestita tramite contratti e che dipenda totalmente dall'autonomia privata può generare inefficienze e produrre perdite di benessere, oltreché una distribuzione iniqua e ingiustificata dei benefici tra le parti. PRETA, ZOBOLI, *op. cit.*, 218 s.; DI PORTO, *op. cit.*, 12 s.

[168] Vengono previsti specifici obblighi in capo ai titolari dei trattamenti di fornire un'informativa che sia effettivamente intellegibile e specifichi quali i dati raccolti, oltre che chiara sulle finalità terze a cui questi potranno essere soggetti.

[169] Il "web scraping" può essere definito come «*a technique to extract data from the World Wide Web (WWW) and save it to a file system or database for later retrieval or analysis. Commonly, web data is scrapped utilizing Hypertext Transfer Protocol (HTTP) or through a web browser.* […] *Due to the fact that an enormous amount of heterogeneous data is constantly generated on the WWW, web scraping is widely acknowledged as an efficient and powerful technique for collecting big data*», ZHAO, voce «Web Scraping», in *Encyclopedia of Big Data*, a cura di SCHINTLER, MCNEELY, Berlin, 2021, consultabile all'indirizzo: *https://www.researchgate.net/publication/317177787_Web_Scraping* (ultimo accesso 16 gennaio 2021).

di quali e quanti dei propri dati vengono raccolti, rendendo così gli interessati maggiormente consapevoli delle modalità e delle finalità del trattamento. Sebbene il richiamo a detta tecnica sia evocativo, è tuttavia necessario verificare previamente la compatibilità del suo utilizzo sia con le norme a protezione dei *database*, e ciò soprattutto per l'incertezza in merito al riutilizzo che di questi dati potrebbe essere fatto successivamente all'estrazione, sia con la normativa a tutela dei dati personali[170]; l'estrazione dell'intero contenuto di un sito web può difatti comportare la violazione dei diritti degli utenti che non hanno dato il consenso a questo tipo di raccolta.

Così chiarito il funzionamento del mercato, è apparso prioritario un intervento normativo da parte delle Istituzioni europee. Infatti, data la natura della materia, è risultata evidente la necessità di una strategia unitaria, avente respiro sovranazionale, che permettesse una regolazione dell'ecosistema digitale in grado di sfruttarne le enormi potenzialità economiche, e che al contempo permettesse la tutela dei diritti fondamentali dei cittadini[171].

2. La strategia europea: Intelligenza Artificiale e dati, una regolazione necessariamente coordinata

Nella prospettiva di contemperare esigenze economiche e diritti delle persone, le Istituzioni europee hanno elaborato una strategia diretta a coordinare e armonizzare le normative regolanti i settori maggiormente interessati dalle tecnologie *data driven*, tra cui *in primis* l'Intelligenza Artificiale[172]. Le grandi potenzialità derivanti dallo sviluppo

[170] Per un'analisi approfondita in merito alle criticità nascenti dall'uso di queste tecniche si rimanda a Monterossi, il quale precisa come il fenomeno non sia recente, avendo detti software contribuito allo sviluppo della rete Internet sin dalle sue prime fasi, ma solo il recente utilizzo ha dato origine a una pluralità di controversie. V. MONTEROSSI, E*strazione e (ri)utilizzo di informazioni digitali all'interno della rete internet. Il fenomeno del c.d. web scraping*, in *Dir. inform*., 2020, 328 s. Interessanti anche le considerazioni di Sammarco in merito alle tensioni con il diritto *sui generis* attribuito al costitutore di una banca dati. V. SAMMARCO, *L'attività di web scraping nelle banche dati ed il riuso delle informazioni*, *ivi*, 219 ss.

[171] L'avvento della società digitale e la diffusione delle tecnologie ha comportato indubitabili vantaggi, sia economici che sociali, a cui però fanno da contraltare alcune criticità strettamente legate al loro stesso funzionamento. In particolare la portata *disruptive* delle tecniche *data analysis* ha fatto emerge l'esigenza di una regolazione diretta a sfruttarne il potenziale economico, pur nel rispetto dei principi cardine dell'ordinamento giuridico. La produzione sempre crescente di dati, e la raccolta degli stessi da parte delle grandi compagnie, ha difatti generato preoccupazioni, sia in merito alla tutela delle persone, che alla tutela dei mercati e della concorrenza.

[172] L'intensità dell'interesse manifestato dall'UE verso l'Intelligenza Artificiale emerge dalla serie crescente, assai ampia e variegata, di documenti adottati da Istituzioni e organi: pareri; proposte;

di dette tecnologie sono infatti strettamente legate alla capacità di gestione e di analisi dei dati da parte delle imprese e delle stesse amministrazioni[173]. È stato così messo a punto un piano d'azione avente l'obiettivo di aumentare gli investimenti, nel dichiarato intento di massimizzare i benefici dell'economia digitale e al contempo nell'ottica di far fronte alla competizione globale, che rischiava di vedere il vecchio continente ricoprire un ruolo marginale rispetto alla Cina[174] e agli Stati Uniti[175]. L'Europa, sebbene non

risoluzioni e comunicazione esplorano, in modo alquanto eterogeneo, le caratteristiche e le conseguenze dell'attuale espansione dell'Intelligenza Artificiale. Cfr. ADINOLFI, *op. cit.*, 13 s.

[173] Difatti, si ricorda, quantità sempre maggiori di dati richiedono capacità di analisi sempre più complesse e strumenti sempre più sofisticati che permettano di individuare collegamenti nascosti e così estrarre valore dagli stessi. In questo si esplica il rapporto simbiotico con l'Intelligenza Artificiale. Quest'ultima è essenziale per permettere all'economia digitale di espandersi; l'accesso e la condivisione di dati, d'altro canto, è cruciale per lo sviluppo delle applicazioni di IA, le quali necessitano di una mole sempre maggiore di informazioni per migliorare le proprie prestazioni in termini di efficacia e affidabilità. PRETA, ZOBOLI, *op. cit.*, 214; FARINA, *op. cit.*, 55 ss.

[174] Il Governo cinese ha approvato un piano di investimenti, denominato Cina 2030, diretto a potenziare l'intero comparto dell'Intelligenza Artificiale, con il dichiarato scopo di rendere la Nazione la prima economia mondiale. Oltre agli investimenti economici, la Cina è altresì impegnata in una politica di favore nel permettere l'impiego di artefatti e applicazioni di Intelligenza Artificiale, a livello anche di amministrazione governativa; non risale a molto tempo fa la notizia di uno *scoring* della popolazione cinese che dovrebbe facilitare l'accesso a servizi pubblici ai cittadini con un punteggio alto. Ancora recentemente si è parlato di "robot poliziotti", o di "avvocati robot". Crescenti investimenti e una politica maggiormente libertaria rendono la Cina un mercato fortemente attrattivo per le aziende che ideano e sviluppano tecnologia di AI. Gli investimenti cinesi inoltre sono indirizzati anche alla costruzione di reti 5G, così da poter gestire in modo più efficiente il flusso di dati, indispensabili per lo sviluppo della tecnologia. L'ubiquità e la pervasività degli strumenti di Intelligenza Artificiale fanno, tuttavia, sorgere perplessità in merito ai meccanismi di tutela degli individui, e ciò soprattutto di fronte al rischio di una politica totalitaria diretta a controllare i cittadini, non lasciando loro alcuno spazio di libertà e di autodeterminazione. Sul punto Soro evidenzia come «in Cina, l'innesto così profondo della tecnologia nella vita privata e pubblica, si è accompagnato a una altrettanto pervasiva ingerenza dello Stato nell'esistenza individuale, in un contesto di sostanziale osmosi tra i grandi provider e il Governo, legittimato ad ottenere dai primi, per generiche ragioni di sicurezza, i dati personali di chiunque». V. SORO, *La protezione dei dati personali nell'era digitale*, in *Nuova giur. civ. comm.*, 2019, II, 343 ss. Sempre in tema di pervasività del controllo si rimanda anche a PASQUALE, *New laws of robotics. Defending human expertise in the age of AI*, Cambridge, 2020, 60 ss. Per un'analisi circa le politiche cinesi di incentivo alla tecnologia digitale e all'intelligenza artificiale si rimanda, tra gli altri, a: NEGRO, *Intelligenza artificiale in Cina. Oltre il presentismo*, in *Sinosfere*, 28.11.2019, consultabile all'indirizzo: *https://sinosfere.com/2019/11/28/gianluigi-negro-intelligenza-artificiale-in-cina-oltre-il-presentismo/* (ultimo accesso 24 gennaio 2021); CHENG *et al*., *The Rise of Robots in China* (2019) 33 *Journal of Economic Perspectives* 71 ss.; BENEDETTI, *op. cit.*, 255 ss.; DALMASTRO, NICITA, *op. cit.*, 121 ss.; SANTOSUOSSO, *Intelligenza Artificiale e diritto*, cit., 5. Una prima timida apertura verso la tutela dei cittadini può essere vista nell'entrata in vigore, da gennaio 2021, del nuovo codice civile cinese; la quarta parte viene dedicata ai diritti della personalità, tra cui il diritto alla privacy e alla protezione dei dati personali, così esportando – in parte – il modello europeo. Per un approfondimento si rimanda a SHENG, XU, CAI, *China promulgates its long-awaited civil code*, consultabile all'indirizzo: *www.pillsburylaw.com* (ultimo accesso 26 gennaio 2021).

[175] In questo quadro, la *deregulation* americana appare favorevole allo sviluppo delle applicazioni di IA, ma con scarsa attenzione finora in merito a questioni di privacy e di tutela dei dati personali. L'Unione Europea, partendo con un po' di ritardo e con risorse non comparabili con quelle messe in campo dalle due superpotenze commerciali, ha scelto in ogni caso un percorso orientato a perseguire la massimizzazione dei benefici dell'IA, riducendone al contempo al minimo i rischi e adottando in tal senso

possa competere con le grandi potenze d'Oltreoceano sul piano degli investimenti, rappresenta un'attrattiva per le imprese digitali in ragione del bacino di utenza ad essa collegato[176]. Non stupisce dunque come agli albori degli anni '90 i primi interventi delle Istituzioni sul punto furono diretti a creare un *framework* normativo che permettesse lo sviluppo del mercato unico digitale[177], con una particolare attenzione all'accesso e alla condivisione dei dati; elementi questi essenziali per mantenere la competitività e per incrementare le opportunità di innovazione delle imprese[178].

Per quanto riguarda le interazioni tra Intelligenza Artificiale e dati, il primo intervento risale al 1981. Con la nascita della rete internet, l'aumento delle capacità tecnologiche e la diffusione delle applicazioni informatiche, si iniziò a sentire l'esigenza di una normativa a tutela dei cittadini; venne così emanata la Convenzione 108[179], a cui tuttavia non seguirono altri interventi normativi di rilievo. Solo recentemente un rinnovato interesse, derivante dai fascinosi successi che l'Intelligenza Artificiale ha conquistato in diversi ambiti[180], ha spinto il legislatore europeo a occuparsi più organicamente e specificamente della materia. In un clima di fervente attesa delle future

---

un approccio antropocentrico, fondato su una concezione etica dell'AI. V. sul punto PRETA, ZOBOLI, *op. cit.*, 215 s.

[176] L'obiettivo di rendere l'Europa competitiva, *in primis* colmando il *gap* di conoscenza tra le parti, viene a più riprese citato nei documenti delle Istituzioni. Sul punto appare emblematica la volontà di sviluppare una strategia di crescita che coinvolga tutti gli attori. L'importanza di una regolazione normativa che sia condivisa con gli operatori pubblici e privati che investono nel settore è fondamentale per permettere una concreta ed efficace politica di investimenti; ciò in ragione soprattutto dell'obiettivo di diffondere l'approccio europeo a livello globale. Tuttavia non appare semplice conciliare culture differenti, pur non facendo riferimento alla Cina ma guardando agli Stati Uniti, l'approccio appare completamente differente sotto diverse prospettive, e in particolare alla politica libertaria che ha sempre connotato il mercato americano. V. ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., 14 ss.

[177] Nel 2015 la Commissione ha adottato una strategia per la creazione del mercato unico digitale. Nel documento l'Unione Europea è descritta come uno spazio economico con enormi potenzialità di crescita, che tuttavia necessita di un piano coordinato tra gli Stati membri, necessario a investire sul potenziale tecnologico. Viene così presentato il mercato unico come un mercato in cui «è garantita la libera circolazione delle merci, delle persone, dei servizi e dei capitali in cui, quale che sia la loro cittadinanza o nazionalità o il luogo di residenza, persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività online in condizioni di concorrenza leale e potendo contare su un livello elevato di protezione dei consumatori e dei dati personali. La realizzazione del mercato unico digitale consentirà all'Europa di mantenersi tra i leader mondiali dell'economia digitale, sostenendo la crescita delle imprese europee su scala mondiale», Comunicazione della Commissione, *Strategia per il mercato unico digitale*, COM (2015) 192 final. Per una panoramica in merito alle azioni chiave oggetto della strategia europea si rimanda a ELIA, *Il Digital single market, il commercio elettronico e la tutela del consumatore*, in *Tecnologia e Diritto*, II, a cura di ZICCARDI e PERRI, Milano, 2019, 327 ss.

[178] PRETA, ZOBOLI, *op. cit.*, 215 ss; ADINOLFI, *op. cit.*, 16 ss.

[179] Consiglio d'Europa, Convenzione sulla protezione delle persone rispetto al trattamento di dati a carattere personale, 28.1.1981, n. 108.

[180] Lo sviluppo di protesi robotiche, software quali Watson e Deep Blu, robot chirurghi, auto *driverless*, *wearebale things* etc., sono solo alcuni tra gli esempi più noti.

evoluzioni, accompagnate da promesse di efficienza ed economicità, sono infatti emerse istanze sempre più pressanti di regolazione del settore, soprattutto di fronte del timore di possibili esternalità negative. Si comprende così la grande risonanza mediatica che ha accompagnato la risoluzione del 2017 del Parlamento europeo, recante norme civili sulla robotica[181]. Il testo si faceva portavoce delle criticità nascenti dall'uso dell'Intelligenza Artificiale, sottolineando le possibili tensioni con le normative vigenti, e invitando all'emanazione di una disciplina di settore che fosse innanzitutto etica e rispettosa dei principi cardine dell'Unione europea, tra cui va annoverata anche la tutela dei dati personali[182].

Interessante come il documento, dall'obiettivo eminentemente programmatico, faccia riferimento – tra le altre cose – alle tre leggi della robotica di Asimov[183] e alla possibilità di riconoscere una personalità definita elettronica ai robot più autonomi. Detti richiami lasciano intuire un sostrato di diffidenza e preoccupazione circa eventuali futuri distopici, da cui discendono istanze di regolazione etica, prima ancora che giuridica, destinata a guidare gli stessi programmatori nella fase di creazione degli algoritmi[184]. Sul punto, in particolare all'articolo 13 del documento, veniva fatto espresso riferimento a uno sviluppo dell'Intelligenza Artificiale secondo principi di

[181] Risoluzione del Parlamento europeo, Norme di diritto civile sulla robotica (2018/C 252/25).

[182] Sul punto interessanti le considerazioni di Adinolfi, la quale evidenzia come in capo alle Istituzioni europee vi siano due orientamenti contrapposti. Da una parte la Commissione si mostra maggiormente diretta verso l'elaborazione di orientamenti interpretativi di normative già in vigore, limitando l'emanazione di strumenti normativi solo qualora emergano effettive esigenze integrative. A questa sembra contrapporsi il Parlamento europeo che pare invece indirizzato verso un profondo rinnovamento del quadro normativo, anche individuando nuove categorie giuridiche idonee alla disciplina dei diversi profili dell'economia digitale. V. ADINOLFI, *op. cit.*, 21.

[183] Le celebri tre leggi della robotica, formulate da Isacc Asimov nel 1942, furono pubblicate per la prima volta nel racconto Runaround, incluso nel romanzo antologico Io, Robot, lo stesso ove per la prima volta compare la parola "robotica". Le tre leggi erano dirette a regolare il funzionamento del cervello dei robot positronici in modo tale che non potessero recare danno agli esseri umani. Nello specifico si tratta di: 1. Un robot non può recar danno a un essere umano, né permettere che, a causa della propria negligenza, un essere umano patisca danno; 2. Un robot deve sempre obbedire agli ordini degli esseri umani, a meno che contrastino con la Prima Legge; 3. Un robot deve proteggere la propria esistenza, purché questo non contrasti con la Prima o la Seconda Legge. V. ASIMOV, *Circolo vizioso* (or. *Runaround*), in *Io, Robot*, 1973, Oscar Mondadori, Milano, 2016, 31 ss. Più tardi, e precisamente nel romanzo "i Robot e l'Impero" del 1985, lo scrittore aggiungerà un'ulteriore legge, detta Legge Zero, che per importanza dovrebbe essere anteposta alle altre: Un robot non può recare danno all'umanità, né può permettere che, a causa del suo mancato intervento, l'umanità riceva danno.

[184] In merito all'esigenza di una regolazione etica indirizzata primariamente ai programmatori degli algoritmi si rimanda a TURANO, *Robotica e roboetica: questioni e prospettive nazionali ed europee*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 125 ss.

efficienza, non maleficenza, autonomia e giustizia[185]; principi questi mutuati dalla bioetica medica[186], ma universalmente riconosciuti come applicabili anche alle nuove tecnologie[187].

Scontate le considerazioni circa le difficoltà tecniche di effettiva applicazione delle leggi di Asimov[188]. Quanto invece all'attribuibilità ai robot più avanzati di una personalità elettronica, detto riferimento appare sotto diversi aspetti prematuro[189]. Il discorso meriterebbe un approfondimento particolareggiato che non è possibile fare in questa sede[190]. Basti qui solamente accennare come, sebbene parte dei commentatori abbia ritenuto la concessione risolutiva delle possibili incertezze legate al regime di responsabilità civile applicabile, non pare necessario, alla luce dell'attuale progresso tecnologico, spingersi fino al riconoscimento di una personalità giuridica, nemmeno

[185] Nella parte dedicata ai "Principi Etici" l'art. 13 prescrive che: «*il quadro etico di orientamento dovrebbe essere basato sui principi di beneficenza, non maleficenza, autonomia e giustizia, nonché sui principi sanciti all'articolo 2 del trattato sull'Unione europea e nella Carta dei diritti fondamentali dell'Unione europea — quali la dignità umana, l'uguaglianza, la giustizia e l'equità, la non discriminazione, il consenso informato, la vita privata e familiare e la protezione dei dati, così come sugli altri principi e valori alla base del diritto dell'Unione come la non stigmatizzazione, la trasparenza, l'autonomia, la responsabilità individuale e sociale — e sulle pratiche e i codici etici esistenti*». Risoluzione del Parlamento europeo, Norme di diritto civile sulla robotica, cit.

[186] BEAUCHAMP, CHILDRESS, *Principles of Biomedical Ethics*, Oxford, 2012.

[187] Il principio di autonomia si riferisce al diritto dei cittadini di prendere una decisione consapevole e informarta sulla sulle modalità e forme di interazione con le macchine; il principio di beneficienza indica come le macchine debbano agire nell'interesse degli esseri umani; il principio di non maleficenza richiama il brocardo "*primum non nocere*", evidenziando, dunque, la necessità di non creare danni all'uomo; infine, il principio di giustizia esprime la necessità di un'equa distribuzione dei benefici associati allo sviluppo tecnologico.

L'esigenza di una regolazione etica della tecnologia è sentita, oltre che dalle Istituzione e dai cittadini, anche dalla comunità scientifica, così come dimostra il documento emanato dall'*Institute of Electrical and Electronics Engineers*, *Inc*. (IEEE) dal titolo *IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (A/IS)*. Cfr. CINGOLANI, ANDRESCIANI, *Robot, macchine intelligenti e sistemi autonomi: analisi della situazione e prospettive*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 47 ss.

[188] Si tratta pur sempre di letteratura e ancor di più nella prospettiva che essendo formulate in modo generico possono essere soggette a diverse interpretazioni o, per rimanere nell'ambito tecnico, a *bug* che ne compromettano il rispetto. D'altronde anche nelle stesse novelle le leggi non vengono rispettate da alcuni robot, dunque appare necessario ridimensionare la portata del riferimento.

[189] In merito alla riflessione circa l'attributo "intelligente" e alla pretesa autonomia delle macchine si rimanda a quanto esposto *supra*, nella prima parte del presente lavoro.

[190] Per un approfondimento sulle prospettive di attribuzione di una personalità elettronica si rimanda tra gli altri a: RUFFOLO, *La personalità elettronica*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di ID., Milano, 2020, 213 ss.; DRIGO, *op. cit.*, 179 ss.; RIZZUTI, *Il* peculium *del robot. Spunti sul problema della soggettivizzazione dell'intelligenza artificiale*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., 283 ss.; CAROCCIA, *Soggettività giuridica dei robot?*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, 2020, 213 ss.; TADDEI ELMI, *Soggettività e responsabilità dei sistemi di IA*, in *Il diritto di Internet nell'era digitale*, cit., 847 ss.; DE ANNA, *Automi, responsabilità e diritto*, cit., 125 ss.

"parziale"[191]. Come sostenuto da autorevole dottrina, la normativa attualmente in vigore, benché necessiti di un aggiornamento e di una rilettura orientata a estenderne la portata applicativa, potrebbe già rispondere adeguatamente allo scopo[192].

Dalla lettura del documento emerge dunque come l'approccio delle Istituzioni europee alla tecnologia sia guidato da una visione eminentemente antropocentrica, ove particolare rilevanza assume la dimensione etica del fenomeno, ma al contempo attenta al potenziale economico e sociale che le tecniche di AI sono in grado di veicolare.

Alla risoluzione del Parlamento seguì l'emanazione di una molteplicità di atti, tra cui documenti programmatici, carte etiche, comunicazioni, raccomandazioni, pareri etc., ognuno diretto a porre l'attenzione su aspetti particolari della materia, facendo così emergere un quadro regolativo sempre più polverizzato. Tra i più significativi si segnala l'emanazione da parte del Consiglio europeo, nel giugno 2018, di uno schema operativo sull'innovazione digitale nel quale si invita la Commissione a "collaborare con gli Stati membri per definire un piano coordinato in materia di intelligenza artificiale"[193] che sia

[191] Si fa riferimento al pensiero di Teubner. Cfr. TEUBNER, *Soggetti giuridici digitali?: sullo status privatistico degli agenti software autonomi*, a cura di FEMIA, Napoli, 2019; ID., *Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten* (tr. *Digital personhood? the status of autonomous software agents in private law*), in *Ancilla Iuris*, 2018, 36 ss.

[192] Non è possibile in questa sede affrontare le criticità legate al regime di responsabilità civile applicabile in caso di danno derivante da un prodotto avente Intelligenza Artificiale. Ormai molto vasta è la produzione sul tema, per un approfondimento si rimanda, tra i contributi più recenti, a: MARCHINI, *Intelligenza Artificiale e responsabilità civile: dal* "Responsibility Gap" *alla personalità elettronica dei robot*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., 231 ss.; RUFFOLO, *Le responsabilità da* artificial intelligence, *algoritmo e* smart product: *per i fondamenti di un diritto dell'intelligenza artificiale* self-learning, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 93 ss.; AMIDEI, *Intelligenza artificiale e responsabilità da prodotto*, *ivi*, 125 ss.; ULISSI, *I profili di responsabilità della macchina dell'apprendimento nell'interazione con l'utente*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 435 ss.; CAPILLI, *Responsabilità e robot*, in *Nuova giur. civ. comm.*, 2019, 621 ss.; AMIDEI, *Intelligenza artificiale e* "product liability": *sviluppo del diritto dell'Unione europea*, in *Giur. it.*, 2019, 1657 ss.; COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, *ivi*, 1686 ss.; RUFFOLO, *Intelligenza artificiale*, machine learning *e responsabilità da algoritmo*, *ivi*, 1689; COMANDÈ, *Intelligenza artificiale e responsabilità tra* liability *e* accountability, cit., 169 ss.; INFANTINO, *La responsabilità per danni algoritmici: prospettive europeo-continentali*, in *Resp. civ. e prev.*, 2019, 1762 ss.; RUFFOLO, *Per i fondamenti di un diritto della robotica* self-learning: *dalla* machinery *produttiva all'*auto driverless: *verso una "responsabilità da algoritmo"?*, in *Intelligenza artificiale e responsabilità: responsabilità da algoritmo?, A.I. e automobili* self-driving, *automazione produttiva, robotizzazione medico-farmaceutica, A.I. e attività contrattuali, le tendenze e discipline unionali*, Milano, 2017, 1 ss.; PALMERINI, *Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ. e prev.*, 2016, 1816 ss.

[193] Il 10 aprile 2018 un gruppo di 24 Stati membri ha firmato una dichiarazione, poi progressivamente accettata da tutti gli Stati (comprese anche Norvegia e Svizzera), ove veniva sancito l'impegno a realizzare un approccio europeo sull'Intelligenza Artificiale. Si trattata evidentemente di una dichiarazione intesa a esprimere, prevalentemente sul piano politico, la volontà degli Stati di appoggiare la strategia europea, che come visto è basata su di un approccio regolativo unitario alla materia. Si rimanda, per un approfondimento, alla comunicazione consultabile all'indirizzo: *https://ec.europa.eu/commission/presscorner/detail/it/IP_18_2902* (ultimo accesso 26 gennaio 2021).

attento a non scoraggiare il mercato, prevedendo lo stanziamento di somme crescenti e dirette a potenziare gli investimenti.

Quanto alla prospettiva etica, sempre nel 2018[194], veniva istituito un gruppo di esperti (AI HLEG)[195] incaricato di elaborare delle linee guida che fossero espressione dei principi cardine del diritto europeo. L'Organismo emanò un primo *draft*, a cui seguì una consultazione pubblica[196] diretta a valutarne i contenuti; venne così inaugurato un forum dedicato al confronto tra diversi *stakeholder* in merito agli aspetti più delicati del settore[197]. Terminata la fase consultiva, nel 2019 furono pubblicate le linee guida etiche per una AI europea[198].

Il testo si dimostra espressione proprio di quella visione antropocentrica che vede nella presenza di pieno ed effettivo controllo dell'uomo sulla macchina una esigenza irrinunciabile. Difatti un espresso riferimento viene fatto alla possibilità di un intervento umano sulle decisioni algoritmiche, ma ancora di più, si dichiara che il ruolo delle tecnologie deve essere sempre servente l'uomo e mai sostitutivo a esso.

Alla stessa *ratio* rispondono le indicazioni circa la necessità di trasparenza di funzionamento, di inclusività, di responsabilità, di robustezza del sistema, di non discriminazione, oltre che di protezione dei dati personali degli utenti[199]. Il rispetto di

---

[194] Comunicazione della Commissione europea, *Piano coordinato sull'intelligenza artificiale*, COM (2018) 795 final.

[195] L'High-Level Expert Group on Artificial Intelligence è un organismo, nominato dalla Commissione europea, composto da 52 esperti rappresentanti il mondo accademico, la società civile e il settore industriale. L'organismo è stato creato per supportare il lavoro delle Istituzioni mediante raccomandazioni su questioni etiche, legali, sociali ed economiche legate allo sviluppo e alla diffusione dell'Intelligenza Artificiale nella società.

[196] High-Level Expert Group on Artificial Intelligence (AI HLEG), *Draft of the AI Ethics Guidelines*, 2018, consultabile all'indirizzo: *https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai* (ultimo accesso 20 dicembre 2020).

[197] Con oltre 4000 membri l'"*European AI Alliance*", composto da soggetti privati, rappresentanti di categoria, imprese, professionisti, oltre che da organismi pubblici, ad oggi rappresenta un punto di incontro tra operatori che condividono l'impegno per la diffusione globale di una AI affidabile. É ancora possibile iscriversi al forum attraverso la registrazione in un apposito portate. Sul punto si rimanda a quanto specificato all'indirizzo: *https://ec.europa.eu/digital-single-market/en/european-ai-alliance*.

[198] High-Level Expert Group on Artificial Intelligence (AI HLEG), *The Ethics Guidelines for Trustworthy Artificial Intelligence (AI)*, 2019, consultabile all'indirizzo: *https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top* (ultimo accesso 4 settembre 2019).

[199] Nel documento vengono indicati sette requisiti fondamentali che ogni prodotto avente Intelligenza Artificiale deve possedere per poter essere considerato affidabile. Nello specifico: 1. *human agency and oversight*; 2. *technical robustness and safety*; 3. *privacy and data governance*; 4. *transparency*; 5. *diversity, non-discrimination and fairness*; 6. *environmental and societal well-being* e 7. *accountability*. La stessa Commissione ha specificato la portata di questi requisiti. Il principio di "azione e sorveglianza umane" intende evidenziare come i sistemi di AI dovrebbero promuovere lo sviluppo di società eque, sostenendo l'azione umana e i diritti fondamentali e non dovrebbero ridurre, limitare o sviare l'autonomia dell'uomo. Con i termini "robustezza e sicurezza" si rimanda alla necessità di algoritmi che siano sicuri,

questi principi permetterebbe la creazione di prodotti tecnologici affidabili[200], capaci dunque di aumentare la fiducia dei cittadini; elemento questo imprescindibile a una proficua distribuzione della nuova tecnologia sul mercato[201].

A coronamento della strategia di settore, e a conferma che lo studio delle nuove tecnologie non può prescindere da un'attenta analisi anche della materia dei dati[202], in diversi documenti una sempre maggiore considerazione viene data alla necessità di

---

affidabili e sufficientemente robusti da far fronte a errori o incongruenze durante tutte le fasi del ciclo di vita dei sistemi di AI. Con "riservatezza e *governance* dei dati" si intende evidenziare come sia necessario prevedere che i cittadini, nell'uso della tecnologia, mantengano il pieno controllo dei propri dati personali e nel contempo i dati che li riguardano non dovranno essere utilizzati per danneggiarli o discriminarli. Con il principio di "trasparenza" viene contemplato il dovere di garantire la tracciabilità dei sistemi di AI. Quanto alla previsione dei requisiti di "diversità, non discriminazione ed equità" si sottolinea come i sistemi di AI dovrebbero tenere in considerazione l'intera gamma delle capacità, delle competenze e dei bisogni umani ed essere accessibili. Attenzione viene posta anche agli impatti che le tecnologie hanno sulla società, prevedendo il requisito del "benessere sociale e ambientale"; viene, infatti, auspicato che i sistemi di AI siano utilizzati per promuovere i cambiamenti sociali positivi e accrescere la sostenibilità e la responsabilità ecologica. Da ultimo, anche se non per importanza, il requisito di "*accountability*" secondo cui dovrebbero essere previsti meccanismi che garantiscano la responsabilità e *l'accountability* dei sistemi di AI e dei loro risultati. Per un approfondimento si rimanda alla Comunicazione della Commissione, consultabile all'indirizzo: *https://ec.europa.eu/commission/presscorner/detail/it/IP_19_1893* (ultimo accesso 20 dicembre 2020).

[200] Il documento pur essendo diretto agli operatori di settore mostrava una natura troppo generica, legata evidentemente alla stessa formulazione dei principi, che come tali erano di difficile applicazione. Al fine di facilitare l'opera di recepimento venne emanato un nuovo documento che traducesse le linee guida in una *checklist* dinamica e facilmente accessibile. Il documento viene, dunque, diretto agli sviluppatori e distributori di Intelligenza Artificiale che desiderino implementare i requisiti indicati dal gruppo di esperti nei propri prodotti. High-Level Expert Group on Artificial Intelligence (AI HLEG), *The assessment list for trustworthy artificial intelligence (ALTAI) for self assessment*, 2020, consultabile all'indirizzo: *https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment* (ultimo accesso 20 dicembre 2020).

[201] Le incertezze legate, in special modo, al soggetto da ritenere responsabile in caso di danni potrebbero difatti scoraggiarne l'utilizzo anche tra gli utenti finali. Così come è stato per i pagamenti elettronici, dopo una prima fase di diffidenza, la creazione di un clima di fiducia mediante il potenziamento degli strumenti di tutela del cittadino ha permesso la diffusione degli *e-commerce*, settore che oggi assorbe una buona percentuale del totale degli acquisti, con tutto quanto ne consegue anche in relazione alla scomparsa dei negozi fisici. Dunque un ruolo di primaria importanza nella strategia europea per l'Intelligenza Artificiale riveste la fiducia del cittadino, non solo nel funzionamento corretto dei prodotti, ma altresì nella definizione di mezzi che siano idonei a tutelarlo nel caso di danni da esso subiti.

[202] Il riferimento alla privacy e alla gestione dei dati era già presente nella risoluzione del 2017, seppure per brevissimi cenni, al considerando "N" ove si fa riferimento al GDPR. Inoltre, nell'allegato alla risoluzione viene fatto riferimento a un codice etico degli ingegneri contenente una parte dedicata alla vita privata. Si prevede esplicitamente che: «*Il diritto alla privacy deve essere sempre rispettato. Un ingegnere robotico dovrebbe garantire che le informazioni private siano conservate in maniera sicura e utilizzate soltanto in modo appropriato. Inoltre, un ingegnere robotico dovrebbe garantire che le persone non siano identificabili personalmente, salvo in circostanze eccezionali e comunque soltanto con un chiaro e inequivocabile consenso informato. Il consenso informato della persona deve essere richiesto e ottenuto prima di qualsiasi interazione uomo-macchina. Di conseguenza, gli ingegneri robotici sono chiamati a definire e applicare le procedure per garantire il consenso valido, la riservatezza, l'anonimato, il trattamento equo e il giusto processo. I progettisti rispetteranno le eventuali richieste di soppressione dei dati e della loro rimozione da qualsiasi insieme di dati*». Risoluzione del Parlamento europeo, Norme di diritto civile sulla robotica, cit., Allegato: Raccomandazioni concernenti il contenuto della proposta richiesta.

garantire la riservatezza e la *governance* dei dati processati dagli algoritmi. La scelta operata dalle Istituzioni mostra la centralità della materia non solo riguardo agli aspetti strettamente tecnico-funzionali dall'AI, ma ancora di più per la creazione di un clima di fiducia nei cittadini. La stessa Commissione, in un comunicato stampa di accompagnamento alla pubblicazione delle linee guida etiche, sul punto, dopo aver ripreso i principi di *privacy by design* e di *data protection*[203], già previsti nel Regolamento 2016/679 UE, fa un'importante precisazione: sottolinea in modo chiaro come la necessità di elaborare sistemi di AI di elevata qualità non possa prescindere dalla qualità degli stessi dati di addestramento[204]. Detto riferimento è particolarmente significativo: per la prima volta in modo espresso viene dato rilievo allo stretto legame funzionale tre le due materie, così dimostrando che solo una visione coordinata e unitaria del fenomeno tecnologico ne permette la comprensione e dunque una regolazione efficace.

Da ultimo lo stesso Libro Bianco[205], di recente emanazione, nel definire le scelte strategiche dirette al raggiungimento degli obiettivi europei, dedica particolare attenzione al coordinamento e alla regolazione dei *data*, nella consapevolezza che l'AI rappresenti pur sempre un'applicazione, anche se tra le più importanti, dell'economia dei dati. In particolare, dopo aver ribadito l'esigenza di spiegabilità e trasparenza, e di un approccio normativo basato sul rischio[206], la Commissione chiarisce come la *data*

---

[203] La Commissione, in un comunicato stampa di accompagnamento al testo, sottolia che: «In the Commission's human-centric approach as set out in its Communication of 8 April 2019, AI is seen as a tool operating in the service of humanity and the public good, aiming to increase individual and collective human well-being. Since people will only be able to confidently and fully reap the benefits of a technology that they can trust, AI's trustworthiness must be ensured. As a means to creating an environment of trust for the successful development, deployment and use of AI, the Commission encouraged all stakeholders to implement the seven key requirements of the Guidelines. Moreover, the Commission will bring the Union's human-centric approach to the global stage and aims to build an international consensus on AI ethics guidelines», comunicato consultabile all'indirizzo: *https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top* (ultimo accesso 15 dicembre 2020).

[204] Nella consapevolezza che gli *output* della macchina sono fortemente condizionati dai dati in ingresso, emerge l'esigenza di assicurare un processo di selezione degli stessi, così da ridurre il rischio di risultati discriminatori o errati dell'algoritmo quale inevitabile conseguenza di dati di bassa qualità.

[205] Commissione europea, *Libro bianco sull'intelligenza artificiale – un approccio europeo all'eccellenza e alla fiducia*, 2020, COM(2020) 65 final.

[206] Di recente il Parlamento europeo ha emanato un progetto di relazione in merito al regime di responsabilità civile per l'intelligenza artificiale. Ivi vengono proposti regimi di responsabilità distinti a seconda dell'intensità del rischio di danni che gli artefatti aventi Intelligenza Artificiale potrebbero causare. Di poco precedente anche la comunicazione della Commissione ove si fa riferimento alla necessità di un approccio basato sul rischio, così come già evidenziato nello stesso White paper. Tale approccio basato sul rischio è importante per garantire la proporzionalità dell'intervento normativo, ma

literacy[207] debba rivestire un ruolo di primaria importanza tra gli obiettivi dell'Unione. In chiusura del documento viene nuovamente affermato come gli interventi debbano essere mirati ad accrescere la fiducia nei consumatori e a incrementare le competenze utili a potenziare le tecnologie e le infrastrutture digitali.

A corredo dunque dell'azione europea sull'Intelligenza Artificiale, non a caso nel medesimo giorno di emanazione del *White Paper*, è stata pubblicata la comunicazione della Commissione dedicata alla strategia europea per i dati, ove vengono esposte le linee programmatiche in materia di *data governance*, aventi il dichiarato scopo di rendere l'Europa «l'economia agile basata sui dati più attrattiva, sicura e dinamica del mondo»[208].

---

richiede che siano definiti criteri chiari per distinguere tra le diverse applicazioni di AI, in particolare per stabilire se esse siano o meno "ad alto rischio". Per stabilire, in generale, se una determinata applicazione debba essere ritenuta ad alto rischio, occorre valutare gli interessi in gioco e considerare se il settore interessato e l'uso previsto per tale applicazione implichino rischi significativi, in particolare per quanto concerne la protezione della sicurezza, dei diritti dei consumatori e dei diritti fondamentali. Tenuto conto di elementi quali la complessità e l'opacità di molti sistemi di AI, nonché delle conseguenti difficoltà che possono sorgere nel garantire l'effettiva applicazione e il rispetto delle norme pertinenti, vengono ritenute inoltre necessarie prescrizioni per la tenuta di registri relativi alla programmazione dell'algoritmo, ai dati utilizzati per addestrare sistemi di AI ad alto rischio e, in alcuni casi, per la tenuta dei dati stessi. Cfr. Commissione europea, *Libro bianco sull'intelligenza artificiale – un approccio europeo all'eccellenza e alla fiducia*, cit.; Relazione della Commissione al Parlamento europeo, *Relazione sulle implicazioni dell'intelligenza artificiale, dell'internet delle cose e della robotica in materia di sicurezza e responsabilità*, 2020, COM(2020) 64 final; Parlamento europeo, *Progetto di relazione recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*, 2020, (2020/2014/(INL)). Da ultimo, ad aprile del 2021, è stata emanta dalla Commissione una Proposta di Regolamento sull'Intelligenza Artificiale ove le applicazioni di AI vengono appunto distinte in base al rischio creato dal loro utilizzo. V. Comunicazione della Commissione, *Proposta di Regolamento che stabilische regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 2021, COM(2021) 206 final.

[207] La Commissione specifica come il piano d'azione per l'istruzione digitale è diretto a migliorare l'uso dei dati e delle tecnologie basate sull'AI, come l'apprendimento e l'analisi predittiva, così da rendere più istruiti gli utenti in relazione a tutto l'ecosistema digitale. Si ritiene, inoltre, che il piano potrebbe far crescere la consapevolezza in merito all'AI a tutti i livelli di istruzione, al fine di preparare i cittadini a decisioni informate. L'uso dell'AI, come l'uso di qualunque nuova tecnologia, comporta, infatti, sia opportunità che rischi. La previsione di un'opera di alfabetizzazione, pertanto, permetterebbe di rispondere adeguatamente sia ai timori dei cittadini di essere privati dei mezzi per difendere i loro diritti e la loro sicurezza di fronte alle asimmetrie informative del processo decisionale algoritmico, sia delle imprese circa l'incertezza giuridica. V. Commissione europea, *Libro bianco sull'intelligenza artificiale – un approccio europeo all'eccellenza e alla fiducia*, cit. Interessanti le considerazioni circa la necessità di una generale alfabetizzazione digitale in DIMITRAKOPOULOU, voce «Digital literacy», in *Encyclopedia of Big Data*, cit., consultabile all'indirizzo: *https://www.researchgate.net/publication/322466802_Digital_Literacy*

[208] Comunicazione della Commissione, *Una strategia europea per i dati*, 2020, COM(2020) 66 final.

Il documento merita una riflessione. Nonostante in apertura venga ancora una volta sottolineato come sia necessario aumentare la fiducia degli utenti, siano essi cittadini o imprese che operano nel digitale, mediante un contesto giuridico unitario e una politica di tutela dei dati che faccia perno sul GDPR, questo si mostra essere solamente una dichiarazione di principio. Difatti, oltre al generale rimando alla *data protection*, la Commissione dedica poca attenzione alla tutela dei cittadini. Ciò che emerge è piuttosto un approccio prevalentemente diretto a guidare una veloce transizione verso una *data driven economy* in grado di competere con i mercati d'Oltreoceano, mediante la previsione di incentivi[209] per il potenziamento del settore *e-commerce*[210], per lo sviluppo delle infrastrutture, per la creazione di *database* pubblici[211] e per accrescere la *data literacy*[212]. Inoltre, a fronte dell'innegabile processo di digitalizzazione

[209] La stessa Commissione nel 2018, in una comunicazione al Parlamento europeo e al Consiglio, sottolinea il ruolo strategico rivestito dall'Intelligenza Artificiale nel mercato, oltre che nello sviluppo sociale. Viene dunque proposto un piano diretto a potenziare gli investimenti di settore, come già previsto nel piano *New Horizon*, così da aumentare gli investimenti pubblici ma anche privati, portando l'UE ad essere competitiva con USA e la Cina. Ulteriori finanziamenti del settore sono stati programmati per il prossimo decennio per un importo fino a 20 miliardi l'anno per i prossimi dieci anni. Si rimanda sul punto alla dichiarazione presente sul sito istituzionale della Commissione, consultabile all'indirizzo: *https://ec.europa.eu/commission/presscorner/detail/it/IP_19_1893* (ultimo accesso 20 dicembre 2020).
Grande importanza viene inoltre rivolta all'ingresso nel mercato delle PMI e delle *startup* altamente tecnologiche, oltre che nel finanziamento nella ricerca e nell'innovazione tecnologica. Oltre agli investimenti di settore, tuttavia, è necessaria un'ampia accessibilità anche ai set di dati, al fine di poter effettivamente sviluppare o potenziare strumenti di AI. V. Comunicazione della Commissione, *L'intelligenza artificiale per l'Europa*, 2018, COM(2018) 237.

[210] La Comunicazione della Commissione europea n. 175/1997 definisce il commercio elettronico come un fenomeno che consiste «nello svolgimento di attività commerciali per via elettronica. Basato sulla elaborazione e la trasmissione di dati (tra cui testo, suoni e immagini video) per via elettronica, esso comprende attività disparate quali: la commercializzazione di beni o servizi per via elettronica; la distribuzione online di contenuti digitali; l'effettuazione per via elettronica di operazioni quali trasferimenti di fondi, compravendita di azioni, emissione di polizze di carico, vendite all'asta; appalti pubblici per via elettronica, vendita diretta al consumatore e servizi post-vendita». Comunicazione della Commissione europea, *Un'iniziativa europea in materia di commercio elettronico*, 1977, COM (97) 175. Per un approfondimento si rimanda a DELFINI, *Il commercio elettronico: inquadramento generale*, in *Diritto dell'Informatica*, a cura di FINOCCHIARO e DELFINI, Milano, 2014, 351 ss.

[211] Se per il settore pubblico, infatti, è già in opera una progressiva "apertura" dei dati ivi prodotti e raccolti, tra gli operatori privati invece la percentuale di dati liberamente accessibili è ancora molto bassa. Le ragioni che scoraggiano un'apertura dei soggetti privati sono chiare, da una parte vi sono motivi ordine puramente economico – come la perdita di un vantaggio competitivo sui concorrenti – dall'altra manca una base di fiducia tra gli operatori in merito al corretto utilizzo dei dati, secondo le norme contrattuali e la normativa di stampo europeo. Proprio questo aspetto viene considerato quale obiettivo primario nella strategia comunitaria. Difatti la condivisione e l'accessibilità rappresentano un elemento fondamentale per la crescita del settore non solo dei servizi digitali, ma anche della robotica e della ricerca scientifica.

[212] Se certamente appare necessario incentivare percorsi diretti a far acquisire competenze tecniche in materia, così da rendere il mercato europeo più competitivo, sarebbe del pari auspicabile un'opera di sensibilizzazione degli utenti in merito ai principi e agli strumenti giuridici diretti alla tutela dei propri dati personali. Detto aspetto sembra tuttavia rivestire un ruolo marginale negli interventi regolativi della materia. In ambito europeo grande rilevanza è stata data alla previsione del consenso degli interessati, quale base giuridica del trattamento. Nonostante la previsione di un'informativa chiara e intellegibile per

dell'economia, date anche le prospettive di crescita del mercato, la Commissione mette in luce un importante aspetto legato alla natura dei dati processati, che pare quindi opportuno approfondire. Se oggi la maggior parte dei dati prodotti possono essere fatti rientrare nella categoria dei dati personali, con la diffusione dell'internet delle cose e dell'industria 4.0 saranno quelli non personali ad essere i più abbondanti[213]. Pertanto, negli ultimi anni è iniziata a emergere l'esigenza di una regolazione unitaria del settore, in ragione della varietà di attività che ne caratterizzano la catena di valore, dedicata in modo particolare alla circolazione dei dati di natura non personale.

3. La strategia dell'Europa sui dati non personali. Il Regolamento 2018/1807 UE e la sua portata applicativa

A coronamento della strategia di sviluppo di un'economia digitale integrata[214], nel giugno del 2018 il legislatore europeo ha adottato il Regolamento 2018/1807 UE[215], instaurando così la c.d. quinta libertà[216] e creando una sorta di "Schengen" per i dati non

---

gli utenti, recenti studi hanno dimostrato come essa rimanga difficilmente comprensibile; finendo così gli interessati per prestare un consenso senza una reale consapevolezza. Interessanti le considerazioni di D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in *I dati personali nel diritto europeo*, cit., 82, ove si riporta che dalle indagini compiute dalle scienze comportamentali emerge come «il semplice rendere possibile una scelta non basta ad assicurare che l'individuo realmente comprenda la questione, ne sia consapevole o l'abbia considerata, aspetti tutti necessari affinché la scelta sia genuinamente autonoma». Le criticità legate allo strumento del consenso verranno approfondite *infra* nel § 3.1, capitolo 4, a cui si rimanda.

[213] Per quanto riguarda i dati raccolti dal settore pubblico, il loro valore è di recente cresciuto portando una maggiore rilevanza e attenzione circa una corretta regolazione. Di pari passo, è aumentato l'impegno per assicurare la pubblicazione dei dati detenuti dal governo a livello nazionale, regionale e locale. In particolare, si è sviluppato il principio dell'*Open Government*, che intende avvalersi dell'utilizzo di *Open Data*, al fine di gestire in modo dinamico, collaborativo e ottimale il rapporto fra Pubblica Amministrazione e cittadini. Inoltre, il 22 gennaio 2019 i negoziatori del Parlamento europeo, del Consiglio dell'Unione europea e della Commissione hanno raggiunto un punto di accordo sulla revisione della cosiddetta Direttiva PSI (*Public Sector Information*). Una volta adottata, la Direttiva PSI sarà rinominata *Open Data and Public Sector Information Directiv*e e renderà riutilizzabili i dati del settore pubblico e quelli finanziati con fondi pubblici. V. PRETA, ZOBOLI, *op. cit.*, 217.

[214] D'ACQUISTO, PIZZETTI, *op. cit.*, 93 s.; DEL PIZZO, *Trattamento dei dati non personali: punti di contatto tra il Regolamento (UE) 2018/1807 e il GDPR*, in *Rivisita Diritto di Internet*, nota di aggiornamento 18 febbraio 2020, consultabile all'indirizzo: *https://dirittodiinternet.it/trattamento-dei-dati-non-personali-punti-contatto-regolamento-ue-20181807-gdpr/* (ultimo accesso 20 dicembre 2021).

[215] La scelta di emanare un regolamento è evidentemente volta ad assicurare maggiore uniformità di applicazione tra gli ordinamenti; l'utilizzo di uno strumento quale la direttiva, avente lo scopo di armonizzare le normative nazionali, avrebbe difatti comportato un'inevitabile asincronia, derivante dalle diverse applicazioni in ciascuno Stato membro, così come già accaduto per la Direttiva 46/95 CE.

[216] Si fa riferimento alla libera circolazione dei dati, già esplicitamente prevista dal GDPR per i dati di natura personale, ora compiutamente affermata anche per i dati non personali. Si parla di quinta libertà in quanto si accompagna alle libertà "classiche" di circolazione di merci, persone, servizi e capitali all'interno del mercato unico europeo. Cfr. sul punto le interessanti considerazioni di CAVO, *Il*

personali. La previsione di misure che ne permettessero il libero flusso transnazionale nasceva dall'esigenza di contrastare pratiche – sempre più diffuse – dirette a ostacolare la libera circolazione dei dati non personali tra le società operanti nel digitale. Ciò rappresentava evidentemente un ostacolo all'effettivo funzionamento del mercato unico; inoltre, essendo i dati elemento fondamentale per l'implementazione delle nuove tecnologie, la libera circolazione di essi avrebbe permesso di potenziare lo stesso settore industriale europeo volto a una rapida trasformazione verso la c.d. Industria 4.0[217]. Pertanto, nell'intento di eliminare le barriere effettive – o ritenute tali – alla libera circolazione, venne così introdotto dal legislatore un espresso divieto per gli Stati membri di istituire obblighi di localizzazione dei dati, a meno che ciò non sia giustificato da motivi di sicurezza pubblica[218]. Alla stessa *ratio* rispondono le previsioni in tema di portabilità dei dati, dirette a scoraggiare partiche di c.d. *vendor lock-in*[219] mediante l'invito, agli stessi operatori, a definire formati standard di raccolta e conservazione dei dati, oltre che ad emanare strumenti di autoregolamentazione quali codici di condotta[220]. Questi ultimi in particolare si dimostrano strumenti maggiormente flessibili rispetto ad un classico intervento normativo, e dunque tali da poter

---

regolamento europeo sulla libera circolazione dei dati non personali, in *Rivisita Diritto di Internet. Digital Copyright e Data Protection*, 2020, 208 ss.

[217] L'odierna realtà, ormai strettamente legata all'automazione, si trova grandemente interessata dal traffico dei dati e in special modo di quelli non personali. Questi sono difatti utilizzati, secondo lo schema della *data value chain strategy*, come risorsa di crescita e di rendimento, grazie a un potenziamento anche delle capacità di organizzazione del lavoro mediante algoritmi predittivi. Cfr. DEL PIZZO, *ibidem*; CAVO, *op. cit.*, 209. L'Autrice sottolinea come «Dette tecnologie possono alimentarsi, oltre che di dati personali, anche di dati non personali, dando vita ad un vero e proprio flusso di informazioni variegate ed utilizzate (ed anche riutilizzate) per perseguire un miglioramento dell'efficienza della produzione ed un risparmio dei costi: dall'utilizzo di robot nella logistica dei processi manifatturieri che, avvalendosi del *machine learning*, sono in grado di selezionare il migliore *setting* logistico, all'applicazione degli algoritmi di apprendimento automatico nell'utilizzo e nella combinazione dei *Big Data*, i quali a loro volta possono essere associati, quanto alla loro provenienza e raccolta, ai *devices* dell'*Internet of Things*, fino all'archiviazione in *outsourcing* di tali dati ricorrendo al paradigma del *cloud computing*». Per un approfondimento in tema di Industria 4.0 e delle criticità legate al trattamento dei dati nel contesto dell'interazione uomo-macchina si rimanda a GRECO, MANTELERO, *Industria 4.0, robotica e privacy-by-design*, in *Dir. inform*., 2018, 875 ss.

[218] L'art. 4, comma 1°, prescrive che «*Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità. Il primo comma del presente paragrafo fa salvo il paragrafo 3 e gli obblighi di localizzazione dei dati stabiliti sulla base del diritto vigente dell'Unione*», reg. UE n. 1807/2018.

[219] Le pratiche di *vendor lock-in* sono riconducili a una varietà di aspetti, siano essi tecnici, giuridici o contrattuali, che comportano, di fatto, un ostacolo al trasferimento dei propri dati a un diverso fornitore di servizi. Particolarmente chiara la definizione del fenomeno data da Cavo: «il *vendor lock-in*, o blocco da fornitore, è un fenomeno che si origina dalla dipendenza dell'utente da specifici fornitori di beni o servizi, poiché i costi e i rischi di un passaggio ad un diverso fornitore risulterebbero particolarmente gravosi», CAVO, *op. cit.*, 210.

[220] Reg. UE n. 1807/2018, Considerando n. 11.

agevolmente adattarsi all'evoluzione tecnologica e alle esigenze degli utenti e delle imprese[221].

Se il Regolamento ha certamente il pregio di facilitare il traffico commerciale, grazie in particolare alle previsioni sull'interoperabilità, esso dimostra tuttavia avere una portata applicativa limitata, *in primis* a causa della stessa definizione di dato non personale per molti versi insoddisfacente. Precisamente, l'art. 3 prescrive che i "dati non personali" debbano essere individuati in quelli non qualificabili come "personali" ai sensi del Regolamento 2016/679 UE (GDPR)[222]. Dalla stessa formulazione della disposizione emerge una prima criticità. Il rimando alla normativa sulla *data protection*, se trova fondamento nell'esigenza di coordinamento tra i due strumenti, comporta altresì un'inevitabile incertezza. La definizione prevista dal GDPR ha infatti una formulazione aperta da cui discende una portata applicativa molto ampia, soprattutto a fronte delle potenzialità delle tecniche di *data analysis*, tale da rendere del tutto residuale il novero dei dati in essa non ricompresi[223]. A ciò si deve necessariamente aggiungere che, pur ipotizzando un'individuazione precisa della natura dei dati trattati, non è operazione semplice separare, tra tutti quelli raccolti, unicamente quelli qualificati come non personali; spesso anzi nei *dataset* non è possibile scindere le due categorie e procedere a trattamenti regolati da normative distinte.

Al fine dunque di far fronte a eventuali incertezze, il legislatore ha espressamente previsto che nel caso in cui non sia possibile scomporre i *dataset* misti[224], questi dovranno essere regolati unicamente dalla normativa sulla protezione dei dati

[221] I codici di condotta, da elaborarsi in stretta cooperazione tra tutti i portatori di interesse, devono quindi indicare le prassi migliori da adottare al fine di permettere la portabilità dei dati da un fornitore di servizi a un altro, in un formato strutturato e leggibile. Essi devono inoltre indicare le informazioni minime che i contratti aventi ad oggetto servizi di trattamento dei dati dovranno necessariamente contenere, così da fornire agli utenti professionali informazioni sufficientemente dettagliate, chiare e trasparenti in merito alla possibilità e modalità delle operazioni di portabilità dei dati. Cfr. MONTAGNANI, *La libera circolazione al bivio: tra tutela dei dati personali e promozione dell'intelligenza artificiale in Europa*, in *Merc. conc. reg*., 2019, 304.

[222] Si veda, sul punto, la definizione proposta all'art. 3: «*ai fini del presente regolamento per "dati" debbono intendersi i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679*», reg. UE n. 1807/2018.

[223] Per un approfondimento in merito alla portata della definizione di dato personale si rimanda *infra* § 3.2.

[224] Per meglio comprendere la composizione di un *dataset* misto si pensi a un *device* facente parte degli IoT e progettato allo scopo di raccogliere dati di natura sanitaria. Oltre a questi dati, verranno raccolti anche metadati, legati dunque alle modalità di funzionamento del *device* stesso, oltre che dati che in astratto non sono riferibili a una specifica persona fisica. Tuttavia dalla combinazione di dati raccolti sarebbe possibile la deduzione di inferenze quali patologie correlabili a un individuo. Così anche i dati raccolti dagli *wearable device*, aventi natura sia personale che non personali, e che risultano spesso inscindibili.

personali[225]. Appare dunque evidente come una tale indicazione limiti significativamente la portata applicativa del Regolamento 2018/1807 UE, e ciò perché una grande parte dei dati non personali raccolti risulta essere inscindibile da alcune informazioni personali[226].

Infine, un ulteriore limite si riscontra nell'assenza di previsioni chiare in merito ad accordi sulle definizioni, sui formati, le rappresentazioni e le strutture comuni a tutti i livelli e gli elementi dei dati[227]. L'estrema versatilità di provenienza dei *dataset* infatti si presenta come un ostacolo alla interoperabilità tra i diversi operatori. Ne discende che la sola enunciazione di un diritto alla portabilità, così come previso dall'art. 6[228], senza

[225] L'art. 2, comma 2°, espressamente sancisce che: «*Nel caso di un insieme di dati composto sia da dati personali che da dati non personali, il presente regolamento si applica alla parte dell'insieme contenente i dati non personali. Qualora i dati personali e non personali all'interno di un insieme di dati siano indissolubilmente legati, il presente regolamento lascia impregiudicata l'applicazione del regolamento (UE) 2016/679*», reg. UE n. 1807/2018. Sul punto interessanti le indicazioni fornite dalle linee guida. In esse si raccomanda di considerare applicabile il Regolamento in analisi solo alla parte dei dati che risulterebbe avere natura non personale. Nel caso in cui invece le parti di dati personali e non siano "indissolubilmente legate" occorrerebbe ritenere applicabile il GDPR a tutto l'insieme, anche quando i dati personali siano solo una minima parte del totale. Quanto alla nozione di "indissolubilmente legato" le linee guida precisano che "inscindibile" è un *dataset* qualora la separazione dei dati sia tecnicamente impossibile, oppure economicamente svantaggiosa. V. Comunicazione della Commissione, *Guidance on Regulation on a framework for the free flow of non-personal data in the European Union*, 2019, COM (2019) 250 final. Si tratta evidentemente di una condizione mutevole che inevitabilmente comporta per gli operatori la difficoltà di differenziare le due tipologie di analisi. Inoltre, preme sottolineare come la separazione dei dati potrebbe comportare per gli operatori economici costi non indifferenti, si pensi per esempio alla necessita di acquisto e sviluppo di differenti e specifici software gestionali differenti per i dati personali e non. Proprio a fronte di tale possibile difficoltà, anche economica, il legislatore non ha previsto alcun obbligo di separazione dei set di dati controllati o elaborati dalle imprese. Cfr. sul punto CAVO, *op. cit.*, 215; DEL PIZZO, *ibidem*; MONTAGNANI, *op. cit.*, 309.

[226] Cfr. CAVO, *op. cit.*, 214 ss.

[227] Lo stesso Regolamento 1807/2018 UE al Considerando n. 29 sottolinea come «*Mentre i consumatori singoli traggono vantaggi dal vigente diritto dell'Unione, essa non facilita gli utenti che intendono cambiare fornitore di servizi nell'ambito della loro attività imprenditoriale o professionale. Anche l'adozione di requisiti tecnici coerenti in tutta l'Unione, per quanto riguarda l'armonizzazione tecnica, il riconoscimento reciproco o l'armonizzazione volontaria, contribuisce allo sviluppo di un mercato interno competitivo per i servizi di trattamento dati*».

[228] All'art. 6 si prevede che: «*1. La Commissione incoraggia e facilita l'elaborazione di codici di condotta di autoregolamentazione a livello dell'Unione («codici di condotta»), al fine di contribuire a un'economia dei dati competitiva basata sui principi della trasparenza e dell'interoperabilità e nell'ambito della quale si tenga debitamente conto degli standard aperti, contemplando, tra l'altro, gli aspetti seguenti: a) le migliori prassi per agevolare il cambio di fornitore di servizi e la portabilità dei dati in un formato strutturato, di uso comune e leggibile elettronicamente, anche in formati standard aperti ove necessario o richiesto dal fornitore di servizi che riceve i dati; b) gli obblighi d'informazione minimi per garantire che gli utenti professionali ricevano informazioni sufficientemente dettagliate, chiare e trasparenti prima della conclusione di un contratto di trattamento di dati, per quanto riguarda le procedure e i requisiti tecnici, i tempi e gli oneri applicati nel caso in cui un utente professionale intenda cambiare fornitore di servizi o ritrasferire i dati nei propri sistemi informatici; c) gli approcci in materia di sistemi di certificazione che agevolano il confronto di prodotti e servizi di trattamento dei dati per gli utenti professionali, tenendo conto delle norme consolidate a livello nazionale o internazionale che agevolano la comparabilità di tali prodotti e servizi. Tali approcci possono includere, tra l'altro, la gestione della qualità, la gestione della sicurezza delle informazioni, la gestione della continuità*

disposizioni in materia di standardizzazione dei dati rischia di rimanere una dichiarazione di principio di difficile realizzazione pratica[229].

Pur essendo prevista, entro il 2022, una prima valutazione in merito all'effettiva applicabilità delle misure introdotte, con una particolare attenzione alle criticità nascenti dall'evoluzione tecnologica, alla luce delle considerazioni svolte, le previsioni del Regolamento già oggi non appaiono sufficienti a una regolazione efficiente del fenomeno digitale. Sarebbe forse stato opportuno, in particolare per esigenze di certezza del dritto, provvedere a individuare quanto meno alcune categorie di dati qualificabili come non personali, fornendo inoltre una valutazione in merito alla composizione dei *dataset* e agli scopi per cui essi dovranno essere utilizzati, così da poter delineare un perimetro certo di applicabilità della normativa[230]. Ciò avrebbe favorito la fiducia degli utenti professionali, come definiti dal Regolamento, in merito al regime giuridico applicabile ai trattamenti da essi posti in essere. Il rimando a una definizione di per sé mutevole comporta infatti un'inevitabile incertezza, che nell'impresa si trasforma in costi di gestione. Inoltre, sebbene le tecnologie emergenti vengano contemplate nel Considerando n. 1[231], gli interrogativi da esse nascenti non paiono compiutamente affrontati; il documento è difatti unicamente incentrato sulla libertà d'accesso e sul

---

operativa e la gestione ambientale. d) tabelle di marcia in materia di comunicazione, con un approccio multidisciplinare volto a sensibilizzare i portatori di interessi a proposito dei codici di condotta.
2. La Commissione provvede affinché i codici di condotta siano elaborati in stretta cooperazione con tutti i portatori di interesse, tra cui le associazioni di PMI e start-up, gli utenti e i fornitori di servizi cloud […]». Art. 6, reg. UE n. 1807/2018.

[229] Sull'opportunità che siano adottati degli standard aperti, si sono da ultimo espressi anche l'Autorità Garante della Concorrenza e del Mercato, l'Autorità per le Garanzie nelle Comunicazioni e il Garante per la protezione dei dati personali, a conclusione dell'indagine conoscitiva, condotta congiuntamente, per meglio comprendere le implicazioni dello sviluppo digitale e dei Big Data sulla privacy, la regolazione, la tutela del consumatore e l'antitrust. Cfr. MONTAGNANI, *op. cit.*, 310.

[230] Sul punto interessante la proposta avanzata da Montagnani secondo cui sarebbe auspicabile individuare delle categorie di dati non personali, identificabili in ragione dell'utilità che rivestono per lo sviluppo industriale, le quali sarebbero necessariamente soggette al Regolamento 1807/2018 UE. Nel caso in cui si fosse in presenza di *dataset* misti, e indissolubilmente legati, ma ove i dati personali rappresentino una minima parte dell'insieme, l'A. ritiene necessari dei meccanismi che permettano comunque l'uso e la circolazione di questi. Quello che viene proposto sarebbe una sorta di regime intermedio, da valutarsi caso per caso, che permetta l'equiparazione tra pseudonimizzazione e anonimizzazione, a condizione che venga garantita la completa sicurezza delle chiavi di decriptaggio. V. MONTAGNANI, *op. cit.*, 312.

[231] «*L'economia si sta velocemente digitalizzando. Le tecnologie dell'informazione e della comunicazione non costituiscono più un settore a sé stante, bensì sono la base stessa di tutti i sistemi economici e delle società innovativi e moderni. I dati elettronici sono al centro di tali sistemi e, quando sono analizzati o utilizzati in associazione a servizi e prodotti, possono generare un ingente valore. Allo stesso tempo, il rapido sviluppo dell'economia dei dati e di tecnologie emergenti come l'intelligenza artificiale, i prodotti e i servizi relativi all'Internet degli oggetti, i sistemi autonomi e la tecnologia 5G sollevano nuove questioni giuridiche relative all'accesso ai dati e al loro riutilizzo, alla responsabilità, all'etica e alla solidarietà.* […]», reg. UE n. 1807/2018, Considerando n. 1.

riutilizzo dei dati. Del pari alcuno spazio viene dedicato al dibattito in merito alla responsabilità e alle prospettive etiche; argomento sempre più pressante alla luce della veloce evoluzione della società nel suo complesso[232].

Pregevoli invece le raccomandazioni in merito alla formulazione e applicazione di codici di condotta tra gli operatori privati che, indicando formati standard e regole di trasparenza commerciale, accrescano la fiducia nelle transazioni. Pur rimanendo strumenti di *soft law*, la cui adesione è rimessa alla discrezionalità delle singole imprese, se accompagnati da previsioni normative in merito a requisiti minimi, potrebbero rappresentare un punto di partenza per una regolazione maggiormente attenta alle esigenze degli operatori del settore. La previsione di interventi normativi appare necessaria a fronte delle caratteristiche stesse del mercato digitale, così come descritto *supra*[233]. La posizione di assoluta preminenza dei giganti delle comunicazioni potrebbe, infatti, comportare l'applicazione di codici di condotta e standard che, lungi dall'essere una misura diretta a garantire i traffici commerciali e stimolarne così la crescita, potrebbe risolversi in un ulteriore ostacolo all'ingresso di nuove imprese sul mercato. Sul punto, le stesse Istituzioni europee hanno mostrato cogliere dette criticità, prevedendo da una parte finanziamenti a sostegno delle nuove realtà imprenditoriali e dall'altra invitando le società a rendere i dati accessibili gratuitamente[234]. Le difficoltà in merito a una qualificazione dei dati quali beni pubblici[235] liberamente accessibili verrà trattata nel prosieguo, basti qui accennare che sul punto i commentatori non trovano accordo dividendosi tra chi ritiene non vi sia necessità di operare tramite correttivi di mercato, quali per esempio le normative antitrust, altri che ritengono opportuno rimodulare la normativa in tema di *intellectual property*, così da poter efficacemente tutelare anche gli investimenti delle imprese, e infine chi ritiene i dati

[232] RUOTOLO, *op. cit.*, 115 s.; CAVO, *op. cit.*, 211.
[233] Si v. *supra* §1.1 del presente capitolo.
[234] Per i dati pubblici è stata già emanata una Direttiva che potenzia la creazione di *database* e la condivisione dei dati, soprattutto in ambito scientifico. Spostando l'attenzione alla condivisione dei dati nel settore privato (B2B *data sharing*), l'Unione Europea ha adottato un approccio di *soft law*, non proponendo misure vincolanti, ma identificando principi e strumenti che le imprese possono volontariamente decidere di adottare. Dunque, la decisione di condividere o meno i propri dati resta sotto la sfera dell'autonomia privata delle parti. Interessante notare come nel 2017 solo il 2% dei dati degli operatori privati era liberamente accessibile ai terzi. V. PRETA, ZOBOLI, *op. cit.*, 217.
[235] Di questa opinione Ruotolo il quale ritiene necessaria una tale qualifica, permettendo così di poter accedere a una tutela collettiva in caso di esternalità negative. L'Autore inoltre sottolinea come la qualificazione come beni pubblici globali consentirebbe di poter modificare anche le condizioni di accesso ai medesimi; rendendo di fatto i dati liberamente accessibili. V. RUOTOLO, *op. cit.*, 106 s. Sul punto interessanti anche le considerazioni di NICITA, *op. cit.*, 1163 ss.

quali patrimonio collettivo, cui dovrebbero avere accesso tutti gli interessati, siano essi imprese, consumatori o istituzioni pubbliche e di ricerca.

Nonostante le criticità riscontrate, il regolamento 2018/1807 UE, nell'eliminare alcuni ostacoli alla libera circolazione, si dimostra essere un tassello fondamentale nella strategia europea sui dati, il cui avveramento non può tuttavia prescindere da una piena armonizzazione con la normativa in materia di dati personali.

4. La strategia europea sui dati personali: dal pacchetto dati al GDPR

Se sotto il profilo economico, come visto, si sono succedute le iniziative unionali dirette a regolare i dati raccolti e trattati al fine di permettere lo sviluppo della *data economy*, la minaccia alle libertà personali compiuta grazie allo sfruttamento dei Big Data fu percepita quale rischio concreto solo a seguito del celebre scandalo "*Data Gate*" del 2013[236]. Difatti, sebbene fosse già presente una normativa a tutela dei dati personali, la c.d. Direttiva Madre emanata nel '95, lo scandalo ne rivelò l'inefficacia di fronte a comportamenti posti in essere da soggetti pubblici che, nascondendosi dietro lo scudo della sicurezza nazionale, violavano liberamente i diritti fondamentali dei cittadini. Ciò ha indotto il legislatore europeo ad accelerare il programma di riforme già avviato nel

[236] Il caso "*Datagate*" nacque a seguito delle rivelazioni dell'agente della NSA (*National Security Agency*) Edward Snowden, le quali portarono all'attenzione globale il fenomeno della sorveglianza di massa. Snowden rivelò, infatti, l'esistenza, dal 2006 e fino al 2013, del programma statunitense di sorveglianza elettronica di massa denominano PRISM. Il programma aveva, dunque, consentito alle autorità americane di *intelligence* di accedere in modo generalizzato e indiscriminato al contenuto di dati e metadati di traffico elettronico, conservati nel territorio degli Stati Uniti, compresi i dati di cittadini europei, o di persone residenti nel territorio di Stati membri dell'Unione europea. In seguito, grazie anche alla pubblicazione di dossier da parte del quotidiano britannico The Guardian, di quello statunitense The Washington post e di Wikileaks, sono stati portati alla luce anche coinvolgimenti con altre Agenzie quali il *Government Communications Headquarters* (GCHQ), organismo di *intelligence* britannico, nonché la predisposizione in alcuni Stati europei di programmi autonomi di sorveglianza su larga scala. Tra questi il più noto è il programma denominato "Tempora", attraverso cui la GCHQ raccoglie i dati personali dei cittadini direttamente dai cavi sottomarini transatlantici, utilizzati per il trasferimento delle comunicazioni elettroniche. A seguito di queste rivelazioni sorse un intenso dibattito tra gli studiosi, oltre che nell'opinione pubblica, in merito alla legittimità dell'uso di tali mezzi di controllo. Per un approfondimento si rimanda, tra gli altri, a STIANO, *Il diritto alla privacy alla prova della sorveglianza di massa e dell'*intelligence sharing*: la prospettiva della corte europea dei diritti dell'uomo*, in *Riv. dir. internaz*., 2020, 511 ss.; ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal* safe harbour *al* privacy shield*)*, *ivi*, 2016, 690 ss.; PIRODDI, *I trasferimenti di dati personali verso paesi terzi dopo la sentenza* schrems *e nel nuovo regolamento generale sulla protezione dei dati*, in *Dir. inform*., 2015, 827 ss.; COMELLA, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza "*safe harbor*" della corte di giustizia dell'unione europea*, *ivi*, 719 ss.; G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, *ivi*, 697 ss; RODOTÀ, *Il mondo nella rete*, cit., 77 ss.

2012[237] con il c.d. pacchetto dati personali[238]. Prima di allora la materia era caratterizzata da un quadro normativo frammentato[239] e ormai obsoleto, in quanto non più idoneo a far fronte all'avanzamento tecnologico e allo sviluppo globale dei nuovi mercati[240]. La Direttiva madre, era stata infatti elaborata in un contesto sociale nel quale non era possibile nemmeno immaginare la diffusione pervasiva di smartphone o social network, gli stessi motori di ricerca avevano appena iniziato a diffondersi tra i cittadini. A fondamento della disciplina era stato dunque preso in considerazione uno schema caratterizzato da un unico scambio di dati tra l'interessato e il titolare del trattamento. In

[237] Nel 2012 la Commissione formulò una proposta di riforma globale della normativa europea in tema di privacy diretta a rafforzare i diritti degli individui e al contempo in grado di stimolare l'economia digitale, settore che già mostrava enormi potenzialità. Sul punto si rimanda al comunicato stampa pubblicato il 25 gennaio 2012 dalla Commissione europea, *Riforma della protezione dei dati nell'UE – Più tutele per i singoli, meno costi per le imprese*, IP/12/46, consultabile all'indirizzo: *https://ec.europa.eu/commission/presscorner/detail/it/IP_12_46* (ultimo accesso 20 dicembre 2021).

[238] Il c.d. *Data Protection Package* si compone di tre atti normativi emanati congiuntamente dalle Istituzioni europee il 27 aprile 2016: il Regolamento UE 679/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati; la Direttiva 680/2016 UE, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali nonché alla libera circolazione di tali dati; la Direttiva 681/2016 UE sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati più gravi.

[239] FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di ID., 2017, 8 s.; ID., *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, diretto da ID., Torino, 2019, 4 ss.; CEROCCHI, COLAROCCO, *I dati personali e la tutela della persona*, in *Il diritto di Internet nell'era digitale*, cit., 381 s. Sul punto interessanti le considerazioni di Passaglia, il quale sottolinea come la normativa dettata dalla Direttiva, il cui obiettivo era il ravvicinamento delle legislazioni nazionali, si connotava per essere tendenzialmente diretta a tutelare le esigenze del mercato comune. Emergeva, dunque, una sostanziale prevalenza sulla dimensione della tutela del diritto individuale; quest'ultimo non era tutelato in quanto tale, ma in quanto la sua protezione «risultava funzionale al perseguimento di uno scopo di omogeneizzazione tra i diritti nazionali, a sua volta diretto a ridurre i c.d. costi di transazione esistenti». Oltre a questa impostazione, non più coerente con il contesto sociale, l'A. precisa come nella stessa finalità della Direttiva debba rintracciarsi la ragione della sua inadeguatezza. Difatti la normativa interveniva in un contesto caratterizzato da profonde differenze a livello di ordinamenti nazionali, a cui l'opera di ravvicinamento era appunto diretta. Tuttavia, proprio le divergenze legislative hanno comportato una declinazione in parte differente tra i diversi Stati membri, finendo così per non permettere la creazione di un sostrato giuridico comune foriero di un effettivo sviluppo del settore. PASSAGLIA, *Il sistema delle fonti normative in materia di tutela dei dati personali*, in *I dati personali nel diritto europeo*, cit., 92 s.

[240] Cfr. RABAI, *op. cit.*, 409 s.; PASSAGLIA, *op. cit.*, 86 s. Interessante anche le considerazioni di PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, 36 ss. e 142 s. Secondo l'A. il ritardo nella definizione di strumenti normativi adeguati al contesto tecnologico, in cui le operazioni di trattamento dati vengono effettuate, va imputato a una spinta delle Istituzioni diretta a "salvare" l'impianto normativo allora vigente mediante un'interpretazione estensiva delle Direttive, e in particolare della Direttiva 46/95 CE. A ciò inoltre – chiarisce l'Autore – deve aggiungersi, ritenuta per il vero la ragione principale al ritardo nei lavori di *restyling* normativo, il processo di allargamento che vedeva impegnata l'UE ad aiutare i Paesi candidati a conformarsi a un *acquis* comunitario particolarmente complesso; opera che sarebbe risultata ancora più complessa in relazione alla materia dei dati, spesso estranea alle tradizioni di quei Paesi, se essa fosse stata soggetta alle modifiche sostanziali di cui mostrava avere bisogno.

una tale linearità di rapporti la previsione dell'istituto del consenso si dimostrava una efficace base di legittimità del trattamento[241]. Tuttavia oggi, a fronte della digitalizzazione che ha reso i cittadini sempre connessi, si assiste alla diffusione di un modello di rapporti profondamente differente rispetto al passato; la raccolta e il successivo trattamento sono infatti guidati da una prospettiva di condivisione e cogestione dei dati (e delle informazioni), destinati a una circolazione globale. Il profondo mutamento dell'intera società ha quindi fatto emergere la necessità di un rinnovamento nella regolazione della materia, che troverà compiuta realizzazione con l'emanazione del Regolamento 2016/679 UE (GDPR) .

I prodromi del nuovo assetto normativo europeo tuttavia risalgono al 2009 e possono probabilmente individuarsi nelle comunicazioni relative al programma di Stoccolma[242]. Nel documento, denominato "Un'Europa aperta e sicura al servizio e a tutela dei cittadini"[243] veniva infatti posta l'attenzione sulla necessità di introdurre strumenti giuridici diretti a regolare efficacemente la materia della protezione dati. La proposta di un quadro normativo completo fu accolta con favore dalle Istituzioni, le quali posero l'accento sulla necessità di un'applicazione sistematica del diritto fondamentale alla protezione dei dati personali nel contesto di tutte le politiche europee[244]. La Commissione pubblicò così un importante documento in cui, per la prima volta, venivano dichiarate le linee d'azione su cui avrebbe dovuto fondarsi il nuovo approccio unitario alla materia[245]. Fu dunque sulla scorta di queste dichiarazioni programmatiche che nel 2012 si diede compiutamente inizio a una stagione di riforme. Si assisté così all'emanazione di una serie di atti diretti a regolare in modo specifico differenti settori

[241] Il legislatore italiano, nella legge di recepimento e nel successivo codice della privacy, ha ritenuto il consenso quale requisito primario di legittimità, seppure nella Direttiva europea, e da ultimo anche nel GDPR, esso abbia il medesimo peso delle altre condizioni previste.

[242] Cfr. la Comunicazione della Commissione, *Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini*, 2009, COM(2009) 262. La comunicazione venne poi ripresa nel Piano d'azione per l'attuazione del programma di Stoccolma nel 2010. Comunicazione della Commissione al Parlamento europeo, *Creare uno spazio di libertà, sicurezza e giustizia per i cittadini europei. Piano d'azione per l'attuazione del programma di Stoccolma*, 2010, COM(2010) 171.

[243] Consiglio europeo, *Programma di Stoccolma – Un'Europa aperta e sicura al servizio e a tutela dei cittadini*, 2010, (2010/C 115/01).

[244] ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina*, cit., 3.

[245] La Commissione ha sottolineato come «la rapidità dell'evoluzione tecnologica e la globalizzazione hanno mutato profondamente il mondo in cui viviamo, ponendo nuove sfide alla protezione dei dati personali […] per far fronte a queste sfide l'UE deve mettere a punto un approccio generale e coerente onde garantire che il diritto fondamentale di ciascuno alla protezione dei dati personali [sia] pienamente rispetto all'interno e all'esterno dell'UE». Comunicazione della Commissione, *Un approccio globale alla protezione dei dati personali nell'Unione Europea*, 2010, COM(2010) 609.

di competenza europea, andando a delineare un quadro normativo particolarmente articolato e complesso.

Tra i primi interventi priorità venne data ai settori maggiormente coinvolti dall'evoluzione tecnologica. Fu così approvata la Direttiva sugli appalti pubblici[246] e la Direttiva sul trattamento dei dati personali all'interno delle comunicazioni elettroniche[247], di cui nel 2017 è stata presentata una proposta di Regolamento[248] che tuttavia ad oggi non è stato ancora promulgato, a causa della difficoltà di accordo tra gli Stati in materia di protezione delle comunicazioni elettroniche e delle apparecchiature terminali degli utenti. A questi possiamo aggiungere il Regolamento in materia di identificazione elettronica, di particolare rilevanza in quanto diretto a regolare il settore dell'*e-commerce*[249], e la Direttiva 1148/2016 UE[250] sulla sicurezza delle reti di comunicazione.

Questi primi interventi legislativi furono di fatto rivolti prevalentemente a una regolazione che permettesse di sfruttare l'enorme potenziale economico veicolato dal digitale, prevedendo alcuni interventi anche in materia di sicurezza di utenti e reti di comunicazioni aventi l'obiettivo di aumentare la fiducia di operatori e cittadini; quest'ultimo elemento imprescindibile a un corretto sviluppo dei mercati è, come visto, centrale nella strategia europea.

Da ultimo, al fine di tracciare un quadro regolativo unitario che potesse al contempo garantire anche una tutela dei diritti fondamentali, furono emanati due importanti normative a tutela dei dati delle persone fisiche: la Direttiva 680/2016 UE[251], relativa

[246] Direttiva 24/2014 UE, sugli appalti pubblici che abroga la precedente Direttiva 18/2004 CE.
[247] Direttiva 58/2002 CE, relativa al trattamento di dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.
[248] L'obiettivo della Commissione con l'emanazione del Regolamento in materia di e-privacy è dunque quello di estendere, in quanto *lex specialis*, l'ambito di applicazione della disciplina sulla tutela dei dati personali anche ai trattamenti posti in essere nell'ambito delle comunicazioni elettroniche. Proposta di regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE, consultabile all'indirizzo: *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017PC0010&from=IT*. Cfr. sul punto ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina*, *ibidem*.
[249] Il riferimento è al Regolamento UE n. 910/2014, che abroga la Direttiva 93/1999 CE. Per un approfondimento si rimanda a FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 9.
[250] Direttiva 1148/2016 UE, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
[251] Si fa riferimento alla Direttiva 680/2016 UE, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di

alla protezione delle persone con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati; il Regolamento 679/2016/679 UE (GDPR), relativo alla protezione delle persone con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Il quadro europeo in materia di dati personali così delineato mostra avere una duplice anima. Gli atti normativi promulgati, infatti, se da un lato sono diretti a potenziare il mercato unico digitale, dall'altro rispondono all'esigenza di tutelare i diritti fondamentali dei cittadini, nel difficile compito di contemperare diritti e interessi tra loro potenzialmente in conflitto.

La tutela della privacy e il diritto alla protezione dei dati personali sono, infatti, diritti che hanno per propria natura una portata applicativa molto ampia, tale che se non contemperata comporterebbe la compromissione di altri diritti ugualmente meritevoli di tutela[252]. Pur rientrando tra il novero dei diritti fondamentali dell'uomo, essi dunque richiedono un'attenta opera di ponderazione da parte del legislatore, soprattutto in un settore economico in forte crescita quale è quello digitale[253].

---

tali dati, che abroga la decisione quadro del Consiglio 2008/977/GAI, diretta a regolare i diritti degli interessanti nel corso dei procedimenti di accertamento penale posti in essere dalle autorità degli Stati membri.

[252] Sul punto ha avuto modo di esprimersi anche la Corte di Cassazione, nel 2015, nella vigenza del d. lgs. n. 196/2003 (c.d. Codice della privacy), specificando come il diritto alla protezione dei dati personali, che si manifesta quale pretesa a esigere una corretta gestione dei propri dati personali, «*pur rientrando nei diritti fondamentali di cui all'art. 2 cost., non è un totem al quale possano sacrificarsi altri diritti altrettanto rilevanti sul piano costituzionale e, conseguentemente, la disciplina in materia va coordinata e bilanciata da un lato con le norme che tutelano altri e prevalenti diritti (tra questi, l'interesse pubblico alla celerità, trasparenza ed efficacia dell'attività amministrativa); e dall'altro, con le norme civilistiche in tema di negozi giuridici*». Cass., 20.5.2015, n. 10280, in *Mass. Giust. civ*., 2015. Nel 2017, le Sezioni Unite, discostandosi parzialmente dall'orientamento sopra citato, sanciscono l'assoluta prevalenza del diritto alla riservatezza per quei dati c.d. super sensibili, cioè idonei a rivelare informazioni sullo stato di salute dell'interessato, i quali devono necessariamente essere criptati anche qualora siano trattati da soggetti pubblici. La Corte specifica che «*il sistema legislativo di protezione dei dati sensibili è ispirato al principio della massima limitazione possibile della circolazione e diffusione degli stessi senza il consenso dell'interessato e dunque La tendenziale assolutezza del principio e la rigorosa definizione del perimetro autorizzatorio al trattamento di tali dati da parte dei soggetti pubblici induce ad escludere che residui in capo ai titolari, individuati D.Lgs. n. 196 del 2003, ex art. 18 e ss. alcun potere discrezionale in ordine all'adempimento delle prescrizioni normative relative al trattamento. L'art. 22 ne impone la continenza e la criptatura o cifratura, senza alcun margine di apprezzamento relativo alla efficacia dello strumento in ordine al concreto uso del dato*», Cass., sez. un., 27.12.2017, n. 30981, in *Foro it*., 2018, I, 2147 ss.

[253] FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 20 s.; ID., *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, cit., 25 s.; SANTORO, *I principi fondanti del GDPR*, in *Tecnologia e diritto*, II, cit., 49 ss.

La stessa Corte di Giustizia si è espressa in tal senso in alcune pronunce tra cui Corte giust. UE, 24.11.2011, cause riunite C-468/10 e C-469/10, in *Foro it.*, 2012, IV, 1, con nota di PALMIERI, *Tutela dei dati personali e interesse alla circolazione delle informazioni: ancora un monito della Corte di giustizia*

Dette considerazioni emergono fin dai primi considerando delle normative richiamate, ove il bilanciamento di diritti e interessi contrapposti rimane elemento fondativo dell'intera disciplina[254]. Esplicito riferimento viene fatto alla generale, e incomprimibile, necessità di contemperare l'autonomia individuale con l'esigenza di non limitare eccessivamente la libertà di iniziativa economica[255]. Sul punto è interessante notare come la sostituzione della Direttiva con il più uniforme GDPR non abbia comportato una modifica del generale approccio di favore del legislatore europeo rispetto al trattamento e alla circolazione dei dati personali, ribadito dall'art. 1, comma 3°, dove si legge che: «*la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*»[256]. Con il GDPR si propone, dunque, l'introduzione di una circolazione dei dati controllata, "sicura" in quanto rispettosa delle disposizioni ivi previste, in un'ottica di contemperamento tra diritti contrapposti[257], e permettendo così la piena attuazione del *Digital Single Market* e la conseguente crescita dell'intera economia europea.

---

sul rispetto degli equilibri faticosamente intrecciati. Sebbene da ultimo con il caso Google Spain la Corte di Giustizia sembra avere in parte mutato il proprio orientamento, mostrando una maggiore propensione a ritenere il diritto alla protezione dei dati personali prevalere su altri diritti, anch'essi meritevoli di tutela; evidentemente anch'essa influenzata dalle rivelazioni circa il programma di controllo massivo posto in essere dal governo americano. Corte giust. UE, grande camera, 13.5.2014, causa C-131/12, *ivi*, 2014, IV, 295 ss., con note di PALMIERI e PARDOLESI, *Diritto all'oblio: il futuro dietro le spalle*.

[254] Questa duplice finalità si osserva, oltre che nello stesso titolo del Regolamento, fin dall'art. 1 del testo, ove si fa espresso riferimento al raggiungimento di due obiettivi: la protezione delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati. Inoltre, al considerando n. 4, viene chiarito come «*Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità* […]. *Il Regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica*». Reg. UE n. 679/2016.

[255] D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, cit., 65 s.; D'ACQUISTO, PIZZETTI, *op. cit.*, 89 ss.

[256] DE GREGORIO, TORINO, *op. cit.*, 450 ss.

[257] FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, cit., 2 ss.; D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, cit., 66 s.

5. Considerazioni conclusive

Le considerazioni in merito alla strategia europea sul digitale e sull'Intelligenza Artificiale devono partire dalla concezione dei dati quale *asset* fondamentale per le imprese e, dunque, quale bene avente un valore patrimoniale e oggetto di scambio nel mercato digitale. La consapevolezza del valore dei dati, oltre che del funzionamento del mercato digitale, è difatti elemento necessario per comprendere la strategia del legislatore europeo nel disciplinare la materia.

Come visto, la necessità di non scoraggiare la crescita economica, veicolata dallo sfruttamento dei Big Data, e il conseguente potenziamento del mercato unico digitale, rappresenta uno tra gli obiettivi – se non il più rilevante – perseguiti delle Istituzioni europee. In questa prospettiva particolare rilevanza assumono allora le applicazioni di Intelligenza Artificiale. Queste, come già rilevato nel capitolo iniziale del presente lavoro, sono necessariamente intrecciate alla materia dei dati. Proprio l'avvento dei Big Data ha permesso alle applicazioni di Intelligenza Artificiale di trovare una nuova linfa e raggiungere risultati impensabili fino ad oggi. Essendo dunque le AI una tra le tecnologie – seppur la più rilevante – del mercato digitale, ne discende come sia necessaria una regolazione coordinata tra i due settori; una regolazione troppo stringente sui dati porterebbe evidentemente al detrimento dell'evoluzione tecnologica e degli investimenti nel settore.

Alla luce delle prassi commerciali e degli ingenti interessi economici che gravitano intorno al trattamento dei dati, ben si comprende la ragione per cui la strategia europea sia diretta a regolare quanto più organicamente la materia. Tra gli obiettivi del legislatore europeo primeggia, infatti, l'implementazione del mercato unico digitale, elemento necessario a rendere, come è stato dichiarato, l'Europa la prima economia agile mondiale[258].

In questa prospettiva di primaria importanza si dimostra la libera circolazione dei dati, requisito imprescindibile per il corretto funzionamento del mercato. Possiamo difatti trovare riferimento al divieto di ostacolare la libera circolazione dei dati nella normativa GDPR, ove la libera circolazione viene dichiarata essere uno degli obiettivi dell'UE e a cui la stessa *data protection* deve essere contemperata. Espressione diretta

[258] La valenza patrimoniale dei dati e il funzionamento del mercato digitale sono trattati *supra* al § 1.

ne è pure il recente Regolamento 1807/2018 UE sulla libera circolazione dei dati non personali; il crescente peso che i dati aventi detta natura stanno acquistando ha difatti spinto il legislatore a emanare una disciplina direttamente applicabile in tutti gli Stati membri.

L'obiettivo primario del Regolamento da ultimo citato è quello di eliminare le barriere al perfezionamento del mercato unico grazie sia alla previsione del divieto di instaurare obblighi di localizzazione dei dati, sia all'invito agli utenti professionali a incrementare l'interoperabilità dei *dataset*. Il Regolamento, sebbene rappresenti un ulteriore e importante tassello nella creazione di un mercato effettivamente libero, risulta tuttavia avere una applicabilità limitata. Lo stesso rimando alla nozione di dato personale elaborata dal GDPR, come visto, ne riduce grandemente la portata applicativa. A ciò deve aggiungersi la considerazione per cui – ad oggi – i maggiori titolari di *dataset* di natura non personale rimangono soggetti privati. L'attuale prassi di mercato ha tuttavia evidenziato come questi ultimi, potendo sfruttare un vantaggio competitivo, non paiono avere particolare interesse a rendere liberamente accessibili e ad agevolare la circolazione dei dati in proprio possesso. Nella prospettiva di incoraggiare una maggiore condivisione dei dati, e incentivarne dunque la circolazione nel mercato, il legislatore ha previsto nel testo del Regolamento in parola alcuni rimandi a codici di condotta e a standard condivisi tra gli operatori. Sebbene tali previsioni rappresentino certamente un buon punto di partenza, a questi tuttavia sarebbe auspicabile associare anche l'emanazione di strumenti che possano trovare un'applicazione più estesa e unitaria nel settore. A fronte anche della complessità del mercato digitale, e alla presenza di situazioni di possibile fallimento di mercato, un intervento normativo che si limiti ad un invito all'emanazione di codici di condotta o di standard tecnici rischia di rimanere una mera dichiarazione di principio in mancanza di un cogente intervento normativo[259].

Alla prospettiva economica sopra richiamata si sono accompagnate, in maniera preponderante dopo il celebre scandalo "*Data Gate*", esigenze di tutela dei dritti dei cittadini. La capacità delle tecnologie di raccogliere e processare dati ha mostrato l'estrema facilità con cui essi possono essere utilizzati senza il consenso degli

[259] Si rimanda all'analisi del Regolamento 1807/2018 UE compiuta *infra* nel capitolo 3.

interessati, nonostante la vigenza della Direttiva 46/95 CE e, ancora prima, della Convenzione n. 108/1981.

Il veloce progresso tecnologico ha reso dunque necessario un aggiornamento delle normative, essendo divenute ormai obsolete e non più adeguate a regolare il fenomeno. A partire dal 2012 venne così inaugurata una stagione di grandi riforme che, per quanto riguarda i dati personali, ha trovato un coronamento nel Regolamento 679/2016 UE (GDPR). Il testo, compiuta espressione del diritto fondamentale alla protezione dei dati personali così come sancito dall'art. 8 della Carta europea dei diritti dell'uomo, introduce e sviluppa alcuni principi fondamentali. Tuttavia è necessario chiarire fin da subito come il Regolamento in parola si inserisca all'interno di una strategia di controllo e di regolazione della materia complessa e articolata, ed è proprio alla luce di questa che esso deve essere letto. Pertanto, alla tutela dei diritti degli interessati si accompagna un'opera di ponderazione necessaria a non comprimere il diritto, di pari rango, alla libera iniziativa economica. Il riferimento a un bilanciamento tra diritti e interessi contrapposti pervade l'intero testo, e ciò è facilmente spiegabile se si tiene a mente, come poc'anzi ricordato, che i dati – anche personali – rivestono un ruolo fondamentale nell'economia mondiale. Ecco quindi che si comprende il riferimento, fin dall'articolo 1, alla tutela delle persone ma anche della libera circolazione dei dati personali e, ancora, alla previsione per cui la libera circolazione dei dati personali non può essere limitata né vietata per motivi attinenti alla protezione delle persone con riguardo al trattamento dei propri dati[260].

Compresa l'anima duale del Regolamento, che in parte è espressione della posizione della stessa Unione europea sulle tecnologie emergenti, l'analisi delle prescrizioni ivi contenute si dimostra di fondamentale importanza. Da quanto rilevato circa gli atti normativi regolanti il settore digitale nel suo complesso, oltre che dalle posizioni espresse in merito alla strategia di sviluppo e potenziamento del settore, l'approccio europeo nei confronti dell'Intelligenza Artificiale e della materia dei dati mostra avere una natura ambivalente, caratterizzata da una tensione tra diverse e talora contrapposte finalità[261]. Si è visto, difatti, come nell'attuale contesto sociale entrino in gioco interessi economici, legati al funzionamento del mercato interno e alla competitività dell'industria a livello globale, a cui però si accompagnano preoccupazioni in ordine sia

[260] Art. 1, reg. UE n. 679/2016.
[261] L'argomento viene approfondito *supra* al § 4 del presente capitolo.

alla tutela delle attività commerciali, sia al rispetto dei valori dell'Unione, soprattutto alla luce della protezione dei diritti fondamentali dei cittadini[262].

Con l'avvento dei Big Data e degli algoritmi di *data mining* appare allora necessario verificare l'efficacia degli strumenti previsti a tutela degli individui nella fase, attualmente più critica, dell'analisi e dello studio dei dati raccolti. Le moderne tecnologie, come visto, possono infatti generare elementi di conoscenza nuovi, potenzialmente anche informazioni appartenenti alla categoria dei dati personali, da *dataset* composti da dati non personali. Ne discendono possibili esternalità negative per gli interessati, che si dubita possano essere efficacemente tutelati dall'attuale assetto della normativa sulla *data protection*[263].

[262] ADINOLFI, *op. cit.*, 14 s.
[263] D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, cit., 66 s.; D'ACQUISTO, PIZZETTI, *op. cit.*, 94.

CAPITOLO 3

Il Regolamento generale sulla protezione dei dati personali alla prova dell'Intelligenza Artificiale: prime criticità applicative

SOMMARIO: 1. Non solo un problema di privacy. – 2. Il "dato personale" all'interno della normativa europea: una nozione aperta. – 3. Il principio di limitazione delle finalità nei trattamenti operati mediante tecnologie *data driven*. – 4. I principi di minimizzazione e limitazione della conservazione. – 5. Il principio di integrità e riservatezza alla prova dei fenomeni di *data breach*. – 5.1. Anonimizzazione e Pseudonimizzazione. – 6. Il principio di esattezza. – 7. Possibili profili di una tutela collettiva. – 8. Considerazioni conclusive.

1. Non solo un problema di privacy

L'istituto della privacy ha subito un'evoluzione di pari passo con il progresso tecnologico. L'avvento sul mercato di algoritmi in grado di raccogliere e analizzare i dati degli utenti ha fatto emergere serie preoccupazioni non solo in merito al profilo della riservatezza[264], ma più genericamente alla dimensione del controllo stesso che

[264] Il fenomeno non è così recente come si è portati a credere, già nel 1973 Stefano Rodotà, a fronte delle preoccupazioni nascenti oltre oceano, derivanti dalla diffusione nell'uso degli elaboratori elettronici, metteva in luce come le criticità legate al trattamento dei dati personali mediante strumenti elettronici, lungi dall'essere un problema relegato agli Stati Uniti, richiedeva una riflessione, urgente in alcuni settori, anche nel nostro Paese. La collezione e la vendita di *dataset* contenenti informazioni personali degli utenti non è un fenomeno nuovo; Rodotà ricorda, infatti, l'esistenza di società che già negli anni '70 avevano come scopo quello di raccogliere informazioni personali, sebbene tali raccolte fossero necessariamente limitate ognuna a un ambito specifico di indagine. Lo stesso Autore ci ricorda come nel periodo di creazione dell'anagrafe tributaria venne offerto, da una società privata, al Ministero delle finanze uno schedario contenente i dati di circa dodici milioni di contribuenti per il prezzo di un miliardo e seicento milioni di lire; offerta che venne prontamente rifiutata. V. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit., 20 s. Interessanti anche le considerazioni di Pizzetti in merito allo sviluppo della trattazione automatica di dati fin dalla prima metà del novecento. L'Autore fa riferimento alle prime schede perforate prodotte dalla società IBM e dirette a raccogliere e organizzare sistematicamente dati e informazioni, permettendone così una più rapida consultazione. Si ritiene che detta possibilità di raccolta e di trattamento automatizzato abbia svolto un ruolo di rilievo a favore degli apparati di controllo nazisti.

l'interessato esercita sui propri dati personali[265]. L'uso che di questi viene fatto potrebbe difatti incidere sul piano economico, sulla libertà di autodeterminazione, sulla libertà di pensiero e finanche sulla libertà personale dell'individuo. La tecnologia, come visto, si nutre di dati, cerca *pattern*, crea dei *cluster* di utenti, genera previsioni e restituisce degli *output*. Gioco forza, un uso scorretto dei dati ben si comprende quali gravi pregiudizi potrebbe comportare per le persone coinvolte. Il panorama delle applicazioni che si servono dei Big Data è infatti già vastissimo; solo per dare un'idea, algoritmi di previsione sono già in uso nel settore assicurativo, bancario, sanitario, commerciale, scolastico e anche giuridico[266].

Non è possibile in questa sede approfondire il tema, si rimanda a PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 54.

[265] Un esempio chiarirà meglio la prospettiva in analisi. Agli inizi degli anni 2000 la nota catena di negozi Target mise a punto un algoritmo di previsione diretto a individuare le proprie clienti incinta, in particolare quelle che si trovavano nel terzo trimestre. L'obiettivo era quello di aumentare le vendite di prodotti neonatali fornendo una pubblicità mirata alle donne in quella specifica fase della gravidanza. Dagli studi comportamentali è emerso come le abitudini di acquisto dei consumatori sono difficilmente modificabili, tuttavia esistono diverse "finestre" in cui è più facile per le aziende spingere le persone a cambiare abitudini. Si tratta di momenti legati a un cambiamento personale: un divorzio, un trasferimento in una nuova città, un matrimonio, la nascita di un figlio, etc. In quest'ultimo caso è emerso che i primi acquisti di prodotti neonatali vengono effettuati dalle gestanti proprio nel terzo trimestre. Il problema era, dunque, individuare quali clienti si trovassero in tale condizione. Dalla combinazione di diversi dati è emerso come le donne che entrano nel terzo trimestre iniziano ad acquistare particolari prodotti, quali per esempio creme corpo senza profumazione e disinfettanti. Grazie alla correlazione di dati, senza dunque avere direttamente accesso alle informazioni sanitarie delle clienti, l'algoritmo creato da Target individuò 25 prodotti il cui acquisto funge da indicatore di una possibile gravidanza. L'algoritmo era anche in grado di stimare la data esatta del parto con una percentuale di errore molto bassa. Individuate le clienti, Target mandava delle pubblicità mirate con una selezione di prodotti per neonati messe appositamente in offerta. Questa modalità di raccolta e di utilizzo dei dati degli utenti è divenuta nota però solo nel 2012, grazie a un articolo del New York Times Magazine che creò grande scalpore nell'opinione pubblica, portando l'attenzione sull'uso inconsapevole dei dati degli utenti. A Minneapolis, una ragazza minorenne ricevette da Target una di queste pubblicità mirate. La comunicazione pubblicitaria, inviata alla ragazza per mail, venne però letta dal padre. Quest'ultimo, evidentemente ignaro delle abitudini della figlia, protestò animatamente con il direttore marketing, perché, a suo parere, la pubblicità indirizzata alla figlia minorenne, ancora studentessa, appariva come un incentivo a rimanere incinta. Il responsabile del settore marketing si scusò con il cliente e dopo qualche giorno lo contattò nuovamente per scusarsi a nome dell'azienda; in quell'occasione curiosamente fu il padre della ragazza a scusarsi, poiché dopo aver parlato con la figlia scoprì come questa fosse effettivamente incinta.
Questo episodio creò un grande clamore mediatico, soprattutto in relazione alla tutela della privacy dei consumatori ignari; tuttavia, ciò che emerge da questo episodio e che obbliga a una riflessione sono le stesse modalità di targettizzazione, e l'utilizzo delle informazioni così inferite per scopi commerciali.
La storia della pubblicità di Target è discussa in dettaglio nell'articolo di DUHIGG, *How Companies Learn Your Secrets*, *The New York Times Magazine*, 16 febbraio 2012. Consultabile all'indirizzo: *https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html* (ultimo accesso m13 gennaio 2021). Sul punto si rimanda anche a SARRA, Business Intelligence *ed esigenze di tutela: criticità del c.d.* Data Mining, in *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, a cura di MORO e SARRA, Milano, 2019, 51 ss.

[266] Un'interessante disamina in merito alle criticità legate all'uso incontrollato di algoritmi nei più svariati ambiti viene affrontata nell'interessante libro di O'NEIL, *Armi di distruzione matematica*, Milano, 2017, a cui si rimanda per un approfondimento.

Per meglio comprendere allora cosa debba intendersi per *data protection* e come l'istituto si differenzi dalla concezione classica di "privacy" è opportuno, seppur brevemente, ripercorrerne le evoluzioni.

Il diritto alla protezione dei dati affonda le radici nel diritto alla riservatezza. Le origini del concetto di privacy, come noi lo intendiamo, vanno fatte risalire alla fine del XIX secolo[267], più precisamente al 1890, anno in cui venne pubblicato sulla rivista Harvard Law Review il celebre saggio di Warren e Brandeis dal titolo "The right to privacy"[268]. L'occasione di riflessione sul tema fu data proprio da una vicenda personale accaduta ad uno dei due autori, che vide diffondere pettegolezzi relativi alla propria famiglia sulle pagine dei giornali scandalistici del tempo[269]. L'esigenza di una maggior tutela della riservatezza, quale protezione della sfera privata e della stessa libertà di agire degli individui, senza timore che le proprie azioni possano divenire di dominio pubblico, ha infatti iniziato a trovare spazio proprio con la diffusione delle

[267] Le origini dell'idea di una sfera intangibile della persona, legata alla vita privata, sono in realtà risalenti nel tempo. Aristotele stesso distingueva tra *polij*, cioè la sfera politica/pubblica e *oicoj*, la sfera privata. L'idea viene poi efficacemente riassunta dalle parole di Lord Chatham, nel 1766, il quale, di fronte al Parlamento, dichiarò: «il più povero degli uomini può nella sua casetta lanciare una sfida opponendosi a tutte le forse della corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la tempesta può entrare e la pioggia può entrare, ma il Re d'Inghilterra non può entrare; tutte le sue forze non osano attraversare la soglia di tale casetta in rovina». V. FARALLI, *Il diritto alla privacy profili storico-filosofici*, in *Persona e mercato dei dati, Riflessioni sul GDPR*, cit., 3.

[268] WARREN, BRANDEIS, *The right to privacy* (1890) 5 *Harvard Law Review* 193 ss. La formulazione dell'istituto viene unanimamente ricondotta all'opera dei due giuristi. Tuttavia, interessante la considerazione di Gambino e Mula i quali sottolineano come il concetto di privacy venne anticipato da studi precedenti e in particolare dal lavoro di COOLEY, *A treatise on the Law of Torts. Or the Wrongs which arise independent of contract*, Chicago, 1888, 29, ove si affermava: «the right to one's person may be said to be a right of complete immunity: to be let alone». Nello stesso lavoro di Warren e Brandeis viene fatto riferimento all'opera del giudice Cooley, sopra citata, nella quale veniva appunto coniata l'espressione "to be let alone". Si trattava però di un'accezione distinta da quella elaborata dai due giuristi, la nozione indicava la libertà di ciascuno di rifiutarsi di esercitare una certa libertà civile. V. GAMBINO, MULA, *Diritti fondamentali, protezione dei dati e cybersecurity*, in *La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele*, a cura di GAMBINO e STANZI, 2020, Pisa, 23 s. Autorevole parte della dottrina ritiene invece che la formulazione del diritto alla privacy vada ricondotto alla dottrina tedesca. V. sul punto BUSNELLI, *Nota introduttiva al commento della l. 31 dicembre 1996, n. 675. Spunti per un inquadramento sistematico*, in *Tutela della privacy (l. 31 dicembre 1996 n. 675)*, a cura di BIANCA *et al*., in *Nuove leggi civ. comm*., 1999, 228 ss. Per un'analisi sistematica dell'evoluzione del diritto alla riservatezza si rimanda a FARALLI, *op. cit.*, 1 ss.; KULESZA, voce «Privacy», in *Encyclopedia of Big Data*, a cura di SCHINTLER, MCNEELY, Berlin, 2017, consultabile all'indirizzo: *doi-org.ezproxy.unibg.it/10.1007/978-3-319-32001-4_172-1* (ultimo accesso 2 gennaio 2021).

[269] BARBARESCHI, GIUBILEI, *L'equilibrio tra la tutela dei dati personali e la manifestazione del pensiero*, in *I dati personali nel diritto europeo*, cit., 453 s.; RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit., 27 s.; PALMIERI, *Trattamento dei dati personali e giornalismo: alla ricerca di un equilibrio stabile*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di PARDOLESI, II, Milano, 2003, 338 s.; PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali*, cit., 40 ss.; DI RESTA, *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, Torino, 2018, 5 ss.; FARALLI, *op. cit.*, 4 ss.

macchine da stampa a rotativa, in grado di diffondere velocemente ed estesamente le notizie. L'istituto, in origine, si componeva così di un carattere oppositivo, in una dimensione pressoché limitata al diritto a non vedere diffuse informazioni personali senza il consenso dell'interessato, a meno che non fossero di pubblico interesse[270]. L'elaborazione del diritto alla privacy nasceva infatti come risposta all'esigenza di contemperare il diritto di cronaca[271]. Pertanto, ben si comprende come di esso i due giuristi bostoniani diedero un contenuto per così dire negativo, quale uno *ius excludendi alios*, un diritto a essere lasciati da soli (*right to be let alone*), a impedire che terzi possano ingerirsi all'interno della propria sfera personale, che comprende non solamente beni fisici ma anche informazioni.

Detta concezione si fondava sull'estensione del concetto privatistico di proprietà, e dunque del relativo sistema di tutela inibitorio, anche alla sfera immateriale della vita privata[272]. In questa prospettiva, l'esigenza di tutela si realizzava in primo luogo impedendo, mediante un'azione inibitoria, il perpetrarsi della violazione e correggendo, con lo strumento della rettifica, la circolazione delle notizie qualora risultassero lesive dei diritti della personalità del singolo[273].

---

[270] Boccaccini rileva come con l'affermazione del *right to privacy* nacque non solamente il concetto moderno di privacy, come diritto individuale, ma anche il tema del rapporto che deve sussistere fra diritti parimenti importanti, quello a informare (dei media) e quello dei cittadini a vedere tutelata la propria dimensione domestica. V. BOCCACCINI, *Le origini della privacy e della protezione dei dati*, in *Tecnologia e Diritto*, II, cit., 39. Interessanti sul punto anche le considerazioni di GAMBINO, MULA, *op. cit.*, 24 s., ove gli Autori sottolineano come proprio in considerazione della dimensione di limite al diritto di cronaca il diritto alla privacy è stato riconosciuto anche a gruppi sociali. Si tratta di un diritto, parzialmente autonomo da quello dei singoli componenti il gruppo, che si sostanzia quale facoltà per la comunità di decidere autonomamente quando, come e in che misura, comunicare informazioni sul gruppo o sui suoi appartenenti. L'indebita diffusione di notizie riferite alla comunità comporterebbe dei turbamenti sia interni, quale per esempio l'emersione di un clima di sfiducia tra gli stessi appartenenti al gruppo, quanto esterni, quando la diffusione porti a discriminazioni nei confronti dei soggetti facenti parte la comunità.

[271] La persona pretende e ottiene tutela della propria vita privata rivendicando che i mezzi di comunicazione rispettino il riserbo su informazioni che non hanno ragione di essere divulgate o che offrono un'immagine deformata dell'interessato; ciò nella prospettiva per cui la lesione dell'identità personale non deriva unicamente dalla diffusione di informazioni false ma anche dalla rappresentazione di notizie vere ma tale da recare un *vulnus* alla persona. V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in I *dati personali nel diritto europeo*, cit., 5 ss.

[272] CEROCCHI, COLAROCCO, *op. cit.*, 379 s.; GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço Jurídico*, 2013, 149 ss. Sul punto Santosuosso ritiene che, contrariamente a quanto gli si attribuisce, il testo di Warren e Brandeis «non parla del diritto di essere lasciati soli, chiudendo la porta della propria abitazione contro le intrusioni, ma parla di diritti personali che vanno oltre il corpo del suo titolare, che attengono alle emozioni e ai sentimenti delle persone». Si v. SANTOSUOSSO, *Intelligenza artificiale e diritto*, cit., 179.

[273] CUFFARO, *ibidem*.

Lo scritto di Warren e Brandeis, tuttavia, non riscostruiva l'istituto come un diritto fondamentale autonomo, al pari del diritto alla manifestazione del pensiero. Ciò è evidentemente da ascrivere alla cultura libertaria che caratterizza l'ordinamento giuridico statunitense[274]; nella Costituzione americana, infatti, il diritto alla manifestazione del pensiero è considerato il fondamento stesso della democrazia, e quindi di ogni libertà, a cui dunque il diritto alla riservatezza doveva contrapporsi[275].

Nato come un diritto della "borghesia"[276], solo con l'affermarsi dell'esigenza di un nuovo spazio di tutela del singolo la privacy acquisterà una dimensione sociale, legandosi ai diritti di libertà, divenendo così premessa necessaria alla libera manifestazione dell'individuo e all'estrinsecarsi della sua personalità[277].

Recentemente, grazie allo sviluppo della tecnologia e all'avvento della società dell'informazione, l'istituto ha subito un'ulteriore evoluzione ricomprendendo una concezione più generale di tutela dei dati del singolo, non più limitata alla riservatezza delle informazioni, che acquisterà una propria dimensione autonoma. La raccolta sempre più sistematica e di massa dei dati dei cittadini ha infatti evidenziato come il

---

[274] A questa impostazione deve forse ricondursi il mancato pieno accoglimento di un diritto alla privacy da parte della giurisprudenza statunitense. Solo nel 1967, in Katz v. United States, 389 U.S. 347 (1967), viene affermato per la prima volta il diritto del singolo alla privacy, quale protezione dalle ingerenze governative. Da notare inoltre come nell'ordinamento statunitense vi sia una più marcata differenziazione tra le tutele accordate nell'ambito privatistico e pubblicistico. Se nei rapporti tra privati e governo le clausole costituzionali rappresentano uno strumento di contrasto nei confronti delle ingerenze non autorizzate nella sfera privata dei cittadini, nell'ambito privato, invece, un importante limite alla privacy viene riscontrato proprio nell'autonomia individuale. Evidenzia Giannone Codiglione come proprio l'impostazione libertaria sia a fondamento dell'accostamento dei principi di libertà individuale con gli obiettivi di promozione del libero mercato, portando a una disciplina in cui si contrappongono la generale ammissibilità degli atti di sfruttamento economico dei propri dati e una tutela volta in larga parte a garantire il benessere del consumatore. V. GIANNONE CODIGLIONE, *Internet e tutele di diritto civile. Dati – persona – mercato: un'analisi comparata*, Torino, 2020, 148 ss.

[275] PIZZETTI, *Privacy e diritto europeo alla protezione dei dati personali*, cit., 43 ss. Anche nella giurisprudenza nostrana il diritto alla privacy, quanto meno nella sua concezione storica, ha assunto un carattere tendenzialmente recessivo. Sul punto si rimanda a BERBARESCHI, GIUBILEI, *op. cit.*, 457, i quali sottolineano come «difficilmente la sfera privata del singolo ha rappresentato un argine alla libertà di espressione: piuttosto, era la tutela della privacy che cessava allorché si fosse scontrata con l'esercizio legittimo del diritto antagonista». Cfr. anche PACE, *Informazione: valori e situazioni soggettive*, in *Dir. soc*., 2014, 743.

[276] Interessanti le considerazioni in merito al carattere multiforme della privacy avanzate da RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit., 28 ss. L'A. riporta come il diritto alla privacy, nella sua accezione classica, può sorgere solo là dove esistano condizioni di soddisfazione di altri bisogni, ciò in quanto parlare di diritto a essere lasciati soli, rivolto alle Istituzioni e alla richiesta di non ingerenza nell'acquisizione di dati dei cittadini, possa acquisire un connotato negativo proprio per quelle fasce di popolazione più deboli. Sottolinea l'Autore che «povertà e privacy sono termini semplicemente contraddittori» e che il diritto di essere lasciati, per i cittadini più fragili, rischia di assumere un carattere negativo quando si «risolve nell'esclusione dell'azione pubblica, nell'abbandono dei più deboli alla violenza sociale».

[277] GAMBINI, *op. cit.*, 152.

mero impedimento dell'accesso altrui alle proprie informazioni non fosse più sufficiente a tutelare gli interessati da possibili esternalità negative[278]. A differenza del 1890, il ventesimo secolo è stato, infatti, caratterizzato da una grande diffusione delle ICT a cui è seguita una produzione di informazioni personali che gli stessi utenti, più o meno consapevolmente, ancora oggi contribuiscono a diffondere nella rete[279]. Nonostante, almeno in Europa, il diritto alla privacy di concezione classica venga fatto rientrare nel novero dei diritti fondamentali dell'uomo[280], grazie prima alla sensibilità delle Corti[281] e

[278] GAMBINI, *op. cit.*, 153; DI RESTA, *op. cit.*, 3 ss.

[279] ROMEO, *Il governo giuridico delle tecniche dell'informazione e della comunicazione*, in *I dati personali nel diritto europeo*, cit., 1247 ss.; GAMBINI, *op. cit.*, 151; DE GREGORIO, TORINO, *op. cit.*, 450 ss. La diffusione di smartphone e applicazioni che connettendosi in rete (IoT) possono raccogliere e trasmettere un gran numero di dati degli utenti, finanche di natura sensibile, comporta una inevitabile tensione tra gli interessi economici dei titolari, come visto nel capitolo precedente, e l'interesse dei consumatori/utenti a non vedere lesi i propri diritti fondamentali. BOCCACCINI, *op. cit*., 40 ss.

[280] Il diritto alla riservatezza è, infatti, codificato all'art. 8 della Convenzione Europea dei Diritti dell'Uomo (CEDU). L'articolo, rubricato "Diritto al rispetto della vita privata e familiare", prescrive: «*1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*». Il riconoscimento di un diritto alla privacy veniva fatto discendere da un'interpretazione evolutiva della disposizione in oggetto, individuando in essa il fondamento per la tutela del singolo dalle ingerenze altrui nella propria sfera di riservatezza, nella quale vanno ricomprese anche le informazioni che si riferiscono alla sfera intima della persona.

[281] In Italia la tutela della privacy ha avuto i primi riconoscimenti nella seconda metà del XX secolo ad opera principalmente del formante giurisprudenziale, per poi trovare un riconoscimento normativo solo con la legge n. 675/1996. Fu dunque merito della sensibilità dei giudici che, pur in mancanza di un riconoscimento normativo, dando una lettura costituzionale delle norme hanno permesso il delinearsi del diritto alla riservatezza quale diritto della personalità, che tuttavia non si limita alla pretesa di essere lasciati soli. Tra i primi riconoscimenti del diritto alla privacy non può non citarsi la sentenza della Corte Costituzionale n. 38 del 12 aprile 1973, ove si riconobbe il diritto alla riservatezza come un diritto inviolabile, sulla base degli artt. 3, 13 e 21 della Costituzione, oltre che degli artt. 8 e 10 della Convezione europea dei diritti dell'uomo. Corte cost., 12.4.1973, n. 38, in *DeJure*. Il maggior contributo alla configurazione del diritto è avvenuto però ad opera della Corte di Cassazione, il cui primo arresto viene fatto risalire al 1975 con l'ormai famosa sentenza n. 2129 sul caso Soraya. La Corte, facendo ricorso alla figura del "domicilio ideale", ha così iniziato a delineare la privacy quale «*tutela di quelle situazioni e vicende strettamente personali e familiari, le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per terzi un interesse socialmente apprezzabile, contro le ingerenze, che sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non siano giustificate da interessi pubblici preminenti*», Cass., 27.5.1975, n. 2129, in *Mass. Giur. it*., 1975, 594. Il caso è stato considerato un "*leading case*" della materia. A partire poi dagli anni '90 la Corte Costituzionale aveva compiuto quel passaggio interpretativo che riunisce sotto la nozione di diritto alla privacy, sia la tutela della riservatezza, che la generale protezione dei dati personali (Corte cost., 26.3.1990, n. 139, in *Giur. it*., 1991, I, 376; Corte cost., 11.3.1993, n. 81, *ivi*, 1995, I, 108, con nota di DI FILIPPO). In dottrina cfr. FARALLI, *op. cit.*, 6; BARBARESCHI, GIUBILEI, *op. cit.*, 460; ROMEO, *op. cit.*, 1247 s.; FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 7; FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in *La protezione dei dati personali in Italia*, cit., 10 ss.; CEROCCHI, COLAROCCO, *op. cit.*, 380. Nel 1998 la Suprema Corte è stata chiamata a decidere un nuovo caso, sempre in materia di diritto alla riservatezza, affermando

successivamente al riconoscimento esplicito dato dall'art. 7 della Carta dei Diritti Fondamentali dell'Unione Europea (Carta di Nizza)[282], ciò non è stato comunque sufficiente a regolare la nuova realtà sociale governata dalla raccolta dati di massa e da trattamenti automatizzati[283]. Alla concezione classica si è dunque affiancata una lettura moderna dell'istituto, quale diritto alla tutela dei dati personali[284].

La prospettiva di indagine muta quando, sul finire del XX secolo, cambia la realtà sociale di riferimento[285]. Con l'avvento di elaboratori elettronici e di algoritmi, perde di centralità l'informazione sulla persona che riveste interesse per la cronaca in quanto notizia[286]. Centralità assumono invece i dati degli utenti nel loro complesso, pur se non significativi se presi in considerazione singolarmente. Cambia l'angolo prospettico, ciò anche in ragione del moltiplicarsi dell'uso che dei dati degli utenti viene fatto[287]. Al centro dell'indagine non vi è più dunque solo la riservatezza della persona, quanto

---

l'esistenza di «*un vero e proprio diritto alla riservatezza anche al di fuori delle ipotesi espressamente previste dalla legge ordinaria*». Cass., 9.6.1998, n. 5658, in *Foro it.*, *1998*, I, 2387.

[282] L'art. 7, Carta dei diritti fondamentali dell'Unione europea, rubricato "Rispetto della vita privata e della vita familiare", sancisce che «*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni*».

[283] A fronte dell'irrefrenabile raccolta di informazioni personali ad opera di enti privati, sebbene non siano a ciò estranei nemmeno gli enti pubblici, a fini di lucro grazie allo sfruttamento commerciale dei profili che si fondano proprio sui dati, la privacy ha iniziato ad assumere il ruolo di baluardo del diritto al rispetto di uno spazio di intimità, «una garanzia di dignità irrinunciabile nei confronti del potere e dell'autorità più forte, pubblica o privata, a difesa di quello che è stato definito un processo di *Datification of everything*». V. FALLETTI, *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in *Dir. inform*., 2020, 170 ss.

[284] Già dagli anni '60 la dottrina più attenta ha iniziato a elaborare un diritto alla protezione dei dati quale diritto dei singoli a limitare l'impiego dei propri dati per finalità differenti da quelle per cui erano stati inizialmente raccolti. Con la diffusione delle tecnologie informatiche, e dunque con la possibilità di conoscere e utilizzare i dati degli utenti per una molteplicità di scopi, si è progressivamente ampliata la concezione di protezione dei dati, fino all'affermazione di un diritto non solo a limitare il trattamento, ma anche a conoscere le modalità e le finalità con cui sono gestiti i dati raccolti; visione che ha trovato un coronamento nel GDPR. V. GAMBINO, MULA, *op. cit.*, 25 ss.

[285] Sul punto Cuffaro precisa come «il mutamento della stessa organizzazione sociale che il linguaggio rende esplicito quando usa l'espressione "dati personali", è stato dunque accompagnato da un radicale mutamento di rotta: la privacy da frutto di una costruzione teorica come diritto della persona della cui elaborazione il giurista può rivendicare la paternità, diviene invece materia di un apparato normativo elefantiaco che nel breve volgere di anni ha visto il susseguirsi di una pluralità di testi segnati da una insistente e progressiva analiticità quasi al punto di mortificare il compito dell'interprete», V. CUFFARO, *op. cit.*, 7.

[286] CUFFARO, *op. cit.*, 6 s.; DE GREGORIO, TORINO, *op. cit.*, 449 ss.

[287] Così come lo sviluppo dell'editoria e della distribuzione della stampa si ritiene siano stati all'origine della creazione dell'istituto della privacy, si ritiene che l'avvento di un nuovo diritto autonomo, quale è il diritto alla protezione dei dati personali, affondi le radici nell'esigenza di contrastare il controllo dei cittadini da parte degli Stati autoritari del Novecento. Si veda sul punto PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 52 ss.

piuttosto la tutela della sfera di controllo che quest'ultima può esercitare direttamente sui propri dati[288].

Emergono nuove esigenze di tutela degli utenti sottoposti a trattamenti sempre più automatizzati; si inizia così a concepire un diritto all'autodeterminazione informativa, declinato come una scelta del singolo di autodefinirsi e determinarsi in relazione alle finalità a cui i propri dati sono destinati[289].

A fare da precursore, come visto, è stato il Consiglio d'Europa che già nel 1981, con l'adozione della Convenzione 108, aveva compreso le prospettive critiche insite nell'utilizzo degli elaboratori elettronici e nelle tecnologie digitali, a quel tempo ancora agli albori, apprestando le prime forme di tutela per gli interessati.

Diverso invece il percorso seguito dell'Unione Europea. La prospettiva regolatoria da cui si è mosso il legislatore comunitario è infatti sostanzialmente legata alla dimensione economica del fenomeno, più che a quella costituzionale e di tutela della persona. La prima regolazione organica espressamente dedicata al trattamento dei dati personali fu infatti la Direttiva 46/95 CE, ove una particolare attenzione veniva data al carattere funzionale della tutela dei dati alla creazione e al corretto funzionamento del mercato unico.

A questa seguì nel 2000 un importante vertice del Consiglio Europeo[290], ove vennero gettate le basi della strategia europea di settore che culminerà con l'emanazione di una

[288] Si rimanda a DE GREGORIO, TORINO, *op. cit.*, 457 ss. Evidenziano gli Autori come proprio la crescente pervasività nell'utilizzo della tecnologia, con il trattamento dei dati anche in modo automatizzato, ha reso non più sufficiente il semplice diritto alla riservatezza come strumento di tutela dei cittadini. Una conferma in questo senso si può cogliere proprio nell'attenzione al trattamento automatizzato dei dati avvenuto nel corso degli anni '80, che fa comprendere a fortiori la rilevanza dei Big Data, non solamente per il singolo individuo, ma per l'intera società.

[289] FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 6 s.; CEROCCHI, COLAROCCO, *op. cit.*, 381 s. Interessante anche la lettura che del diritto alla protezione dei dati personali fa Orfino. L'Autore ritiene, infatti, come esso sia espressamente qualificato dal Regolamento non solo come un diritto individuale, ma pure come un interesse pubblico rilevante per le società contemporanee; una garanzia per la loro democraticità, identificandosi dunque come un baluardo stesso della sicurezza nazionale. V. ORFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *Medialaws – riv. dir. media*, 2018, 83 ss.

[290] Il 23 e 24 marzo del 2000 si tenne a Lisbona una riunione del Consiglio Europeo che si rivelerà fondamentale per definire una strategia diretta a cogliere le potenzialità del nuovo contesto tecnologico, e in particolare la *data driven innovation*. Prendendo coscienza della necessità di creare un contesto normativo unitario che permettesse lo sviluppo economico e sociale promesso dalla digitalizzazione, la Presidenza del consiglio chiarì le linee di intervento che avrebbero caratterizzato i futuri interventi delle istituzioni. «1. L'Unione europea si trova dinanzi a uno svolta epocale risultante dalla globalizzazione e dalle sfide presentate da una nuova economia basata sulla conoscenza. Questi aspetto della vita delle persone e richiedono una trasformazione radicale dell'economia europea […]. 2. Il ritmo rapido e sempre crescente dei mutamenti rende urgente un'azione immediata da parte dell'Unione per sfruttare appieno i

serie di atti normativi diretti a regolare in modo specifico le principali attività di trattamento dati[291]. Nella consapevolezza della necessità di una normazione in linea con l'evoluzione tecnologica, il legislatore europeo predispose così strumenti normativi facenti parte di una strategia di *governance* dei dati diretta a non scoraggiarne l'utilizzo, in ragione delle evidenti prospettive economiche legate allo sviluppo di un mercato unico digitale.

Solo successivamente il diritto alla protezione dei dati personali, grazie anche al ruolo svolto della Corte di Giustizia[292], venne riconosciuto quale diritto fondamentale autonomo. Questo venne infatti ricompreso in modo esplicito dalla Carta dei diritti fondamentali dell'UE (Carta di Nizza), all'art. 8[293], a cui nel 2009 il trattato di Lisbona, come noto, ha riconosciuto lo stesso valore giuridico dei Trattati. Ne discende come la carta abbia acquisito un'efficacia diretta, come previsto dall'art. 6, par. 1, TUE,

---

vantaggi derivanti dalle opportunità che si presentano. Ne consegue la necessità per l'Unione di stabilire un obiettivo strategico chiaro e di concordare un programma ambizioso al fine di creare le infrastrutture del sapere, promuovere l'innovazione e le riforme economiche, e modernizzare i sistemi di previdenza sociale e d'istruzione […]». Consiglio Europeo, Conclusioni della Presidenza alla riunione di Lisbona del 23 e 24 marzo 2000.

[291] La necessità di una regolazione coerente e coordinata in un settore come quello dei dati, avente vocazione globale, è di tutta evidenza fondamentale per permettere lo sviluppo del mercato unico digitale nel quadro dei principi e valori dell'UE. Tra i maggiori interventi possiamo annoverare il Regolamento sulla libera circolazione dei dati non personali (Regolamento 1807/2018 UE); il Regolamento sulla cyber-sicurezza (Regolamento 881/2019 UE); la Direttiva sui dati aperti (Direttiva 1024/2019 UE) e, infine, il Regolamento generale sulla protezione dei dati personali (Regolamento 679/2016 UE, GDPR).

[292] La Corte di Giustizia ha ricoperto un ruolo fondamentale permettendo, in via pretoria, l'affermarsi di un diritto alla protezione dei dati personali tale da garantire una tutela ai singoli, soprattutto in relazione all'evoluzione tecnologica. La concezione della privacy, dunque, si emancipò dal ruolo di eccezione alle libertà economiche sancite dai Trattati, acquisendo un'autonoma rilevanza, fino a divenire un diritto fondamentale dell'uomo. ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina*, cit., 5.

[293] L'art. 8, Carta dei diritti fondamentali dell'Unione Europea, rubricato "Protezione dei dati di carattere personale", prescrive che: «*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*». Il testo dell'articolo in parola prevede un insieme di regole e principi, consentendo di creare un sistema di contrappesi che va oltre al concetto di consenso come base di legittimità del trattamento. Cfr. ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina*, *ibidem*. É interessante notare come la disposizione, così come anche il precedente articolo dedicato alla riservatezza, siano inserite nel Capo 1 dedicato alla dignità. Recentemente anche la giurisprudenza di merito italiana ha richiamato il concetto di dignità in relazione alla tutela dei dati personali. Il Tribunale di Milano ha, infatti, affermato che per assicurare il rispetto della dignità umana la protezione dei diritti inviolabili dell'uomo rappresenta il criterio che deve orientare l'interpretazione del sistema normativo e il bilanciamento dei diritti. Trib. Milano, 28.9.2016, n. 10374 in *Foro it.*, 2016, I, 3594, con nota di PARDOLESI. Sul punto interessanti le considerazioni di Boccacini, il quale sottolinea come tale impostazione sarebbe l'unica compatibile con il principio personalistico che anima la nostra Costituzione «la quale vede nella persona umana un valore etico in sé e vieta ogni strumentalizzazione della medesima per alcun altro fine eteronomo e assorbente». V. BOCCACINI, *op. cit.*, 38.

divenendo una fonte vincolante di diritto primario. Il diritto alla protezione dei dati fu poi oggetto di un esplicito richiamo al primo capoverso dell'art. 16 del TFUE[294]. L'articolo dispone inoltre che il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale, oltre che a quelle dirette a regolare la libera circolazione di tali dati[295]. Le normative dirette a regolare la materia devono dunque essere lette proprio alla luce di dette previsioni. Il diritto alla protezione dei dati personali assume un ruolo di primaria importanza quale diritto fondamentale dell'uomo, soggetto tuttavia, come visto, a un'attenta ponderazione in relazione a diritti e interessi concorrenti, tra cui in particolare quello alla libera circolazione dei dati.

Così chiarito cosa debba intendersi per diritto alla protezione dei dati, l'evoluzione tecnologica ha reso evidente un ulteriore profilo cruciale legato alla definizione stessa di dato personale. Detta nozione merita una particolare attenzione, in special modo perché appare avere un perimetro in qualche modo sfumato e in continua evoluzione. Il "dato personale" all'interno delle normative rappresenta infatti uno strumento tecnico-giuridico che permette la tutela dei differenti diritti collegati all'identità personale degli utenti[296]. Tuttavia, la capacità dei Big Data di scovare correlazioni, attraverso un mix di dati correlati e non, solleva molteplici interrogativi attorno alla concezione stessa di cosa debba intendersi per dato personale e, di conseguenza, all'ambito di applicazione del GDPR, come di seguito si cercherà di chiarire[297].

---

[294] L'art. 16 TFUE, prescrive: «*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea*».

[295] DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in *I dati personali nel diritto europeo*, cit., 184. Per un approfondimento in merito sia al fondamento costituzionale del diritto alla protezione dei dati personali, sia nella prospettiva sovranazionale, si rimanda a CALZOLAIO, voce «protezione dei dati personali», in *Digesto VII ed*., *Disc. pubbl*., Milano, 2017, 616 ss.

[296] DI RESTA, *op. cit.*, 3 s. L'A. precisa come il dato sia un contenitore vuoto all'interno del quale è dunque l'interprete a inserire uno specifico contenuto relativo al patrimonio informativo dell'interessato.

[297] DE GREGORIO, TORINO, *op. cit.*, 467.; CALZOLAIO, *op. cit.*, 605 ss.

2. Il "dato personale" all'interno della normativa europea: una nozione aperta

La maggiore consapevolezza circa il funzionamento degli algoritmi, e di come essi si "nutrano" di dati, ha riportato al centro del dibattito la necessità di un controllo delle informazioni processate. Come si è già avuto modo di rilevare, infatti, affinché sia possibile sfruttare a pieno le potenzialità della *data driven economy* è necessario potenziare la fiducia degli utenti nell'utilizzo delle tecnologie digitali. Pertanto, proprio in ragione di tale considerazione una particolare attenzione è stata dedicata *in primis* ai dati personali, il cui uso smodato e non regolato avrebbe potuto confliggere con i diritti fondamentali degli utenti.

Il concetto di dato personale ha trovato una prima definizione molto ampia nella Convenzione 108[298]; a questa sono seguite ulteriori specificazioni, grazie all'opera interpretativa della Corte di Giustizia, poi trasfuse nella Direttiva 46/95 CE[299] e, più recentemente, nell'art. 4 del GDPR. L'articolo da ultimo citato chiarisce che per "dato personale" debba intendersi: «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*»[300].

Prima di analizzare la definizione riportata preme fare alcune considerazioni al fine di evitare possibili sovrapposizioni terminologiche. Innanzitutto è necessario sottolineare come alcun riferimento venga fatto, né direttamente né indirettamente, alla riservatezza, dovendo i due concetti rimanere distinti. Il dato personale, infatti, non

[298] L'articolo 2, rubricato "Definizioni", specifica che «"*dati a carattere personale" significa ogni informazione concernente una persona fisica identificata o identificabile («persona interessata»)*». Convenzione n. 108/1981.

[299] Nella Direttiva la definizione di dato personale si fa più corposa arricchendosi di alcune chiarificazioni terminologiche legate all'evoluzione tecnologica. Negli anni '90 si assiste, infatti, a una prima fase di datificazione, grazie alla crescita e alla diffusione della rete internet, dando il via a trattamenti di grandi masse di dati degli utenti. Il legislatore europeo, dunque, precisa nel testo che qualsiasi informazione riguardante una persona fisica identificata o identificabile deve essere considerato un dato personale; a ciò segue, e qui la novità, anche una specificazione di cosa debba intendersi con il termine identificabile: «*si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica , economica, culturale o sociale*», art. 2, dir. CE n. 46/95.

[300] Art. 4, reg. UE n. 679/2016.

coincide necessariamente con un dato riservato, ben potendo i dati personali, quali sono per esempio il numero di matricola o quello di telefono, essere conosciuti da molte persone[301]. Del pari i dati personali non coincidono con i c.d. dati sensibili[302]; con tale espressione si fa riferimento a dati espressivi di informazioni di particolare rilevanza, quali per esempio la razza, lo stato di salute, etc[303]. A questa particolare categoria viene dedicata, espressamente all'art. 9 GDPR, una forma di tutela che potremmo definire rinforzata, proprio in ragione dei pregiudizi che potrebbero sorgere se ne fosse concesso liberamente il trattamento[304].

Chiarito dunque come la nozione di dato personale debba essere tenuta distinta da quella di dato riservato e di dato sensibile, da una prima lettura della definizione da ultimo coniata dal legislatore europeo essa appare particolarmente estesa. La *ratio* di una formulazione generica risiede evidentemente nell'esigenza di flessibilità, necessaria in una materia che richiede una pronta adattabilità alle evoluzioni tecnologiche.

Entrando nello specifico, occorre precisare alcune espressioni utilizzate al fine di meglio comprendere lo stesso perimetro di applicazione della tutela apprestata dal Regolamento. Innanzitutto, essenziale appare l'indicazione che dato personale può essere qualsiasi informazione. Sebbene dalla lettura delle norme del testo in analisi i due concetti sembrino coincidere, lo stesso legislatore europeo ne traccia un confine. Difatti il dato, sia esso considerato singolarmente o nell'insieme aggregato, rappresenta la fonte dell'informazione; questa viene estratta o inferita dal dato personale, ne rappresenta dunque il significato. Le informazioni posseggono una dimensione semantica che

[301] DEL FEDERICO, POPOLI, *op. cit.*, 66.

[302] NERVI, *Il perimetro europeo: portata applicativa e definizioni*, in *I dati personali nel diritto europeo*, cit., 173 s. Sul concetto di dato personale e di dato sensibile previsto dalla Direttiva CE n. 46/95 si veda PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 183 ss. Per una considerazione in merito alle categorie particolari di dati, in un confronto con quanto previsto dal d.lgs. n. 196/2003, si rimanda a DELL'UTRI, *op. cit.*, 231 ss.; CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici*, in *La protezione dei dati personali in Italia*, cit., 204 ss.; DI RESTA, *op. cit.*, 15 ss.

[303] In particolare il legislatore definisce, nell'art. 4 GDPR, i dati genetici quali «*dati personali relativi alle caratteristiche genetiche ereditarie o acquisite da una persona fisica, e che risultano in particolare dell'analisi di un campione biologico della persona fisica in questione*». I dati biometrici, invece, sono quei «*dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*». Da ultimo viene fornita anche una definizione di dati relativi alla salute, ritenendo tali quelli «*attinenti alla salute fisica e mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*».

[304] Il legislatore europeo, pur abbandonando la nozione di dato sensibile, ha previsto la definizione di nuove categorie di dati espressivi di informazioni di particolare rilevanza, quali caratteristiche genetiche, culturali, razziali, politiche, sessuali e biometriche degli utenti.

manca invece al dato. Ne discende un concetto di "dato" quale una categoria generale, avente una dimensione estremamente flessibile, il cui contenuto viene determinato dall'interprete in ragione dello specifico patrimonio informativo preso in considerazione[305]. Si tratta dunque di una nozione dinamica che si costruisce anche in relazione al "soggetto" che osserva, ciò in particolare se ad osservare i dati sono delle applicazioni di AI, le quali, come visto, grazie alla correlazione tra molte variabili possono inferire dati personali anche da *dataset* di natura più strettamente non personale. Ne discende allora che mediante l'utilizzo di sistemi informatici la distinzione tra dato personale e non viene a sfumare, non essendo la natura di questo qualcosa di statico, di originario e persistente, dovendo invece essere parametrata alla capacità di indentificare (direttamente o meno) una persona fisica[306]. Qualsiasi formato può essere idoneo allo scopo di rendere identificabile un soggetto, rientrando a pieno titolo tra i dati personali non solo i file testuali ma anche formati audio, video, immagini, caratteri alfanumerici, biometrici, etc.

Continuando nella lettura della disposizione, il legislatore precisa come debbano rientrare nella categoria di dati personali quei dati che permettano l'identificazione di una persona fisica, sia in modo diretto che indiretto, dunque anche quale risultato emergente dall'incrocio di più dati[307]. Pertanto, così come chiarito dal Considerando n.

---

[305] Precisa Di Resta come il dato personale appaia come «un'entità neutra, un medio giuridico» e allo stesso tempo debba essere considerato un bene giuridico. V. DI RESTA, *op. cit.*, 4.

[306] Sul punto interessanti le considerazioni di Calzolaio il quale sostiene che «la natura del dato non è più necessariamente qualcosa di originario e persistente, ma è strettamente legata al soggetto (ivi compresa, in particolare, la macchina) che lo osserva e lo analizza. Più precisamente, se l'analisi è sviluppata dalla macchina – e non dall'uomo con le sue sole forze di analisi – la distinzione tra dato personale e dato non personale tende a sfumare, poiché la macchina può trarre dati e informazioni personali anche da dati insignificanti per le capacità di indagine dell'uomo». Si rimanda a CALZOLAIO, *op. cit.*, 607.

[307] Interessante l'analisi compiuta da CEROCCHI, COLAROCCO, *op. cit.*, 383 ss. nella quale le AA. ritengono che nell'espressione "concernenti" vadano ricompresi tre fattori alternativi: il contenuto, dunque cosa esprima lo specifico dato; la finalità, cioè lo scopo a cui è diretta la raccolta, in particolare qualora il dato venga utilizzato per valutare una persona o per condizionarne i comportamenti; infine, il risultato, dunque l'impatto che l'uso dei dati ha sui diritti della persona. Cfr. sul punto anche PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 185; DEL FEDERICO, POPOLI, *op. cit.*, 58 ss.; DI RESTA, *op. cit.*, 5 ss.

Dette considerazioni sembrano inoltre ricalcare il parere del Gruppo di Lavoro art. 29, emanato nel 2007, in merito al concetto di dato personale. Nel documento viene chiarita la portata del termine "dato personale" al fine di armonizzarne l'interpretazione del testo negli Stati membri, analizzandone in modo puntuale i quattro elementi che ne compongono la definizione. In particolare, in merito alla locuzione "concernente" si precisa che un'informazione riguarda una persona qualora con essa vi sia una relazione di contenuto, di finalità o di risultato. Sul ruolo rivestito dalle raccomandazioni e dai documenti emanati dal Gruppo di Lavoro art. 29, interessanti le considerazioni svolte da Passaglia. L'Autore, difatti, sottolinea come detti documenti possano rientrare nella nozione di *soft law*. Ciò in quanto sebbene essi

26, dovranno essere esclusi dal perimetro di applicazione del Regolamento quei dati che invece possono considerarsi anonimi[308], che non possono cioè essere, con misure ragionevoli[309], riassociati all'interessato[310].

Evidentemente, anche la previsione di rendere assoggettati alla regolazione i dati concernenti le persone identificabili, e non solo quelle direttamente identificate, permette di estendere la portata applicativa della definizione. A fronte di una tale indicazione, infatti, l'interprete è chiamato a tenere in considerazione non solamente il

---

non possano configurarsi alla stregua di fonti di produzione, dimostrano avere un'indiscutibile rilevanza riuscendo a orientare i comportamenti nella prassi. V. PASSAGLIA, *op. cit.*, 108.
Per un approfondimento sul ruolo del Gruppo di Lavoro art. 29 e sul Comitato europeo per la protezione di dati si rimanda a ZAMBRANO, *Il Comitato europeo per la protezione dei dati*, in *I dati personali nel diritto europeo*, cit., 983 ss.; PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 33 s.; IPPOLITI MARTINI, *Comitato europeo per la protezione dei dati*, in *La protezione dei dati personali in Italia*, cit., 725 ss.; ID., *Comitato europeo per la protezione dei dati*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 552 ss.

[308] Il concetto di dato anonimo verrà ripreso nel prosieguo, basti qui sottolineare che anonimi possono essere dati grezzi, quindi nati come tali, oppure resi tali con un'operazione successiva alla loro raccolta, volta a separare in modo durevole le caratteristiche che li rendano personali. Si rimanda a DE GREGORIO, TORINO, *op. cit.*, 467 ss., ove gli Autori sottolineano come non esista un'unica definizione di dato anonimo, dovendo questa essere parametrata al contesto del trattamento posto in essere. Ciò che deve essere verificato – chiariscono gli Autori – sono i mezzi che possono essere ragionevolmente utilizzati dal titolare per re-identificare gli interessati. Ne discende, allora, che i dati risultano anonimi solo nel momento in cui, condizione che potrebbe anche mutare nel tempo, non vi siano mezzi ragionevoli diretti a ottenere da quei dati delle informazioni di natura personale.

[309] Astrattamente oggi è sempre possibile identificare una persona fisica, per questo motivo non pare possibile una piena e permanente anonimizzazione dei dati. É dunque necessario fare una valutazione caso per caso diretta a comparare, da una parte, i rischi per i diritti dell'interessato e, dall'altra, gli interessi del titolare del trattamento. L'attività di identificazione di un soggetto è, infatti, complessa, potrebbe comportare differenti mezzi e operazioni, alcune anche particolarmente costose. É apparso pertanto opportuno procedere con un bilanciamento tra interessi contrapposti, introducendo un criterio di valutazione incentrato sulla ragionevolezza. Si è inteso valutare nel concreto i singoli dati con un test che prenda in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati per permettere l'identificazione dell'interessato. Si tratta di una valutazione evidentemente dinamica legata: al costo dei mezzi utilizzabili in relazione al valore della possibile identificazione e al prevedibile sviluppo della tecnologia in rapporto al tempo di utilizzabilità del dato per la finalità che si vuole perseguire. Cfr. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 184 ss.

[310] Un'indicazione in merito a cosa debba intendersi per dato personale è presente nel Considerando n. 26, reg. UE n. 679/2016, il quale precisa che: «È *auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di 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. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca*».

singolo dato raccolto, ma anche l'intero contesto di riferimento, quindi l'insieme dei mezzi il cui utilizzo possa permettere di identificare un individuo. A ciò deve infine aggiungersi come nemmeno sia necessaria una specifica indicazione della persona fisica in modo univoco, potendo essere considerati dati personali anche quelli che permettono di identificare un soggetto quale appartenente ad un gruppo. Nel perimetro applicativo del Regolamento possono così essere compresi anche quel novero di trattamenti digitali, quali la profilazione, in cui l'utente non riveste importanza in quanto singolo ma quale appartenente a un determinato gruppo.

Il carattere particolarmente fluido e dinamico della nozione di dato personale, in parte già presente nel testo della Direttiva madre, è il risultato di un'evoluzione giurisprudenziale resasi necessaria a fronte delle inevitabili incertezze applicative che sono discese da una formulazione così aperta. Estendendosi la nozione di dato personale al di là delle informazioni che dicono qualcosa in merito ad una persona fisica, dovendo, come visto, verificare anche il contesto in cui i dati sono raccolti e verranno utilizzati[311], appare complesso, e ciò soprattutto in un quadro ove la tecnologia assume un ruolo di assoluto rilievo[312], predeterminare a priori quali siano dati personali e, a contrario, quali invece non lo siano. Sul punto è così intervenuta la Corte di Giustizia[313], ampliando il

[311] Evidenzia Montagnani come la nozione di dato personale può ricomprendere «anche quelle informazioni che possono essere usate per modificare lo stato o il comportamento di un individuo, oppure possono avere un qualche effetto sui suoi diritti e interessi. Per quanto esista una certa differenza tra informazioni sulla persona o informazioni che incidono sulla persona – giacché queste ultime non necessariamente convogliano contenuto ma si limitano ad essere utilizzabili in maniera tale da alterare la sfera all'interno della quale un soggetto opera – entrambe rientrano nella definizione di dato personale, che si caratterizza quindi per essere particolarmente fluida e dinamica. […] A seconda del contesto si può verificare anche il caso che un'informazione abbia natura di dato personale in un momento storico – perché incide sul comportamento dell'interessato – ma non in un altro, la qual cosa contribuisce ulteriormente a rendere difficile determinare a priori quali informazioni siano dati personali e, a contrario, quali siano invece dati non personali». V. MONTAGNANI, *op. cit.*, 306.

[312] Un accenno merita il testo della Dichiarazione dei Diritti di Internet – presentata il 29 luglio 2015 – al cui art. 5, rubricato "Tutela dei dati personali", viene proposta una definizione di dato personale avente un taglio che appare maggiormente diretto a ricomprendere i trattamenti posti in essere dagli artefatti digitali quali gli IoT. Difatti si prescrive che «[…] *2. Tali dati* [personali, ndr] s*ono quelli che consentono di risalire all'identità di una persona e comprendono anche i dati dei dispositivi e quanto da essi generato e le loro ulteriori acquisizioni e elaborazioni, come quelle legate alla produzione di profili*». Per un approfondimento in merito alla Dichiarazione dei Diritti di Internet quale efficace strumento di *soft law* si rimanda a SARRA, *op. cit.*, 43 ss.

[313] Fondamentale il ruolo avuto dalla Corte di Giustizia nel periodo di vigenza della Direttiva madre. Le pronunce, che si sono mostrate essere di ampia portata, hanno difatti contribuito a instaurare un vero e proprio dialogo con il legislatore europeo, dal cui esito è scaturito il successivo GDPR. Si pensi al caso Nowak, ove la Corte ha precisato che la stessa indicazione che vede i dati personali come «*"qualsiasi informazione", altro non faccia che riflettere l'obiettivo del legislatore europeo di attribuire un'accezione estesa a tale nozione*». La Corte, continuando nell'analisi dell'istituto, specifica che la categoria di dati personali non può essere limitata alle informazioni sensibili o di ordine privato, «*ma*

novero dei dati rientranti nella categoria di quelli personali; giurisprudenza che verrà poi ripresa dal legislatore nella formulazione dell'art. 4 sopra riportato.

Per limitarsi ad un esempio paradigmatico, legato proprio alle applicazioni digitali e all'uso che viene fatto dei dati degli utenti, si può citare la decisione del noto caso Breyer[314]. Nel caso di specie i Giudici hanno precisato che anche gli indirizzi IP dinamici sono da considerarsi dati personali e come tali, dunque, assoggettabili alla normativa europea, *ratione temporis* la Direttiva 46/95 CE. Gli indirizzi IP (*Internet Protocol*) sono delle stringhe di numeri costituite da 32 bit, suddivisi in quattro gruppi da 8 bit ciascuno, generate al fine di identificare specificamente un terminale e necessarie per la connessione alla rete internet. Anche gli IP dinamici hanno il medesimo compito, tuttavia questi, a differenza degli statici, cambiano ad ogni connessione, pur rimanendo il numero di indirizzi IP assegnabile a ciascuna unità periferica limitato. Una volta terminata la connessione l'indirizzo dinamico non è più collegato allo specifico terminale, dunque per identificarlo è necessario accedere ad ulteriori informazioni in possesso dei gestori ISP (*Internet Service Provider*) della rete utente. Di per sé solo, pertanto, l'IP dinamico non permette di re-identificare il terminale connesso; ciò sarebbe astrattamente possibile ma solo con l'uso di dati in possesso di un soggetto terzo.

---

comprende potenzialmente ogni tipo di informazioni, tanto oggettive quanto soggettive, sotto forma di pareri o di valutazioni, a condizione che esse siano concernenti la persona interessata». Nel caso Nowak, dunque, vennero considerati dati personali gli scritti di un esame, e le correzioni apportate, nei confronti delle quali l'interessato esercitava il proprio diritto di accesso. Corte giust. UE, 20.12.2017, causa C-434/16, in *Dir. inform*., 2017, 857. Cfr. NERVI, *op. cit.*, 163; DEL FEDERICO, POPOLI, *op. cit*., 59; MONTAGNANI, *op. cit.*, 306; DI RESTA, *op. cit.*, 6.

[314] Il caso è particolarmente interessante perché il gestore di servizi di media online era un'Istituzione pubblica, la quale giustificava la raccolta e la conservazione dei dati nei file di *log*, pur sostenendo non fossero catalogabili tra quelli di natura personale, con l'esigenza di salvaguardare il funzionamento del sito istituzionale contro possibili attacchi di pirateria informatica. Dopo un primo rigetto, la Corte d'Appello tedesca riformò parzialmente la sentenza affermando che l'indirizzo IP dinamico può essere considerato un dato personale solo nel caso in cui l'utente, al momento della navigazione, fornisca delle informazioni personali che ne permettano il riconoscimento. Dunque, per la Corte d'Appello, solo in quel caso il gestore di servizi online non avrebbe potuto conservare i dati utente, violando altrimenti la Direttiva CE n. 46/95. Il caso fu, dunque, portato all'attenzione della Corte di Giustizia, la quale ha chiarito che per essere qualificato come personale non è necessario che il dato porti all'identificazione di una persona fisica. È infatti sufficiente che ne permetta, con ragionevoli mezzi, l'identificabilità, anche mediante l'uso di dati in possesso di soggetti terzi. Pertanto, potendo l'amministrazione pubblica convenuta accedere ai dati in possesso dell'ISP, mediante un ordine giurisdizionale, tale mezzo di accesso è stato ritenuto ragionevole. Ne consegue che anche gli IP dinamici debbano essere considerati dei dati personali indiretti, in quanto è ragionevolmente possibile ricollegarli al soggetto fruitore del servizio. Corte giust. UE, 19.10.2016, causa C-582/14, in *Dir. inform*., 2016, 748 con nota di MERLA. Sul punto interessanti le considerazioni di MONTAGNANI, op. cit., 307; DI RESTA, *La "nuova privacy" europea*, cit., 10 ss.; CEROCCHI, CORALOCCO, *op. cit.*, 387 ss.

A fronte di tali considerazioni gli indirizzi IP non furono inizialmente ricompresi nella definizione di dato personale dettata dal Legislatore. Il mancato riconoscimento nella categoria non è di poco conto, ciò infatti comporta la non applicabilità della normativa sulla *data protection*, ritenuta tra quelle maggiormente restrittive, a tutela degli interessati. Ne consegue che il distributore di contenuti di media online avrebbe potuto registrare il traffico dati degli utenti senza il rispetto dei principi generali sanciti dal GDPR, potendo finanche rivendere a terze parti dette informazioni senza il loro previo consenso.

Si è così espressa la Corte di Giustizia, specificando che anche i dati che possano permettere una identificazione indiretta degli utenti devono rientrare nella nozione di dato personale. Pertanto, essendo gli indirizzi IP dinamici dei dati che, seppur con la necessità di essere collegati a dati ulteriori in possesso di soggetti terzi, possono portare alla specifica identificazione della persona fisica, debbono rientrare nella categoria dei dati personali. L'indirizzo è stato poi trasfuso nel GDPR, ove nel Considerando n. 30[315], vengono specificamente ricompresi come esempi di identificativi online, seppure transitori, degli utenti[316].

Questo caso, che rappresenta solo un esempio delle possibili tensioni interpretative, evidenzia come la categoria di dato personale muta al progredire della tecnologia, richiedendo un'attenta valutazione anche dell'intero contesto da cui il dato viene estratto. La nozione allora appare inevitabilmente aperta a nuovi elementi di volta in volta idonei a identificare gli interessati[317].

Il tema appare di particolare importanza per il presente lavoro proprio in ragione delle capacità degli algoritmi di *data analysis* di inferire dati personali dalle correlazioni tra dati eterogenei. Dette capacità sono rese possibili anche grazie alla diffusione degli

[315] Il Considerando n. 30, reg. UE n. 679/2016, precisa che «*Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (*cookies*) o identificativi di altro tipo, quali i* tag *di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle*».

[316] Cfr. sul punto CEROCCHI, COLAROCCO, *op. cit.*, 387 ss.; DE GREGORIO, TORINO, *op. cit.*, 468 ss.

[317] MONTAGNANI, *op. cit.*, 306. Ne emerge così una classificazione di dato personale particolarmente estesa che richiama il "modello delle strategie dipendenti dal contesto", elaborato da un noto studio inglese e riportato brevemente dal nostro Garante della Privacy. Secondo detto studio il dato viene qualificato come personale perché in grado di identificare o avere effetti su di una persona in base al contesto di riferimento. Per un interessante approfondimento degli altri modelli di classificazione, compreso quello proposto dal Gruppo dei Garanti Europei per la protezione dei dati personali, si rimanda a DI RESTA, *La "nuova privacy" europea*, *ibidem*.

applicativi digitali, quali sono gli IoT, i quali creano delle *digital breadcrumbs*[318] che, collegate ad altre informazioni raccolte dal gestore della rete, consentono di re-identificare un individuo[319]. Pertanto, anche nelle applicazioni di AI ove vengano trattati dati di sistema, si pensi ad alcune tipologie di dati raccolti e trattati dalle auto *driverless*, che di per sé considerati non potrebbero dirsi "personali", possono in realtà, proprio grazie alla capacità di analisi dei sistemi informatici, portare all'identificazione di specifici soggetti. La questione non è di poco conto; sul punto un esempio potrà forse chiarirne meglio l'importanza: tra i dati di sistema di una macchina autonoma possono essere fatti rientrare anche quelli di tracciamento; proprio perché autonoma, è necessario che il percorso compiuto dalla vettura sia registrato nel sistema, dovendo questo analizzarlo per determinare le scelte di guida. Pur non essendo specificato il nome del guidatore, l'analisi di questi dati potrebbe facilmente portarne all'identificazione. Se poi quest'ultimo, perché affetto da una particolare condizione patologica, si dovesse recare in struttre specializzate, quali case di cura, centri di ribailitazione etc., si potrebbe dedurre con particolare semplicità anche informazioni sensibili concernenti il suo stato di salute. Ancora, questi dati così analizzati potrebbero essere venduti a terzi (senza il consenso dell'interessato qualora non venissero considerati come dati personali) che ben potrebbero utilizzarli per personalizzare offerte pubblicitarie non desiderate; per tacere di possibili scenari di sorveglianza globale.

Le derive legate allo sfruttamento dei dati da parte delle tecnologie *data driven* fanno dunque emergere alcuni profili di criticità legati alla sussistenza per gli utenti di un effettivo diritto al controllo dei propri dati personali. Emerge allora con chiarezza la centralità ricoperta dal GDPR nella regolazione della materia che qui ci occupa[320]. Una conferma viene anche dall'art. 2 del Regolamento ove espressamente si prescrive che esso trovi applicazione in relazione ai procedimenti totalmente o parzialmente

[318] Si fa riferimento alla felice espressione coniata da WABER, *People Analytics: How social sensing Technology will transform business and what It tells Us about the New World of Work*, New York, 2013, 6, il quale precisa come «We all leave vast traces of digital breadcrumbs on our computers: contents of documents, programme usage, and most notably the information sent to other people through e-mail messages».

[319] RABAI, *op. cit.*, 410 ss.

[320] Lo sfruttamento di dati mediante le tecnologie di Intelligenza Artificiale si basa, dunque, sia su di un uso primario, conforme allo scopo per cui sono stati raccolti, che su di un uso secondario degli stessi, di cui difficilmente si conosce l'esistenza al momento della loro raccolta. Proprio questo uso secondario fa emergere una delle maggiori criticità in merito all'effettività dell'utilizzo del GDPR per regolare la tecnologia digitale.

automatizzati[321], nonché al trattamento non automatizzato di dati personali contenuti in archivi o destinati a figurarvi[322]. La disposizione, espressione del principio di neutralità tecnologica[323] esplicitato nel Considerando n. 15[324], risponde così allo scopo di regolare la generalità di processi compiuti in modo sistematico e organizzato sui dati personali

[321] L'art. 2 definisce l'ambito di applicazione materiale del Regolamento, precisando come debbano essere assoggettati alla normativa tutti i trattamenti che siano interamente o parzialmente automatizzati, nonché quelli non automatizzati purché diretti all'uso di dati contenuti in archivi o destinati a figurarvi. L'espresso riferimento ai trattamenti automatizzati riprende quanto previsto sia dalla Convenzione 108 che dalla Direttiva CE n. 46/95, all'art. 2, lett. *b*). Ciò che emerge è l'esigenza di regolazione di un settore sempre più guidato da strumenti tecnologici e analisi sistematiche, anche qualora il trattamento dei dati personali si limiti a una loro raccolta. Sul punto sottolinea Pizzetti come il concetto di trattamento automatizzato, sebbene fosse stato riferito inizialmente agli archivi e ai trattamenti automatizzati, ha avuto una lettura estensiva, così da permetterne l'applicazione anche ai trattamenti effettuati sulla rete e nell'ambito delle comunicazioni digitali. V. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 195.

[322] Esclusi dall'ambito di operatività del Regolamento sono, dunque, quei trattamenti sostanzialmente personali o domestici. Detta visione si conferma anche in ragione della lettura estensiva che la Corte di Giustizia ha elaborato in relazione alla nozione di trattamenti domestici o personali. I Giudici hanno, infatti, ritenuto applicabile la Direttiva madre anche in caso di mera pubblicazione in un sito internet di un soggetto privato di una lista contenente dati personali. Nel caso di specie la Corte, pur avendo riconosciuto come la pubblicazione era avvenuta nel contesto di una attività di volontariato, ha chiarito come il carattere personale di un trattamento può essere invocato solo nel caso in cui l'attività svolta dal titolare rimanga all'interno della sua sfera individuale, senza alcuna espressione all'esterno, sia essa effettiva che potenziale. La Corte precisa come «*l'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa o ai loro passatempo, costituisce un trattamento di dati personali interamente o parzialmente automatizzato ai sensi dell'art. 3, punto 1, della Direttiva 95/46 CE*». Corte giust. UE, 6.11.2003, causa C-101/01, in *Dir. e giust*., 2004, 122. Per un approfondimento in merito ai trattamenti che non ricadano nell'ambito di applicazione del Regolamento si rimanda a NERVI, *op. cit.*, 167 ss.; SPAGNARO, *L'ambito di riferimento materiale del nuovo regolamento*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 23 ss.; SCORZA, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA, BELISARIO, I, Milano, 2018, *sub* art. 2, 12 ss.; ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina*, cit., 10; DI RESTA, *op. cit.*, 26 ss.

[323] In virtù di tale principio, ormai consolidato nel dibattito internazionale, «la norma giuridica deve essere tecnologicamente neutra e dunque non deve riferirsi ad una particolare tecnologia affermata in un dato momento storico. Ne consegue che la norma tecnologicamente neutra non condiziona il mercato, preferendo questa o quella tecnologia, né influenza lo sviluppo della tecnologia». FINOCCHIARO, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, cit., 238.

[324] «*Al fine di evitare l'insorgere di gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate. La protezione delle persone fisiche dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio. Non dovrebbero rientrare nell'ambito di applicazione del presente regolamento i fascicoli o le serie di fascicoli non strutturati secondo criteri specifici, così come le rispettive copertine*». Considerando n. 15, reg. UE n. 679/2016. Sul punto Proietti evidenzia come il principio in parola si declini in una protezione delle persone fisiche «neutrale sotto il profilo tecnologico, senza dover dipendere dalle tecniche impiegate; deve applicarsi allo stesso modo sia per quanto concerne il trattamento automatizzato, sia per il trattamento manuale dei dati. Il tutto per impedire l'insorgere di rischi di elusione». V. PROIETTI, *op. cit.*, 94.

degli utenti, senza correre il rischio di una veloce obsolescenza a fronte dell'evoluzione tecnologica[325].

Accertato quindi il ruolo di assoluto rilievo ricoperto dal Regolamento 679/2016 UE, pare necessaria una verifica in merito alla compatibilità degli strumenti ivi previsti con l'attuale contesto tecnologico. Punto di partenza obbligato al fine di inquadrare il fenomeno dei Big Data, e il loro trattamento mediante applicazioni di Intelligenza Artificiale, è l'analisi dei principi generali che governano il GDPR, previsti dall'art. 5, oltre che quelli di *privacy by design* e *by default*, sanciti all'art. 25, al fine di verificare possibili criticità applicative[326].

3. Il principio di limitazione delle finalità nei trattamenti operati mediante tecnologie *data driven*

Da una prima lettura del testo del Regolamento si deve constatare come l'intero assetto normativo non sembra essere pienamente compatibile con i trattamenti di dati operati mediante applicazioni di Intelligenza Artificiale. Questa disarmonia emerge infatti fin dai principi di carattere generale[327] previsti all'art. 5, rivelandosi questi ultimi quale riflesso di una visione in parte ancora legata a un contesto tecnologico caratterizzato da un rapporto lineare tra titolare e interessato.

Una particolare attenzione meritano i principi limitazione e minimizzazione, diretti a regolare il momento iniziale del trattamento, cioè il momento della selezione e della raccolta dei dati personali, in quanto, insieme al principio di limitazione della conservazione, si dimostrano essere confliggenti con le modalità di funzionamento delle tecnologie che utilizzano processi di *data mining*.

---

[325] A fronte di un mercato unico sempre più pervaso dall'utilizzo delle tecnologie, e dei rischi che questo comporta per i cittadini, ben si comprende l'esigenza di estendere il più possibile l'ambito di applicazione della normativa in parola; così come era avvenuto grazie a un'interpretazione estensiva della Direttiva madre, limitando fortemente il novero dei trattamenti esclusi. Ne discende, allora, come siano soggetti al Regolamento tutti quei trattamenti, automatizzati o non, effettuati su dati personali degli utenti posti in essere nel territorio dell'Unione Europea o che trattino dati appartenenti a cittadini europei. SCORZA, *op. cit.*, 10 s.

[326] Cfr., per una panoramica, DELL'UTRI, *op. cit.*, 187 ss.; SANTORO, *op. cit.*, 52 ss.; DE GREGORIO, TORINO, *op. cit.*, 459 ss.

[327] Secondo Piraino l'espressione "principi generali", impiegata per descrivere la norma in oggetto, non risponderebbe pienamente al suo significato tecnico. Si sottolinea, infatti, come non tutti i criteri elencati dalla disposizione esprimano «finalità ultime o valori consacrati in precetti». Si v. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Nuove leggi civ. comm.*, 2017, 379.

Andando con ordine, il principio di limitazione delle finalità, di cui all'articolo 5, lett. *b*), prescrive che i dati debbano essere raccolti «*per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità*». Il Considerando n. 39 chiarisce inoltre come detti fini debbano essere espressamente indicati al momento della raccolta, così che l'interessato possa avere contezza dell'effettivo utilizzo a cui i propri dati sono destinati.

Il principio in parola trova la sua prima espressione nella Convenzione 108, precisamente nell'art. 5, lett. *b*)[328], per poi essere ripreso integralmente dalla Direttiva 46/95 CE[329], con l'unica aggiunta della necessità che le finalità perseguite siano esplicitamente dichiarate agli interessati. Nel suo nucleo centrale, fin dalla prima formulazione, il principio è evidentemente diretto a limitare la raccolta dei dati degli utenti unicamente a quei trattamenti posti in essere per fini, predeterminati, che siano legittimi. Si ritiene dovrebbe essere accolta un'accezione in un certo senso restrittiva del termine "legittimo", dunque indicativo di quei trattamenti rilevanti in quanto diretti a realizzare interessi meritevoli di tutela; ad esempio le finalità di ricerca, ma anche quelle commerciali, espressione della libertà di iniziativa economica, possono certamente essere considerate interessi meritevoli di tutela da parte dell'ordinamento[330].

In un contesto caratterizzato da una linearità di rapporti tra titolare e interessato, quale era quello alla base della emanazione della Direttiva madre, il principio di

---

[328] L'art. 5, lett. *b*), Convenzione n. 108/1981, rubricato "Qualità dei dati", prescrive: «I *dati a carattere personale oggetto di elaborazione automatica devono essere: a. ottenuti ed elaborati lealmente e legalmente; b. registrati per fini determinati e legittimi e non devono essere utilizzati in modo incompatibile con tali fini; c. adeguati, pertinenti e non eccessivi in rapporto ai fini per i quali sono registrati; d. esatti e, se necessario, aggiornati; e. conservati sotto una forma che permetta l'identificazione delle persone interessate per un periodo non superiore a quello necessario per i fini per i quali essi sono registrati*».

[329] L'art. 6, lett. *b*), Direttiva CE n. 46/95, in merito alla qualità dei dati precisa che: «*1. Gli Stati membri dispongono che i dati personali devono essere:* […] *b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate*».

[330] Quanto al concetto di legittimità del trattamento ivi previsto si rimanda alla considerazione di Dell'Utri, il quale solleva alcune perplessità in merito alla lettura del termine che ne vede una identificazione con la liceità. Ciò in ragione del principio per cui deve ritenersi consentita ogni attività che non sia espressamente proibita o soggetta a limitazione. L'A. evidenzia, invece, come le due categorie debbano essere distinte, dovendosi ricondurre alla liceità «l'insieme degli atti o dei comportamenti destinati a non interferire, in negativo, con l'integrità degli interessi propri della generalità dei consociati»; mentre alla categoria della legittimità appartengono tutte le attività «destinate alla realizzazione degli interessi che trovano, tra le norme, quando non tra i valori di carattere generale o implicito dell'ordinamento, i segni distinguibili della considerazione o del rispetto». V. DELL'UTRI, *op. cit.*, 207 s.

limitazione delle finialità si mostrava rispondere adeguatamente alle esigenze di tutela degli interessati. Questi ultimi, infatti, informati dal titolare in merito al preciso scopo perseguito mediante l'utilizzo dei propri dati, potevano apprestare un consenso consapevole[331]. Tuttavia, con la digitalizzazione sempre più pervasiva di ogni aspetto della società, a cui è seguita la disponibilità di quantità di dati sempre maggiori, sono emerse alcune tensioni legate alle stesse modalità di trattamento. Iniziarono infatti ad essere impiegate con maggiore frequenza tecniche di *data analysis*, capaci di estrarre informazioni ulteriori dai *dataset*, rendendo così i dati utilizzabili per finalità differenti rispetto a quanto dichiarato al momento della raccolta.

Una maggiore centralità iniziò dunque ad assumere la previsione circa la "compatibilità" dei trattamenti posti in essere successivamente alla raccolta con i fini dichiarati inizialmente agli interessati; si spiega così l'aggiunta nel testo della Direttiva 46/95 CE del termine "successivamente", quale espressione dell'orientamento interpretativo ormai consolidato e diretto a ricomprendere anche tutti quei trattamenti secondari aventi fini ulteriori rispetto a quanto dichiarato inizialmente[332].

Il parametro della "compatibilità" introdotto nella Direttiva madre, e poi trasfuso nel Regolamento, se da una parte permette un'pplicazione estensiva del principio in parola, dall'altra ha tuttavia fatto emergere alcune criticità legate alla sua stessa formulazione piuttosto ampia. La scelta del legislatore europeo di non prevedere inizialmente una esplicita indicazione in merito ai requisiti di compatibilità fu evidentemente diretta a non limitare eccessivamente le prospettive di riutilizzo dei dati da parte dei titolari, oltre che all'esigenza di flessibilità e adattabilità dei criteri alle evoluzioni del mercato. Ciò, tuttavia, ha comportato un'inevitabile incertezza. Nel 2013 è così intervenuto il Gruppo di Lavoro art. 29 con l'emanazione di uno specifico parere[333]. L'Organo ha chiarito come la valutazione in merito alla compatibilità dei fini ulteriori non debba seguire criteri formalistici ma essere guidata dalla verifica in concreto circa la sussistenza di parametri quali: il rapporto tra le finalità; il contesto della raccolta; la ragionevole aspettativa dell'interessato; l'impatto degli stessi e la presenza di garanzie che

[331] V. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 246 ss.; DI RESTA, *op. cit.*, 44 ss.
[332] In merito all'ambiguità della formula prevista dall'art. 5, in merito alle finalità dei trattamenti anche in relazione alle nuove tecnologie, si v. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, in *Intelligenza Artificiale, protezione dei dati personali e regolazione*, cit., 58 ss.
[333] Gruppo di Lavoro art. 29, *Opinion 3/2013 on purpose limitation*, 2013.

permettano di ridurre l'impatto dei trattamenti ulteriori sulla sfera privata del singolo cittadino[334]. Una tale indicazione risponderebbe, secondo il parere del Gruppo, all'esigenza di una previsione flessibile ed effettiva, che permetterebbe la tutela dei diritti degli interessati senza una irragionevole compressione della libertà di iniziativa economica dei titolari del trattamento.

Le indicazioni del Gruppo di esperti vennero successivamente recepite nel testo del Regolamento, al Considerando n. 50 e all'articolo 6, ove infatti vengono espressamente ripresi alcuni indici elaborati nel parere sopra citato e diretti a parametrare la compatibilità dei trattamenti ulteriori[335]. Si tratta tuttavia di una previsione in parte ancora generica, tale da renderne la stessa applicazione piuttosto incerta. La normativa così formulata, difatti, permette al titolare, a cui solo spetta la valutazione, di allargare in misura molto ampia la finalità dei trattamenti, potendosi così allontanare anche molto da quanto dichiarato al momento della raccolta[336].

L'unica presunzione di compatibilità espressamente contemplata è rivolta ai trattamenti posti in essere a fini di archiviazione nel pubblico interesse, a fini statistici, storici o di ricerca scientifica[337]. In questi casi, infatti, il legislatore ha ritenuto sempre legittimo il riutilizzo delle informazioni, purché vengano garantite tutele adeguate per i cittadini, di cui viene data una espressa indicazione all'art. 89, ove si fa riferimento alla possibilità di utilizzare tecniche di anonimizzazione o pseudonimizzazione, mezzi ritenuti idonei a tutelare i diritti degli interessati. Al contempo tuttavia si concede agli

---

[334] Cfr. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 250 ss.

[335] «*Laddove il trattamento per una finalità diversa da quella per la quale i dati personali sono stati raccolti non sia basato sul consenso dell'interessato o su un atto legislativo dell'Unione o degli Stati membri che costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia degli obiettivi di cui all'articolo 23, paragrafo 1, al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento tiene conto, tra l'altro: a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione*». Art. 6, p. 4, reg. UE n. 679/2016.

[336] PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 59.

[337] Il legislatore qualifica, dunque, detti trattamenti come *ex lege* non incompatibili con le finalità originarie. In continuità con la previgente disciplina, proprio in ragione della necessità di salvaguardare interessi di particolare valore, si giustifica un parziale sacrificio dei diritti dei singoli. Cfr. DELL'UTRI, *op. cit.*, 209; DE GREGORIO, TORINO, *op. cit.*, 461 ss.

Stati un ampio potere di deroga dei diritti previsti dal Regolamento, qualora essi pregiudichino gravemente il conseguimento delle finalità di pubblico interesse.

La previsione si mostra dunque evidentemente molto ampia, lasciando ancora una volta al titolare una libertà di valutazione particolarmente estesa in merito alle misure da apprestare per garantire i diritti dei singoli. La diffusione sempre più estesa di usi secondari, ritenuti dai titolari compatibili con quanto dichiarato al momento della raccolta, comporta inevitabilmente una profonda perdita di controllo dei propri dati da parte degli utenti, i quali si trovano allora ad essere di fatto soggetti a trattamenti in modo sempre più inconsapevole. Ciò appare ancora più evidente nel caso di utilizzo di tecnologie digitali ove finanche la determinazione dello scopo primario del trattamento risulta di difficile previsione.

Così chiarita la portata applicativa, dato il carattere estremamente flessibile della valutazione di compatibilità richiesta al titolare, la formulazione del principio in parola, sebbene di fatto permetta lo sviluppo e l'utilizzo delle tecniche di *data anlysis*, non sembra pienamente efficiente a governare l'evoluzione tecnologica che guida il mercato digitale. Le stesse modalità di funzionamento degli algoritmi sembrano, infatti, mostrare una certa conflittualità con il principio in parola; ciò soprattutto in una prospettiva di tutela dei diritti fondamentali degli interessati[338].

Come visto, i moderni trattamenti sono tendenzialmente diretti a raccogliere e conservare tutti i dati prodotti, non procedendo ad una scelta né in termini di quantità né operando una valutazione nel merito degli stessi. La vera ricchezza dei dati risiede proprio nella loro versatilità di utilizzo, non potendo così il titolare sempre prevedere, a priori, a quali finalità potranno essere destinati.

La visione di un trattamento diretto al perseguimento di scopi ben precisi e determinati compiutamente a priori si dimostra in parte espressione obsoleta e non più in linea con il trattamento dei dati di massa, ove invece si assiste ad una vera e propria catena di trattamenti, aventi diverse finalità che si vanno determinando in seguito all'analisi che dei dati viene fatta[339]. Inoltre, potendo uno stesso *dataset* essere usato per

---

[338] PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, *ibidem*; ID., *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 249.

[339] MULA, *Elaborazione e sfruttamento dei dati mediante algoritmi*, in *La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele*, cit., 127 ss. DE GREGORIO, TORINO, *op. cit.*, 460 ss., secondo gli Autori il principio in parola potrebbe del pari costituire un argine allo sviluppo di monopoli e di situazioni dominanti nel mercato. Tuttavia si ritiene altresì necessaria un'attenta ponderazione, in quanto la

il perseguimento di scopi differenti, cambiando gli algoritmi di analisi mediante cui scoprire correlazioni tra le variabili, particolari difficoltà si riscontrano in merito ai cosiddetti dati inferiti, o meglio alle informazioni che vengono inferite dai dati raccolti. Le finalità qui si vanno definendo durante l'arco del trattamento stesso, non potendosi preventivare al momento della raccolta quali informazioni potranno essere ricavate e, di conseguenza, l'utilizzo delle stesse[340]. A ciò si aggiunga come esistono modelli di business diretti a raccogliere dati da rivendere a imprese terze, aventi evidentemente finalità di cui il titolare che ha dato origine al primo trattamento non ha, né può avere, contezza al momento della raccolta[341].

Il rischio concerto è dunque la progressiva perdita di controllo dei propri dati da parte degli interessati, diritto questo riconosciuto, si ricorda, quale diritto fondamentale dell'uomo e di cui il GDPR dovrebbe rappresentare espressione massima di garanzia. Ci si domanda quale controllo possa residuare per l'utente/interessato se egli non ha contezza degli usi a cui i propri dati sono destinati; il problema si mostra sempre più attuale proprio in relazione all'impiego di tecniche di Intelligenza Artificiale che si fondano sul *data mining*. Come visto, l'obiettivo di dette tecniche è proprio quello di far emergere informazioni, trovare correlazioni, spesso dirette a creare *cluster* di dati per fare previsioni. Si è ricordato in apertura del presente lavoro come questa modalità di funzionamento non permette di prevedere dal principio, e a priori, quali saranno gli usi a cui i dati raccolti verranno destinati; ciò sia perché uno stesso *dataset* può essere usato per molteplici scopi, differenti algoritmi potranno far emergere differenti correlazioni,

---

limitazione dello scopo della raccolta potrebbe limitare lo sviluppo di capacità di previsione e creazione di modelli, così limitando anche la stessa portata innovativa dei Big Data. Dette considerazioni appaiono certamente fondate, difatti una rigida applicazione del principio comporterebbe un detrimento per lo stesso mercato delle tecnologie digitali, in quanto la limitazione degli sbocchi innovativi scoraggerebbe anche potenziali investimenti nel settore.

[340] Le preoccupazioni in merito alla compatibilità del principio con l'utilizzo di dati "derivati" è stata recentemente oggetto di riflessione del Consiglio d'Europa. Nella declarazione del 13 febbraio 2019 viene, infatti, sottolineato il crescente utilizzo di dati derivati nell'addestramento degli algoritmi di Intelligenza Artificiale, diretti a riconoscere correlazioni statistiche al fine di creare profili utenti sempre più particolareggiati. V. Consiglio d'Europa, *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*, 13 febbraio 2019. In argomento FINOCCHIARO, *Riflessioni su intelligenza artificiale e protezione dei dati*, cit., 245 s.

[341] In particolare, per i trattamenti mediante applicazioni di Intelligenza Artificiale si veda ANGELINI, *Intelligenza Artificiale e* governance*. Alcune riflessioni di sistema*, in *Intelligenza Artificiale, protezione dei dati*, cit., 293 ss. Interessanti anche le considerazioni di Mula in merito all'uso che viene fatto dei dati raccolti. L'A. evidenzia come oltre ai c.d. *first party data*, cioè quei trattamenti che gli operatori pongono in essere sui *data* dagli stessi posseduti, i titolari sono alla ricerca continua di nuovi dati (compresi metadati), ricavabili non solamente dai propri canali ma anche dall'acquisto di dati da terzi. V. MULA, *op. cit.*, 133.

ma soprattutto perché spesso solo a seguito dell'analisi dei dati sarà possibile determinare a quali usi destinare il patrimonio informativo acquisito.

Sono proprio gli usi secondari che dunque mostrano tutte le fragilità del principio in parola, quanto meno nella sua attuale formulazione. Da questa infatti ne discende la predisposizione di informative estremamente generiche, ove si fa riferimento a finalità di marketing, di profilazione o anche solo alla cessione di dati a terze parti senza altre precisazioni, così trasformando il consenso in un mero simulacro. Per contrastare detta prassi si è proposto di rendere necessaria la richiesta di un nuovo consenso in caso di uso ulteriore che non possa dirsi astrattamente compatibile con quanto dichiarato al momento della raccolta. Le difficoltà di questa soluzione sono evidenti, non solo perché si rimanda ancora una volta al parametro di compatibilità, che come visto comporta inevitabili incertezze applicative, ma soprattutto alla luce delle dinamiche di mercato sopra richiamate. Se, infatti, potrebbe essere in alcuni casi astrattamente più agevole provvedere ad una nuova richiesta di consenso, come nel caso in cui sia lo stesso titolare a porre in essere trattamenti secondari; qualora invece si tratti di un soggetto terzo appare di tutta evidenza la complessità di realizzazione della misura, potendo finanche risultare sproporzionata in relazione allo scopo. Ciò in quanto le modalità di raccolta e conservazione non rendono sempre possibile risalire a monte a tutti gli interessati. Come visto, i dati non solo sono quantitativamente enormi ma anche grandemente differenziati, provenendo da una moltitudine di diverse "sorgenti", come dimostrato dalla varietà di formati di raccolta. Diviene allora complesso ipotizzare che un titolare possa riuscire a raccogliere, in un momento potenzialmente anche molto successivo alla prima raccolta, il consenso di tutti i singoli interessati.

4. I principi di minimizzazione e limitazione della conservazione

Considerazioni in parte analoghe possono essere fatte in merito al principio di minimizzazione dei dati, previsto alla lettera "c" della medesima disposizione, il quale è

funzionalmente legato ad un ulteriore principio, quello di limitazione della conservazione[342].

Il testo prevede che i dati raccolti debbano essere adeguati, pertinenti e limitati (anche nel tempo di conservazione), a quanto strettamente necessario al perseguimento delle finalità dichiarate. Anche detta disposizione riprende quanto già previsto dalla Direttiva, e prima ancora dalla Convenzione 108 da cui si discosta per una sostituzione, più formale che sostanziale, del principio di non eccedenza con quello di limitazione. Sul punto un'importante precisazione viene dal Considerando n. 39 ove si chiarisce che i trattamenti dovrebbero involgere i dati personali solamente quando le finalità perseguite non possano essere ragionevolmente conseguite in altro modo. Ne discende dunque un *favor* nei confronti di quei procedimenti che non permettono la re-identificazione dell'interessato[343].

Dal combinato disposto delle disposizioni richiamate emerge pertanto come nell'articolazione del principio di minimizzazione si intreccino profili sia quantitativi che qualitativi. La previsione del canone della pertinenza (e adeguatezza) attiene alla necessaria presenza di un nesso eziologico tra il dato raccolto e le finalità perseguite, dovendo questo sussistere per tutto l'arco temporale del trattamento. Quanto ai profili quantitativi, il canone della limitazione impone di circoscrivere l'ambito delle operazioni ai soli dati personali che siano indispensabili allo scopo perseguito, dovendo ricorrere, dove possibile, primariamente a dati anonimizzati o pseudonimizzati. Qualora dunque l'utilizzo di dati così trattati sia idoneo a limitare l'impatto nella sfera del singolo, si è sostenuto come lo stesso principio di pertinenza imponga un vero e proprio obbligo di trattamento pseudonimizzato o anonimizzato[344]. L'utilizzo di queste tecniche si ritiene possa limitare i rischi di possibili danni nei confronti degli interessati, in quanto i dati così trattati non sarebbero direttamente e "facilmente" re-indirizzabili alla singola persona fisica a cui sono riferiti. Come si vedrà nel prosieguo, lo stesso

[342] L'art. 5, lett. *c*), reg. UE n. 679/2016, prescrive che i dati personali debbano essere «*c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»)*».

[343] Una conferma deriverebbe anche da una lettura attenta del principio di pertinenza, fin dalla sua formulazione nella Direttiva CE n. 46/95. Sul punto Pizzetti sottolinea che se in relazione alle finalità perseguite possono essere trattati dati pseudonimi, «allora il principio di pertinenza […] specialmente con riferimento ai sistemi informatici o ai programmi informatici […], può giustificare o addirittura imporre il trattamento pseudonimizzato dei dati». V. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 257. Dello stesso parere anche DI RESTA, *op. cit.*, 48 s.

[344] Si v. DELL'UTRI, *op. cit.*, 209 ss.

legislatore europeo dedica una particolare attenzione a queste tecniche, e, in particolare, a quelle di anonimizzazione, ritenendole strumenti idonei a garantire la sicurezza dei dati, fino ad escludere dall'orbita del Regolamento i dati risultati anonimi.

Si conviene che ove correttamente utilizzate queste tecniche permettano effettivamente di ridurre il rischio di possibili esternalità negative per gli utenti, in particolare in caso di *data breach* a cui possono seguire conseguenze pregiudizievoli per gli individui anche in relazione alla tutela della riservatezza delle proprie informazioni. Tuttavia, come si vedrà, è necessario prestare attenzione soprattutto per quanto riguarda i dati resi "anonimi", in quanto ad essi verrebbero accordate minori tutele, non essendo ai *dataset* così identificati applicabili le garanzie apprestate dal GDPR[345].

Continuando nell'analisi del principio di minimizzazione, è fin da subito opportuno chiarire come le considerazioni in merito al funzionamento delle applicazioni *data driven*, come sopra riportate, evidenzino una particolare criticità proprio nel momento della raccolta dei dati, rendendone l'applicazione in detta fase problematica. Si è infatti visto come i sistemi di Intelligenza Artificiale si fondino, quanto meno il *machine learning*, su di una raccolta e un uso massivo dei dati, senza una selezione né quantitativa né qualitativa; ciò in quanto non potendo prevedere quali saranno le correlazioni che il sistema troverà non è possibile operare a priori una limitazione degli *input* forniti alla macchina. Anzi, la ricchezza dei sistemi *data driven* risiede proprio nella capacità di far emergere correlazioni da dati differenti, trovando ricorrenze statistiche che un analista umano difficilmente troverebbe.

A fronte di queste considerazioni autorevole dottrina ha sostenuto come il principio in parola debba invece trovare un'ampia applicazione nelle fasi successive del trattamento[346]. Questo, infatti, dovrebbe operare durante tutto l'arco del trattamento e, in particolare, nelle fasi successive alla raccolta, tra le quali rientra anche la cessione a terzi dei dati; proprio in quest'ultima fase, si sostiene, assumerebbe un ruolo rilevante il principio in analisi. In forza di questo il titolare dovrebbe infatti limitare la trasmissione unicamente ai dati che siano strettamente necessari al singolo trattamento successivo. In questa prospettiva il principio di minimizzazione potrebbe allora assumere centralità nel

[345] Si rimanda *infra* al §3, capitolo 2, dedicato alla regolazione dei dati non personali.
[346] Si v. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 119 s.

controllo delle applicazioni di Intelligenza Artificiale, le quali sono caratterizzate da una complessa e lunga catena di trattamenti[347].

Dette considerazioni sono certamente condivisibili per alcune modalità di trattamento, tuttavia appare difficile ipotizzarne una generica applicazione. Come visto, il titolare non sempre può operare una selezione dei dati, non potendo astrattamente identificare a priori quelli unicamente diretti a raggiungere gli obiettivi prefissati, a maggior ragione se essi sono trasmessi a un terzo. Queste difficoltà sono legate *in primis* alla varietà di provenienza dei dati, oltre che alla quantità degli stessi. Si ricorda che le tecnologie *data driven*, come visto, per funzionare in modo efficiente ed efficace necessitano di un numero sempre crescente di dati da processare[348]. A differenza che nel passato, ove gli analisti scartavano i dati ritenuti irrilevanti, nel caso dei Big Data la raccolta e l'analisi non viene più effettuata su di un campione selezionato ma sull'intero insieme dei dati. Detto cambiamento è addebitabile in parte all'aumento della capacità di memoria delle macchine, ma soprattutto alla considerazione per cui anche dati in apparenza irrilevanti possano in realtà acquistare valore nell'insieme aggregato[349]. La forza della tecnologia, anzi, risiede proprio in questo: la capacità di trovare correlazioni in un'enorme quantità di dati e così facendo generare ricchezza. È proprio la composizione dei Big Data a rendere possibile l'emersione di *pattern*, di correlazioni statistiche, senza che sia possibile indentificare nello specifico quali dati abbiano più peso degli altri.

Un esempio potrà forse aiutare a comprendere l'estrema difficoltà di applicazione di questi principi nell'attuale società digitale. É ormai di dominio pubblico la presenza sul mercato di algoritmi deputati a creare un *credit score* che misuri l'affidabilità creditizia degli individui. Questi algoritmi vengono comunemente impiegati nelle società di credito a supporto degli operatori finanziari. I dati che vengono processati e che concorrono a "creare" questo punteggio sono vari, ma il procedimento rimane

[347] Si v. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, *ibidem*.
[348] Sul punto le considerazioni di Pizzetti, il quale ne sottolinea l'importanza nella regolazione delle tecniche di Big Data. Ciò in quanto evidentemente meno dati si utilizzano e minori saranno i rischi per gli interessati. Tuttavia l'A. ritiene che detto principio debba essere necessariamente coordinato con quello di esattezza, dal momento che il rischio di danni causati da trattamenti operati mediante applicazioni *data driven* deriva altresì dall'uso di dati errati e incompleti. É evidente che anche qualora vengano utilizzati solamente quei dati necessari al trattamento, ma essi risultino sbagliati, si ricade ugualmente nel rischio di provocare errori nel comportamento delle macchine, da cui ben potrebbero derivare danni agli utenti finali. V. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 62 s.
[349] DE GREGORIO, TORINO, *op. cit.*, 462 ss.

monitorato in ragione del carattere sensibile degli stessi. Tuttavia, soprattutto oltreoceano, questi punteggi vengono trattati come dati vicarianti e utilizzati insieme ad altre informazioni per formare i cosiddetti *bucket* (panieri) entro cui categorizzare gli individui al fine di predirne il comportamento per le più svariate finalità. Uno studio del 2015 ha mostrato come le compagnie di assicurazione utilizzassero i *credit score* tra i parametri diretti a determinare i premi assicurativi per la RC auto, più che i dati relativi alla qualità della guida. In Florida, adulti senza nessuna segnalazione sulla patente, ma con un'affidabilità creditizia bassa, si sono trovati a pagare un premio assicurativo maggiore rispetto ad automobilisti con un'ottima affidabilità creditizia ma con una condanna per guida in stato di ebrezza[350].

Questo esempio mostra come siano oggi i dati *proxy*, i dati indiretti, e i collegamenti emersi dalla loro analisi, ad essere sempre più utilizzati per perseguire l'obiettivo del titolare del trattamento. Emerge dunque l'estrema difficoltà di compiere una selezione sia sulla quantità che nel merito di quali dati raccogliere, rendendo di fatto i principi di minimizzazione e di limitazione delle finalità non in linea con una concezione moderna del trattamento.

A completare il quadro, una particolare connessione viene fatta con il principio di limitazione nella conservazione dei dati. Il legislatore europeo, nella lettera *e*) dell'art. 5[351], impone che i dati personali siano conservati per il tempo strettamente limitato al conseguimento delle finalità sottese al trattamento. Sul punto lo stesso Considerando n. 39[352] precisa come il titolare debba stabilire un termine preciso per la cancellazione o

[350] O'NEIL, *op. cit.*, 240 ss.

[351] L'art. 5, lett. *e*), reg. UE n. 679/2016, prevede che i dati personali debbano essere «*e) 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»)*»;

[352] Sul punto il Considerando n. 39, reg. UE n. 679/2016, precisa che «[…] *I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica*».

per la verifica periodica del permanere della necessità dei dati per le finalità perseguite[353].

Le difficoltà, sopra ricordate, in merito alla definizione delle finalità da perseguire nel momento della raccolta dei dati si intrecciano strettamente con le considerazioni in merito ai principi di minimizzazione e di limitazione della conservazione. Tuttavia, qui esse sembrano finanche più acuite dal momento che mostrano una tensione sempre crescente con le tecniche di Intelligenza Artificiale. Pur ammettendo che sia possibile determinare a priori gli scopi a cui destinare la raccolta e l'analisi dei Big Data, non è infatti sempre agevole stimare un termine per l'utilizzo dei *dataset*, essendo questi spesso soggetti a riutilizzo da parte di terzi, oltre che nell'addestramento degli algoritmi di Intelligenza Artificiale. Come visto, infatti, cambiando i parametri degli algoritmi di analisi possono emergere correlazioni prima nascoste e da queste è possibile estrarre nuova ricchezza.

Ulteriori difficoltà sorgono poi per i dati raccolti per finalità di ricerca scientifica. La stessa natura dell'attività non permette di stabilire a priori un periodo di conservazione predeterminato, potendo notoriamente la ricerca necessitare di tempi anche molto lunghi. Nella consapevolezza delle peculiarità di questi trattamenti all'art. 5, lett. *e*), il legislatore ha previsto una parziale eccezione. La disposizione prevede dunque che i dati trattati per finalità di archivio storico, analisi statistica e ricerca scientifica possano essere conservati per tempi più lunghi, nel rispetto delle garanzie previste dall'art. 89 GDPR. Sul punto anche la nostra Autorità Garante per la privacy, nell'indagine conoscitiva sui Big Data, ha sottolineato la possibile tensione nascente tra il principio in parola e le finalità di ricerca[354]. Per limitare a monte possibili conflitti destinati ad incidere negativamente su dette attività, lo stesso art. 89 incoraggia l'uso di tecniche che non permettano l'identificazione degli interessati, purché ciò sia compatibile con le finalità del trattamento, lasciando infine alle singole normative nazionali la previsione di possibili deroghe per il settore.

Appare evidente come per alcuni settori, tra cui quello medico, risulti molto complesso operare una anonimizzazione, e in parte anche una pseudonimizzazione, dei

[353] F. RESTA, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA, BELISARIO, I, Milano, 2018, *sub* art. 5, 58 ss.; PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 264 ss.; SANTORO, *op. cit.*, 55 ss.
[354] AGCom, *Indagine conoscitiva sui Big Data*, cit.

dati mantenendo al contempo una loro utilità ai fini della ricerca. Inoltre, la stessa libertà concessa agli Stati membri potrebbe comportare una disarmonia tra gli ordinamenti, finendo così per essere di ostacolo alla stessa ricerca scientifica, che invece necessita di normative uniformi che permettano l'interoperabilità dei dati e il coordinamento tra enti e istituti.

Se, dunque, la determinazione di un termine preciso di utilizzo dei dati non pare opera semplice, lungimirante si mostra invece la previsione di una verifica circa il loro utilizzo temporalmente scadenzata. Questa indicazione, più delle altre, potrebbe essere diretta a misurare e controllare i trattamenti e dunque verificare la continua compatibilità con le misure a tutela degli interessati; a tutta vista più efficacemente che l'indicazione di previsioni *ex ante* di difficile applicabilità. In alcuni casi determinati, inoltre, il legislatore ha previsto un esplicito meccanismo di controllo periodico; si pensi per esempio all'art. 45, rubricato "trasferimento sulla base di una decisione di adeguatezza", che sancisce un obbligo di riesame almeno ogni quattro anni dell'adeguatezza delle misure di protezione di uno Stato terzo.

Proprio alla luce delle prassi operative del mercato digitale, la previsione di verifiche periodiche appare meritevole di una più ampia declinazione all'interno del dettato normativo. La veloce evoluzione del settore necessita infatti di un controllo puntuale della compatibilità e dell'efficacia degli strumenti introdotti dal GDPR; esigenza che emerge soprattutto per quei trattamenti che hanno posto in essere misure di pseudonimizzazione e anonimizzazione.

Sarebbe stata forse opportuna una previsione, sulla scorta di quanto indicato all'art. 45, di un esteso e temporalmente scadenzato controllo periodico che ricomprenda una verifica del rispetto di tutte le previsioni dal Regolamento: dalla valutazione di impatto, all'informativa sul trattamento, all'efficacia delle tecniche di anonimizzazione etc. Una previsione di tal fatta si mostrerebbe un efficace strumento non solo direttamente rivolto a garantire la tutela degli interessati, ma anche quale diretta concretizzazione del principio di *accountability*. La responsabilizzazione del titolare dovrebbe, infatti, comprendere un obbligo di controllo costante e soprattutto espressamente cadenzato, non lasciato alla sua libera determinazione, così da garantire un perimetro di sicurezza necessario per tutta la durata del trattamento.

Se i principi sopra richiamati si sono dimostrati, come visto, potenzialmente in conflitto con l'attuale contesto digitale, preme sottolineare come nello stesso articolato siano previsti altri canoni che invece si dimostrano efficaci nella regolazione del fenomeno dei Big Data, e di cui quindi parrebbe opportuna una maggiore valorizzazione. Si tratta dei principi di esattezza, integrità, riservatezza e responsabilizzazione[355].

5. Il principio di integrità e riservatezza alla prova dei fenomeni di *data breach*

Di primaria importanza nel contesto tecnologico attuale si dimostra il principio di integrità e riservatezza, in quanto diretto a ridurre i rischi di episodi *data breach*, a cui sempre più spesso si assiste[356]. Il rilievo attribuito alla sicurezza costituisce una novità rispetto a quanto previsto dalla Direttiva, nella quale il riferimento a misure tecniche adeguate al rischio veniva compreso unicamente in un Considerando[357].

Il legislatore ha inteso ora incorporare il parametro della sicurezza all'interno di tutti i trattamenti. L'idea di sicurezza diviene parte stessa del trattamento e parametro di valutazione della responsabilità del titolare, così come previsto dall'art. 24[358]. La *ratio* di tale scelta risiede nella necessità di garantire misure tecniche di protezione dell'integrità dei dati, oltre che delle reti, e ciò in ragione della fragilità derivante dalla circolazione sempre più estesa dei *dataset*.

Caratteristica, e per un certo senso fortuna, della rete è proprio il suo essere accessibile a una platea indistinta di soggetti. Se ciò garantisce efficienza nei traffici,

---

[355] Sul principio di responsabilizzazione si rimanda alle considerazioni *infra* §5, capitolo 4, in tema di responsabilità del titolare del trattamento.

[356] L'art. 5, lett. *f*), reg. UE n. 679/2016, prescrive che i dati debbano essere «*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)*».

[357] Il Considerando n. 46, Direttiva CE n. 46/95, precisa che «*considerando che la tutela dei diritti e delle libertà delle persone interessate relativamente al trattamento di dati personali richiede l'adozione di adeguate misure tecniche ed organizzative sia al momento della progettazione che a quello dell'esecuzione del trattamento, in particolare per garantirne la sicurezza ed impedire in tal modo qualsiasi trattamento non autorizzato; che spetta agli Stati membri accertarsi che il responsabile del trattamento osservi tali misure; che queste devono assicurare un adeguato livello di sicurezza, tenuto conto delle conoscenze tecniche e dei costi dell'esecuzione rispetto ai rischi che i trattamenti presentano e alla natura dei dati da proteggere*».

[358] PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 57 e 166 s.

dall'altro lato aumenta il rischio di attacchi esterni, diretti non solo ad acquisire informazioni riservate, ma anche a impedire il funzionamento delle reti stesse[359].

Ben si comprende allora come il tema generale della *cybersecurity*[360] rivesta oggi un ruolo fondamentale, in ragione delle possibili esternalità negative non solamente per i diritti dei singoli, ma anche per l'intera collettività[361]. È necessario sottolineare in via preliminare come il profilo della sicurezza non coincida con la protezione dei dati e la tutela della riservatezza. Difatti, come visto, questi ultimi non sono diritti assoluti, potendo dunque essere derogati per perseguire differenti interessi del pari meritevoli di tutela, tra i quali ben potrebbe rientrare la sicurezza. Sulla scorta di queste considerazioni si può pensare, per fare un esempio attuale, alle applicazioni di tracciamento dirette a monitorare il contagio da Covid-19, il cui funzionamento postula una necessaria compressione dei diritti alla privacy e alla tutela dei dati in virtù di un interesse ritenuto prevalente, in questo caso la salute pubblica[362]. Ma si può fare riferimento anche ad applicazioni di monitoraggio della popolazione che attraverso tecniche di riconoscimento facciale, già in uso in diversi ordinamenti, sono dirette a reprimere la criminalità organizzata e di stampo terroristico.

---

[359] Già nel 1973 Rodotà sottolineava l'aumento di un rischio di appropriazione di informazioni rilevanti facilitato, rispetto al passato, dalla conservazione in un unico spazio di un'enorme quantità di dati a cui poter accedere con relativa facilità. V. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit.

[360] Il concetto di *cybersecurity* trova diverse declinazioni in ragione sia delle finalità che delle stesse politiche di sicurezza adottate dagli Stati. Una nozione sufficientemente ampia, maggiormente in linea con i fini del presente lavoro, definisce la materia come «quell'insieme di tecnologie, programmi, processi e tecniche concepiti e messi in atto per proteggere dispositivi, dati e reti informatiche». V. CONTALDO, PELUSO, *Cybersecurity*, Pisa, 2018, 8.

[361] Il tema è molto vasto e tocca prospettive legate anche alla repressione dei crimini e al terrorismo, di cui non è possibile fare una disamina. Per un approfondimento in merito alla sicurezza informatica e alle ricadute che possono involgere le applicazioni aventi Intelligenza Artificiale si rimanda a BENEDETTI, *op. cit.*, 239 ss.

[362] Ai sensi dello stesso GDPR è possibile derogare alle previsioni circa la protezione di dati in particolari eventualità, tra cui la necessità di tutelare la sanità pubblica (art. 9, par. 2, lett. *h*)), ferma la necessità di apprestare idonee garanzie per i diritti degli interessati. Sul punto, infatti, precise indicazioni sono state fornite dal EDPB, il quale ha emanato delle specifiche linee guida (Guidelines *04/2020 on the use of location data and contact tracing tools in the context of COVID-19*). Inoltre in punto di compatibilità con le previsioni normative europee si è espresso anche il nostro Garante della privacy (Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni, 2020). É evidente che un'applicazione che registra i dati di localizzazione e di salute degli interessati, per poi comunicare un *alert* in caso di contatto con soggetti risultati positivi, necessiti di attente garanzie per i cittadini, non fosse altro che per la natura estraneamente sensibile dei dati raccolti. Se il diritto alla privacy e alla protezione dei dati fosse un diritto assoluto non sarebbe possibile in alcun modo trattare questa tipologia di informazioni personali, se non per fini direttamente legati alla salute del singolo individuo. La previsione di possibili deroghe in ragione di un interesse parimenti meritevole di tutela, quale è la salute pubblica, ne dimostra ancora una volta il carattere necessariamente relazionale dello stesso; la sicurezza del singolo, dunque, trova una limitazione nella sicurezza collettiva. Si v. le interessanti considerazioni di GAMBINO, MULA, *op. cit.*, 30 ss.

Alle finalità di tutela della sicurezza e incolumità pubblica si affiancano, tuttavia, rischi di un controllo pervasivo della popolazione diretto alla repressione politica o alla marginalizzazione culturale; si pensi alla denuncia della comunità internazionale in merito all'uso da parte del governo cinese di strumenti di riconoscimento facciale per individuare la popolazione degli Uiguri[363].

Accanto ai profili di sicurezza pubblica emergono anche profili di sicurezza delle reti e delle comunicazioni da possibili attacchi esterni, di cui oggi si sente sempre più spesso parlare e che hanno richiamato l'attenzione circa le misure necessarie a garantire "l'incolumità" dei dati raccolti e trattati. L'urgenza di misure di sicurezza è stata avvertita non solo per le imprese, ma anche per il settore pubblico; anzi, il problema diviene ancora più critico proprio per quanto riguarda le comunicazioni con le infrastrutture pubbliche[364]. Al fine di garantire comunicazioni certe e sicure si è proposta l'introduzione di chiavi crittografiche, e di infrastrutture c.d. PKI (*Public Key Infrastructure*)[365]; strumenti questi che permetterebbero una verifica dell'identità e della

[363] La persecuzione dei cittadini cinesi di etnia uigura, appartenenti al credo islamico, è oggetto di attenzione sul panorama internazionale. L'uso della tecnologia AI ai fini di monitoraggio della popolazione non è nuova nel panorama cinese; recentemente il colosso cinese Huawei ha pubblicato un report, poi rimosso dal sito dell'azienda a seguito di un articolo del Washington post, in cui annunciava lo sviluppo di un software di riconoscimento facciale che permette di tracciare la popolazione indicandone sesso ed etnia; inoltre il programma è programmato per inviare direttamente un alert alla polizia in caso di riconoscimento di una persona di etnia uigura. Per un approfondimento si rimanda all'articolo di HARWELL, DOU, *Huawei tested AI software that could recognize Uighur minorities and alert police, report says*, 8 dicembre 2020, consultabile all'indirizzo: *www.washingtonpost.com* (ultimo accesso 23 maggio 2021). In tema si rimanda anche a MOZUR, *One month, 500,000 face scans: how China is using A.I. to profile a minority*, 14 aprile 2019, consultabile all'indirizzo: *www.nytimes.com* (ultimo accesso 23 maggio 2021); SOL, *Come la Cina usa l'intelligenza artificiale per controllare gli uiguri*, 15 aprile 2019, consultabile all'indirizzo: *www.ilsole24ore.com* (ultimo accesso 23 maggio 2021); *La Cina userà il riconoscimento facciale per identificare gli uiguri?*, 20 dicembre 2020, consultabile all'indirizzo: *www.ilpost.it* (ultimo accesso 23 maggio 2021); LUPIS, *Allarme etnico. Aumenta la repressione degli uiguri in Cina: con l'auto di Huawei*, 10 dicembre 2020, consultabile all'indirizzo: *www.huffingtonpost.it* (ultimo accesso 23 maggio 2021); ID., *Dalla* face detenction *ai droni uccello, in Cina è dittatura*, 31 marzo 2021, *ivi* (ultimo accesso 23 maggio 2021).

[364] Non sono mancati, sul punto, interventi del legislatore europeo diretti a implementare la sicurezza anche delle reti. Di particolare rilevanza la Direttiva UE 680/2016; la proposta di revisione del Regolamento UE *e-privacy* in luogo della Direttiva CE 58/2002, oltre che la Direttiva UE 1148/2016 in materia di sicurezza delle reti e dei sistemi informativi. Quest'ultima assume centralità in quanto diretta nello specifico a disciplinare l'obbligo di adozione di misure di sicurezza relativo anche ai dispositivi interconnessi e ai dati (sia personali che non) necessari all'erogazione di servizi di carattere essenziale.

[365] L'infrastruttura a chiave pubblica permettere di certificare l'identità dei soggetti da cui provengono i messaggi. La crittografia permette la sicurezza nelle comunicazioni; si ha infatti la certezza di comunicare un messaggio che può essere letto solo da chi possiede la chiave crittografica necessaria a decifrarlo, nulla ci dice circa l'identità di chi possiede la chiave pubblica. Al fine di ovviare a detta incertezza si è proposta la cosiddetta PKI, la quale permetterebbe di garantire che la persona che distribuisce una chiave pubblica sotto una certa denominazione sia effettivamente chi dichiara di essere. Questa chiave di sicurezza si dimostra particolarmente importante nei collegamenti effettuati nella c.d. *smart road*, ove chiaramente appare necessario garantire non solamente l'integrità dei messaggi inviati e ricevuti dall'infrastruttura ma

integrità delle comunicazioni sia per chi trasmette i messaggi che per chi li riceve. Attenzione inoltre è stata dedicata ai rischi per i *device* che appartengono agli IoT; le fragilità derivano, come già sottolineato, direttamente dal loro collegamento pressoché costante alla rete internet. La presenza di misure di sicurezza adeguate appare dunque necessario proprio in ragione della sempre maggiore pervasività di detti strumenti nella quotidianità dei cittadini; esigenza che trova una particolare urgenza per quelle applicazioni che raccolgono dati sensibili quali per esempio i *wearable devices* che trattano, tra gli altri, anche dati relativi alla salute degli utenti[366].

É esperienza ormai comune come la connessione continua alla rete possa comportare alcune vulnerabilità, soprattutto nel momento della trasmissione delle informazioni. Gli attacchi alla sicurezza delle reti e dei dati sono molto diffusi ed estremamente vari. I dati statistici sulla sicurezza informatica mostrano che sempre più spesso gli utenti divengono complici inconsapevoli al compimento di attività illegali, fungendo da vettore per gli attacchi diretti alla confidenzialità dei messaggi, all'integrità degli stessi e alla disponibilità delle reti[367].

Solo per dare un'idea della diversità e complessità delle tecniche di *data breach*, si pensi, tra quelle più conosciute: alla scansione delle porte[368]; al *phishing*[369]; al

altresì l'identità stessa dei soggetti che interagiscono. Semplificando, detta infrastruttura, che si compone non solamente di software e hardware, ma anche di persone fisiche, emette dei certificati digitali che garantiscono l'identità di chi è associato alla chiave pubblica. Per un approfondimento sul concreto funzionamento si rimanda a D'ACQUISTO, NALDI, *op. cit*., 134 ss. Sulle criticità in tema di sicurezza nascenti dagli autoveicoli connessi si rimanda *infra* al capitolo 5.

[366] Sul punto si rimanda a Zanuzzi, la quale evidenzia come, oltre ai deficit legati alla struttura dei *device*, tra i rischi tipici debba essere ricompresa la perdita del potere di controllo sui dati da parte degli interessati. L'A. ritiene, allora, come la previsione dell'art. 32 del GDPR si mostri particolarmente adatta a regolare la materia, in quanto pensata proprio per i trattamenti digitali e massivi di dati. ZANUZZI, *Internet of Things e privacy. Sicurezza e autodeterminazione informativa*, in *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, cit., 105 ss.

[367] GAMBINO, MULA, *op. cit.*, 29.

[368] Si tratta di un attacco che cerca di sfruttare le vulnerabilità specifiche del software che è in esecuzione sul computer che si vuole attaccare. Infatti, nei protocolli di comunicazione che vengono usati in internet (i protocolli TCP/UDP) ogni servizio è associato a uno specifico numero di porta. Quando il computer usa quel servizio deve indicare il numero di porta associato e deve "aprire" quella porta. In questo caso si cerca prima di individuare quali computer sono attivi, quindi quali porte sono "aperte" sul computer oggetto di attacco e di individuare quale software viene usato su quel computer per svolgere quel servizio. A quel punto, l'hacker può sfruttare le vulnerabilità specifiche di quel software per condurre un attacco. Per un approfondimento si rimanda a D'ACQUISTO, NALDI, *op. cit.*, 193.

[369] Il *Phising* può essere definite come «*one type of social engineering attack, and every person should be read and protect themselves. That used to send an email and fake websites. Attackers are trying to get a victim's personal information such as username, password, bank account information and credit card details in electronic communication. The attacker sends to the email or message to the victims, to enter secret information on the scam website which looks and feels like a legitimate website.* […] *The main goal of, phishing is to steal the credential information, or sometimes malware is installed on a victim's*

pharming[370]; all'attacco *man-in-the-middle*[371]; al *denial of service*[372] e gli attacchi *flood*[373].

Ovviamente, oltre a una possibile lesione dei diritti dei soggetti a cui i dati personali appartengono, venendo questi a conoscenza di terzi senza un consenso e potendo essere oggetto di frodi, la violazione della sicurezza comporta dei costi economici anche per le imprese che gestiscono i dati[374]; ne discende dunque la necessità di strumenti di

---

system». VADARIYA, JADAV, *A survey on phishing URL detection using Artificial Intelligence*, in *Proceedings of International Conference on recent trends in machine learning, IoT, Smart Cities and Applications*, *ICMISC*, Singapore, 2021, 19. Il termine deriva dall'assonanza con "*fishing*" (pescare), richiamando così la metafora di una pesca all'amo degli utenti internet. D'acquisto e Naldi evidenzino come, sebbene fosse una partica nata a metà degli anni '90, essa sia ancora in uso oggi. Uno studio ha mostrato che oltre il 90% delle persone non riesce a distinguere il sito vero da uno contraffatto. V. D'ACQUISTO, NALDI, *op. cit.*, 195. Interessanti anche le considerazioni di Di Resta, il quale precisa come le moderne tecniche di *phishing* si compongano di una fase di profilazione degli utenti, che ne permette così una sorta di confezionamento su misura per gli utenti presi di mira. V. DI RESTA, *op. cit.*, 178.

[370] Il *Pharming* è un attacco che mira a sposare il traffico diretto verso un sito web a un altro indicato dall'hacker. «*In essence, a pharmer uses a vulnerability in a Domain Name System (DNS) to fool it into directing traffic destined for a legitimate site – which looks just the real thing. To understand this, you need to understand how the DNS works.* […] *Pharming intercepts this transaction and substitutes a false IP address in place of the real one, and traffic gets redirected*». VITTAL, *Phishing, Pharming, and other Scams* (2005) 22 *GP Solo – Privacy and security* 31. Per un approfondimento sulle modalità di attacco si rimanda a D'ACQUISTO, NALDI, *ibidem*; DI RESTA, *ibidem*.

[371] Il termine "*man in the middle*" (MITM) qualifica quegli attacchi in rete in cui l'hacker si inserisce nella comunicazione tra due dispositivi. Così facendo l'hacker può manipolare i dati nel percorso tra un dispositivo a un altro. Questo tipo di attacchi può colpire qualunque punto della rete. Essi sono di solito indirizzati verso le connessioni radio, che non necessitano di una connessione via cavo alla rete, e vengono realizzati mediante appositi apparati di ricezione e trasmissione posizionati in prossimità della vittima. Con l'utilizzo dei droni oggi la prossimità fisica degli apparati ricetrasmittenti non è più un ostacolo a questo tipo di attacchi. Si sono registrate intrusioni, per esempio, in reti UMTS, WiFi, Bluetooth e contro lo stesso protocollo HTTPS. In argomento si rimanda a VITTAL, *op. cit.*, 12 ss.; D'ACQUISTO, NALDI, *op. cit.*, 198 s.; DI RESTA, *ibidem*.

[372] L'attacco *Denial of Service* (DOS) consiste nell'indirizzare al server di rete una grande quantità di richieste di accesso. Il grande numero di richieste rappresenta un carico di lavoro eccessivo per il server il quale, non riuscendo a farvi fronte, finisce per non soddisfarne nessuna. L'obiettivo di questi attacchi è proprio quello di rendere il servizio di rete inaccessibile agli utenti. Sul punto si rimanda a VITTAL, *ibidem*; BOKKA, SADASIVAM, *Deep Learning Model for Detection of Attacks in the Internet of Things Based Smart Home Environment*, in *Proceedings of International Conference on recent trends in machine learning*, cit., 727; D'ACQUISTO, NALDI, *op. cit.*, 200 s.

[373] Come per gli attacchi DOS anche negli attacchi "*Flood*" la tecnica si compone dell'invio di grandi moli di pacchetti verso l'obiettivo dell'attacco. A differenza degli attacchi DOS, in questo caso si tratta di pacchetti "segnalazione". L'hacker, dunque, chiede di instaurare una connessione TCP, senza completarla e lasciando così la porta aperta, e di pacchetti ICMP (questo è il protocollo IP che serve per alcune funzioni di misura e controllo della rete, per esempio per verificare il funzionamento di un dispositivo). Un esempio è stato l'attacco al fornitore di servizi anti-spamming Panix. D'ACQUISTO, NALDI, *op. cit.*, 201.

[374] Sul punto D'acquisto e Naldi, riportano come esempio la stima, compiuta dal Ponemon Insitute, sui costi derivanti dalla violazione alla sicurezza. «Il costo viene tipicamente normalizzato per record violato, ovvero dividendo il costo totale stimato per il numero di record che sono stati violati. Per il 2015 il Ponemon Institute ha stimato un costo globale normalizzato di 153 dollari per record (il dato specifico per l'Italia è pari a 112€ se consideriamo specificamente le violazioni intenzionali). I dati indicati devono ovviamente considerarsi come stime. Il problema della valutazione dei costi è infatti di non facile

protezione, adeguati e aggiornati, che permettano di minimizzare il rischio di *data breach*. Come visto, dai trattamenti di dati personali, e ciò in particolare nell'epoca dei Big Data, possono discendere ingenti danni a un numero considerevole di utenti, così dimostrandosi l'attività di trattamento avere una intrinseca natura rischiosa.

Oltre ai casi di attività che il legislatore qualifica come tipicamente e manifestamente pericolose, previste espressamente per legge (si pensi all'elencazione prevista nel testo unico di pubblica sicurezza r.d. n. 773/1931), sono considerate altresì pericolose tutte quelle attività che per la loro natura, o per le caratteristiche dei mezzi adoperati, comportino una rilevante possibilità di verificarsi di un danno, a fronte della loro potenzialità offensiva[375].

Questo criterio di valutazione, di elaborazione giurisprudenziale, ha permesso nell'ultimo decennio di ampliare ulteriormente il novero delle attività pericolose. Si è così andato creando un sistema tendenzialmente casistico, ove hanno iniziato ad assumere rilievo elementi diversi dai mezzi adoperati e dalla natura intrinseca degli atti compiuti, come lo specifico oggetto dell'attività o i suoi destinatari[376]. Una lettura evolutiva, al passo con l'emersione di nuove attività legate allo sviluppo dei traffici economici e delle conosocenze tecnico-scientifiche, si mostra diretta a superare l'opinione tradizionale, che vede il termine "pericolo" riferito alla sola salute fisica dei danneggiati. Una tale visione restrittiva non pare, infatti, più in linea con le moderne attività che, pur non incidendo sul piano fisico, possono arrecare danni a diritti fondamentali della persona[377]. Su questi criteri deve dunque fondarsi anche la valutazione dell'attività di trattamento dati.

Di poca rilevanza appiono le considerazioni per cui il carattere immateriale dei dati, e delle relative misure di sicurezza, di per sé solo valga a escludere la pericolosità

---

soluzione, perché occorre tracciare tutte le conseguenze della violazione, che a loro volta sono ignote perché coperte dalla privacy». Si v. D'ACQUISTO, NALDI, *op. cit*., 202.

[375] Detto criterio valutativo è stato elaborato dalla giurisprudenza, sul punto ormai costante e consolidata. Si veda, tra le tante, Cass., 27.7.1990, n. 7571, in *Resp. civ. e prev*., 1991, 458; Cass., 28.2.2000, n. 2220, in *Foro it.*, 2000, I, 1828; Cass., 10.2.2003, n. 1954, in *Dir. e giust.*, 2003, 98; Cass., 7.5.2007, n. 10300, in *Mass. Giust. civ.*, 2007, 5; Cass., 19.7.2018, n. 19180, in *Foro it.*, 2018, I, 3968. In dottrina si rimanda, per una lettura evolutiva dell'istituto e per un'elencazione delle possibili attività pericolose, a C.M. BIANCA, *Diritto Civile*, *5*, *La Responsabilità*, Milano, II, 2019, 704 ss.

[376] MIRABILE, *Le tendenze evolutive della giurisprudenza riguardo alla nozione di attività pericolosa*, in *Resp. civ. e prev.*, 2018, 454 ss.

[377] Di diverso avviso MIRABILE, *op. cit.*, 464 ss., il quale ritiene non possa qualificarsi come rischiosa l'attività di trattamento dati, dando una lettura riduttiva del dettato normativo, essendo questo diretto unicamente a permettere l'estensione del regime probatorio previsto dall'art. 2050 c.c. anche all'illecito trattamento dei dati.

dell'attività[378]. Difatti, pur trattandosi di beni immateriali, i dati personali hanno assunto un ingente valore, non solo economico. La sempre maggiore estensione della dimesione digitale nella quotidianità della vita sociale ha portato aduna costruzione di un io digitale, che non sempre può dirsi coincidente con quello fisico, che si compone proprio grazie ai dati che gli utenti condividono online.

In questa prospettiva i dati rappresentando pertanto un'estrinsecazione della stessa personalità degli utenti, espressione della loro identità, che, pur mostrandosi in una dimesione digitale, non pare meno rilevante. Appare allora evidente come uno sfruttamento non regolato di questi dati possa comportare ingenti danni. Si pensi alle attività di profilazione degli utenti che vengono poste a fondamento non solo di pratiche commerciali, ma anche dell'accesso a beni e serivizi, al credito. Per fare un esempio d'oltreoceano si pensi all'ormai noto caso COMPAS[379]; un profilo errato nei diversi contesti di utilizzo può dunque generare danni più o meno ingenti, sia per il singolo che per l'intero *cluster* in cui esso viene catalogato.

A queste considerazioni in merito alla rilevanza socio-economica dei dati si deve aggiungere come le stesse modalità di trattamento comportino una particolare difficoltà di gestione per il titolare, sia in ragione dell'ingente numero di dati raccolti e soggetti a un'analisi algoritmica, sia in merito alla stessa sicurezza dei sistemi, sempre più soggetti ad attacchi esterni. La ragione è da rinvenirsi prevalentemente nella sempre maggiore complessità delle applicazioni *data driven*, che vedono spesso l'impiego di algoritmi di Intelligenza Artificiale, tali da non permettere un effettivo potere di controllo e di gestione dei titolari; questi ultimi, infatti, non sempre posseggono le competenze tecniche necessarie a comprendere il funzionamento dei sistemi. Le AI, come visto, si "nutorno" di un numero sempre maggiore di dati per poter funzionare correttamente, generando inoltre una perdita di controllo sugli stessi, a cui possono seguire esternalità negative.

Lo stesso legisaltore europeo sembra allora propendere per l'identificazione dell'attività come rischiosa. Sul punto una specifica indicazione viene prevista al Considerando n. 75, nel quale si evidenzia come dai trattamenti possano derivare rischi

[378] CICORIA, *Quale danno in materia di* privacy*?*, in *Giust. civ.*, 2007, 39 ss.; COMANDÈ, *Privacy informatica: prospettive e problemi*, in *Danno e resp.*, 1997, 147.
[379] Per un'interessante disamina degli utilizzi degli algoritmi per la profilazione degli utenti, e delle criticità nascenti da detta attività, si rimanda a O'NEIL, *op. cit.*

per i diritti e le libertà delle persone fisiche; si fa riferimento al caso di trattamenti discrminatori, di furto o usurpazione di identità, di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti la salute, il comportamento, gli spostamenti, etc[380].

Ne discende come le ingenti prospettive di danno, la natura dei diritti protetti e la loro importanza, le difficoltà tecniche di controllo e gestione dei sistemi, il numero sempre maggiore dei dati raccolti e analizzati, oltre che le capacità di inferire dati di natura personale anche da *dataset* diversamente composti, possano far qualificare le attività di trattamento dati come attività rischiose[381].

Alla luce di dette considerazioni, è apparso evidente il bisogno di una tutela fondata su di un principio di precauzione[382], di derivazione ambientale[383]. A detta *ratio* risponde, tra gli altri, l'art. 32, regolante le misure tecniche per garantire la sicurezza dei

[380] I danni in capo agli interessati possono essere fisici, materiali o immateriali. Si pensi per esempio alla distruzione, alla perdita, alla modifica, alla divulgazione non autorizzata e all'accesso ai dati trattati senza il consenso dell'interessato. Possono inoltre derivare danni economici derivanti da indebito sfruttamento dei dati personali e danni non patrimoniali legati alla dimensione strettamente personale dell'individuo. Del medesimo tenore le previsioni dei Considerando n. 75 e 85, reg. UE n. 679/2016.

[381] CICORIA, *op. cit.*, 42 ss.

[382] V. RENNA, *Sicurezza e gestione del rischio nel trattamento dei dati personali*, in *Resp. civ. e prev.*, 2020, 1342 ss. In arg. Palazzani evidenzia come proprio in un settore interessato da un velocissimo sviluppo tecnologico, quale quello dell'IA, tale per cui ne diviene difficile finanche il monitoraggio, discenda un'inevitabile incertezza conoscitiva della materia e delle possibile criticità che da essa derivano. L'Autrice dunque ritiene indispensabile comprendere e interpretare il Regolamento alla luce del principio etico di precauzione. Inoltre si propone un'attività di formazione dei programmatori dedicata specificamente a mettere in luce le problematicità etiche e giuridiche connesse allo sviluppo tecnologico. V. PALAZZANI, *op. cit.*, 58 ss.

[383] Come è noto, il principio di precauzione è stato elaborato nell'ambito del diritto internazionale a partire dalla metà degli anni '80 del secolo scorso, con particolare riferimento alla protezione dell'ambiente marino, per poi estendere la sua portata applicativa anche ad altri settori della tutela dell'ambiente, fino alla tutela umana in generale. Si veda la Comunicazione della Commissione (COM (2000) 1 final) sul principio di precauzione, consultabile all'indirizzo: *www.euro-lex.europa.eu* (ultimo accesso 15 febbraio 2021). Per un approfondimento dottrinale in merito alla portata del principio in parola si rimanda, senza pretesa di esaustività, a DI BENEDETTO, *La funzione interpretativa del principio di precauzione nel diritto internazionale*, in *Dir. comm. int.*, 2006, 321 ss.; BUTTI, *Principio di precauzione, Codice dell'ambiente e giurisprudenza delle Corti comunitarie e della Corte Costituzionale*, in *Riv. giur. amb.*, 2006, 809 ss.
Interessanti le considerazioni di Cirone che riporta la proposta di alcuni studiosi brasiliani secondo cui la tutela della privacy dovrebbe seguire le caratteristiche della tutela ambientale. Gli studiosi pongono al centro del proprio ragionamento un parallelismo tra inquinamento ambientale e interferenza delle tecnologie sul comportamento umano. Viene dunque sottolineato come «una tale ricostruzione teorica potrebbe condurre all'esigenza di muovere, nel delineare i contenuti di una efficace disciplina, da una ridefinizione del concetto di tutela dei dati personali a cui occorrerebbe guardare non in chiave solo individualistica, bensì nella sua funzione sociale, garantendo il rispetto di tutti gli altri diritti fondamentali e di un opportuno bilanciamento tra gli stessi». V. CIRONE, *Big Data e tutela dei diritti fondamentali: la ricerca di un (difficile) equilibrio nell'ambito delle iniziative europee*, in *Il ragionamento giuridico nell'era dell'Intelligenza Artificiale*, cit., 161.

trattamenti[384], oltre che la previsione di una valutazione di impatto per i trattamenti che comportino maggiori rischi; ciò proprio nella prospettiva per cui è più complesso operare una volta che il danno si sia esternato, piuttosto che mettere in atto misure che ne prevengano l'accadimento.

In questa prospettiva tra le più rilevanti espressioni del principio di integrità si dimostra allora la previsione, ampliativa rispetto all'impostazione della normativa previgente, di estendere la portata degli obblighi di protezione anche alla stessa "architettura" del trattamento[385]. L'art. 25[386] espressamente richiede la predisposizione di misure tecniche e organizzative dirette alla tutela della sicurezza di dati e sistemi sin dalla progettazione (c.d. *privacy by design*[387], anche se sarebbe più corretto parlare di *data protection by design*) e per impostazione predefinita[388] (c.d. *privacy by default*). Viene così introdotto un approccio proattivo alla materia, prevedendo il coinvolgimento di tutti gli attori sin dalle prime fasi di "costruzione" e per tutta la fase del trattamento[389].

---

[384] Il rischio preso in considerazione è quello che discende dal trattamento illecito. Non si ritiene che debba essere in esso ricompreso il rischio c.d. lecito, così intendendosi quelle possibili conseguenze negative che possono risultare sgradite all'interessato ma che di per sé non sono lesive dei suoi diritti. Cfr. sul punto MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., 288 ss.

[385] Il ruolo della sicurezza di dati e sistemi riveste nella normativa europea una posizione di rilievo. Essa, come si evince da una lettura coordinata delle disposizioni, ha difatti una natura polifunzionale, essendo sia diretta alla tutela del diritto fondamentale alla protezione dei dati personali, sia al perseguimento delle legittime finalità del trattamento, che, infine, alla garanzia stessa del mercato digitale. Per un approfondimento sul punto si rimanda a BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in *I dati personali nel diritto europeo*, cit., 781 ss.; PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 128 ss.; PERRI, *Sicurezza giuridica e sicurezza informativa dal d.lgs. 196/03 al Regolamento generale sulla protezione dei dati*, in *Tecnologia e diritto*, II, cit., 3 ss.

[386] Per un'analisi approfondita in merito all'articolo 25 si rimanda a PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 111 ss.; BIANCHI, D'ACQUISTO, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA, BELISARIO, I, Milano, 2018, *sub* art. 25, 246 ss.

[387] Tra le possibili definizioni di "*privacy by design*" si ritiene di condividere quella proposta da Klitou secondo cui il termine fa riferimento all'insieme di «pratical measures, in the form of technological and/or design-based solutions, aimed at bolstering privacy/data protection laws, better ensuring or almost guaranteeing compliance, and minimizing the privacy-intrisive capabilities of the technologies (i.e. PITs) concerned». KLITOU, *A solution, but not a panacea for defending privacy: The challenges, criticism and limitations of privacy by design*, (2014) *Privacy Technologies and Policy: First Annual Privacy forum, APF 2012* 86.

[388] Per "*privacy by default*" si intende la predisposizione del trattamento in modo tale che esso, per impostazione predefinita, tratti unicamente i dati personali necessari alla specifica finalità e che, in generale, sia rispettoso delle prescrizioni del GDPR. Si è ipotizzata una maggiore implementazione di detto principio, operando come un automatismo inserito nella fase di progettazione del trattamento, proprio nei sistemi di Intelligenza Artificiale. Cfr. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 112.

[389] Si rimanda a Zanuzzi, la quale ritiene detto approccio essenziale in un ambiente sempre più smart, ove la diffusione degli IoT appare sempre più pervasiva. V. ZANUZZI, *op. cit.*, 108 ss.

É interessante notare come la tecnologia abbia un carattere evidentemente ambivalente, da un lato essa introduce e aumenta il rischio di violazione dei diritti degli interessati, dall'altro diviene strumento idoneo alla concreta attuazione dei principi e dei diritti enucleati dalla stessa normativa sulla *data protection*[390]. Si spiegano così i riferimenti, sebbene indicati a mo' di esempio, alle tecniche di pseudonimizzazione e di criptazione, quali misure volte a garantire la tutela dei diritti degli interessati[391]. Quanto alle misure di pseudonimizzazione e di anonimizzazione, tuttavia, è bene fin da subito chiarire come esse non siano scevre da possibili rischi derivanti da attacchi di hacker[392]. A ciò deve aggiungersi come anche la predisposizione di contromisure per rafforzare la sicurezza abbia un costo per le aziende, le quali sono chiamate a valutare quanto investire in detti strumenti, non potendo però quantificare con precisione il beneficio derivante da tale implementazione.

A questi rilievi di natura prettamente economica, legati ad una impostazione proprietaria della sicurezza informatica, devono infine accompagnarsi considerazioni in merito ai diritti e alle libertà degli interessati, innestandosi il GDPR in un tessuto giuridico che vede i dati non solamente quale *asset* economico, ma anche come

---

[390] BRAVO, *op. cit.*, 799 ss.

[391] Una volta avvenuto l'attacco alla sicurezza, è previsto un obbligo di comunicazione alle autorità garanti, *ex* art. 33, e, in caso di rischi elevati per i diritti e le libertà delle persone fisiche, anche all'interessato. La previsione di comunicazione all'interessato in caso di *data breach* non è assoluta. L'art. 34 prevede, infatti, alcune ipotesi in cui, benché la violazione comporti dei rischi elevati sui diritti delle persone, il titolare non è obbligato a comunicare le violazioni alla sicurezza subite. L'art. 34, reg. UE n. 679/2016, prescrive che «*1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. 2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d). 3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia. 4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta*». Per una panoramica in merito ai rischi e alle modalità di *data breach* si rimanda a RODOLFI, *La fuga di dati e la minaccia dei* data breach, in *Tecnologia e Diritto*, II, cit., 139 ss.

[392] Per un approfondimento si rimanda *infra* § 5.1, dedicato espressamente alle tecniche di anonimizzazione e pseudinimizzazione.

espressione di un diritto costituzionalmente garantito[393]. In quest'ottica la materia della sicurezza dei trattamenti necessita anch'essa di un bilanciamento, particolarmente delicato, tra diritti di eguale dignità. Detto bilanciamento viene tuttavia demandato integralmente al titolare, il quale si trova tendenzialmente libero nella scelta delle misure da adottare[394], non essendo previsti requisiti minimi di sicurezza, a differenza di quanto indicato nel codice privacy (d. lgs. n. 196/2003) prima della recente modifica ai sensi del d. lgs. n. 101/2018. Il nostro legislatore nel recepimento della Direttiva 46/95 CE aveva, infatti, previsto una serie di processi e strumenti la cui adozione veniva considerata quale minima dotazione in materia di sicurezza, che, pertanto, ogni titolare doveva adottare[395]. Il Regolamento, nella sua attuale formulazione, invece non compie alcuna elencazione di misure minime di sicurezza; ne discende che la valutazione in merito all'adeguatezza delle misure adottate, nell'ottica di una completa strategia di sicurezza, dovrà essere valutata caso per caso, lasciando così liberi i titolari nella scelta degli strumenti e della stessa architettura di sicurezza.

Considerazioni in parte analoghe possono essere fatte in merito all'art. 32[396]. La norma è strettamente collegata all'art. 25, pur dovendo rimanere da questa distinta. L'art. 25 viene, infatti, indirizzato a guidare l'operato dei titolari prima ancora che venga posto in essere un trattamento, essendo diretto a regolare la sicurezza dei trattamenti in generale.

L'art. 32, invece, trova applicazione una volta che il trattamento sia iniziato e pertanto è diretto a misurare la sicurezza dei dati trattati, più che il trattamento in generale[397]. Oltre a questa necessaria distinzione, alcuni elementi accomunano le due disposizioni, tra cui, in particolare, la genericità dei riferimenti alle possibili tecniche

[393] Illuminanti le considerazioni di Rodotà, il quale sottolinea come garantire la sicurezza dei trattamenti permette la tutela della vita privata degli interessati, permettendo, in ultima analisi, anche di garantirne la stessa identità. V. RODOTÀ, *La privacy tra individuo e collettività*, in *Politica del diritto*, 1974, 545 ss.

[394] Sebbene gli articoli 25 e 32 predispongano un assetto formalmente vincolato, in quanto diretto alla soddisfazione dei principi, garanzie e diritti, si sottolinea come esso possa essere attuabile in maniera pressoché discrezionale dai soggetti che pongono in essere i trattamenti. V. sul punto BRAVO, *op. cit.*, 802.

[395] Si rimanda all'allegato B al d. lgs. n. 196/2003. In argomento PERRI, *op. cit.*, 13 ss.; DI RESTA, *op. cit.*, 139 ss.

[396] Per un approfondimento sulle misure di sicurezza si rimanda a PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 128 ss. Quanto ai possibili rischi legati all'IoT, Zanuzzi evidenzia come l'art. 32 del GDPR possa essere idoneo a regolare adeguatamente l'ambiente digitale, in quanto pensato proprio per i trattamenti massivi di dati. V. ZANUZZI, *op. cit.*, 106.

[397] PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 110.

ritenute idonee a garantire un livello di sicurezza adeguato[398]. La ragione della genericità della formulazione dell'art. 32, così come per l'art. 25, può essere fatta discendere dalla difficoltà di prevedere in termini generali e astratti i rimedi adottabili. Ciò in ragione non solamente della natura dei singoli trattamenti, ma soprattutto della diversa intensità dei rischi che discendono dall'uso delle nuove tecnologie. La scelta del legislatore europeo è stata dunque quella di lasciare libera la scelta delle misure tecniche e organizzative adottabili, puntando piuttosto ad una maggiore responsabilizzazione dei titolari[399].

Una formulazione così generica delle disposizioni richiamate necessita tuttavia di un'attenta riflessione circa l'effettiva portata applicativa delle stesse. Non sono infatti mancate, tra la più attenta dottrina d'oltreoceano, preoccupazioni in merito alla mancata previsione, presente invece nel progetto di regolazione e poi abbandonata, del conferimento alla Commissione del potere di adottare atti delegati al fine di precisare i criteri e i requisiti riguardanti la protezione dei dati[400].

A questi rilievi deve poi aggiungersi una considerazione che involge la natura stessa del rapporto tra tecnologia e diritto. La statuizione di una norma avente una previsione generica solleva una questione circa la concreta difficoltà di traduzione del precetto normativo in linguaggio processabile dall'algoritmo. La complessità risiede infatti proprio nella molteplicità di interpretazioni che possono essere date in generale alle norme e, in particolare, all'art. 25 GDPR, il quale evidentemente può essere soggetto a differenti modalità di attuazione concreta.

---

[398] Sul punto, come già sottolineato, un rimando viene fatto alle tecniche di pseudonimizzazione, alla cifratura dei dati, richiamando, quindi, quanto già previsto dall'art. 25 in tema di *privacy by design* e *by default*.

[399] Sul punto, nell'analizzare il passaggio tra Direttiva e Regolamento, Pizzetti evidenzia come l'introduzione di specifiche disposizioni dedicate alla sicurezza rappresenti uno tra gli elementi più innovativi del GDPR. Nella Direttiva madre erano previsti unicamente due articoli (16 e 17) sul punto, dove invece il Regolamento dedica una intera sezione, specificando il complesso di obblighi diretti ad assicurare un elevato livello di sicurezza dei trattamenti posti in essere. L'A. dunque, nel complesso, dà una valutazione positiva alle disposizioni in commento, accrescendo queste sia la rilevanza del diritto alla protezione dei dati personali, sia contribuendo a incrementare la fiducia degli stessi utenti nel contesto digitale. Difatti, mirando la valutazione sul trattamento stesso e sul titolare, dandone una maggiore responsabilizzazione in merito alle scelte compiute, da un lato evidentemente aggrava notevolmente il peso dei doveri del titolare, dall'altra parte, tuttavia, è idonea ad assicurare un maggiore livello di protezione dei trattamenti, garantendo anche ai titolari una più solida credibilità verso gli utenti e una maggiore capacità di autotutela». V. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 154 s. In argomento si rimanda anche a SIMEONE, Machine Learning *e tutela della Privacy alla luce del GDPR*, in *Diritto e Intelligenza Artificiale*, cit., 289 ss.; ROTOLO, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA, BELISARIO, I, Milano, 2018, *sub* art. 32, 293 ss.

[400] La scelta di espungere questa previsione può essere fatta discendere dalle stesse limitazioni ai poteri delegati alla Commissione previsti dall'art. 290 del Trattato sul Funzionamento dell'Unione europea.

Le disposizioni, si ricorda, sono precetti generali e astratti, che necessitano di interpretazione; questa non è di per sé opera semplice né univoca, potendo mutare nel tempo anche in relazione al mutare degli orientamenti giurisprudenziali o a causa di successivi interventi legislativi. Ne discende allora l'incompatibilità con un sistema algoritmico, il quale richiede invece regole precise e certe; sarebbe infatti complesso procedere nel tempo a modifiche a livello strutturale dell'algoritmo necessarie a implementare le evoluzioni normative. Se pertanto alcuni precetti sono sufficientemente chiari e univoci da poter essere implementati all'interno di sistemi informatici che trattano i dati personali (ad esempio l'uso della crittografia o di tecniche che controllano gli accessi a un sistema), nel complesso delle varie e numerose disposizioni che regolano la materia appare difficile ipotizzare l'emersione di un sistema di norme tale da poter assumere un carattere generale e valere quale una *mandatory rule*[401]. Inoltre, le difficoltà di implementazione di una *data protection by design* direttamente nel codice del *software* (c.d. *hardcoding*), diretta dunque a garantire una *compliance*, discendono anche dalla complessità del sistema normativo che regola i dati personali, non essendo questo unicamente rappresentato dal Regolamento 679/2016 UE.

A fronte di detti rilievi, un ruolo rilevante potrebbero allora assumere le Autorità di controllo, la quali dovrebbero essere chiamate a intervenire non solamente in caso di ricorso o ispezione, ma anche mediante una consultazione preventiva. Sarebbe infatti auspicabile che dette Autorità potessero emanare provvedimenti di carattere anche generale nel caso in cui gli strumenti e l'architettura stessa del trattamento non risultino adeguati a limitare i rischi di impatti negativi sugli interessati[402].

5.1 Anonimizzazione e Pseudonimizzazione

A fronte della crescente rilevanza dei trattamenti operati mediante tecnologie *data driven* a cui, come visto, sono ricollegabili tangibili rischi in merito alla protezione dei

[401] V. BRAVO, *op. cit.*, 830 s.

[402] Sul punto Pizzetti evidenzia come, non essendo possibile ipotizzare un obbligo per i titolari di dimostrare l'adeguatezza delle misure predisposte a tutte le persone fisiche che possono essere coinvolte, primaria importanza rivestono le Autorità di controllo nazionali. A queste è, infatti, demandato il compito di verificare il rispetto del Regolamento, così come previsto dall'art. 57, ivi compreso dunque il compito di verificare la congruità delle misure di sicurezza adottate. V. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 48 s. Del medesimo parere anche BRAVO, *op. cit.*, 833 ss.

dati personali degli interessati, all'interno del testo del Regolamento una particolare attenzione viene dedicata ai processi di anonimizzazione e pseudonimizzazione. Entrambi questi processi, se ben congegnati, possono essere considerati quali strumenti espressivi del principio, pervasivo della disciplina, di *privacy by design*, previsto all'art. 25 GDPR, così come precisato dal Considerando n. 78[403]. Si comprende così il ruolo di assoluta preminenza che dette tecniche rivestono all'interno dello schema normativo europeo. É altresì opportuno specificare come anch'esse non siano esenti da rischi, e come dunque sia opportuna una valutazione in concreto delle modalità operative al fine di verificarne la permanenza di utilità nel tempo. Appare, allora necessario analizzare brevemente il funzionamento di dette misure al fine di poter verificare in concreto l'efficacia di una loro implementazione nelle tecnologie *data driven*.

L'anonimizzazione e la pseudonimizzazione sono processi che si differenziano sensibilmente, non solo in ragione delle rispettive modalità operative, ma anche concettualmente. Questi, infatti, perseguono differenti finalità di tutela, pur rimanendo misure ritenute parimenti idonee a tutelare i diritti degli interessati e a permettere una più agevole circolazione dei dati.

[403] Un importante ampliamento viene previsto nel Considerando n. 78, il quale precisa che «*La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici*». La disposizione, oltre che collegare al principio di *accountability* i doveri dei titolari circa l'implementazione delle misure di sicurezza, prevede dunque un esplicito richiamo anche ai produttori delle applicazioni che trattano i dati, affinché prevedano misure di tutela della privacy fin dalla progettazione, in modo da permettere ai titolari di poter adempiere agli obblighi previsti dalla normativa. Una previsione di tale portata sarebbe compatibile con gli strumenti di Intelligenza Artificiale che, come visto, si compongono di catene complesse di titolari fino a risalire al produttore del software. In argomento SIMEONE, *op. cit.*, 288 ss.

La pseudonimizzazione opera la sostituzione di un attributo univoco di un dato con un altro attributo non immediatamente intellegibile[404]. Questo processo permette così di dissociare i dati dai soggetti a cui appartengono, rendendone di fatto più complessa l'identificazione. È, tuttavia, sempre possibile rendere nuovamente riferibile il dato alla persona. Questo perché la pseudonimizzazione, operando tendenzialmente mediante una sostituzione di un attributo, non altera la catena di passaggi necessari all'attribuzione del dato alla persona fisica. Ne discende che una volta che lo pseudonimo sia impiegato in combinazione con tutti i mezzi necessari ad effettuare la sostituzione di attributi a ritroso, questo è inequivocabilmente riferibile all'individuo. La persona interessata potrebbe essere ancora identificata in maniera indiretta, rimanendo così i dati pseudonimi assoggettati alla disciplina sulla *data protection*. Limitandosi la pseudonimia a ridurre l'intellegibilità dell'insieme di dati, si mostra essere una misura di sicurezza, certamente utile se ben realizzata, ma non una modalità per rendere i dati anonimi.

La scelta dell'impiego di detta tecnica può discendere dalla necessità di apprestare uno strumento che sia diretto a garantire la sicurezza dei dati ma che al contempo non ne renda incerta l'attribuzione. Difatti alcuni trattamenti, per loro stessa natura, generano degli effetti sugli interessanti tali per cui si richiede che essi mantengano un diritto di accesso al dato. In questi casi rimane allora indispensabile non recidere completamente il legame tra il dato trattato e il soggetto da cui proviene, come invece si propongono di fare le tecniche di anonimizzazione. La tutela introdotta con la pseudonimizzazione è volta dunque a garantire la confidenzialità del dato, non più immediatamente intellegibile, oltre che, come avviene nel caso dell'applicazione di tecniche crittografiche, a garantire l'integrità contro manipolazioni anche accidentali[405].

Per quanto concerne l'anonimizzazione, una particolare attenzione viene posta dal legislatore europeo su dette tecniche, ciò in quanto ritenute un presidio particolarmente efficace e tale da poter escludere i dati così trattati dal perimetro di applicazione del

[404] Il risultato delle tecniche di pseudonimizzazione può essere indipendente dal dato originario. Ciò accade quanto viene fornito un valore casuale a un attributo del dato, oppure può essere calcolato a partire dal valore inziale dell'attributo, o da un insieme di questi, così come avviene in alcune tecniche crittografiche. Per un approfondimento Cfr. D'ACQUISTO, NALDI, *op. cit*., 39; DE GREGORIO, TORINO, *op. cit.*, 468 ss.

[405] D'ACQUISTO, NALDI, *ibidem*. Di confidenzialità garantita dalla pseudonimizzazione parla anche TRAVAGLIA, *Big data e Regolamento europeo sulla protezione dei dati personali*, in *accademia.edu*, 2017, 11.

Regolamento 679/2016 UE. A fronte, dunque, della rilevanza che assumono detti trattamenti si ritiene necessario chiare come vengano posti in essere al fine di evidenziare come essi, per quanto ritenuti efficaci, non siano comunque immuni da possibili violazioni di sicurezza.

Tra le principali tecniche utilizzate per anonimizzare i dati possiamo annoverare le tecniche di randomizzazione, che si sviluppano operando una distorsione dei dati, e quelle di generalizzazione dei dati; entrambe dette modalità sono concepite per introdurre incertezza nell'attribuzione del dato a un determinato soggetto. Nello specifico, la distorsione opera una modifica sulla veridicità dei dati, aggiungendo c.d. rumore statistico ai valori, così da recidere il più possibile il legame con la persona da cui essi provengono. La generalizzazione, invece, consente di modificare la scala o l'ordine di grandezza degli elementi costitutivi i dati. In quest'ultimo caso l'incertezza è legata al fatto che più ampia sarà la scala di valori degli attributi, tanto maggiore sarà il numero di soggetti potenzialmente riferibili ad essi; così facendo diviene sempre meno probabile attribuire il dato alla singola persona[406]. Ovviamente, in entrambi i casi il titolare sarà chiamato a contemperare il processo di anonimizzazione con l'utilità del dato, così derivato, ai fini del trattamento. Difatti, se il rumore prevale sul dato utile questo diviene inaccurato e quindi inidoneo a qualsiasi tipo di analisi. Allo stesso modo un dato troppo generalizzato rischia di perdere ogni valenza semantica, così finendo con l'essere incapace di esprimere qualsiasi nesso di correlazione utile a descrivere un fenomeno.

Pertanto, semplificando, il processo di anonimizzazione, consente di "sottrarre" gli elementi identificativi presenti nei dati, così pervenendo a una nuova rappresentazione degli stessi; ne consegue che più elementi vengono "sottratti" tanto più esiguo sarà l'insieme dei mezzi ragionevolmente idonei a svelare l'identità della persona interessata[407]. Così come le tecniche di pseudonimia, anche in questo caso si tratta di un trattamento che viene compiuto solo successivamente alla raccolta dei dati, pertanto

[406] D'ACQUISTO, NALDI, *op. cit.*, 35 ss.

[407] Il concetto di ragionevolezza non viene ulteriormente declinato all'interno del dettato normativo. Sul punto è così intervento il Gruppo di Lavoro art. 29 con il parere n. 5/2014, dedicato alle tecniche di anonimizzazione. Il Gruppo di esperti ha chiarito come debbano essere prese in considerazione tutte le metodologie possibili dirette a re-identificare il soggetto interessato, oltre che l'entità dei costi legati al loro utilizzo. Si tratta, evidentemente, di una valutazione compiuta caso per caso e necessariamente soggetta a una rivalutazione periodica, a fronte del mutare delle condizioni del titolare e dello stato dell'arte. Gruppo di Lavoro art. 29, Parere 5/2014 sulle tecniche di anonimizzazione, 2014. Sul punto Cfr. TRAVAGLIA, *op. cit.*, 12.

anch'esso necessita di una idonea base giuridica (che può alternativamente essere il consenso dell'interessato, l'adempimento di un obbligo contrattuale o un legittimo interesse), necessaria a renderne legittimo l'impiego[408].

Tuttavia è necessario chiarire come allo stato attuale della tecnica non sia possibile compiere un procedimento di anonimizzazione irreversibile[409]. Sono infatti noti, e spesso anche oggetto di scalpore mediatico, episodi di attacchi diretti a rendere nuovamente identificabile un *database* pseudonimizzato o anche anonimizzato. Si pensi, per esempio, alla re-identificazione dei dati sui percorsi effettuati dai tassisti di New York, resi pseudonimi mediante la sostituzione dei dati identificativi (licenza e targa dell'automobile) con il corrispondente codice hash[410]; al notissimo caso di re-identificazione dei clienti dei Netflix che il colosso aveva "protetto" fornendo degli pseudonimi ai propri utenti[411]; o, infine, all'esperimento compiuto sul finire degli anni '90 che ha mostrato come anche tecniche di generalizzazione possono essere efficacemente trattate con processi di *reverse engineering*, rendendo così conoscibili dati sensibili quali quelli attinenti alla salute[412]. Ne discende dunque come sia sempre

[408] TRAVAGLIA, *ibidem*; D'ACQUISTO, NALDI, *op. cit.*, 190 ss.

[409] Il concetto di anonimia deve, dunque, essere costruito nel tempo, dovendo necessariamente passare attraverso una puntuale verifica dello stato dell'arte e della concreta possibilità di re-identificare gli interessati.

[410] Il *database* conteneva un numero molto alto di *record*, circa 170 milioni, relativi alle corse dei passeggeri, con l'indicazione del tempo e del luogo di inizio e fine percorso. É stato effettuato un attacco a c.d. forza bruta che, sfruttando la conoscenza della sintesi adottata per il numero di licenza, ha provato tutte le possibili combinazioni (circa 3 milioni) fino a rivelare il dato in chiaro nascosto dai codici pseudonimi resi pubblici. Rivelata la licenza di guida, grazie al collegamento con altre banche dati è stato possibile ricostruire le identità dei tassisti.

[411] Il *database* di Netflix è molto esteso. Questo si compone di più di 100 milioni di valutazioni, in una scala da 1 a 5, su più di 18.000 film. La compagnia ha reso pubbliche le valutazioni espresse da 500.000 utenti, in un dato periodo di tempo, dopo essere stati criptati con l'impiego di pseudonimi e aver aggiunto del "rumore" statistico, modificando in modo casuale alcuni *rating*. L'obiettivo era quello di stimolare lo sviluppo di algoritmi più efficienti nella classificazione. Nonostante l'uso di queste tecniche ha fatto scalpore la rivelazione che il 99% dei *record* conteneva una combinazione univoca di valutazioni su 8 film, espresse in un periodo di 14 giorni. Grazie a questa osservazione è stata effettuata una corrispondenza con il *database* pubblico di IBM. Grazie a questa comparazione è stato possibile far corrispondere in modo univoco le combinazioni di film nel periodo in cui erano state espresse, consentendo un *mapping* c.d. *proof-of-concept* (una metodologia ripetibile) tra gli utenti di cui si conoscevano le identità e quelli anonimizzati di Netflix. Per un approfondimento si rimanda a NARAYANAN, SHMATIKOV, *Robust De-anonymization of Large Sparse Datasets* (2008) *IEEE Symposium on Security and Privacy* 111 ss. Il caso di Netflix è anche riportato nel Parere 5/2014, sulle tecniche di anonimizzazione, del Gruppo di Lavoro art. 29, cit.

[412] Si fa riferimento a uno studio pubblicato nel 1990 che mostrò come grazie alla combinazione di un *ZIP code* a 5 cifre, la data di nascita e il sesso era possibile individuare una percentuale superiore all'80% della popolazione americana. Grazie all'impiego di questi dati resi pubblici da parte di una compagnia assicurativa, incrociandoli con le liste elettorali pubbliche dello Stato del Massachusetts, fu possibile re-identificare i cittadini e scoprire – tra gli altri – anche i dati di ospedalizzazione dello stesso Governatore dello Stato. V. D'ACQUISTO, NALDI, *op. cit*., 190.

possibile, benché estremamente difficile o economicamente svantaggioso, ricondurre i dati "anonimi" al soggetto da cui provengono.

Lo stesso legislatore europeo consapevole di tale condizione, nel riferirsi all'anonimizzazione, nella Direttiva 46/95 CE, prima, e nel Regolamento, poi, ha posto attenzione all'impiego dei mezzi idonei allo scopo. Viene così chiarito che al fine di determinare se una persona sia identificabile o meno, e dunque se si tratti di un dato anonimo, è necessario prendere in considerazione tutto l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal titolare o da terzi per re-identificare l'interessato. Se a seguito di detta valutazione la persona interessata non è ritenuta identificabile, allora ai dati così trattati non verranno applicate le disposizioni del GDPR[413].

Alla luce delle considerazioni sopra svolte, appare allora chiaro come il concetto di anonimato sia necessariamente relativo; la stessa qualificazione come anonimo di un dato non può che avere un carattere dinamico, essendo configurata in relazione sia ai soggetti coinvolti che all'evoluzione tecnologica. Ne discende una necessaria e continua verifica dei dati così qualificati e ciò in particolare perché la re-identificazione dei soggetti interessati potrebbe comportare il verificarsi di possibili danni per gli individui, non essendo il *dataset* ritenuto anonimo soggetto all'applicazione del GDPR[414].

Come si è già avuto modo di sottolineare, la mancata applicazione della normativa sulla *data protection* ha risvolti di non poco conto. Un *dataset* reso anonimo non viene considerato assoggettato al Regolamento in virtù della considerazione per cui i dati al suo interno non possono più condurre a identificare le persone fisiche a cui appartengono. Ne discende allora una maggiore libertà nei trattamenti e nella circolazione degli stessi, non dovendo il titolare apprestare tutte le garanzie previste a tutela del diritto alla protezione dei dati personali degli interessati. La mancata identificabilità degli interessati fungerebbe come una garanzia indiretta in caso di un eventuale uso non autorizzato dei dati da parte dei terzi, in quanto pur poterebbero venire a conoscenza di informazioni anche sensibili queste non verrebbero comunque ricollegate alla singola persona fisica a cui ineriscono.

La rilevanza che viene data anche a livello normativo alle tecniche di anonimizzazione discende inoltre dalla convinzione che esse sarebbero sufficienti a

[413] D'ACQUISTO, NALDI, *ibidem*; DE GREGORIO, TORINO, *op. cit.*, 470 ss.
[414] V., in argomento, FINOCCHIARO, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, cit., 243.

evitare possibili esiti discriminatori nei confronti degli individui, in quanto non più identificabili. É evidente come questa soluzione tecnica, se ben implementata, comporti in potenza un grande vantaggio per gli utenti, oltre che per le imprese a cui viene accordata una maggiore libertà nella determinazione dei trattamenti. Tuttavia, proprio in ragione dello sviluppo tecnologico appare necessario prestare una particolare attenzione. Come visto non solo ad oggi non esistono processi di anonimizzazione definitivi, semmai economicamente svantaggiosi, ma pur sempre possibili. A ciò deve aggiungersi come le applicazioni di *data mining* siano proprio dirette a inferire nuovi dati, persino personali, anche da *dataset* non personali; dunque appare evidente come il processo di anonimizzazione non possa essere considerato come una sorta di rimedio generale, e ciò proprio in virtù del continuo progredire della tecnica.

A fronte di queste criticità, in parte non superabili, possono allora essere introdotte alcune *best practice* tra gli stessi operatori, così da ridurre quanto più possibile i rischi di un attacco alla sicurezza. Innanzitutto, centralità dovrà assumere un'informativa completa e intelligibile anche in merito a questi processi, sebbene diretti a fornire agli interessati una forma accentuata di tutela. Ciò in quanto ben potrebbero gli utenti rifiutare questi trattamenti, rendendo così necessaria la predisposizione di procedure di *opt-out*. Nel contesto attuale buona prassi sarebbe inoltre quella di limitare al minimo, e solo ove strettamente necessario, la pubblicazione dei dati, rendendoli accessibili solo a soggetti determinati. Potrebbero inoltre essere introdotte delle clausole contrattuali, e ciò appare particolarmente utile nella regolazione dei trattamenti caratterizzati da una lunga catena di titolari, che vietino la re-identificazione dei dati.

Lungi dall'essere esautorato, il ruolo della normazione primaria potrebbe rivestire in materia una particolare importanza. Proprio grazie all'applicazione del principio di responsabilizzazione, così come introdotto e regolato dal GDPR, sarebbe possibile incentivare le *practice* virtuose delle imprese operanti nel settore[415]. Una grande rilevanza, dunque, dovrebbe assumere il principio di *accountability*, non solo quale strumento direttamente rivolto a garantire la tutela dei danneggiati, ma soprattutto quale

[415] Si rimanda a Simeone, il quale sottolinea il ruolo centrale che il principio di responsabilizzazione ricopre, anche in relazione al dovere dei titolari di implementare soluzioni tecniche e organizzative adeguate al rischio. Si ritiene uno strumento di regolazione efficace in quanto renderebbe la normativa europea in parola maggiormente "flessibile", così potendo adeguarsi alle future evoluzioni tecnologiche veicolate dalle applicazioni di Intelligenza Artificiale. V. SIMEONE, *op. cit.*, 288.

leva per spingere i titolari a operare sia nei rapporti con gli interessati, che in quelli tra imprese, nell'implementazione della *data protection* in tutte le fasi del trattamento.

6. Il principio di esattezza

Di particolare rilievo per l'oggetto del presente lavoro si dimostra infine il principio di esattezza[416], il quale, essendo diretto a evitare distorsioni nella rappresentazione dei dati, costituisce un presupposto necessario all'effettività del diritto all'autodeterminazione informativa.

Il principio in parola mostra tutta la sua centralità proprio nei trattamenti articolati su filiere complesse, quali quelli operati mediante metodologie di AI. Come visto, dette tecniche sono estremamente influenzate dalla qualità dei dati in ingresso, infatti esse permettono la "creazione" di nuovi dati e di informazioni, spesso partendo da frammenti di dati (*raw data*), mediante la combinazione e la ricerca di ricorrenze statistiche; è evidente che i dati errati o incompleti conducano a risultati errati o discriminatori[417]. Il principio di esattezza acquista allora una rilevanza fondamentale, legandosi anche a una necessaria affidabilità, non solamente dei dati, ma anche delle modalità di raccolta e di analisi degli stessi.

É indispensabile per avere *dataset* di qualità che le capacità degli analisti di verificare se i dati siano utilizzabili o meno per il successivo trattamento siano affidabili. Del pari lo devono essere le modalità di analisi probabilistica utilizzate allo scopo di trarre nuovi dati da quelli raccolti in origine[418]. Se i dati raccolti e trattati sono esatti, nell'accezione di corretti e aggiornati, e la stessa filiera di trattamento fin dalla

---

[416] «[i dati personali sono, ndr] *esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*», art. 5, lett. *d*), reg. UE n. 679/2016.

[417] La stessa varietà di dati resi disponibili agli algoritmi per l'analisi comporta in una certa misura una inevitabile incertezza in merito alla loro accuratezza. De Gregorio e Torino sul punto richiamano le parole di Boyd e Crawford secondo cui sarebbe direttamente proporzionale il rapporto che lega l'incremento delle fonti di provenienza dei dati e l'aumento del rischio di dati inaccurati. Si v. DE GREGORIO, TORINO, *op. cit.*, 465.

[418] Di catena di affidabilità parla PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 260 s. L'Autore richiama inoltre la necessità che il concetto di esattezza venga parametrato anche alla dimensione "tempo", ciò in quanto la realtà è in continua evoluzione, comportando così l'inevitabile "invecchiamento" dei dati e la loro perdita di esattezza, intesa come "corrispondenza alla porzione di realtà".

fase di progettazione risulta affidabile, ne discende con tutta evidenza come ciò possa limitare in concreto il rischio *output* errati o discriminatori.

Sul punto il legislatore europeo introduce dunque nel testo del Regolamento un obbligo per il titolare particolarmente impegnativo, anche in relazione alla sua estensione[419]. Viene prevista la verifica circa l'esattezza e aggiornamento dei dati rispetto alle finalità per le quali sono trattati, secondo quello che è stato definito uno specifico onere di «fedeltà contenutistica»[420]. Ne discende allora come la nozione di esattezza del dato sia un concetto eminentemente relazionale, da valutare in correlazione al fine e all'utilizzo stesso che ne dovrà essere fatto. Appare infatti evidente che la correttezza e adeguatezza dei dati debba essere valutata in relazione agli scopi perseguiti. Come sottolinea autorevole dottrina, non tutti i dati debbono essere costantemente aggiornati, ben potendo dati anche molto risalenti nel tempo rispondere adeguatamente agli scopi del trattamento[421].

Da quanto fin qui rilevato appare chiaro come il principio in parola si dimostri di particolare rilevanza proprio in relazione ai trattamenti effettuati con algoritmi di Intelligenza Artificiale. Dalla lettura del testo infatti emergerebbe per certi versi un divieto di utilizzo e raccolta indiscriminato dei dati, c.d. pesca a strascico[422], senza cioè aver definito gli scopi perseguiti e senza una verifica circa la loro utilità e correttezza. Previsione questa che sembra essere diretta proprio a regolare quei trattamenti che si fondano sull'uso di tecnologie *data driven*.

---

[419] Il titolare è chiamato a comunicare a tutti coloro a cui egli abbia trasmesso i dati le eventuali rettifiche, cancellazioni o richieste di limitazione di trattamento. È tuttavia previsto un limite a questo obbligo, che altrimenti avrebbe potuto comportare un eccessivo aggravio degli oneri del titolare, prevedendo che l'obbligo non sussista nel caso in cui si riveli impossibile, a fronte della natura del trattamento, o implichi uno sforzo sproporzionato. Il punto 3 dell'art. 34, reg. UE n. 679/2016, prevede che «*Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni: a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia*».

[420] DELL'UTRI, *op. cit.*, 210. Sul punto Di Resta, facendo uno specifico richiamo all'ambito giornalistico, parla di introduzione di uno "standard di diligenza" che verrebbe così a gravare sul titolare del trattamento nella gestione dei dati raccolti. V. DI RESTA, *op. cit.*, 46.

[421] V. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 60 s.; F. RESTA, *op. cit*., 58 s.

[422] PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 61.

Lo stretto collegamento del principio di esattezza con il principio di finalità comporta nondimeno una prima tensione tra il dettato normativo e la prassi applicativa, e ciò proprio in ragione delle modalità di funzionamento delle applicazioni di AI, le quali si fondano su di un uso indiscriminato di un numero considerevole di dati, senza alcuna selezione né quantitativa né qualitativa. Tuttavia, una implementazione del principio in analisi permetterebbe di limitare il rischio di esternalità negative derivanti da trattamenti viziati da c.d. *bias*[423]. Se, come visto, non pare attualmente operabile una selezione nella quantità dei dati raccolti, dal momento che il valore delle tecniche di *data mining* risiede proprio nell'estrarre informazioni – e così ricchezza – da un numero considerevole di variabili, è necessario prestare una concreta attenzione allora alla qualità del dato, così da poter limitare i rischi di *output* distorti[424].

Il principio di esattezza potrebbe dunque essere implementato in particolare nella fase iniziale di raccolta, mediante specifici obblighi per i titolari del trattamento diretti allo scopo di verificare a monte le caratteristiche intrinseche dei dati che ne definiscono la qualità. Tra queste ultime possono rientrare: la descrizione in modo accurato della realtà che i dati intendono rappresentare; l'attualità e dunque l'aggiornamento dei dati; la non contraddittorietà e, infine, la completezza, cioè la presenza di un numero di attributi sufficiente a rappresentare correttamente il fenomeno analizzato[425].

Nell'attuale assetto normativo il principio di esattezza viene tuttavia declinato, più che in obblighi specifici per i titolari del trattamento, nella previsione di una prerogativa dell'interessato, il quale ha il diritto di chiedere la rettifica o l'integrazione dei propri dati personali[426]. L'interessato viene così chiamato a farsi parte attiva, instaurando il principio in parola un confronto dialettico tra diritti e interessi in parte confliggenti. Si ritiene, tuttavia, che proprio alla luce dei rischi nascenti dall'utilizzo di tecnologie di AI,

[423] Sul punto si avrà modo di ritornare *infra* nel prossimo capitolo, a cui si rimanda.

[424] Diverse proposte sono state avanzate facenti perno proprio su di una maggiore valorizzazione della qualità dei dati utilizzati per addestrare i sistemi di AI. Sul punto si rimanda *infra* al capitolo 4 del presente lavoro.

[425] TRAVAGLIA, *op. cit.*, 5.

[426] Interessante la considerazione di Dell'Utri secondo cui dai principi di esattezza e minimizzazione deriverebbe la necessità di un confronto tra gli interessati e il titolare del trattamento. Dal confronto troverebbe composizione l'eventuale scontro tra la «dimensione oggettiva della funzionalità minima del trattamento (così come della rispondenza oggettiva del contenuto dei dati alla realtà da essi rispecchiata), al valore soggettivamente attribuito, dai rispettivi titolari, così come a quelli che, per converso, invocano un profilo specifico dell'esattezza della rappresentazione, nella sua idoneità a rispettare le forme o i modi attraverso i quali ciascuno percepisce riflessivamente i termini della propria identità personale partecipata al contesto di relazione». DELL'UTRI, *ibidem*.

le quali possono avere un impatto nei confronti di qualunque persona fisica e dell'intera società[427], dunque non solamente nei confronti dei singoli interessati così come definiti dal GDPR, il principio in analisi avrebbe forse meritato la previsione di un obbligo specifico anche nei confronti dei titolari. Sul punto un riferimento si trova invece unicamente nel Considerando n. 71[428], che per sua stessa natura non ha valenza normativa, essendo rivolto ad indirizzare l'interprete nella lettura delle disposizioni.

Nonostante il carattere come visto quasi evanescente del concetto di esattezza[429], dovendosi necessariamente comporre in relazione alle finalità oltre che al tempo di utilizzo dei dati, questo appare un elemento imprescindibile a una efficace regolazione del fenomeno digitale. Se correttamente declinato esso infatti potrebbe contribuire a limitare il rischio di esternalità negative per gli interessati e al contempo non limitare eccessivamente le potenzialità di sfruttamento delle tecniche di *data mining*, oggi sempre più presenti nel mercato.

7. Possibili profili di una tutela collettiva

Alle considerazioni fin qui svolte è necessario aggiungerne una di natura eminentemente tecnica. La pratica dei trattamenti dei dati mediante algoritmi di AI ha evidenziato un ulteriore profilo di inadeguatezza della normativa sulla *data protection*. La raccolta e la conservazione dei dati dei singoli interessati viene oggi spesso diretta a creare dei "gruppi", nella prospettiva che tutti gli individui appartenenti allo stesso

[427] Nella valutazione circa la natura del principio di esattezza Pizzetti evidenza come, a differenza degli altri principi elencati nell'art. 5, questo abbia un evidente spessore di carattere collettivo. Il principio in parola impegnerebbe «il titolare a una ancor più approfondita valutazione di rischio, soprattutto rispetto all'orizzonte degli effetti dei trattamenti. Il titolare, infatti, deve avere come punto di riferimento non solo l'interessato ma la tutela delle libertà e dei diritti delle persone fisiche che possono essere coinvolte e, in sostanza, della società come tale». V. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiali*, cit., 62.

[428] Il Considerando n. 71, reg. UE n. 679/2016, precisa che «[…] *Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti*».

[429] PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 262.

gruppo si comportino nel medesimo modo e rispondano ai medesimi stimoli. Queste tecniche fanno perno sui cosiddetti *co-pattern*s, come possono essere, ad esempio, i *frequent flyers* su una data tratta aerea o gli appassionati di *running* che fanno uso di strumenti di geolocalizzazione per misurare le proprie prestazioni, ma anche tutte le persone che risiedono in un dato periodo in una determinata zona di una città. Questi dati sono idonei, mediante la loro analisi, a individuare linee di tendenza di comportamenti dell'intera categoria a cui essi si riferiscono[430].

La dimensione presa in considerazione non è più dunque quella del singolo, bensì quella collettiva, ove l'individuo assume rilevanza solo in quanto facente parte di un gruppo. Proprio da questa prospettiva emerge un vuoto di tutela, risultando difficilmente applicabili i principi e gli strumenti predisposti dal GDPR. La prassi di funzionamento delle tecnologie rende infatti improbabile che le informazioni contenute in *big dataset* siano facilmente riconducibili a singoli individui determinati o determinabili. Emergendo dunque dal trattamento dei Big Data un rischio collettivo, è stata avanzata la proposta di introdurre la previsione di forme di *collective redress*, cioè di tutela collettiva di interessi anche non riferibili a individui determinati[431], sulla scorta di quanto previsto nel diritto internazionale in materia di tutela delle minoranze.

In dottrina tuttavia non è ritenuto pacifico il riconoscimento dei gruppi. Almeno con riferimento all'ordinamento internazionale, la configurabilità del diritto di un gruppo è stata messa in dubbio a livello concettuale, non solo rispetto alla possibilità di concepire un gruppo come autonomo titolare di posizioni giuridiche proprie, ma anche in relazione alla difficoltà di definire in maniera sufficientemente precisa il gruppo stesso[432].

Sul punto si sono espresse le Istituzioni europee. Il Parlamento ha evidenziato come, a causa delle quantità di dati e dei sistemi utilizzati per la loro analisi, i *Big Data* possano «condurre non solo a violazioni dei diritti fondamentali dei singoli, ma anche a una disparità di trattamento e a una discriminazione indiretta nei confronti di gruppi di persone con caratteristiche simili, in particolare per quanto concerne l'equità e le pari opportunità di accesso all'istruzione e all'occupazione, quando si offre un lavoro alla persona o la si valuta oppure quando si determinano le nuove abitudini di consumo

[430] RUOTOLO, *op. cit.*, 108.
[431] RUOTOLO, *op. cit.*, 111 ss.
[432] Sul punto si rimanda a RUOTOLO, *op. cit.*, 109; KLABBERS, *International Law*, Cambridge, 2017, 124.

degli utenti dei media sociali»[433]. Nel 2017 è altresì intervenuto il Comitato consultivo della Convenzione 108, emanando delle linee guida ove si riconosce la presenza di una «collective dimension of risks related to the use of data», che dovrebbe condurre a una «broader idea of control over the use of data, according to which individual control evolves in a more complex process of multiple impact assessment of the risks related to the use of data»[434].

La portata delle indicazioni delle linee guida, pur avendo il pregio di mettere in luce la complessità delle dinamiche attuali dei trattamenti di massa, si dimostra in concreto piuttosto limitata. All'indicazione sopra richiamata, infatti, non si accompagna alcuna previsione specifica di misure di tutela collettiva, limitandosi il Comitato consultivo a richiamare problemi di responsabilità sociale ed etica. Di fatto il testo si limita a invitare gli Stati membri a potenziare l'applicazione dei principi generali già previsti dalle normative, a imporre ai titolari una valutazione preventiva dei rischi e, infine, a rispettare il principio di precauzione. L'unica prospettiva operativa riguarda la previsione di una forma particolare di consenso "informato", il quale dovrebbe comprendere un'interfaccia che simuli gli effetti dell'elaborazione e dell'uso dei dati e il loro potenziale impatto.

La previsione di una tutela collettiva potrebbe comportare diversi vantaggi, sia in termini di facilitazione nell'identificazione dell'interesse leso, che nella determinazione del danno, non più legato alla sfera individuale ma a quella del gruppo nel suo complesso. Nonostante gli innegabili aspetti positivi, sorgono del pari alcune difficoltà. In primo luogo appare difficile, a differenza di quanto avviene per i gruppi sociali aventi una propria struttura organizzata, individuare in maniera sufficientemente precisa i gruppi di *co-patterns*, e di conseguenza il loro riconoscimento come autonomi titolari di un interesse, aventi legittimazione ad agire in sede giurisdizionale. Sul punto interessanti le considerazioni dell'Avvocato Generale, nella causa C-498/16, il quale ha riconosciuto l'opportunità di azioni collettive quali strumenti idonei a tutelare adeguatamente i diritti dei cittadini danneggiati. Tuttavia, si evidenzia come, escludendo strumenti di diritto non vincolante, questa tipologia di azioni non sia contemplata nell'ordinamento europeo; ne discende allora come ad esse non possa essere

[433] COM (2016) 288 final, punto 19.
[434] Comitato consultivo della Convenzione 108, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big data*, consultabile all'indirizzo: *www.coe.int*.

riconosciuta valenza per via meramente giurisprudenziale, richiedendosi piuttosto uno specifico intervento legislativo in materia[435].

A fronte di dette criticità allora potrebbe trovare applicazione estensiva la proposta della Commissione, in tema di diritti dei consumatori, di individuazione *ex ante* di organizzazioni rappresentative di una pluralità di individui che si facciano portavoce di interessi comuni[436].

8. Considerazioni conclusive

La diffusione delle tecnologie digitali ha comportato un profondo cambiamento nella società, a nuove modalità di interrelazione sono seguite nuove esigenze di tutela dei singoli. Esempio paradigmatico è l'evoluzione dell'istituto della privacy che, da diritto legato alla tutela della riservatezza quale contrappeso al diritto di cronaca, è divenuto diritto fondamentale dell'uomo.

Col progredire delle applicazioni digitali, come visto, è iniziata a emergere una forma di tutela che, sebbene affondi le radici nella privacy, ha assunto un carattere autonomo in quanto diretta alla protezione generale dei dati personali degli utenti. Di questo diritto, anch'esso ricompreso tra i diritti fondamentali dell'uomo, ne è espressione compiuta il recente Regolamento 679/2016 UE (GDPR).

Il tema dei dati personali è di centrale importanza per l'oggetto del presente lavoro. Si ricorda, infatti, che le applicazioni *data driven*, tra cui le AI, trattano un numero considerevole di dati, tra cui anche quelli personali. Esse inoltre hanno la capacità di inferire informazioni personali da *dataset* di natura non personale, potendo così in astratto incidere significativamente sui diritti degli interessati. Ne discende dunque la particolare importanza rivestita dal GDPR per la materia. Infatti, dopo aver chiarito cosa debba intendersi con "dato personale", avendo la nozione una dimensione particolarmente estesa e flessibile, soprattutto in ragione delle sopra citate capacità delle

[435] Corte giust. UE, 15.1.2018, causa C-498/16, in *Dir. inform.*, 2018, 136. Punto n. 123 delle Conclusioni dell'Avvocato Generale, consultabili all'indirizzo: *curia.europa.eu*.

[436] Sul punto si rimanda alle considerazioni di RUOTOLO, *op. cit.*, 115, il quale precisa alcuni aspetti della raccomandazione della Commissione in merito alle organizzazioni, le quali non dovrebbero avere scopo di lucro. L'Autore ritiene, inoltre, che dovrebbe sussistere «un nesso diretto tra i loro obiettivi principali e i diritti conferiti dalle norme dell'Unione di cui si lamenta la violazione per i quali l'azione è esperita e che le stesse abbiano sufficienti capacità, in termini di risorse finanziarie e umane e di competenza legale, per rappresentare una molteplicità di ricorrenti agendo nel loro interesse».

tecnologie digitali, appare chiaro come la normativa europea sui dati trovi applicazione anche nella regolazione delle IA.

L'indagine si è così concentrata sugli aspetti più delicati che potenzialmente potrebbero entrare in conflitto con la modalità di trattamenti di dati di massa, partendo in via obbligata dai principi generali e da come essi vengano declinati all'interno della normativa europea; ciò in quanto essi appaiono in parte poco compatibili nella regolazione delle moderne tecnologie digitali. Se i principi richiamati ben si adattavano a una struttura lineare di trattamento, quale quella a fondamento della Direttiva madre, lo sviluppo dei Big Data ha fatto emergere alcune tensioni con il dettato normativo, in particolare per quanto concerne la concreta applicabilità dei principi di minimizzazione e di limitazione della conservazione e delle finalità.

La raccolta e l'analisi di un numero molto esteso di dati collide evidentemente con il principio di minimizzazione, ma non solo. Del pari il principio di limitazione delle finalità si dimostra incompatibile con alcune modalità di trattamento. Come visto, non è sempre agevole per il titolare predeterminare a priori gli scopi dei trattamenti, in quanto essi vanno componendosi e delineandosi proprio a seguito dell'analisi che dei dati raccolti viene fatta.

Così evidenziate le maggiori criticità, nel dettato normativo sono presenti canoni che invece ben potrebbero adattarsi alla nuova realtà tecnologica e che dunque meriterebbero una maggiore attenzione. In particolare, il principio di esattezza, come si vedrà in seguito, riveste una sostanziale importanza proprio nel contesto delle applicazioni di AI. La previsione di un obbligo di utilizzo di dati di qualità, infatti, diminuendo possibili *bias*, potrebbe comportare una minore incidenza di risultati errati o discriminatori.

Di particolare importanza nel contesto delle tecnologie digitali è anche il tema della sicurezza dei trattamenti, come dimostra la centralità che esso assume all'interno del GDPR. Oggi la *cybersecurity* è un tema particolarmente sentito, non solamente dai soggetti privati, ma anche dalle istituzioni pubbliche, a fronte di attacchi sempre più estesi alla sicurezza delle comunicazioni e delle reti. Proprio la presenza di una connessione alla rete, e quindi della trasmissione dei dati, rende le tecnologie odierne particolarmente sensibili ad attacchi alla sicurezza, forieri di possibili danni non

solamente per gli interessati ma anche per gli stessi titolari dei trattamenti e, in alcuni casi, finanche per l'intera collettività.

Il legislatore europeo, dunque, consapevole della sensibilità e dell'urgenza di una efficiente regolazione della materia, ha previsto la sicurezza quale elemento essenziale dell'intero trattamento; il riferimento all'implementazione di misure di *privacy by design* e *by default* ne è compiuta espressione. Sul punto espliciti richiami vengono fatti anche alle tecniche di anonimizzazione e di pesudonimia, ritenute strumenti idonei a tutelare i diritti degli interessati. Tuttavia, come si è mostrato, anche dette tecniche presentano alcuni profili di criticità, sia perché non sono immuni da potenziali attacchi hacker, sia perché non hanno un carattere definitivo, e ciò anche nel caso di anonimizzazione. Ne discende come sia indispensabile un'attenta ponderazione e un bilanciamento nell'utilizzo di dati così trattati.

Tra i possibili interventi normativi sul punto, sarebbe auspicabile l'introduzione di specifici obblighi nei confronti dei titolari; in particolare questi potrebbero essere chiamati a un controllo temporalmente scadenzato e volto a verificare la compatibilità, in relazione allo stato dell'arte, degli strumenti e della stessa architettura del trattamento con quanto previsto dal GDPR a tutela delle persone fisiche.

Così evidenziate le prime criticità applicative della normativa europea nel contesto della concreta applicabilità alle applicazioni di AI, l'indagine verrà ora rivolta in particolare alle decisioni automatizzate, non essendo pacifica l'effettività degli strumenti di tutela introdotti dall'art. 22 del Regolamento generale sulla protezione dei dati.

CAPITOLO 4

Black box society e decisioni automatizzate

SOMMARIO: 1. Profilazione e decisioni automatizzate. – 2. La Convenzione 108 e le sue recenti modificazioni. – 3. Le decisioni automatizzate nel GDPR. – 3.1. Le basi di legittimità del trattamento. Quale spazio per il consenso dell'interessato. – 4. Il diritto alla spiegazione, un dibattito ancora acceso. – 4.1. La *black box society*. – 4.2. Quali possibili soluzioni all'opacità intrinseca dei sistemi. – 5. Le previsioni del GDPR a tutela degli interessati: l'*accountability*, la valutazione di impatto e la responsabilità per illecito trattamento dei dati personali. – 5.1. La valutazione di impatto. – 5.2. La responsabilità per illecito trattamento dei dati personali. – 6. Possibili prospettive di tutela. – 6.1. La *blockchain* quale possibile alleato nella filiera di dati di qualità. – 7. Considerazioni conclusive.

1. Profilazione e decisioni automatizzate

La possibilità che una macchina possa prendere in maniera del tutto autonoma, senza dunque la supervisione dell'uomo, alcune decisioni aventi una ricaduta sugli utenti oggi non è così lontana; anzi, sempre più settori sono interessati dall'uso di applicazioni di AI che permettono di limitare, fino in alcuni casi a marginalizzare, l'apporto umano. Si pensi agli algoritmi utilizzati per contrattare nei mercati finanziari senza alcun intervento dei broker. L'impiego delle tecnologie digitali non è tuttavia limitato al settore finanziario ma è ormai molto vasto e interessa diversi settori dell'economia mondiale; che si tratti di utilizzo di algoritmi nel marketing, nel settore medico o automobilistico, si assiste sempre più a una trasformazione digitale dell'intera società.

I vantaggi derivanti da una decisione completamente automatizzata affidata a sistemi informatizzati sono certamente notevoli. I processi così congegnati sono, infatti, economici, rapidi, rispondono all'esigenza di semplificazione riducendo l'apparato burocratico, le decisioni appaiono prevedibili e certe e, infine, si ritengono imparziali. Tuttavia, come visto, all'uso di questi sistemi algoritmici si legano anche alcuni rischi

che è necessario analizzare attentamente[437]. Innanzitutto, la dichiarata imparzialità degli algoritmi decisori è espressione di un fraintendimento. Si ritiene che le macchine siano terze e imparziali in quanto non sarebbero soggette a preconcetti e costrutti valoriali che potrebbero invece affliggere il decisore umano. Ciò tuttavia non è pienamente rispondente al vero; se difficilmente gli algoritmi sono progettati per essere discriminatori, ciò non toglie che nella pratica possano esserlo. Si ricorda, infatti, che le applicazioni che si fondano sull'analisi dei dati sono da essi fortemente influenzate. Dall'analisi effettuata in merito al funzionamento delle applicazioni di AI è difatti emerso in modo evidente come il paradigma dell'imparzialità delle macchine non abbia un effettivo fondamento, in quanto gli stessi dati di addestramento sono espressione di una realtà che di per sé non è imparziale; ne discende gli *output* del sistema ben possano essere afflitti da *bias* e dunque essere errati o discriminatori.

Gli algoritmi non sono inoltre infallibili, come tutti gli artefatti hanno una percentuale di errore, per quanto bassa, ineliminabile. Si tratta allora di comprendere se, a fronte di un errore inevitabile, gli strumenti normativi oggi vigenti apprestino un'effettiva garanzia per i cittadini; per l'argomento che qui ci occupa, in particolare, ci si domanda se le disposizioni a protezione dei dati personali siano idonee a regolare i sistemi algoritmici.

---

[437] Gli algoritmi possono causare danni con il loro funzionamento, non solamente nel caso in cui il funzionamento sia afflitto da errori, ma anche quando essi stanno funzionando esattamente per come sono programmati. Per rimanere nell'esempio delle applicazioni utilizzate nei mercati finanziari si pensi all'*High Frequency Trading* (HFT), reso possibile dall'impiego di algoritmi, che è venuto all'attenzione delle autorità di vigilanza a seguito del c.d. Flash Crash verificatosi presso il New York Stock Exchange il 6 maggio 2010. In quella occasione alcuni algoritmi di trading in modo autonomo, dunque senza alcuna supervisione umana, iniziarono a vendere alcune azioni facendo registrare una flessione di circa il 10% dell'indice Dow Jones in pochi minuti, per poi recuperare le perdite entro la chiusura della stessa giornata. Queste oscillazioni nel mercato azionario sono sempre presenti, tuttavia l'impiego di algoritmi rende possibile una maggiore volatilità delle azioni. Grazie a questa velocità gli algoritmi divengono anche i principali beneficiari della turbativa, dal momento che essi possono vendere e acquistare titoli in tempi molto ristretti. La velocità operativa si dimostra essere proprio la loro maggiore caratteristica; gli algoritmi di trading difatti possono vendere per primi di fronte al ribasso dei prezzi e comprare al momento del rialzo, anticipando le mosse di un operatore fisico. In arg. INFANTINO, *op. cit.*, 1762 ss.; DENOZZA, *Logica dello scambio e "contrattualità": la società per azioni di fronte alla crisi*, in *Giur. comm*., 2015, 5 ss.; STRAMPELLI, *L'informazione societaria a quindici anni dal T.U.F.: profili evolutivi e problemi*, in *Riv. soc*., 2014, 991 ss. Oltre all'episodio del 2010 il fenomeno si è manifestato nuovamente, sempre nei mercati finanziari americani, nel 2013. A seguito di una notizia falsa circa un attentato a Barack Obama, gli HFT hanno processato la notizia, in anticipo rispetto agli operatori umani, intuendo un ribasso sui mercati e, dunque, anticipandone la verificazione e al contempo amplificandone la portata. Nell'arco di 15 minuti, mentre nel mercato finanziario si verificava una rarefazione di liquidità, a fronte di scambi per oltre 30 miliardi di dollari, gli algoritmi di trading maturarono 600 milioni di dollari di profitti. In arg. CONSULICH, *Il nastro di* Möbius*. Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa tit. cred.*, 2018, 195 ss.

Si è visto come i trattamenti operati mediante l'utilizzo di tecnologie *data driven* abbiano potenzialmente un impatto molto incisivo sulla privacy dei cittadini. La capacità degli algoritmi di inferire dati personali anche da *dataset* non personali e la capacità di re-identificare dati resi anonimi comportano un serio rischio per la privacy degli interessati. Soggetti terzi, infatti, potrebbero avere accesso, potenzialmente anche per scopi illeciti, alla sfera privata degli utenti, costituita da tutta quella serie di dati, anche sensibili, che considerati nel complesso rappresentano un'estrinsecazione della loro personalità nell'ecosistema digitale. L'accesso non autorizzato a questi dati si delinea, dunque, quale una indebita intrusione nella sfera privata degli individui, di cui spesso questi non sono a conoscenza.

Se è vero che, fuori dai casi di attacchi esterni a sistemi chiusi, aventi lo scopo di accedere a informazioni protette, sono gli utenti stessi a "fornire liberamente" i propri dati nel web, ciò non toglie che nel pensiero comune il singolo utente sceglie di fornire i propri dati solo al fine di poter usufruire di uno specifico e determinato servizio, non dunque in astratto per ogni trattamento anche successivo. Che questi stessi dati vengano poi raccolti e analizzati, spesso per costruire un profilo degli utenti diretto a finalità terze, l'interessato difficilmente ne è cosciente e tantomeno consapevole.

La predisposizione di misure di sicurezza quali l'anonimizzazione e la pseudonimizzazione dovrebbero rispondere proprio allo scopo di impedire che i dati possano essere ricondotti ai singoli utenti, così permettendone un trattamento sicuro e una più agevole circolazione all'interno del mercato digitale. Tuttavia si è visto come le tecniche sopra richiamate non siano in realtà efficienti nel lungo, ma spesso nemmeno nel breve periodo, proprio a fronte delle capacità degli algoritmi di ricavare dati personali e di re-identificare quelli resi anonimi mediante la correlazione statistica di una grande mole di dati. Ne discende, dunque, un'evidente perdita di controllo degli interessati sui propri dati, in pieno contrasto con il principio di autodeterminazione che rappresenta invece un nodo centrale del GDPR.

I rischi divengono, se possibile, ancora più evidenti nel caso in cui i dati raccolti e analizzati vegano utilizzati in trattamenti comportanti decisioni totalmente automatizzate. In questi casi si manifesta una più forte esigenza di tutela degli interessati, i quali, come visto, non sono coscienti del processo di analisi e di come esso venga compiuto potendo vederne unicamente l'esito, senza comprenderne le ragioni a

fondamento. La grande diffusione del fenomeno si accompagna a una sostanziale inconsapevolezza degli individui di esserne oggetto, ne discende dunque l'urgenza di una riflessione giuridica sul tema.

Una specifica previsione normativa è presente nel GDPR e precisamente all'art. 22, ove vengono apprestate alcune forme di tutela in caso di sottoposizione dell'interessato a decisioni basate unicamente su di un trattamento automatizzato, compresa la profilazione.

É bene fin da subito chiarire cosa si intenda con il termine profilazione[438], in quanto detto trattamento non esaurisce la categoria; si tratta, infatti, sì di un trattamento automatizzato, ma da esso non discende sempre, anche se spesso è così, una decisione automatizzata che incide sull'interessato[439]. Pertanto, adottando la definizione presente all'art. 4 del Regolamento 679/2016 UE, per profilazione si intende: «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*»[440]. Alla profilazione, in quanto espressione di uno specifico trattamento dei dati, devono dunque applicarsi i principi generali statuiti dal Regolamento, ivi comprese le basi di legittimità

[438] Ad occuparsi del tema fu per la prima volta il Consiglio d'Europa, nel 2010, con la raccomandazione CM/Rec (2010) 13, nella quale venivano previste alcune specifiche disposizioni in tema di profilazione, ivi inclusa una definizione. Sebbene il legislatore europeo abbia preso spunto da quanto previsto dalla raccomandazione in parola, permangono alcune differenze tra i due testi. In particolare, differentemente da quanto previsto dal Consiglio d'Europa, le disposizioni del Regolamento si applicano unicamente alle attività di profilazione che attengono ai dati personali, laddove nella raccomandazione si parlava invece genericamente di dati. Difatti, è bene notare come l'attività di profilazione si divida idealmente in tre fasi: la fase di immagazzinamento dati, che potrebbe anche non avere a oggetto dati di natura non personale; la fase di analisi, al fine di far emergere ricorrenze statistiche e, infine, la fase di inferenza nella quale, sulla base di alcune variabili o caratteristiche di un soggetto, vengono dedotte nuove variabili. Evidentemente l'approccio del Regolamento si mostra più tradizionale, ancorandosi al dato personale quale elemento imprescindibile per l'applicazione della normativa. Cfr. PIERUCCI, *Elaborazione dei dati e profilazione delle persone*, in *I dati personali nel diritto europeo*, cit., 424 s.

[439] Sul punto il Gruppo di Lavoro art. 29, nelle recenti linee guida pubblicate nel 2017, riporta un esempio per meglio comprendere la differenza tra profilazione e decisione automatizzata. Viene fatto il caso di una multa per eccesso di velocità comminata unicamente sulla base di prove raccolte da telecamere, in modo così totalmente automatizzato, giungendo il dispositivo a una decisione sul comminare o meno la contravvenzione. La profilazione, invece, potrebbe incidere sull'importo della multa, determinandolo in base a una valutazione che coinvolga diversi fattori, quali, per esempio, le abitudini di guida o se il guidatore abbia commesso o meno altre violazione del codice della strada. Cfr. Gruppo di Lavoro art. 29, *Guidelines on automated individual decision-making and profiling for the purposes of regulation* 2016/679 (WP251), 2017. In argomento PIERUCCI, *op. cit.*, 413 ss.

[440] Art. 4, n. 4, reg. UE n. 679/2016.

previste dall'art. 6[441]; a questi si accompagnano alcune indicazioni specifiche in merito sia agli obblighi informativi (artt. 13, 14), che al diritto di opposizione di cui all'art. 21[442].

Considerazioni in parte distinte devono invece essere fatte in merito alle decisioni automatizzate a cui il legislatore fa riferimento nell'art. 22. L'espressione "decisione automatizzata" (*Automated decision making*), non ricompresa tra le definizioni previste all'art. 4, è usata per indicare, più in generale, quel processo posto in essere da un sistema algoritmico in grado di inferire in modo autonomo – dunque senza una effettiva partecipazione di un essere umano – da un *dataset* una decisione rilevante per gli interessati. Risulta pertanto evidente come la profilazione ben potrebbe rientrare nel novero delle decisioni automatizzate, qualora alla creazione di un profilo segua una decisione che su questo si basi; del pari potrebbero esserci attività di profilazione che non sfocino in una decisione e decisioni automatizzate senza alcuna previa attività di profilazione degli utenti[443].

Nella prassi applicativa tuttavia spesso le decisioni automatizzate si fondano su di una previa profilazione degli utenti[444]. Si pensi alla decisione di concedere o meno un mutuo affidata a una macchina, la valutazione di questa si fonderà su di una preliminare profilazione dell'individuo diretta a valutarne il grado di affidabilità. Tutte le applicazioni che propongono suggerimenti ai propri utilizzatori si fondano su di una profilazione della persona, avente l'obiettivo di creare *cluster* di profili simili[445]. Le proposte si fondano su di una ricorrenza statistica che, per semplificare, risponde a questa regola: siccome ad altri utenti è piaciuto questo ulteriore prodotto anche tu (che

---

[441] Si rimanda alle considerazioni svolte *supra* al §3, in quanto trovano applicazione anche in materia di profilazione.

[442] Per una veloce disamina in argomento si rimanda a PIERUCCI, *op. cit.*, 427 ss.

[443] Per fare un esempio concreto, l'algoritmo che ha scelto le sedi di assegnazione degli insegnanti, a cui si rimanda *infra* per un approfondimento, non ha fondato la decisione su di una previa profilazione del corpo docente. In argomento si rimanda a COSTANTINI, *Profilazione e* "automated decision making" *in ambito lavorativo nella giurisprudenza italiana*, in *Lavoro nella giur.*, 2016, 984 ss.

[444] Nel parere del Gruppo di Lavoro art. 29, (WP251) 2017, cit. viene evidenziato come siano possibili tre diverse metodologie di utilizzo della profilazione: la prima, si compone di una generica attività di raccolta dati, anche mediante modalità non necessariamente automatizzate; la seconda presuppone delle decisioni fondate sull'attività di profilazione e, infine, ci sono le decisioni totalmente automatizzate. In argomento v. CAIA, nel *Commentario GDPR e normativa privacy*, cit., *sub* art. 22, 222 s.

[445] Si pensi per esempio a quando al termine di un acquisto di un prodotto da una nota piattaforma online, ma pressoché ormai è la norma, questa propone l'acquisto di altri prodotti che "potrebbero interessare". In questi casi l'algoritmo non fa altro che verificare cosa altri utenti, aventi profili simili, hanno acquistato prima e dunque suggerire i medesimi prodotti. Così come avviene per esempio con i suggerimenti di Spotify.

hai un profilo simile) potresti essere interessato al medesimo acquisto, dunque te lo consiglio. L'algoritmo non fa altro che trovare ricorrenze tra dati arricchendo e raffinando i *cluster* di utenti. Se poi la proposta di acquisto si rivela giusta, dunque il prodotto consigliato viene acquistato, l'algoritmo avrà una conferma di aver fatto una previsione corretta, riproponendo ad altri utenti lo stesso contenuto.

Se questo tipo di funzionamento può essere facilmente riconoscibile, per altre applicazioni la questione diviene più sfumata. Ci sono algoritmi che stimano il prezzo e propongono a ogni utente quello che ritengono sia disposto a spendere per un determinato bene, in ragione di una profilazione che tiene conto anche delle abitudini di acquisto fatte in precedenza. Anche i social network si fondano su di una profilazione degli utenti; questa è in realtà la loro principale attività svolta, in quanto essa rappresenta la reale fonte di reddito delle piattaforme. I profili creati sono, infatti, alla base della pubblicità mirata; è proprio la raccolta dei dati personali, necessaria alla creazione dei profili, a essere il corrispettivo all'utilizzo "gratuito" dei servizi resi. Tuttavia questo utilizzo che viene fatto dai titolari dei trattamenti, come nel caso appena visto, non è sempre chiaro agli interessati, che anzi ne rimangono spesso ignari.

Le tecniche di profilazione trovano una maggiore diffusione nei settori del marketing, la possibilità di "prevedere", anche se spesso si potrebbe parlare di "creare", i bisogni degli utenti comporta evidentemente un grande vantaggio per le aziende, che possono proporre una pubblicità mirata sui bisogni dei clienti. Un vantaggio potrebbe derivare anche per l'utente, quest'ultimo infatti, vedendosi proporre beni e servizi di cui ha bisogno, risparmierebbe il tempo che altrimenti avrebbe dovuto impiegare per la ricerca. Questo tipo di trattamento, tuttavia, non si limita al marketing, l'uso che dei profili viene fatto è molto variegato; si pensi alle *filter bubbles*[446]. Questa espressione è stata resa famosa da Pariser, che per primo ne coniò il termine in un saggio del 2011[447].

[446] Sul punto si v. Bianca, la quale cita la definizione, riporata dall'Oxford dictionary, scondo cui per *filter bubble* si intende «*A situation in which an Internet user encounters only information and opinions that conform to and reinforce their own beliefs, caused by algorithms that personalize an individual's online experience.* […] *the personalization of the web could gradually isolate individual users into their own filter bubbles*». M. BIANCA, *La* filter bubble *e il problema dell'identità digitale*, in *Medialaws – riv. dir. media*, 2019, 44.

[447] PARISER, *The filter bubble. What the Internet is hiding from you*, Milano, 2011 (trad. 2012). Tuttavia il fenomeno non è recente, si pensi alle famose camere d'eco, termine riferito originariamente ai media tradizionali, che già riunivano comunità di persone con una certa propensione politico-ideologica. Comprando un giornale, difatti, si è tendenzialmente consapevoli dell'area politica a cui si avvicina la testa giornalistica e, dunque, di fatto si crea una sorta di frammentazione tra i lettori. Diversi sono stati gli studi del fenomeno, si rimanda senza pretesa di esaustività a KISZL, FODOR, *The "Collage Effect" –*

Le c.d. bolle di filtraggio preoccupano i commentatori in quanto esse rischierebbero di ledere non solo l'autodeterminazione dell'individuo, ma, ove fossero utilizzate per fini politici, anche la stessa democrazia[448]. Queste bolle sono il risultato di una profilazione degli individui, a cui segue la proposizione agli stessi solamente di contenuti selezionati in base alle risultanze di detti profili, in una sorta di pregiudizio confermativo. Se dal punto di vista commerciale, come visto, possono derivare anche esternalità positive, emergono tuttavia preoccupazioni ove queste bolle vengano utilizzate per condizionare in modo pressoché inconsapevole gli individui, chiudendoli in una sorta circolo autoreferenziale che marginalizza ogni forma di pluralismo di idee e conoscenze.

La posizione in merito all'influenza determinata dalle *filter bubble* nel contesto digitale non è tuttavia pacifica. Negli anni, infatti, sono stati condotti differenti studi da quali emergerebbe una portata ridimensionata del fenomeno[449], il quale sarebbe in realtà controllabile non generando un effettivo isolamento degli individui nella rete. Il condizionamento delle *filter bubble* sarebbe invece più evidente, sebbene comunque non decisivo, per quegli individui che utilizzano i *social media* come mezzo principale di informazione. Vi sono però alcuni studi da cui emerge come le fonti con opinioni politiche maggiormente differenziate sembrino essere proprio i *social media*[450].

É in ogni modo nozione di comune esperienza che alla fruizione di un certo contenuto online segua una considerevole visibilità di messaggi aventi il medesimo

---

against filter bubbles: interdisciplinary approaches to combating the pitfalls of information technology (2018) 6 *The Journal of Academic Librarianship* 753 ss.; BOZDAG, VAN DEN HOVEN, *Breaking the filter bubble: Democracy and design* (2017) 4 *Ethics and Information Technology* 249 ss.; FLEXMAN, GOEL, RAO, *Filter Bubbles, Echo Chambers, and Online News Consumption* (2016) S1 *Public Opinion Quarterly* 298 ss.

[448] Per un approfondimento in merito all'incidenza negativa delle *filter bubble* nella costruzione dell'identità digitale degli individui si rimanda a M. BIANCA, *op. cit.*, 39 ss.; FASAN, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *Biolaw Journal – Rivista di BioDiritto*, 2019, 13 ss.

[449] In argomento l'interessante lo studio di KITCHENS, JHONSON, GRAY, *Understanding echo chambers and filter bubbles: the impact of social media on diversification and partisan shifts in news consumption* (2020) 4 *Mis Quarterly* 1619 ss.; BAKSHY, MESSING, ADAMIE, *Exposure to ideologically diverse news and opinion on Facebook*, 2015, consultabile all'indirizzo: *https://education.biu.ac.il/sites/education/files/shared/science-2015-bakshy-1130-2.pdf* (ultimo accesso 13 maggio 2021) e FLEXMAN, GOEL, RAO, *op. cit.*, 307 ss. ove gli Autori evidenziano come, a seguito di uno studio della cronologia del *browser* di circa 50.000 utenti nel Regno Unito, è emerso che il fenomeno delle *filter bubble* abbia in realtà un effetto relativamente modesto.

[450] Si rimanda a uno studio compiuto dai ricercatori dell'Università di Oxford pubblicato nel 2017. *Digital News Report* (2017) *Retuers* , consultabile all'indirizzo *https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf* (ultimo accesso 13 maggio 2021). Dall'analisi compiuta è inoltre emerso come la maggior parte degli americani predilige i portarli dei media tradizionali, quali il New York Times, per la lettura di notizie.

contenuto, in una sorta di paradosso confermativo. Nulla vieta di ricercare altre fonti, opinioni differenti, così da poter "uscire" dalla bolla di filtraggio in cui ci si trova, ma ciò presupporrebbe una certa maturità dell'utente, che mal si adatta ad alcune fasce per lo più giovani, come dimostra la diffusione delle *fake news*.

Con questa espressione si indica quel fenomeno, connaturato dall'essere tipicamente digitale, di creazione e diffusione di notizie false. Se di per sé la mera falsità non è meritevole di tutela, sono gli effetti che derivano dalla diffusione di tali notizie a una platea indistinta, quale è quella che popola la rete, che potrebbe generare un danno ingiusto. Si noti, inoltre, che proprio la diffusione pressoché incontrollata di tali notizie alimenta continuamente l'evento dannoso configurando una tipica ipotesi di illecito permanente. La divulgazione di notizie dal contenuto non veritiero potrebbe comportare la violazione simultanea di interessi contrattuali ed extracontrattuali, essendo la fattispecie caratterizzata da una plurilesività della condotta, e dunque causare danni patrimoniali e non. Per esempio, una notizia falsa in merito a un concorrente, o a un prodotto, può configurarsi quale concorrenza sleale; potrebbe configurarsi anche una pratica commerciale scorretta se la notizia viene diretta al consumatore per manipolarne le decisioni relative all'acquisto di un bene o di un servizio, così pregiudicandone la capacità di autodeterminazione. Del pari una *fake news* potrebbe avere un contenuto diffamatorio e dunque generare un *vulnus* all'onore e/o al decoro dell'interessato[451].

Accanto a questo fenomeno, crescente preoccupazione destano anche le alterazioni digitali di immagini e video, che, mediante la tecnologia, divengono sempre meno riconoscibili, come accade nel c.d. *deepfake*[452]. In questi contesti l'interessato viene così

[451] Sotto il punto di vista dell'elemento soggettivo dell'illecito, essendo riconducibile alla previsione degli artt. 2043 e 2059 c.c., il criterio di imputabilità applicabile pare dunque essere quello della colpa. Ne discende allora come chiamato a rispondere sia, oltre chi "crea" la notizia non veritiera, anche il *provider* che ne abbia avuto effettiva conoscenza, anche in assenza di comunicazioni di terzi, e che abbia colposamente omesso di rimuovere i contenuti illeciti. Il *provider*, si ricorda, ai sensi del d. lgs. n. 70/2003 non è tenuto a un obbligo di sorveglianza, né di alcuna attiva preventiva diretta a ricercare i fatti che indichino la presenza di attività illecite; ciò tuttavia non toglie che qualora egli ne giunga a conoscenza debba informare l'autorità di sorveglianza, sia intervenire per impedire il protrarsi della situazione lesiva. Il tema meriterebbe un maggiore approfondimento che non è possibile fare in questa sede. Si rimanda sul punto ad ANDREOLA, Fake news *e danno da false informazioni in internet*. *I parte*, in *Resp. civ. e prev*., 2020, 1064 ss.; ID., Fake news *e danno da false informazioni in internet*. *II parte*, *ivi*, 2000 ss.; FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. inform.*, 2020, 475 ss.; CASINI, *Lo stato nell'era di Google*, in *Riv. trim. dir. pubb.*, 2019, 1126 ss.

[452] In argomento il Garante per la Privacy ha recentemente pubblicato una scheda informativa sui rischi dell'uso malevolo di questa nuova tecnologia. Il documento è consultabile all'indirizzo: *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278* (ultimo accesso 30 maggio 2021).

ulteriormente leso, rispetto alle ordinarie ipotesi di danni discendenti dalla diffusione di informazioni false. L'alterazione di video o immagini di una persona ne compromette, infatti, la stessa identità digitale. Quest'ultima si compone di tutti quei dati e informazioni che, resi disponibili dall'utente, rappresentano un tratto distintivo della rappresentazione del suo "io" digitale. La falsificazione della rappresentazione del sé può dunque comportare una lesione del diritto ad una libera espressione della personalità degli utenti, avente copertura costituzionale all'art. 2[453].

Diversi dunque, come visto, i profili di rischio a cui gli individui sono esposti nell'ambiente digitale. Tornando alle riflessioni in merito alle tecniche di profilazione, emerge con chiarezza come queste di per sé comportino un rischio se possibile ancora più incidente proprio in relazione alla stessa libera determinazione degli utenti nella formazione della propria identità. La creazione di profili mediante correlazioni statistiche potrebbe, infatti, comportare una normalizzazione della persona, escludendo ogni espressione singolare che esuli da quanto rientrante della normalità statistica. Inoltre la continua opera di controllo e monitoraggio dei comportamenti degli individui, i quali vengono raccolti al fine di "migliorare" il profilo, potrebbe impattare anche sulle libertà personali, e in special modo quelle di espressione e di associazione; sapendosi sempre sotto controllo gli utenti potrebbero limitarsi, se non addirittura censurarsi, per non rischiare di essere discriminati sulla base dei dati raccolti in rete. A ciò si aggiunge inoltre il rischio di esclusione e discriminazione derivante da un profilo inaccurato, a cui difficilmente gli interessati potranno avere pieno accesso a fronte della diffusa opacità di funzionamento degli algoritmi[454]. Ciò è ancora più evidente se si rammenta quanto evidenziato in merito alla difficoltà di comprensione delle ragioni a fondamento degli *output*, in particolare nel caso di *deep learning*, che comporta una concreta difficoltà di contestazione del risultato[455].

[453] ANDREOLA, Fake news *e danno da false informazioni in internet, I parte*, cit., 1670 ss.
[454] Cfr. PIERUCCI, *op. cit.*, 414 ss.
[455] Ciò è particolarmente evidente nelle reti neurali artificiali che, come già ricordato, si compongono di uno strato nascosto ove vengono effettuati calcoli matriciali; proprio questo strato costituisce il cuore della c.d. *black box*. Le criticità per gli interessati emergono in relazione all'analisi compiuta dai sistemi; gli algoritmi non si limitano a ripetere le esperienze immagazzinate nei *dataset*, ma ricombinano i dati che acquisiscono con il rischio di perpetrare *bias* e possibili elementi discriminatori ivi presenti. Cfr. FALLETTI, *op. cit.*, 175.

Sono diverse le esperienze di decisioni algoritmiche errate o discriminatorie che hanno avuto una grave incidenza sugli interessati[456]. Un richiamo, per così dire obbligato, non può non essere fatto al famoso caso COMPAS[457], ove un cittadino afroamericano è stato condannato a sei anni di reclusione sulla base dei risultati dati dal software che lo classificava come ad alto rischio di recidiva.

Nel caso di specie, nel 2013 Eric Loomis veniva fermato dalla polizia mentre guidava un'autovettura usata in una sparatoria. L'uomo veniva condannato a una pena di sei anni di reclusione e cinque di libertà vigilata avendo i giudici, attraverso l'utilizzo del software COMPAS, ritenuto l'imputato un individuo ad alto rischio di recidiva[458]. Il software, il cui codice sorgente è coperto da segreto, prometteva, infatti, di stimare inferendo da una serie di dati tra cui la fedina penale dell'imputato e le risposte date ad un questionario di 137 domande, il rischio di recidiva[459].

La difesa di Loomis aveva avanzato richiesta di accesso al codice sorgente dell'algoritmo al fine di poter comprendere, ed eventualmente contestare, l'esito della valutazione compiuta. Tale richiesta veniva tuttavia rigettata dalla Corte sulla base della natura proprietaria del software in uso. Veniva dunque impugnata la sentenza, fondandosi la difesa sulla violazione del diritto costituzionalmente garantito a un giusto processo, avanti alla Corte d'Appello che rinviava la questione alla Corte Suprema dello

[456] Sul punto si rimanda a FALLETTI, *op. cit.*, 193 ss., la quale riporta alcune vicende avvenute oltreoceano. Si fa riferimento alla controversia olandese inerente all'uso del software SyRi, deputato a controllare le domande di sussidi pubblici, dimostratosi operare in modo discriminatorio.

[457] State v. Loomis, 881 N. W.2d 749, 767 (Wis. 2016). In argomento Simoncini evidenzia come l'utilizzo di *evidence-based risk assessment tools* nelle decisioni giudiziarie risale a circa dieci anni prima del caso in esame. Nel settembre del 2004 la conferenza giudiziaria degli Stati Uniti aveva approvato una strategia orientata alla riorganizzazione del sistema probatorio federale, al fine di promuovere la riduzione della recidiva. L'utilizzo, dunque, di *software* automatizzati per valutare i rischi di recidiva rientrava in detta strategia; inoltre l'impiego di tali strumenti era stato incentivato in particolare nei *parole boards*, incaricati di determinare l'ammontare della cauzione per il rilascio dell'imputato, orientamento ancora oggi diffuso tra le corti americane. V. SIMONCINI, *Diritto costituzionale e decisioni algoritmiche*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., 46.

[458] Nel febbraio del 2013, Eric Loomis veniva arrestato mentre guidava un'auto usata in una sparatoria. Arrestato, si dichiarava colpevole di oltraggio a pubblico ufficiale e, inoltre, non contestava di essersi appropriato di un veicolo senza consenso del proprietario. In conseguenza di questi fatti l'imputato veniva condannato a sei anni di reclusione. Per giungere a questa sentenza il Giudice aveva adoperato il software COMPAS (*Correctional offender management profiling for alternative sanctions*), il quale indicava l'imputato quale ad alto rischio di recidiva, citandone l'*output* anche nella motivazione della sentenza. Nel caso di specie il produttore di COMPAS, società privata, si rifiutò di rivelare in giudizio la metodologia e le linee guida utilizzate dal software per le sue decisioni, nonostante il punteggio sulla valutazione del rischio elaborato dall'algoritmo fosse stato citato in sentenza.

[459] Si riteneva che questo algoritmo fosse in grado di prevedere il rischio di recidiva di una persona sulla base di una analisi complessa che implicava l'uso di informazioni raccolte mediante un questionario, composto da 137 domande, suddivise in diverse sezioni, e informazioni corrispondenti ai casellari giudiziari pubblici. In arg. FALLETTI, *op. cit.*, 176.

Stato del Wisconsin. La difesa di Loomis sosteneva che il giudice della Contea avesse violato il diritto dell'imputato a conoscere le ragioni a fondamento della sentenza, dal momento che gli era stato impedito di conoscere le logiche a fondamento della previsione effettuata dal software, che ricopriva una parte rilevante della motivazione. Queste argomentazioni sono state tuttavia respinte dalla Corte Suprema la quale, confermando la sentenza di primo grado, ha sostenuto come l'utilizzo del software nel caso di specie non abbia violato il diritto al giusto processo. La Corte ha ritenuto corretta l'argomentazione dei giudici che avrebbero difatti chiarito come la considerazione dei punteggi dati da COMPAS sia stato solo uno degli elementi considerati nella sentenza, la quale sarebbe dunque stata supportata anche da altri fattori indipendenti[460]. Pertanto, l'uso del sistema automatizzato non è stato determinante per la decisione finale, dimostrandosi solo uno strumento di aiuto per i giudici, i quali sono comunque liberi di basarsi solo su parti di esso e rifiutarne altre. Inoltre, la Corte ha chiarito come proprio la natura proprietaria di COMPAS impedisca che si possano divulgare informazioni relative al modo in cui i fattori vengono pesati o alla determinazione dei punteggi di rischio, ritenendo dunque prevalente il diritto alla tutela proprietaria degli algoritmi sulle istanze di *disclosure* degli interessati[461].

[460] Nel 2016 la Corte Suprema dello Stato del Wisconsin ha affermato la legittimità della procedura, rigettando il ricorso di Loomis sulla base dell'assunto che la mancata conoscenza sul funzionamento dell'algoritmo non violasse il suo diritto a un processo equo e accogliendo invece la tesi delle società fornitrici dei software, secondo cui gli algoritmi sono segreti industriali che non possono essere divulgati, nemmeno agli imputati a cui si applicano. La corte Suprema del Wisconsin ha affermato, infatti, che l'utilizzo di un algoritmo, quale COMPAS, non presenti problemi di costituzionalità in materia di *due process* nel caso in cui il software operi trattando i singoli casi individualmente e utilizzando informazioni accurate. Evidentemente, per permettere ciò è necessario che nella fase di addestramento, o di apprendimento, la rete neurale sia alimentata con dati oggettivi e veritieri. Tuttavia, nonostante abbia confermato la costituzionalità dell'utilizzo di COMPASS, la Corte Suprema ne ha posto al contempo numerose restrizioni. É stato, infatti, statuito come l'algoritmo non possa più essere utilizzato per determinare se un imputato debba essere incarcerato o meno, ovvero per calcolare la durata della detenzione. La Corte ha inoltre previsto un obbligo di motivazione in sentenza sia in merito all'uso del software, sia per l'elaborazione del punteggio espressione del rischio di recidiva. Tuttavia, a questi rilievi la Corta ha infine evidenziato come l'algoritmo rimanga pur sempre un mero strumento di ausilio per il giudicante, così ridimensionando la sua utilità decisoria. Nel 2017 la decisione è stata confermata, divenendo così definitiva, dalla Corte Suprema USA, che ha declinato la propria competenza in materia. In arg. CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giur. econ.*, 2019, 47 s.; FALLETTI, *op. cit.*, 170 ss.; ISRANI, *Algorithmic due process: mistaken accountability and attribution in State v. Loomis*, 31 agosto 2017, consultabile all'indirizzo: *https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1* (30 maggio 2021). In argomento anche VAGNI, *The role of human judge in judicial decisions, preliminary remarks on legal interpretation in the age of artificial intelligence*, in *La decisione nel prisma dell'intelligenza artificiale*, a cura di CALZOLAIO, Milano, 2020 187 ss.

[461] V. SIMONCINI, *op. cit.*, 47.

Altro esempio è il caso dell'algoritmo di Deliveroo, oggetto di una recente ordinanza del Tribunale di Bologna che ne ha dichiarato il funzionamento discriminatorio[462].

In entrambi questi casi si assiste a un funzionamento per così dire corretto dell'algoritmo, in quanto rispondente a quanto in esso programmato, a cui tuttavia sono seguiti effetti discriminatori. Tra le maggiori criticità emerge proprio il profilo legato alla difficoltà di contestazione delle scelte del sistema. Nel caso Deliveroo non era infatti possibile forzare il software nella considerazione di ulteriori parametri, non previsti *ab origine*, finendo dunque questo per ledere il principio di uguaglianza e il diritto allo sciopero. Nel caso COMPAS, invece, la mancata possibilità di contestazione degli esiti discende direttamente dalla impossibilità di verificare con esattezza quali variabili, tra le molte, avessero inciso in maniera preponderante nella scelta, elemento questo rimasto coperto da segreto.

Appare dunque evidente la necessità di predisporre degli strumenti di tutela che possano essere efficacemente attivati dagli individui soggetti a una decisione automatizzata. Proprio in relazione a detto fenomeno un primo tentativo regolatorio venne posto in essere dal Consiglio d'Europa nel 1981.

2. La Convenzione 108 e le sue recenti modificazioni

Come si è già avuto modo di evidenziare, la circolazione dei dati e la sottoposizione degli utenti a un trattamento in tutto o in parte automatizzato non è un fenomeno recente. É emersa, infatti, fin dagli inizi degli anni '80 del secolo scorso una sempre più sentita esigenza di tutela degli utenti, potendo il trattamento incontrollato dei dati personali mediante sistemi informatizzati arrecare potenzialmente ingenti danni. Una

[462] Si fa riferimento alla recente ordinanza del Trib. Bologna, 31.12.2020, in *Riv. it. dir. lav*., 2021, II, 175. Nel caso di specie i fattorini della nota azienda di *food delivery* "Deliveroo" lamentavano di aver subito una discriminazione a opera dell'algoritmo, implementato nella piattaforma aziendale, il quale assegnava i turni di "scelta" delle fasce di lavoro a seconda di un punteggio assegnato a ciascun lavoratore. Questo punteggio si fondava sui turni di lavoro effettivamente svolti, diminuendo il *ranking* nel caso in cui il *rider*, prenotatosi per un turno di lavoro, non avesse disdetto la prenotazione entro 24 ore. Nei fatti se il *rider* non si presentava entro 15 minuti dall'inizio della sessione nella zona di lavoro, connettendosi all'apposita applicazione fornita di geolocalizzazione, veniva penalizzato nelle statistiche e dunque perdeva la possibilità di scegliere "prioritariamente" le sessioni di lavoro. Sebbene l'algoritmo non sia più in uso, il Tribunale di Bologna ha ritenuto il suo operato discriminatorio. L'algoritmo, infatti, non permetteva ai lavoratori di presentare documenti ulteriori che potessero modificare la decisione presa, operando in automatico una volta registrata la mancata presa di servizio. Evidentemente questo funzionamento di fatto penalizzava l'adesione dei lavoratori a forme di autotutela collettiva, in particolare astensioni totali dal lavoro, ledendo così un diritto loro garantito costituzionalmente.

conferma si trova nello stesso preambolo della Convenzione 108, ove viene appunto dichiarato che: «*Gli Stati membri del Consiglio d'Europa, firmatari della presente Convenzione, considerando che scopo del Consiglio d'Europa è quello di realizzare una unione più stretta tra i suoi membri, nel rispetto in particolare della prevalenza del diritto nonché dei diritti umani e delle libertà fondamentali; considerando che è auspicabile estendere la protezione dei diritti e delle libertà fondamentali di ciascuno, e in particolare il diritto al rispetto della vita privata, tenuto conto dell'intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica; riaffermando allo stesso tempo il loro impegno a favore della libertà d'informazione indipendentemente dalle frontiere; riconoscendo la necessità di conciliare i valori fondamentali del rispetto della vita privata e della libera circolazione delle informazioni tra i popoli* […]»[463].

La prima esplicita previsione normativa a tutela delle persone fisiche risale dunque al 1981, anno in cui la Commissione Europea emanò la Convenzione 108. Si tratta di un documento di grande importanza, in particolare in ragione della sua portata applicativa[464]. La Convenzione, strumento di diritto internazionale, trova infatti una diretta forza cogente nei confronti degli Stati firmatari, così rispondendo all'esigenza di garantire una più agevole circolazione dei dati anche all'infuori del perimetro dell'Unione Europea, ma al contempo di salvaguardare i diritti fondamentali degli individui. Il documento fu, infatti, promulgato col dichiarato scopo di apprestare una tutela uniforme dei diritti delle persone fisiche, in particolare in relazione all'elaborazione automatica dei dati personali che la riguardano[465].

Elemento rilevante è certamente la particolare attenzione prestata all'interno del dettato normativo alla qualità dei dati. Nella Convenzione viene, infatti, prescritto come essi debbano essere ottenuti legalmente, utilizzati per fini legittimi e determinati,

[463] Preambolo, Convenzione n. 108/1981.

[464] L'emanazione della Convenzione agli inizi degli anni '80 del secolo scorso testimonia come le nuove tecnologie guidate dall'analisi dei dati, le quali iniziavano a operare mediante decisioni automatizzate, richiedessero l'emanazione di strumenti *ad hoc* per contemperarne i rischi per gli interessati. Lo scopo della Convezione, primo documento in Europa in materia, mirava infatti a garantire la tutela dei dati personali proprio nei confronti delle decisioni automatizzate. In argomento si rimanda a DE GREGORIO, TORINO, *op. cit.*, 458 ss.; GIANNONE CODIGLIONE, *Internet e tutele di diritto civile*, cit., 123 s.

[465] «*Scopo della presente Convenzione è quello di garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)*». Art. 1, Convenzione n. 108/1981.

adeguati e non eccessivi rispetto ai fini perseguiti con il trattamento, conservati per il tempo strettamente necessario e infine esatti e, se necessario, aggiornati. Molti di questi principi saranno, come visto, ripresi dalle disposizioni della Direttiva 46/95 CE e, successivamente, ampliati nel testo del GDPR.

Ciò che emerge dalla lettura del testo originario è, tuttavia, la considerazione per cui fin dai i primi anni '80 fosse evidente il rischio concreto di lesioni dei diritti e delle libertà dei cittadini a seguito di un uso non regolamentato delle tecniche informatiche di elaborazione dati, che allora iniziavano a diffondersi.

Le preoccupazioni crebbero di pari passo con l'evoluzione tecnologica, rendendo necessario un aggiornamento delle normative di settore. Il Trattato, oggi firmato da 55 Stati, fu così sottoposto negli anni ad alcune modifiche, la prima delle quali nel 2004. Il testo attualmente vigente è il risultato di un recente aggiornamento, mediante un Protocollo del maggio 2018, attraverso cui il Consiglio d'Europa ha affrontato alcuni problemi legati all'utilizzo di nuove tecnologie dell'informazione e della comunicazione. Con detto aggiornamento il documento diviene così un ponte tra i vari quadri normativi appartenenti a diverse regioni del mondo e il perimetro di tutela apprestato in Europa dal Regolamento 679/2016 UE[466].

Difatti il testo attualmente vigente (che ha convenzionalmente mutato il nome della Convenzione in 108+) in molti punti richiama quanto statuito dal GDPR, non solo in merito ai principi generali applicabili a tutti i trattamenti, ma anche alla qualità dei dati e ai diritti degli interessati, così apprestando un quadro di garanzie uniforme all'interno degli ordinamenti degli Stati firmatari.

Tra le maggiori novità introdotte si può notare: un ampliamento della categoria dei dati "sensibili"; una maggiore trasparenza relativa all'elaborazione dei dati[467]; un rafforzamento della responsabilità dei titolari e responsabili del trattamento; la ricomprensione di un obbligo di applicazione del principio di tutela dei dati fin dalla

[466] BOCCACCINI, *op. cit.*, 45.

[467] L'art. 8, rubricato "Transparency of processing", prevede che: «*1. Each Party shall provide that the controller informs the data subjects of: a. his or her identity and habitual residence or establishment; b. the legal basis and the purposes of the intended processing; c. the categories of personal data processed; d. the recipients or categories of recipients of the personal data, if any; and e. the means of exercising the rights set out in Article 9, as well as any necessary additional information in order to ensure fair and transparent processing of the personal data. 2. Paragraph 1 shall not apply where the data subject already has the relevant information. 3. Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts*». Convenzione n. 108/1981, nel testo modificato dal protocollo del 2018.

progettazione e, infine, la previsione di nuovi diritti delle persone con riguardo ai processi decisionali automatizzati basati sugli algoritmi.

In merito a questi ultimi si osserva come all'art. 9 sia previsto un elenco di prerogative per gli interessati. In particolare, si statuisce che ogni individuo abbia il diritto di poter conoscere, su richiesta, le motivazioni alla base del trattamento, laddove i risultati del processo automatizzato siano ad esso applicabili[468]. Si tratta dunque di una previsione molto estesa, applicabile in ogni caso in cui un individuo sia soggetto a una decisione automatizzata a lui riferita. Il testo originario della Convenzione viene così ampliato ricomprendendo in gran parte quanto previsto dal GDPR; la *ratio* risiede evidentemente nell'esigenza di apprestare una normativa il più possibile omogena, introducendo alcuni obblighi, ritenuti a presidio dei diritti fondamentali degli individui, anche per quegli Stati che, non facendo parte dell'Unione Europea, non sono soggetti all'applicazione delle disposizioni del Regolamento in parola. Ciò si era reso necessario alla luce della consapevolezza in merito alla natura evidentemente transnazionale dei trattamenti operati mediante tecnologie *data driven*, tra cui l'AI. Una normativa che fosse limitata territorialmente rischiava, infatti, di non apprestare un'adeguata ed efficace regolazione dei trattamenti digitali, qualora ad uno o più soggetti non fossero applicabili le medesime disposizioni, così rischiando inoltre di dare spazio a possibili fenomeni di *forum shopping* verso ordinamenti più permissivi e meno garantisti.

Consapevole dell'urgenza di apprestare una base di principi condivisi sul panorama internazionale il comitato consultivo della Convenzione 108 ha così recentemente

[468] L'art. 9, rubricato "Rights of the data subject", prescrive che: «*1. Every individual shall have a right: a. not to be subject to a decision significantly affecting him or her based solely on an automated processing of data without having his or her views taken into consideration; b. to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her, the communication in an intelligible form of the data processed, all available information on their origin, on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing in accordance with Article 8, paragraph 1; c. to obtain, on request, knowledge of the reasoning underlying data processing where the results of such processing are applied to him or her; d. to object at any time, on grounds relating to his or her situation, to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms; e. to obtain, on request, free of charge and without excessive delay, rectification or erasure, as the case may be, of such data if these are being, or have been, processed contrary to the provisions of this Convention; f. to have a remedy under Article 12 where his or her rights under this Convention have been violated; g. to benefit, whatever his or her nationality or residence, from the assistance of a supervisory authority within the meaning of Article 15, in exercising his or her rights under this Convention. 2. Paragraph 1.a shall not apply if the decision is authorised by a law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests*». Convenzione n. 108/1981, nel testo modificato dal protocollo del 2018.

emanato delle linee guida in materia di Intelligenza Artificiale, indirizzate ai *policy maker* e agli sviluppatori degli stessi algoritmi[469]. Dopo aver evidenziato come le applicazioni di Intelligenza Artificiale rappresentino uno strumento utile, specialmente nel supportare politiche inclusive, viene fatta luce sulle possibili ripercussioni negative che un uso non regolato della tecnologia può comportare sia per gli individui che per l'intera società. L'obiettivo della Convenzione, e delle linee guida, si innesta dunque in una strategia di tutela della dignità, dei diritti e libertà fondamentali di ogni individuo, in particolare con riferimento alla protezione dei dati, attraverso la previsione di alcune misure che, se implementate dai Governi e dai produttori delle tecnologie, avrebbero anche il pregio di accrescere la fiducia degli utenti[470].

Il comitato dunque richiama l'attenzione su di un approccio basato su di un principio di precauzione, rivolto *in primis* ai produttori e agli sviluppatori dei servizi di AI. Questi vengono così chiamati a valutare e ponderare i rischi discendenti dalle applicazioni digitali e porre in essere appropriate misure di prevenzione e di sicurezza. Un esplicito richiamo viene fatto alla necessità di un'educazione anche etica degli esperti, i quali dovrebbero tutelare i diritti umani fin dalla progettazione (*human rights by design*) e così ridurre il rischio di potenziali pregiudizi (*bias*) e discriminazioni.

Proprio in relazione alla necessità di evitare possibili pregiudizi una particolare attenzione viene posta anche alla verifica circa la qualità dei dati, secondo una declinazione atta a ricomprendere la natura, l'origine e la quantità, per tutte le fasi di funzionamento degli algoritmi. Si invitano infine i programmatori a utilizzare dati c.d. sintetici[471]; l'utilizzo di questi viene infatti presentato come una possibile soluzione atta a minimizzarne la quantità, in applicazione del principio di minimizzazione sancito dal

---

[469] Comitato Consultivo Convezione 108, *Linee guida in materia di intelligenza artificiale e protezione dei dati*, 2019, T-PD (2019) 01.

[470] Il Comitato ricorda, infatti, come «La protezione della dignità umana e la tutela dei diritti umani e delle libertà fondamentali, in particolare il diritto alla protezione dei dati personali, sono essenziali nello sviluppo e nell'adozione di applicazioni AI che possono avere conseguenze sugli individui e la società. Ciò è particolarmente importante quando le applicazioni AI vengono utilizzate nei processi decisionali». Si invitano, dunque, gli Stati e le parti interessate a prestare una particolare attenzione ai principi di liceità, correttezza, responsabilità e sicurezza fin dalla progettazione.

[471] L'espressione "dati sintetici" viene utilizzata per indicare quei dati generati da un modello con l'obiettivo di essere "rappresentativi" di quelli originali. Una definizione è presente nel documento, emanato dall'OCSE nel 2007, "Glossario dei termini statistici", ove si precisa come il termine sia espressivo di «*An approach to confidentiality where instead of disseminating real data, synthetic data that have been generated from one or more population models are released*». OECD, *Glossary Of Statistical Terms*, 2007, 768, consultabile all'indirizzo: *http://ec.europa.eu/eurostat/ramon/coded_files/OECD_glossary_stat_terms.pdf* (ultimo accesso 4 aprile 2021).

GDPR, oltre che a prestare attenzione all'applicazione di modelli algoritmici decontestualizzati. Quest'ultimo invito discende dalla consapevolezza delle modalità di addestramento delle tecniche di AI. Come visto nel primo capitolo del presente lavoro, gli algoritmi sono progettati per rispondere ad un determinato compito e addestrati con una mole considerevole di dati. É evidente, dunque, come l'accuratezza del sistema sia legata unicamente allo specifico compito per cui è stato addestrato. L'utilizzo di applicazioni di AI decontestualizzate potrebbe comportare dei rischi, sia perché non è più possibile fare affidamento sui test effettuati prima della messa in commercio del sistema, sia perché in un contesto di utilizzo differente i dati di addestramento potrebbero non essere sufficientemente rappresentativi, rischiando così di generare risultati discriminatori o comunque dannosi per gli utenti.

Per quanto riguarda i *policy maker* il comitato invita a una maggiore implementazione dei principi di responsabilizzazione dei titolari mediante la previsione di obblighi di controllo e di trasparenza, fatta salva la riservatezza tutelata dalla legge, oltre che di una valutazione preliminare d'impatto. Oltre a ciò si invitano i governi ad investire risorse nell'alfabetizzazione digitale e negli strumenti per monitorare e sostenere programmi di vigilanza sugli algoritmi, da demandare alle autorità di controllo e a comitati di esperti[472].

Dalla lettura delle linee guida emerge, dunque, con chiarezza come sia necessario intervenire in un momento prodromico al trattamento dei dati, cioè nel momento stesso della progettazione dei sistemi digitali. Il Consiglio d'Europa, così come le Istituzioni europee, puntano l'attenzione su di un'opera di sensibilizzazione e di alfabetizzazione etica, prima ancora che giuridica, nell'evidente scopo di implementare soluzioni che siano dirette a tutelare, fin dalla progettazione, i diritti fondamentali dell'uomo. Se pregevoli sono gli inviti rivolti a programmatori e sviluppatori, essi tuttavia rischiano di rimare solo delle dichiarazioni di principio in assenza di previsioni che siano cogenti. Sul punto invece di maggiore impatto poterebbe essere l'estensione della portata del principio di *accountability*, nella sua declinazione prevista dal GDPR, la cui

[472] Comitato Consultivo Convezione 108, *Linee guida in materia di intelligenza artificiale e protezione dei dati*, cit.

applicazione nel contesto dell'utilizzo di sistemi algoritmici si dimostra tra gli strumenti più efficaci a presidio delle garanzie per gli interessati[473].

A completamento del quadro regolativo attualmente vigente fondamentali si dimostrano dunque le previsioni del Regolamento 679/2016 UE e in particolare l'art. 22, specificamente dedicato alle decisioni automatizzate.

3. Le decisioni Automatizzate nel GDPR

Si è già avuto modo di evidenziare la centralità ricoperta dal GDPR nella regolazione dell'Intelligenza Artificiale fin dalla previsione dei principi generali, sebbene essi meritino in parte un ripensamento e in parte un'implementazione. La diffusione di sistemi che operano una profilazione degli utenti e di processi decisionali automatizzati comporta tuttavia l'emersione di differenti criticità; si teme, infatti, finanche un rischio per gli individui di essere espropriati del diritto di costruire e controllare la propria immagine sociale[474].

Alla luce di tali considerazioni il legislatore europeo ha previsto all'interno del Regolamento una serie di requisiti necessari a rendere i trattamenti automatizzati conformi alla normativa[475], tra cui in particolare: specifiche prescrizioni in tema di trasparenza e correttezza; maggiori obblighi di *accountability*; indicazioni in merito alle basi giuridiche specifiche del trattamento; garanzie per gli individui, tra cui la previsione di un diritto di opposizione alla profilazione e, infine, l'indicazione dell'obbligo di una valutazione di impatto sulla protezione dei dati (*data protection impact assessment*), qualora non siano soddisfatte determinate condizioni[476].

---

[473] FINOCCHIARO, *Il principio di* accountability, *GDPR tra novità e discontinuità*, a cura di CATERINA, in *Giur. it*., 2019, 2777 ss.

[474] Tra questi si sottolinea il possibile rischio di una standardizzazione delle identità personali, ridotte e uniformate per essere ricomprese in *cluster* di utenti, e dell'esclusione sociale della diversità. V. HILDEBRANDT, *Learning as a machine: Crossovers between Humans and Machines* (2017) *Journal of Learning Analytics* 6 ss. L'identità personale risulta inevitabilmente ridotta nella sua espressione digitale; ciò sia in quanto può essere rappresentato solo ciò che è leggibile dal sistema informatico, dunque solo ciò che è codificabile, sia in quanto le attività di profilazione degli utenti, sempre più diffuse, tendono a marginalizzare ogni difformità da quello che viene rilevato quale regolarità statistica. Sul punto si veda FLORIDI, *ibidem*; MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, in *Persona e mercato dei dati*, cit., 190 ss.; PIERUCCI, *op. cit.*, 415 ss.; BOLOGNINI, PELINO, BISTOLFI, *Il regolamento privacy europeo*, Milano, 2016, 272 ss.

[475] CAIA, *op. cit.*, 221 ss.

[476] CAIA, *op. cit.*, 228.

Appare dunque necessaria un'attenta analisi delle disposizioni del GDPR in ordine alla verifica circa una loro efficacia nella regolazione del fenomeno che qui ci occupa.

Di primaria importanza, in argomento, l'art. 22, rubricato "processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione", il quale prescrive che: «*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona*»[477]. La fattispecie richiama l'art. 14 del previgente codice privacy italiano[478], considerato da attenta dottrina una norma generale sulla distribuzione del potere decisionale nella realtà digitale[479]. La disposizione, a differenza di quanto poi previsto nel Regolamento, come è noto, non impediva l'uso di elaborazioni automatizzate dei dati personali, ma impediva che al risultato di questo trattamento fosse dato un valore definitivo, trasformandosi in un giudizio automatico sull'utente[480].

La scelta dunque dell'attuale formulazione dell'art. 22 è il frutto di un rilevante ampliamento della portata applicativa della disciplina previgente; diretta conseguenza delle riflessioni in merito ai possibili eventi lesivi incidenti sull'individuo e sulla stessa collettività. Il legislatore, difatti, nella formulazione del testo trasfuso nel Regolamento espunge il riferimento specifico ai provvedimenti amministrativi o giurisdizionali; viene

---

[477] «*1. L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona. 2. Il paragrafo 1 non si applica nel caso in cui la decisione: a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento; b) sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato; c) si basi sul consenso esplicito dell'interessato. 3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del trattamento, di esprimere la propria opinione e di contestare la decisione. 4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato*». Art. 22, reg. UE n. 679/2016.

[478] «*1. Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato. 2. L'interessato può opporsi ad ogni altro tipo di determinazione adottata sulla base del trattamento di cui al comma 1, ai sensi dell'articolo 7, comma 4, lettera a), salvo che la determinazione sia stata adottata in occasione della conclusione o dell'esecuzione di un contratto, in accoglimento di una proposta dell'interessato o sulla base di adeguate garanzie individuate dal presente codice o da un provvedimento del Garante ai sensi dell'articolo 17*». Art. 14, d. lgs. n. 196/2003 (Codice Privacy), ora abrogato.

[479] RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, 324 ss.

[480] MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, cit., 248 s.

ampliata la portata del divieto in generale a tutti i trattamenti che comportino una decisione unicamente automatizzata, purché essa incida significativamente sui diritti degli interessati[481].

L'art. 22, che prosegue con alcune eccezioni, è tuttavia ancora oggetto di dibattito tra gli studiosi in relazione a diversi aspetti. In primo luogo ha destato interesse l'avverbio "unicamente", il quale se interpretato restrittivamente potrebbe limitare oltremodo la portata applicativa del precetto, fino a renderlo nella gran parte dei casi inapplicabile; a una interpretazione letterale e restrittiva seguirebbe, infatti, l'esclusione di tutti quei processi nei quali si riscontra un minimo intervento umano. Nella prassi dunque basterebbe la mera presenza di un operatore per sottrarsi all'applicazione della norma, rendendola così di fatto lettera morta[482].

A fronte di dette considerazioni la dottrina più illuminata ritine invece che al termine "unicamente" debba essere data una interpretazione estensiva e sistematica, alla luce anche degli obiettivi di tutela della normativa europea, fino a ricomprendere tutte le decisioni in cui la fase preparatoria, quale può essere la valutazione delle prove, e i giudizi discrezionali siano operati autonomamente dalla macchina; a prescindere dunque dalla presenza di un essere umano che formalmente, ma non nella sostanza, prenda la decisione finale, limitandosi magari a conformarsi all'esito elaborato dal sistema[483]. Questa impostazione è stata anche confermata dall'*UK Information Commissioner's Office*, il quale ha sostenuto che l'avverbio "unicamente" intende ricomprendere i processi automatici nei quali gli esseri umani, pur formalmente presenti, non esercitano alcuna reale influenza sulla decisione finale, non ritenendosi questa modalità di apporto umano sufficiente a escludere l'applicabilità della disposizione in esame[484].

L'interpretazione da ultimo richiamata si dimostra essere quella più in linea con l'intero spirito della normativa europea; quest'ultima, si ricorda, è diretta ad apprestare una tutela effettiva nei confronti degli interessati soggetti al trattamento dei propri dati

[481] In arg. PIERUCCI, *op. cit.*, 436 ss.
[482] WACHTER, MITTELSTADT, FLORIDI, *Why a right to explanation of automated decision-making does not exist in the general data protection regulation* (2017) 2 *International Data Privacy Law* 79 ss.
[483] MALGIERI, COMANDÈ, *Why a right to legibility of automated decision-making exists in the general data protection regulation* (2017) 4 *International Data Privacy Law* 251 ss.; CAIA, *op. cit.*, 223; PELLECCHIA, *op. cit.*, 1213 ss.; PIERUCCI, *op. cit*., 437 s.
[484] UK information Commissioner's Office, *Feedback request- profiling and automated decsion*-making, 6.4.2017. Sul punto si v. anche CAIA, *ibidem*.

personali e ciò a maggior ragione in quei procedimenti ove il rischio di lesioni sia particolarmente intenso, come nel caso dei trattamenti automatizzati[485]. Una interpretazione letterale e restrittiva, al contrario, comporterebbe una facile elusione delle garanzie introdotte nel dettato normativo, limitandosi queste a essere applicabili nei rari casi in cui fosse totalmente esclusa la presenza umana.

Le stesse linee guida del Comitato Europeo per la Protezione dei Dati hanno avallato una ricostruzione più estensiva, escludendo dunque che il titolare del trattamento possa eludere il divieto dell'articolo in oggetto limitandosi a una formale attribuzione a un essere umano della decisione, senza che esso partecipi effettivamente e compiutamente al processo decisorio[486].

Sempre in merito alla portata applicativa della norma, si ritiene necessaria una interpretazione sistematica anche della previsione dell'ultima parte del primo comma secondo cui la decisione automatizzata debba produrre effetti sulla sfera giuridica dell'interessato, o incidere in modo analogo significativamente sulla sua persona. Sul punto il Regolamento non prevede alcuna specificazione su cosa debba intendersi con detta espressione; anche in questo caso tuttavia un'interpretazione restrittiva comporterebbe un'eccessiva limitazione delle tipologie di trattamenti assoggettati alla disciplina in parola. Ne discenderebbe, infatti, l'esclusione di tutte quelle situazioni in cui verrebbero lesi solamente degli interessi non riconosciuti quali diritti della persona.

Una tale ricostruzione, oltre che non in linea con gli scopi del Regolamento, ha generato incertezze in merito a trattamenti molto diffusi, ma che nella pratica non possono dirsi ledere un diritto degli interessati, tra questi per esempio la pubblicità mirata. Controversa era vista l'applicazione della norma anche ai trattamenti che operavano mediante algoritmi di determinazione del prezzo dinamico, in quanto anch'essi non avrebbero inciso direttamente sui diritti degli utenti.

Al fine di chiarire la portata specifica della norma si è dunque espresso, nel parere citato più volte, il Gruppo di Lavoro art. 29, il quale ha precisato che per "effetto giuridico" deve intendersi un'attività che abbia un impatto sui diritti di un individuo, come ad esempio la libertà di associazione, ma anche quelle attività che colpiscano lo

[485] In argomento PELLECCHIA, *ibidem*, la quale sottolinea come dovrebbero ricadere nelle ipotesi di divieto tutti quei trattamenti in cui la fase istruttoria, su cui la decisione finale si basa, sia totalmente automatizzata.

[486] Gruppo di Lavoro art. 29, *Guidelines on automated individual decision-making and profiling for purposes of regulation 2016/679*, più volte aggiornate (ultima versione in data 6 febbraio 2018).

status giuridico degli utenti o i loro diritti in base a un contratto[487]. Quanto invece all'espressione "effetti analoghi" a quelli giuridici, si intende fare riferimento a quei trattamenti che, sebbene non influiscano direttamente sull'esercizio dei diritti, colpiscano in modo significativo altri interessi meritevoli di protezione[488]. Sul punto è lo stesso Gruppo di esperti che porta come esempio le pratiche di pubblicità mirata, in quanto detti trattamenti possono determinare un effetto significativo a seconda delle specifiche caratteristiche dell'individuo che ne è oggetto.

Per meglio comprendere si pensi per esempio a un soggetto che si trovi in difficoltà economiche; questi viene sottoposto a una profilazione all'esito della quale gli vengono indirizzate regolarmente pubblicità di giochi d'azzardo online, invogliandolo a iscriversi al servizio e finendo così col peggiorare la sua situazione finanziaria. Oppure si pensi ai già citati algoritmi di determinazione differenziata del prezzo (c.d. *dynamic pricing*) che potrebbero incidere significativamente sugli interessati nel caso in cui prezzi proibitivi impedissero l'accesso a beni o servizi[489]. Ne discende dunque che l'espressione debba essere interpretata nel senso di ricomprendervi tutte quelle situazioni che influenzino in modo significativo le circostanze, il comportamento o anche le scelte degli individui[490].

Le incertezze interpretative, lungi dal limitarsi alla portata applicativa, si estendono anche alla ricostruzione del contenuto precettivo della norma in parola, anch'esso oggetto di un acceso dibattito tra i maggiori commentatori. Ci si è domandati, infatti, se il legislatore europeo, con la previsione dell'art. 22, abbia introdotto un generale divieto di trattamenti automatizzati o se, invece, non si tratti piuttosto di un mero potere soggettivo di opposizione concesso all'interessato; dibattito questo che affonda le radici nella formulazione, pressoché analoga, contenuta nel testo della Direttiva Madre[491].

---

[487] Gruppo di Lavoro art. 29, *Guidelines on automated individual decision-making and profiling for purposes of regulation 2016/679*, cit., 21 s.

[488] Gruppo di Lavoro art. 29, *Guidelines on automated individual decision-making and profiling for purposes of regulation 2016/679*, cit. In argomento v. DE GREGORIO, TORINO, *op. cit*., 469 ss.; PIERUCCI, *op. cit*., 441 s.

[489] V. PELLECCHIA, *op. cit.*, 1219 ss.

[490] Sul punto le linee guida hanno precisato che la decisione automatizzata deve essere in grado di influenzare significativamente le circostanze, il comportamento o le scelte delle persone interessate e avere un impatto prolungato o permanente sull'interessato. Gruppo di Lavoro art. 29, *Guidelines on automated individual decision-making and profiling for purposes of regulation 2016/679*, cit.

[491] MALGIERI, COMANDÈ, *op. cit.*, 243 ss.; MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, cit., 186; MENDOZA, BYGRAVE, *The right not to be subject to automated decisions based on profiling*, in *EU Internet Law: Regulation and Enforcement*, a cura di SYNODINOU *et al.*, Berlin, 2017, 77 ss.; BYGRAVE, *Minding the machine: Article 15 of the data protection directive and automated profiling* (2001) *Computer Law and Security Rev*. 17 ss.; HILDEBRANDT, *The Dawn of Critical*

La questione non è di poco conto. Le due situazioni giuridiche hanno un differente impatto sulla realizzazione delle strategie europee e, in particolare, sulla stessa tutela dei diritti degli interessati. La raccolta massiva di dati, personali e non, difatti genera un concreto rischio di violazione della sfera di riservatezza del singolo, il quale prede il controllo sui propri dati, non potendo essere costantemente informato sui passaggi che tale raccolta subisce; ciò rende dunque di fatto impossibile il concreto esercizio del diritto all'autodeterminazione, che invece il Regolamento intende assicurare agli utenti nei confronti del potere decisionale degli apparati tecnologici[492].

La lettura della disposizione come introduttiva di un generale divieto rappresenterebbe allora una misura oggettiva, che opererebbe a prescindere dall'attivazione di alcuna iniziativa individuale dell'interessato. Questo tipo di strumento instaura una tutela per così dire strutturale al trattamento, apprestando una forma di protezione in modo automatico.

Diversamente invece nel caso in cui la norma fosse considerata un potere soggettivo. In questo caso sarebbe sempre possibile, naturalmente nei limiti delle condizioni di liceità previste dall'art. 6, porre in essere un trattamento automatizzato; la valutazione di opportunità sarebbe rimessa interamente al titolare, il quale è libero di determinare mezzi e architettura che ritiene adeguati allo scopo del trattamento[493]. Ne discende che qualora l'interessato intendesse sottrarsi alla decisione automatizzata avrebbe l'onere di intervenire in opposizione, ad eccezione dei casi specificamente previsti dal comma secondo, a mente dei quali invece il trattamento automatizzato è sempre possibile. Questa ricostruzione, si sostiene, troverebbe fondamento nella formulazione testuale, nella quale non si parla esplicitamente di divieto, oltre che nella considerazione per cui

---

Transparency right for the profiling era, in *Digital Enlightment Yearbook*, a cura di HILDEBRANDT *et al.*, Amsterdam, 2012. In argomento Pierucci, la quale evidenzia come «se il diritto di cui all'art. 22.1 dovesse essere necessariamente esercitato dall'interessato, esso sostanzialmente si tradurrebbe in un diritto di ottenere l'intervento umano nel processo decisionale, rendendo così superfluo l'art. 22.3 che prevede il diritto di ottenere tale intervento anche nei casi di deroga all'art. 22.1». V. PIERUCCI, *op. cit.*, 437. *Contra* invece Finocchiaro, la quale ritiene che si sia in presenza di una convinzione errata e fondata sulle precedenti versioni del Regolamento, poi non approvate. Pertanto secondo l'Autrice la norma non vieterebbe le decisioni automatizzati *tout court*, bensì di assumere decisioni unicamente con sistemi automatizzati. V. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 1670 ss.; ID., *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in *Intelligenza Artificiale. Il diritto, i diritti, l'etica*, cit., 245 s. A sostegno di detta posizione anche WACHTER, MITTELSTADT, FLORIDI, *op. cit.*, 76 ss.

[492] V. FALLETTI, *op. cit.*, 171; MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, cit., 187.

[493] MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, cit., 186.

le eccezioni previste dal comma secondo sarebbero particolarmente ampie, accompagnate da garanzie – come vedremo – deboli, tali per cui se la norma fosse ricostruita quale un divieto non troverebbe effettiva applicazione[494].

Tuttavia, tenendo a mente anche gli scopi a cui è diretto il Regolamento, si ritiene maggiormente auspicabile un'interpretazione della disposizione quale un generale divieto, e ciò soprattutto nella prospettiva di una efficace relazione strumentale tra mezzo e fine[495]. Il divieto generale infatti – come evidenza il Gruppo di Lavoro art. 29 – sarebbe il *medium* tecnico maggiormente coerente con il fine del Regolamento, che si ricorda essere quello di apprestare un bilanciamento tra i diritti dei titolari allo sfruttamento economico dei dati e la tutela della privacy degli interessati. Pertanto, la norma in esame deve essere interpretata come un generale divieto e cui segue anche l'indicazione di specifiche eccezioni[496].

La ricostruzione della norma come di un potere di opposizione lasciato alla determinazione del singolo si dimostrerebbe, invece, nella prassi operativa poco efficiente. L'uso di tecniche di profilazione, si ricorda, viene spesso posto in essere all'insaputa dell'interessato, anche nel caso in cui il trattamento si fondi sul consenso. Come si vedrà in seguito, l'istituto del consenso oggi non appare più uno strumento efficace nella regolazione dei trattamenti digitali e ciò in ragione della complessità tecnica della materia. Pare allora difficile ritenere una misura efficace, e soprattutto adeguata al rischio che discende dall'utilizzo di decisioni automatizzate, la previsione di una mera facoltà di opposizione esercitabile dal singolo, il quale potrebbe non essere nemmeno consapevole di essere soggetto a queste tipologie di trattamenti.

A questa considerazione deve aggiungersi come proprio il progredire della tecnologia ha comportato la caduta della logica soggettiva, che presidia la tradizionale tutela giuridica della persona[497]. Nella prospettiva di regolazione del potere digitale il singolo utente occupa una posizione non più centrale, avendo piuttosto il fenomeno un

[494] WACHTER, MITTELSTADT, FLORIDI, *op. cit.*, 76 ss.
[495] MESSINTETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, cit., 187.
[496] Interessante la simmetria riscontrata da Messinetti, la quale evidenzia come «il divieto di assoggettare l'individuo ad un processo decisionale interamente automatizzato e quello di interferire nella sfera soggettiva altrui in cui si attua il comando di inviolabilità della personale umano. In questa prospettiva, è chiaro che il divieto previsto dall'art. 22 GDPR costituisca una declinazione, naturale, specifica nell'infosfera, di quello generale che tutela la persona umana. Da questo profilo, la soluzione ermeneutica offerta all'alternativa tra diritto soggettivo e divieto trova un fondamento assai solido», MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, *ibidem*.
[497] MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, cit., 188.

impatto rilevante sui gruppi di persone e sulla stessa società. Ne discende come sia necessario, proprio al fine assicurare un presidio minimo di garanzie per gli utenti, che strumenti di tutela siano pensati quale parte integrante, avente automatico rilievo, della disciplina complessiva del rapporto tecnologia-singolo. In questa ottica le tutele di natura oggettiva si dimostrano essere quelle più efficaci.

3.1 Le basi di legittimità del trattamento. Quale spazio per il consenso dell'interessato

Chiarita la natura dell'art. 22 e la sua portata applicativa, il legislatore europeo prevede al secondo paragrafo un elenco di eccezioni al divieto così introdotto, a mente delle quali il trattamento è ritenuto legittimo nel caso in cui: sia necessario per la conclusione o l'esecuzione di un contratto; sia autorizzato dal diritto dell'Unione, o di uno Stato membro o, infine, se si basi sul consenso dell'interessato. Da una prima lettura si può notare come la disposizione sia maggiormente restrittiva rispetto all'art. 6, il quale individua le basi di legittimità applicabili in generale[498], dimostrandosi così maggiormente attenta alla regolazione dei trattamenti operanti decisioni automatizzate che, come visto, comportano specifici rischi per i diritti degli interessati.

Nonostante l'indicazione data nel parere – più volte richiamato – del Gruppo di Lavoro art. 29[499] di apprestare una interpretazione restrittiva al secondo comma dell'articolo in analisi, la portata delle eccezioni ivi previste si dimostra comunque particolarmente estesa e tale da rischiare di rendere vano nella pratica il divieto apprestato. Lungi dall'essere unicamente una problematica che affligge, come si vedrà,

[498] Il testo del Regolamento, come già si è avuto modo di notare, rispetto alla previgente Direttiva, ha ampliato le basi di legittimità del trattamento, ridimensionando il ruolo centrale fino ad allora assunto dal consenso dell'interessato. È, infatti, possibile porre in essere un trattamento anche in ragione dell'adempimento di un obbligo negoziale, o legale, nonché per la salvaguardia degli interessi vitali dell'interessato o per l'esecuzione di un compito di interesse pubblico, o connesso all'esercizio di pubblici poteri, di cui è investito il titolare del trattamento (lett. *e*). Sul punto Iuliani sottolinea come proprio l'ampliamento della base giuridica dei trattamenti, da cui discende l'estensione della legittimazione al trattamento, ha permesso di superare una concezione personalistica del consenso e, dunque, reso possibile i trattamenti che si fondano sui Big Data. V. IULIANI, *Note minime in tema di trattamento dei dati personali*, in *Eur. e dir. priv*., 2018, 293 ss. Per un approfondimento in merito alle condizioni di liceità previste dall'art. 6 si rimanda a MULA, *op. cit.*, 135 ss.; OGRISEG, *Le basi giuridiche del trattamento dati*, in *Tecnologia e Diritto*, II, cit., 75 ss.; POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, *GDPR tra novità e discontinuità*, a cura di CATERINA, in *Giur. it.*, 2019, 2783 ss.

[499] Gruppo di Lavoro art. 29, *Guidelines on automated individual decision-making and profiling for purposes of regulation 2016/679*, cit.

l'istituto del consenso, su entrambe le altre eccezioni statuite possono essere fatte considerazioni analoghe.

Se la subordinazione del trattamento a una base contrattuale tra titolare e interessato può a prima vista sembrare una efficace limitazione, essendo il titolare chiamato a dimostrare la "necessità" del trattamento, in realtà detta previsione non si dimostra sufficiente a limitare l'estensione dell'eccezione in parola, pur se nella accezione di mancanza di altre alternative possibili al trattamento automatizzato. A questa deve essere data una lettura sistematica, in linea con le previsioni e gli obiettivi del Regolamento. Si ricorda, infatti, come l'intero testo, fin dalle sue prime disposizioni, sia diretto ad apprestare un attento bilanciamento tra diritti confliggenti. Come visto, dal tenore della normativa alcuna gerarchia può essere fatta tra diritti di pari rango; i diritti a tutela della persona sono posti sullo stesso piano di quelli legati alla libertà di iniziativa economica, dunque questi ultimi non sono sempre comprimibili di fronte ai primi[500].

Proprio da tali considerazioni di fondo deve muovere la valutazione in merito all'attributo della "necessità" previsto alla lettera *a*) dell'articolo in analisi. La valutazione che il titolare del trattamento è chiamato a compiere dovrà dunque essere fondata su di un criterio di ragionevolezza, tale per cui i trattamenti automatizzati sono ritenuti legittimi ogni qualvolta non sia ragionevolmente possibile, sia dal punto di vista economico che per quanto riguarda i possibili mezzi utilizzabili, porre in essere trattamenti differenti. Se fosse altrimenti, infatti, si paralizzerebbe l'impiego di questa tipologia di applicazioni, dal momento che in linea di massima sarebbero ben pochi i trattamenti automatizzati assolutamente indispensabili per portare a termine un contratto. Si tratta così di una valutazione sostanzialmente di opportunità a cui è chiamato il titolare, in modo del tutto simile a quella compiuta nel procedimento di anonimizzazione dei dati, a cui non può che seguire una certa ampiezza nell'uso e nella diffusione di tali tipologie di trattamento.

Quanto alla previsione di un'autorizzazione del diritto dell'Unione o di altro Stato membro, detta indicazione è stata introdotta evidentemente per permettere l'utilizzo delle nuove tecnologie nelle operazioni di contrasto alla criminalità e per la tutela di

[500] Si pensi per esempio all'art. 1, comma 3°, ove espressamente si precisa come «*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*». Questa impostazione si discosta dalla nostra tradizione giuridica, ove invece i diritti della persona sono ritenuti prevalenti rispetto ai diritti di stampo economico, pur essendo anch'essi costituzionalmente garantiti.

interessi pubblici[501]. Consapevole dell'eccessiva ampiezza della formulazione, il legislatore prevede infine la necessaria predisposizione, nello stesso testo di legge, di misure adeguate alla tutela dei diritti e delle libertà degli interessati. Non viene tuttavia previsto alcuno specifico parametro di adeguatezza, lasciando la valutazione nella piena disponibilità dei singoli ordinamenti. Sebbene possa essere fatto un collegamento alle indicazioni previste all'art. 89 GDPR, esse, come già si è evidenziato, prevedono un generale riferimento alle tecniche di minimizzazione e anonimizzazione, quali strumenti adeguati alla tutela dei diritti degli individui[502]. Si conferma dunque anch'essa una previsione molto estesa, lasciata alla libera determinazione degli Stati, a cui si aggiunge la difficoltà di un eventuale coordinamento tra i diversi ordinamenti ove, chiaramente, potrebbero essere previste misure di sicurezza anche molto differenti.

Una particolare attenzione merita, infine, il rimando all'istituto del consenso, da questo infatti discendono le maggiori criticità[503].

Il consenso al trattamento dei dati personali sembra in parte richiamare il consenso richiesto in ambito sanitario, tuttavia i due istituti, pur avvicinandosi sotto certi aspetti, sono sostanzialmente differenti. Come nell'ambito medico il consenso del paziente legittima la prestazione sanitaria, così nella materia dei dati il consenso dell'utente è considerato una tra le basi di legittimità, seppur spesso la più importante, del trattamento. Entrambi gli istituti sono espressione del diritto all'autodeterminazione del singolo, da cui discende necessariamente come l'utente/paziente debba prestare un consenso che sia effettivamente libero e informato[504]. A questo parallelismo di funzioni segue, tuttavia, una declinazione necessariamente distinta. Il consenso sanitario si innesta, infatti, in un percorso condiviso tra medici e paziente, in cui i primi sono

[501] La Germania, in attuazione di tale eccezione, nel 2017 ha stabilito che il diritto a non essere sottoposti a decisioni totalmente automatizzate non si applica nell'ambito dei rapporti assicurativi. V. SIMEONE, *op. cit.*, 286. In argomento si rimanda anche all'interessante saggio di ORFINO, *op. cit.*, 82 ss.

[502] Si rimanda alle considerazioni fatte *supra* al capitolo 3, § 5.1.

[503] Il legislatore europeo ne fornisce una definizione all'art. 4, secondo cui con il termine consenso si fa riferimento a una «*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento*». Art. 4, n. 11, reg. UE n. 679/2016.

[504] L'istituto del consenso è necessaria espressione del principio di autodeterminazione informativa che pervade l'intero testo normativo. Cfr. SIANO, MONTUORI, *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in *Le nuove frontiere della privacy nelle tecnologie digitali*, a cura di BUSIA, LIGUORI, POLLICINO, Roma, 2016, 105 ss.; CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi, giuridica e studi comportamentali*, in *Oss. dir. civ. comm.*, 2018, 89 ss.

chiamati a informare il secondo nella prospettiva di una pianificazione delle cure, mostrandosi dunque quale passaggio necessario all'interno di una "alleanza terapeutica"; da qui nasce la necessità di un consenso effettivamente libero e informato, in cui il contenuto delle informazioni deve essere parametrato al singolo caso e alle condizioni specifiche del paziente[505]. Non così invece per il consenso nella materia dei dati. Evidentemente qui la prospettiva cambia radicalmente, ad un rapporto di prossimità si contrappone la distanza; alla condivisione si sostituisce una determinazione unilaterale destinata a un numero indeterminato di utenti.

Se con la Direttiva madre i due strumenti potevano forse dirsi più vicini, con il GDPR la differenza diviene insanabile. Si è infatti già avuto modo di ricordare come l'istituto in analisi abbia rivestito un ruolo centrale all'interno delle disposizioni della previgente Direttiva 46/95 CE[506]. Il testo, entrato in vigore ormai più di vent'anni fa, si mostrava espressione di una differente realtà sociale (e tecnologica), nella quale trovava spazio un rapporto lineare tra titolare e interessato; in questo contesto il potere di disposizione che il singolo esercitava attraverso la dazione di un consenso informato poteva essere considerato uno strumento valido ed efficace[507].

Con il progredire della tecnologia, tuttavia, è mutato anche l'ordine dei rapporti, confinando il singolo individuo in un ruolo sempre più marginale; al centro dei moderni

[505] Il percorso che ha portato al riconoscimento del diritto all'autodeterminazione del paziente risale nel tempo e affonda le radici in un più ampio discorso in tema di diritto alla salute, ma soprattutto di riconoscimento della dignità della persona. La materia meriterebbe un approfondimento che non è possibile effettuare nel presente lavoro, si rimanda, tra gli altri, a: COPPINI, *Diritti del paziente e consenso informato*, in *La nuova responsabilità medica*, a cura di RUFFOLO, Milano, 2018, 167 ss.; CACACE, *Autodeterminazione in salute*, Milano, 2017, 21 ss.; SANTOSUOSSO, *Diritto, scienza, nuove tecnologie*, cit., 44 ss. e 73 ss.; QUAGLIARELLO, FIN, *Il consenso informato in ambito medico: un'indagine antropologica e giuridica*, Bologna, 2016; DE GAUDIO *et al.*, *Consenso informato*, in *Governo clinico e medicina perioperatoria*, a cura di GULLO e MURABITO, Milano, 2012, 163 ss.; PUCELLA, *Autodeterminazione e responsabilità nella relazione di cura*, Milano, 2010, 14 ss. e 195 ss.

[506] Il ruolo centrale avuto dall'istituto, e ripreso anche dal codice privacy, viene oggi a essere sostanzialmente ridimensionato dalla previsione del Regolamento, che vede nel consenso solo una tra le possibili basi di legittimità tutte aventi un eguale peso. La normativa italiana, fortemente rimaneggiata dal d. lgs. n. 101/2018, ha mantenuto il ruolo centrale del consenso unicamente per i trattamenti aventi a oggetto dati sensibili. V. OGRISEG, *op. cit.*, 78 ss.; DI RESTA, *op. cit.*, 61 ss.; CAGGIA, *Libertà ed espressione del consenso*, in *I dati personali nel diritto europeo*, cit., 249 ss.; BRAVO, *Il consenso e le altre condizioni di liceità*, in *Il nuovo Regolamento europeo sulla privacy*, cit., 138 ss.; ID., *Le condizioni di liceità del trattamento di dati personali*, in *La protezione dei dati personali in Italia*, cit., 130 ss.

[507] La ricostruzione all'interno delle normative europee, nella Direttiva madre prima e nel Regolamento poi, dell'interesse dell'individuo ai propri dati in termini di libertà fondamentale ha giustificato che la liceità dei trattamenti fosse consentita solo in presenza del consenso dell'interessato. V. CAGGIANO, *op. cit.*, 73; PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 213 ss. Una valorizzazione dell'istituto, il quale continuerebbe a rivestire un ruolo chiave nei trattamenti digitali, viene fatta da SIANO, MONTUORI, *op. cit.*, 109 ss.

trattamenti non è più, infatti, la persona fisica di per sé, quanto piuttosto i gruppi di utenti e in definitiva l'intera società[508].

Prima di affrontare il tema dell'effettività dell'istituto, nella sua declinazione all'interno dell'infosfera, pare opportuno soffermarsi preliminarmente sulla natura dello stesso, profilo ancora oggi fonte di dibattito tra i maggiori commentatori[509]. Il modo di intendere la natura del consenso, infatti, si intreccia alla ricostruzione che viene fatta dello stesso diritto alla protezione dei dati personali, a fronte anche della natura complessa dei dati quali asset patrimoniale, da una parte, ed espressione della personalità del singolo utente dall'altra[510].

Un'impostazione tradizionale, facente perno sulla natura non patrimoniale dei dati, riconduce il diritto alla protezione dei dati nell'alveo dei diritti fondamentali della persona e come tale connotato dunque dall'assolutezza, indisponibilità, intrasmissibilità e imprescrittibilità[511]. Seguendo una tale ricostruzione al consenso prestato

---

[508] Cfr. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019, 124 ss. In argomento anche Caggia, il quale sottolinea come la minore centralità ricoperta dall'istituto all'interno del Regolamento sarebbe espressione di un cambiamento di paradigma – sebbene non ancora del tutto sufficiente – dello stesso legislatore europeo; quest'ultimo sembra maturare la consapevolezza che «in una società sempre più condizionata dall'economia della rete, dell'affermarsi dei modelli di analisi basati sui Big Data e dall'uso di strumenti predittivi, la manifestazione del consenso si riduce ad una pratica astratta, così che farne oggetto di declamazione di principio sul piano della disciplina positiva rischia di apparire una mera operazione retorica». CAGGIA, *op. cit.*, 253. Analoghe perplessità in merito all'effettiva applicazione dell'istituto emergono anche in merito agli IoT. La necessità di un consenso, qui necessaria anche ai sensi della Direttiva UE n. 58/2002 art. 5 sulla riservatezza delle comunicazioni, si scontra sia con le difficoltà nascenti dall'eventuale mancanza di uno schermo nelle applicazioni di IoT terminali, ove dunque l'informativa viene posta unicamente sul sito web dell'azienda, sia nelle concrete modalità di richiesta dello stesso, nel caso in cui l'utente non sia a conoscenza del trattamento effettuato da uno o più specifici oggetti connessi. Per un approfondimento in tema si rimanda a GIOVANELLA, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, in *I dati personali nel diritto europeo*, cit., 1228 ss.

[509] Per una disamina in merito alle diverse teorie circa la natura del consenso si rimanda a VIVARELLI, *op. cit.*, 40 ss.; DI RESTA, *op. cit.*, 69 ss.; RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inform.*, cit., 695 ss.; CAGGIA, *op. cit.*, 254 ss. Per una visione sotto un'ottica negoziale D'IPPOLITO, *op. cit.*, 634 ss.; BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, cit., 142 ss.; ID., *Le condizioni di liceità del trattamento di dati personali*, cit., 140 ss.

[510] In argomento Ricciuto evidenzia come «La disciplina del fenomeno del trattamento dei dati nella prospettiva del diritto civile è – e sarà e non potrà che essere – sempre caratterizzata da una ineliminabile intersezione dei piani e delle logiche dei diritti assoluti con le situazioni giuridiche dei rapporti obbligatori. E di questa intersezione è espressione, per l'appunto, il consenso, con la sua valenza definitoria degli ambiti di manifestazione del fenomeno». RICCIUTO, *La patrimonializzazione dei dati personali*, in *I dati personali nel diritto europeo*, cit., 36.

[511] Questa considerazione prescinderebbe dall'adesione alla teoria pluralista piuttosto che quella monista, pur preferibile in quanto a essa ha aderito il diritto vivente, in relazione alla ricostruzione dei diritti della personalità. Il dibattito è tuttora aperto. V. BRAVO, *Il consenso e le altre condizioni di liceità*, cit., 143. In argomento illuminanti le considerazioni di Alpa che, criticando la teoria pluralista, evidenzia come «nelle stesse esperienze in cui i diritti della personalità sono sorti come tipizzati si è consumato felicemente il

dall'interessato non potrebbe allora essere data alcuna valenza dispositiva o transattiva in relazione ai dati personali; questi, infatti, andando a "costruire" la personalità dell'individuo, espressione del suo essere, non dovrebbero ricadere sotto una logica proprietaria che li considera come beni di cui il soggetto può disporre[512]. Pertanto l'atto del consenso acquista un carattere meramente autorizzativo, con efficacia costitutiva nell'altrui sfera personale[513]. Così ricostruito l'istituto è dunque funzionale alla realizzazione della propria identità personale e assolve alla funzione di rendere lecita la circolazione dei dati, eliminando l'illiceità del comportamento altrui, dal momento che ne verrebbe così permessa l'ingerenza nella propria sfera giuridica.

L'atto autorizzativo, evidentemente unilaterale, non reciderebbe inoltre il rapporto tra il soggetto e le proprie informazioni, che si ricorda essere attributi della sua personalità; l'individuo, pur autorizzando il trattamento, mantiene infatti un potere di controllo sui propri dati, garantito da alcune facoltà quali, in particolare, la possibilità di opposizione al trattamento, la revoca del consenso, la rettifica e la cancellazione dei dati. Proprio mediante l'esercizio di queste facoltà l'interessato interverrebbe nel procedimento di regolamentazione delle modalità del trattamento.

---

tentativo di costruire intorno ad essi una categoria generale, una nozione unitaria dei diritti della personalità, che ne supera i contorni specifici: in tal modo si riafferma l'esigenza di superare la frammentazione della persona umana e di dare ingresso ai nuovi interessi emergenti dalla vita sociale, non ancora considerati dal legislatore», ALPA, *I diritti della personalità*, *Le persone e la famiglia*, 1, *Le persone fisiche e i diritti della personalità*, a cura di in ALPA e G. RESTA, nel *Trattato Sacco*, Torino, 2006, 78. In argomento anche Galgano, per il quale i diritti della personalità preesisterebbero a un loro riconoscimento all'interno dell'ordinamento. Secondo l'A. si tratterebbe, dunque, di diritti «esistenti indipendentemente da ogni norma giuridica che li riconosca e che il diritto soggettivo si limita a garantire […] perché spettanti all'uomo in quanto tale, indipendentemente dal tipo di sistema politico o sociale entro il quale egli vive». GALGANO, nel *Trattato di diritto civile*, 1, III ed., a cura di ZORZI, Padova, 2015, 171 ss.

[512] In Argomento Pizzetti sottolinea, invece, come ogni qual volta che il trattamento dei dati personali si fonda sul consenso dell'interessato saremmo all'interno di una prospettiva proprietaria del dato, così come accade quando i dati sono forniti/trattati per eseguire un contratto. Ne sarebbe una prova anche la previsione per cui l'interessato può in ogni momento revocare il consenso, facendo così venir meno la liceità del trattamento. Cfr. PIZZETTI, *La protezione dei dati personali e la sfida dell'intelligenza artificiale*, cit., 16 ss.

[513] Posizione questa sostenuta da MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in *Libera circolazione e protezione dei dati personali*, a cura di PANETTA, Milano, 2006, 996 ss.; MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. piv.*, 1998, 350 ss., in particolare l'A. evidenzia come il consenso dell'interessato, quale permesso autorizzativo, permette di non assoggettare più i dati personali a una logica di repressione di «qualunque circuito conoscitivo posto in essere». Si v. anche FICI, PELLECCHIA, *Il consenso al trattamento*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di PARDOLESI, Milano, 2003, I, 485; BRAVO, *Il consenso e le altre condizioni di liceità*, cit., 144; RICCIUTO, *La patrimonializzazione dei dati personali*, in *I dati personali nel diritto europeo*, cit., 37.

Questa ricostruzione, pur in parte condivisibile, non sembra tuttavia tenere conto della prassi; negli odierni trattamenti la funzione di regolamentazione rimessa all'interessato è difatti fortemente ridimensionata. É al titolare che la legge assegna il potere di definire le finalità e le modalità stesse del trattamento, finendo l'interessato col prestare solo un mero assenso a un trattamento interamente determinato da altri[514].

Secondo altro orientamento dottrinale il consenso dovrebbe essere qualificato quale ipotesi di consenso dell'avente diritto (*ex* art. 50 c.p.), dunque quale atto giuridico non negoziale avente la funzione di scriminare l'antigiuridicità dell'attività di trattamento dei dati. Ne discende come all'atto del consenso non segua alcun trasferimento, né costituzione, di un diritto reale sui dati; l'istituto difatti rappresa il presupposto che esime il destinatario dal dovere, valevole *erga omnes*, di astenersi dal compimento di atti che determinino una lesione della persona[515]. Si ricorda che il consenso dell'avente diritto non comporta la perdita del diritto, né questo diviene oggetto di rinuncia né di un atto di disposizione. Dando il consenso l'interessato viene sottoposto ad atti lesivi, generalmente vietati dall'ordinamento, ma in questo specifico caso, e solo per un tempo determinato, ammessi[516]. Sotto quest'ottica l'istituto parrebbe accostarsi alla figura della "tolleranza", ma da essa deve essere tenuto distinto. Quest'ultima, infatti, non priva l'atto lesivo della sua antigiuridicità, limitandosi il soggetto che ha la titolarità del diritto a sopportare/tollerare il comportamento altrui; nella ricostruzione in parola, invece, l'atto lesivo diviene lecito, seppur in misura necessariamente circoscritta nei

[514] La marginalizzazione del ruolo dell'interessato nella determinazione degli scopi e delle modalità del trattamento discende anche dalla considerazione per cui oggi i titolari si rivolgono a una platea indistinta di interessanti; sarebbe allora troppo dispendioso economicamente, oltre che poco efficiente ostacolando eccessivamente il traffico commerciale, che ogni trattamento fosse soggetto a una specifica contrattazione con il singolo interessato; secondo la stessa logica che ha portato all'emersione dei contratti standard. In argomento si v. BRAVO, *Il consenso e le altre condizioni di liceità*, cit., 145 s.

[515] V. PATTI, in *La protezione dei dati personali, Commentario al D. lgs. 30 giugno 2003, n. 196 ("codice privacy")*, a cura di C.M. BIANCA e BUSNELLI, *sub* art. 23, Padova, 2007, 553; CAGGIANO, *op. cit.*, 83 s. In argomento anche VIVARELLI, *op. cit.*, 43 s.; RICCIUTO, *La patrimonializzazione dei dati personali*, in *I dati personali nel diritto europeo*, cit., 35.

[516] In arg. BRAVO, *Il consenso e le altre condizioni di liceità*, cit., 148, sottolinea che, con una tale ricostruzione, l'istituto del consenso si configura come una «limitazione ammessa dall'ordinamento, per i diritti della personalità, in presenza della quale tuttavia non viene mutata la titolarità del diritto soggettivo in parola, ma vengono ammessi atti lesivi del diritto stesso, che potranno essere compiuti da determinati soggetti a ciò legittimati e, in questo senso, può parlarsi di parziale disponibilità dei diritti della personalità». L'A. riporta l'autorevole posizione di De Cupis secondo cui «i diritti della personalità possono essere muniti di quel particolare e più modesto aspetto della facoltà di disposizione che è costituito dalla facoltà di consentire alla lesione: quanto si dice che essi sono indisponibili, sprovvisti della facoltà di disposizione, l'espressione deve essere intesa con questo temperamento». DE CUPIS, *I diritti della personalità*, nel *Trattato Cicu-Messineo*, 4, II ed., Milano, 1982, 96.

limiti del consenso prestato a un determinato soggetto e per un determinato trattamento[517].

Questa impostazione dottrinale, in mancanza di elementi normativi contrari, si sostiene avrebbe il pregio di ricostruire l'istituto in maniera unitaria tra i diversi ambiti, tra cui va ricompreso quello medico. Il consenso sarebbe dunque un atto non negoziale scriminante l'antigiuridicità o l'illiceità del trattamento posto in essere da un soggetto diverso dall'interessato e, al contempo, esercizio dell'autodeterminazione di quest'ultimo[518].

Tuttavia questa posizione incontra resistenza da parte della dottrina che ritiene come essa finirebbe per intendere l'attività di trattamento come intrinsecamente illecita, andando in tal molto a confliggere con un'interpretazione sistematica del Regolamento. Sebbene alcune previsioni specifiche, quali ad esempio l'art. 9, parrebbero in sintonia con una siffatta ricostruzione, è necessario ricordare come il testo vada interpretato in un contesto di bilanciamento tra diritti di pari rango e non quale espressione di un sistema univoco di protezione dell'interessato. Come è noto, infatti, il GDPR intende sì tutelare i diritti e le libertà degli individui, ma è anche diretto a instaurare un vero e proprio diritto al trattamento dei dati personali da parte del Titolare, pur nel rispetto delle previsioni regolamentari[519]. Infine, la visione di un trattamento come atto in sé lesivo dei diritti dell'interessato non tiene conto neppure dell'effettiva e concreta regolazione degli interessi che nell'attuale contesto socio-economico sottendono ai trattamenti. Si pensi, solo per fare un esempio, all'avvocato che tratta i dati dei clienti. Non pare revocabile in dubbio che il trattamento sia posto in essere nell'interesse del cliente a cui viene fornita assistenza legale.

In senso opposto parte della dottrina che vede nel consenso un atto di autonomia negoziale, esaltando dunque la natura dispositiva dell'istituto. Questa posizione si fonda su di una visione dei dati personali quali beni giuridici, dunque economicamente valutabili e suscettibili di circolare sul mercato[520], da cui discende che l'interessato

[517] Cfr. BRAVO, *Il consenso e le altre condizioni di liceità*, *ibidem*.
[518] CAGGIANO, *op. cit.*, 85.
[519] V. BRAVO, *Il consenso e le altre condizioni di liceità*, cit., 150.
[520] Autorevole dottrina, infatti, precisa come «il dato personale costituisce un bene in quanto suscettibile di formare oggetto di diritti. I dati sono cedibili, trasferibili, scambiabili, e, normalmente, danno vita a rapporti che al livello più generale possono qualificarsi come negozi (in quanto vi è un atto di volontaria disposizione da parte del soggetto), ad un livello medio si qualificano come obbligatori (in quanto fanno sorgere in capo ad un soggetto obblighi giuridificati di contenuto patrimoniale), e la livello più alto si

possa liberamente disporre del loro trasferimento. Il consenso, quale atto di disposizione – si sostiene – non comporterebbe la rinuncia alla personalità; così come avviene nel caso di autorizzazione alla riproduzione della propria immagine da cui evidentemente non discende una rinuncia alla personalità del soggetto che presta l'autorizzazione[521]. Pertanto, a una ricostruzione che vede i dati quali beni economicamente valutabili, da cui dunque è possibile trarre delle utilità, si ritiene possano essere applicabili quegli schemi giuridici utilizzati nelle attività negoziali concernenti attributi della personalità. In questa prospettiva l'istituto in parola diviene una manifestazione di volontà di natura contrattuale, dalla quale sorgono obbligazioni in capo al dichiarante e che può essere sia oneroso, che gratuito, così come sottoposto a termine e condizione; da questo possono anche generarsi in capo al titolare del trattamento una serie di diritti e obbligazioni.

Questa ricostruzione è stata avallata da parte della giurisprudenza che ammette la negoziabilità degli attributi della persona mediante atti dispositivi, i quali devono essere distinti dal diritto della personalità in sé considerato, in quanto diritto personalissimo e inalienabile[522].

Alla luce della varietà e della complessità dell'argomento, che si intreccia con la natura evidentemente composita dei diritti sopra richiamati, parte della dottrina ha suggerito di abbandonare la ricerca di una necessaria categorizzazione, la quale finirebbe con l'essere frustata, non riuscendo a rinvenire una formula idonea a ricomprendere la situazione in esame nel suo complesso[523].

---

qualificano come contrattuali (in quanto la cessione del dato fa sorgere obblighi giuridici in capo a tutte le parti del rapporto)». ZENO ZENCOVICH, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, in *La disciplina del trattamento dei dati personali*, a cura di CUFFARO, RICCIUTO, ZENO ZENCOVIC, Torino, 1997, 740 ss. Sul punto anche CAGGIA, *op. cit.*, 255.

[521] In argomento BRAVO, *Il consenso e le altre condizioni di liceità*, cit., 154; RICCIUTO, *La patrimonializzazione dei dati personali*, in *I dati personali nel diritto europeo*, cit., 37 s.; CAGGIA, *ibidem*.

[522] Può estendersi lo schema logico argomentativo in tema di diritto all'immagine ove la Cassazione precisa che «*il consenso alla pubblicazione della propria immagine costituisce un negozio unilaterale, avente ad oggetto non il diritto, personalissimo ed inalienabile, all'immagine, ma soltanto l'esercizio di tale diritto e, pertanto, sebbene possa essere occasionalmente inserito in un contratto, tale consenso resta distinto ed autonomo dalla pattuizione che lo contiene, con la conseguenza che esso è sempre revocabile* […]». Cass., 29.1.2016, n. 1748, in *Annali it. dir. aut*., 2016, 749 s.

[523] Il rilievo è di Sica il quale ritiene che il consenso potrebbe essere definito quale «elemento della fattispecie legale a contenuto e disciplina composita: ergo, non "il" ma "i" consensi». V. SICA, *Il consenso al trattamento dei dati: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, 621 ss.

A questo rilievo si aggiunge quello secondo cui il dibattito sulla negoziabilità o meno dell'atto del consenso abbia un rilievo applicativo marginale[524]. Non solamente perché sul punto sarebbe presente una disciplina speciale sul consenso qualificato al trattamento, ma in particolare perché la stessa categoria dogmatica sarebbe messa in crisi dalla sempre maggiore diffusione dei trattamenti digitali. Se, come visto, con l'emanazione della Direttiva madre il dibattito sull'istituto poteva avere una maggiore rilevanza, dato il ruolo preminente che esso rivestiva, in particolare nel nostro codice della privacy, ora il consenso non sembra più il mezzo adeguato allo scopo[525]. Diverse ricerche sono state fatte in merito alla verifica circa l'effettività dell'istituto, i cui risultati paiono confermare in maniera univoca come esso sia ormai in grande misura uno strumento inefficace[526].

Paradigmatico il rilievo per cui anche tra gli utenti che si dichiarano sensibili alla materia, poca attenzione venga in realtà dedicata a una effettiva lettura e comprensione delle informative presentate loro[527]. Gli studi comportamentali effettuati hanno

[524] CAGGIANO, *op. cit.*, 82.

[525] In argomento Poletti evidenzia che se pure si ammettesse che il consenso abbia avuto un periodo di reale fasto, attualmente pare essere in forte declino. Cfr. POLETTI, *op. cit*., 2784 ss.

[526] Già nel 1973 Rodotà evidenziava come l'istituto del consenso non fosse uno strumento adeguato per la difesa degli utenti, né per il controllo di chi lo richiede. L'Autore, infatti, chiariva come il consenso avrebbe potuto adempiere a dette funzioni solo qualora a esso fosse corrisposta una situazione di potere idonea a bilanciare quello altrui. Già agli inizi degli anni '70 attenta dottrina rilevava come esso servisse piuttosto a mascherare una situazione di disparità tra le parti. Ciò si dimostra particolarmente vero nella materia del trattamento dati mediante tecnologie digitali, ove tra il titolare e l'interessato vi è un vero e proprio divario conoscitivo a cui si accompagna anche un dislivello di potere tra le parti. Cfr. RODOTÀ, *Elaboratori elettronici e controllo sociale*, cit., 134 s.

[527] Dalla ricerca condotta congiuntamente dall'Autorità per le garanzie nelle comunicazioni, l'Autorità Garante per la protezione dei dati personali e l'Autorità garante della concorrenza e del mercato, è merso che oltre il 50% degli utenti legge solo in parte le informative, e oltre il 30% non le legge affatto. V. AGCom, *Big data Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera n. 217/17/CONS*, 8 giugno 2018, 4. In argomento anche MULA, *op. cit*., 140 ss. Interessante il saggio di Gatt, Montanari, Caggiano ove si mostrano i risultati di un esperimento in merito alla percezione, consapevolezza ed effettività dei mezzi di tutela della privacy, concentrando l'attenzione in particolare sul consenso. Da una prima analisi è emerso come la maggior parte degli intervistati, pur dichiarandosi a conoscenza delle criticità legate alla privacy e pur ritenendo importante la tutela dei propri dati, non abbia di fatto modificato le impostazioni predefinite di installazione. Utilizzando particolari tecniche di controllo del tempo utilizzato dagli intervistati per apprestare o meno il consenso, come per esempio i metodi di *eye tracking*, è inoltre emerso come essi non abbiano letto l'informativa (nemmeno coloro che hanno modificato le impostazioni predefinite) e in generale persista una generale confusione degli utenti sul tema. All'esito di queste considerazioni, dunque, non si può che dubitare dell'efficacia di detto strumento, per lo meno così come oggi previsto, al fine di apprestare un'adeguata forma di tutela per le persone, essendo evidente come esso sia prestato spesso inconsapevolmente. Cfr. GATT, MONTANARI, CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, 2017, 363 ss. In argomento anche CAGGIANO, *op. cit.*, 68 e 92 ss. L'Autrice riporta l'esito di alcuni studi comportamentali dai quali è emerso come la scelta degli utenti di prestare o meno il consenso si formi sostanzialmente in base a euristiche e scorciatoie cognitive, che non dipendono dunque da come la richiesta di consenso viene

dimostrato come le reiterate richieste di consenso a cui sono esposti gli utenti ne riducono l'attenzione, in particolare con riferimento alla lettura delle informative, a cui dunque consegue una debolezza cognitiva e una compromissione del processo decisionale[528].

A questo esito possono essere imputate differenti cause. Innanzitutto spesso le informative si dimostrano particolarmente articolate, tali da renderne difficile la comprensione e finanche scoraggiarne la lettura; esse spesso sono redatte in un linguaggio eccessivamente tecnico, a cui l'utente finisce per aderire senza una effettiva consapevolezza[529]. Questa condizione di asimmetria conoscitiva e di mancanza di effettiva comprensione è particolarmente evidente nei trattamenti posti in essere mediante tecnologie *data driven* e di AI, ove dunque anche un arricchimento di informazioni, come prospettato in applicazione del principio di trasparenza, più che essere un rimedio all'opacità dei sistemi algoritmici finirebbe col rendere gli utenti ancora meno inclini a un'analisi di quanto loro prospettato; alla completezza di informazioni anche tecniche seguirebbe allora una mera adesione acritica e inconsapevole.

Dagli studi sociologici in materia si sono evidenziate tre principali concause che hanno portato al fallimento della *disclosure* obbligatoria: innanzitutto si è rilevato come per gli utenti le richieste di consenso vengano percepite come uno strumento finalizzato esclusivamente a proteggere i professionisti; è emersa inoltre una diffusa frustrazione e mancanza di fiducia provocata da un linguaggio tecnico poco comprensibile a cui si accompagnerebbe, infine, una sensazione di impotenza derivante dalla persistente indifferenza in merito alle richieste di chiarezza e sinteticità. A ciò dunque segue una generale avversione degli utenti/consumatori i quali, sebbene generalmente consapevoli

---

formulata o da come le informative sono presentate. Si evidenzia pertanto come se pure l'informativa risulti completa, in particolare in merito agli impatti negativi derivanti dai trattamenti, a pesare sulla scelta di concedere il consenso risulta maggiormente il beneficio immediato (che discende dall'usufruire del servizio offerto) piuttosto di eventuali future conseguenze negative. L'A. chiarisce, infatti, come le decisioni vengano sostanzialmente condizionate dalla generale percezione delle proprie capacità di controllo in un determinato momento (paradosso del controllo) e dalla difficoltà per la mente umana di valutare tutti i costi e i benefeci di una determinata azione (razionalità limitata).

[528] Cfr. POLETTI, *ibidem*; CAGGIANO, *op. cit.*, 94 ss.; AULINO, *Il consenso al trattamento dei dati e carenza di consapevolezza: il* legal design *come un rimedio* ex ante, in *Dir. inform.*, 2020, 305 ss.; SIMEONE, *op. cit.*, 291 ss.

[529] Burrell definisce questa condizione come opacità intellettiva. V. BURRELL, *How the machine 'thinks': Understanding opacity in machine learning algorithms* (2016) 1 *Big Data & Society* 1 ss.

delle informative a loro disposizione, non sono disposti a investire tempo ed energie per comprendere effettivamente quanto ivi presente[530].

Nonostante quanto emerso dagli studi empirici, la strategia europea in tema di dati non pare diretta a un sostanziale rimodellamento dell'istituto, limitandosi piuttosto a una dettagliata elencazione delle informazioni che il titolare deve fornire all'interessato. Per quanto specificamente previsto in merito al consenso, non pare infatti sufficiente la previsione che esso debba essere prestato liberamente dagli utenti[531]. Diverse sono state le interpretazioni date alla nozione di "libertà" richiesta dall'art. 4, n. 11, GDPR. Si è sostenuto che per essere libero il consenso debba essere informato[532]; si nota, sul punto, che sebbene l'informazione sia condizione necessaria, essa non è tuttavia sufficiente ai fini della validità dell'atto. Difatti, se innegabile che solo in virtù della completezza di informazioni che viene fornita all'interessato questi è effettivamente posto nella condizione di poter liberamente compiere una scelta di acconsentire o meno al trattamento, a ciò devono aggiungersi ulteriori considerazioni. Il consenso deve essere

[530] Si v. TABARRINI, *Comprendere la "Big Mind"*, cit., 565 ss., che sul punto richiama la c.d. trappola del consenso, in relazione alla posizione di preminenza di detto istituto quale base giuridica dei trattamenti. L'Autrice evidenzia come alla tradizionale asimmetria conoscitiva che corre tra professionista e utenti si debba aggiungere nel rapporto anche una terza parte. Difatti nei trattamenti digitali si assiste a un rapporto a tre, ove la asimmetria conoscitiva interessa anche la relazione tra tecnici ICT e professionisti, ricadendo di conseguenza anche nel rapporto tra questi ultimi e gli utenti finali.
Per far fronte alla frattura derivante dalla non comprensibilità degli utenti Diakopoulos suggerisce di implementare programmi di *data literacy*, oltre che di valorizzare il ruolo della stampa, la quale sarebbe chiamata a informare il grande pubblico in merito a come le decisioni algoritmiche impattino nella quotidianità degli utenti, dando dunque la possibilità ai singoli di formare un pensiero critico in materia. Si v. DIAKOPOULOS, *Algorithmic accountability reporting: on the investigation of black boxes* (2014) *Two Center for Digital Journalism*, consultabile all'indirizzo: *https://academiccommons.columbia.edu/doi/10.7916/D8ZK5TW2* (ultimo accesso 30 maggio 2021).
Interessante anche la proposta di Aulino di un approccio incentrato sul *legal design*. L'Autrice propone la valorizzazione del ruolo della tecnologia anche nel contesto delle informative privacy mediante una rimodulazione grafica di queste ultime, in modo da renderle concise e intuitive per gli utenti. Questo tipo di approccio – evidenzia Aulino – consentirebbe di aumentare la "consapevolezza situazionale" degli utenti e permettere così una scelta effettivamente informata. V. AULINO, *op. cit.*, 309 ss.

[531] Con il GDPR il legislatore europeo, nonostante abbia introdotto significative novità rispetto alla disciplina previgente, non sembra aver recepito le tensioni che, come visto, caratterizzano il principio di finalità in relazione ai Big Data, né le criticità legate all'autodeterminazione della persona interessata. In arg. Mantelero evidenzia come l'impostazione data nel Regolamento non pare essere adeguata alla tutela effettiva degli individui, in particolare per quei trattamenti digitali operati mediante tecnologie *data driven*. V. MANTELERO, *La privacy all'epoca dei Big Data*, in *I dati personali nel diritto europeo*, cit., 1192 ss.

[532] Cfr. per un approfondimento in merito all'accezione dal dare al termine si v. G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019 /770 e il Regolamento (UE) 2016/ 679*, in *La circolazione dei dati*, cit., 64 ss.; PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 215 ss.; SIANO, MONTUORI, *op. cit.*, 110 ss.; BRAVO, *Il consenso e le altre condizioni di liceità*, cit., 157 ss.; ID., *Le condizioni di liceità del trattamento di dati personali*, in *La protezione dei dati personali in Italia*, cit., 151 ss.

manifestato serenamente dall'individuo, dunque senza che esso sia stato soggetto a forzature o pressioni dirette a coartare la volontà. Infine, si ritiene che il consenso possa considerarsi effettivamente libero solo nella misura in cui esso non sia condizionato all'ottenimento di un bene o di un servizio essenziale per l'interessato[533]. Ne discende allora come esso debba dunque essere "patrimonialmente disinteressato". Il consenso viene infatti considerato non libero qualora sia prestato per avere qualcosa in cambio, salvo che sia necessario per l'esecuzione di un contratto[534]. Impostazione, quest'ultima, confermata dallo stesso Garante per la protezione dei dati personali, che ha espressamente chiarito come «*non possa definirsi libero, ma necessitato, il consenso al trattamento dei dati personali che l'interessato deve prestare (aderendo ad un testo predisposto unilateralmente dalla controparte contrattuale) quale condizione per il conseguimento della prestazione richiesta. In tal modo, infatti, i dati personali, lecitamente raccolti dal titolare (e conferiti dall'interessato) per il perseguimento di una determinata finalità (l'esecuzione del rapporto contrattuale), vengono di fatto piegati ad un utilizzo diverso dallo scopo originario che ne aveva giustificato la raccolta, in violazione del principio di finalità*»[535].

Il Regolamento prevede inoltre che l'informativa presentata agli utenti debba essere chiara, intellegibile e specifica. Sul punto sono gli stessi articoli 12-15 a prevedere quali informazioni il titolare è tenuto a fornire all'interessato al momento della raccolta dei dati presso questi o presso terzi[536]. Per quanto le disposizioni si mostrino puntuali,

---

[533] In arg. VIVARELLI, *op. cit*., 62. Vengono, dunque, ritenute illegittime quelle pratiche che richiedono la concessione del consenso a trattamenti terzi necessario per usufruire del servizio. Lo stesso art. 7, comma 4°, reg. UE n. 679/2016, prevede espressamente che «*Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*».

[534] Così considerato pare, dunque, escludersi che il consenso possa essere commercializzato. Sul punto THOBANI, *Il consenso al trattamento dei dati come condizione per la fruizione di servizi on-line*, in *Internet e diritto civile*, a cura di C. PERLINGIERI e RUGGERI, Napoli, 2015, 466.

[535] Da ultimo 18.1.2018, Ordinanza di ingiunzione nei confronti di Telecom Italia S.p.A. (doc. web. 7665804). Conf. Provvedimento, 4.7.2014, n. 330, Linee guida in materia di attività promozionale e contrasto allo spam (doc. web 2542348); Provvedimento, 26.3.2010, Marketing: necessario il consenso per l´invio di comunicazioni promozionali via e-mail (doc. web 1727662). In argomento si v. anche VIVARELLI, *ibidem*.

[536] La previsione particolareggiata del contenuto delle informative si dimostra espressione del principio di trasparenza affermato all'art. 5 GDPR. In argomento Di Lorenzo ritiene, infatti, che il Regolamento «riferisce la trasparenza, anzitutto, al dovere di *clare loqui* posto a carico del titolare del trattamento, ancor prima e indipendentemente dalla valutazione del merito delle informazioni o delle comunicazioni da fornire all'interessato». Pertanto la mancata osservanza del dovere di trasparenza può comportare l'illiceità del trattamento. V. DI LORENZO, *Spunti di riflessione su taluni "diritti dell'interessato"*, in

quanto meno per alcuni aspetti, si sono già evidenziate alcune difficoltà, in particolare quelle legate all'identificazione a priori degli scopi della raccolta[537]. Per l'argomento che qui ci occupa, l'art. 13, alla lettera *f*), prescrive un obbligo di informazione circa l'esistenza di un processo decisionale automatizzato e, in questi casi, un obbligo di comunicazione delle informazioni significative sulla logica utilizzata, nonché sull'importanza e sulle conseguenze previste per l'interessato.

La previsione risponde alla necessità che all'interessato siano fornite tutte le informazioni che gli permettano di esercitare pienamente il proprio diritto all'autodeterminazione in merito all'uso che viene fatto dei suoi dati personali. Come accennato in precedenza, e come si avrà modo di approfondire nelle prossime pagine, proprio il funzionamento spesso opaco degli algoritmi utilizzati nei trattamenti dei dati rappresenta un ulteriore ostacolo all'effettività dell'istituto del consenso; non potendo fornire in modo intellegibile le informazioni necessarie a chiarire il funzionamento e le logiche sottese alle decisioni della macchina, il consenso prestato dall'utente si mostra in realtà non pienamente consapevole e in parte nemmeno libero.

Sul punto, in una recentissima ordinanza, la Suprema Corte ha avuto modo di esprimersi proprio in merito alla validità del consenso prestato dagli utenti a un servizio di *rating* reputazionale che si fondava su di una profilazione algoritmica[538].

Nel caso di specie il Garante per la protezione dei dati personali aveva disposto il divieto di effettuare qualsiasi operazione di trattamento dei dati a una piattaforma web che forniva un servizio di elaborazione di profili reputazionali concernenti persone fisiche e giuridiche. Il Garante, proprio a fronte del funzionamento del servizio, in grado di impattare pesantemente sulla vita privata degli utenti censiti, aveva riscontato l'assenza di una idonea cornice normativa quale base di legittimità del trattamento.

Persona e mercato dei dati, cit., 241; CAGGIA, *op. cit.*, 260 ss.; CALISAI, *I diritti dell'interessato*, in *I dati personali nel diritto europeo*, cit., 336 ss.

[537] Cfr. DI LORENZO, *op. cit.*, 242 s. In argomento Caggia sostiene che l'istituto sia diretto a porre un correttivo a un problema attuale di concentrazione di potere in capo ad alcuni soggetti, rispetto a un potenziale controllo su una massa enorme di dati. Una conferma viene fatta discendere dal ruolo esercitato dalle tecniche utilizzate per la raccolta del consenso. L'Autore, infatti, ritiene che si sia portati a escludere la possibilità di ricorrere alla denuncia circa l'assenza di libertà del consenso nelle ipotesi di trattamenti riferiti a singole persone; in questo caso pur non potendo escludere la presenza di uno squilibrio contrattuale, questo non appare come un elemento strutturale della relazione. Diversa, invece, la struttura della relazione quando l'attività di raccolta viene posta in essere nei confronti di un pubblico indistinto in rete. V. CAGGIA, *op. cit.*, 266 s.

[538] Cass., 25.5.2021, n. 14381, in *Guida al dir*., 2021, 23.

Il provvedimento era stato impugnato dall'associazione che forniva il servizio, sostenendo che la base di legittimità fosse da rinvenire nel consenso prestato dagli stessi utenti. Avverso alla decisione del Tribunale, che accoglieva le doglianze di parte attrice, l'Avvocatura Generale dello Stato, per conto del Garante, ricorreva in Cassazione denunziando l'omesso esame del fatto rappresentato dalla dedotta inconoscibilità dell'algoritmo utilizzato, da cui conseguiva la mancanza del requisito della trasparenza del sistema, funzionale a rendere consapevole il consenso.

Fermo restando il ruolo che può assumere il consenso quale base di legittimità del trattamento, la Corte chiarisce che affinché questo possa essere considerato validamente prestato il Titolare è chiamato a fornire all'utente le informazioni in merito a un trattamento chiaramente individuato e definito nei suoi elementi essenziali, così che il consenso possa ritenersi liberamente e specificamente espresso[539]. Nel caso di specie, invece, gli utenti prestavano un generico consenso all'utilizzo della piattaforma, senza essere messi a conoscenza del funzionamento dell'algoritmo di *rating*, a nulla rilevando che la verifica della bontà delle valutazioni fosse poi lasciata al "mercato"[540].

Non può dunque dirsi consapevole un consenso prestato ove il funzionamento dell'algoritmo e gli elementi di cui esso si compone rimangano ignoti o non conoscibili da parte degli interessati.

Il caso si mostra particolarmente interessante proprio per il principio di diritto affermato dalla Suprema Corte, che pare mettere in evidenza i limiti dell'istituto in parola, ponendo così un freno a tutti quei trattamenti algoritmici che si fondano su di un consenso degli utenti che, seppure raccolto espressamente, nei fatti si dimostra, come visto, inconsapevole.

---

[539] La Cassazione si era già espressa chiarendo che ai fini della liceità del trattamento basato sul consenso fosse necessario non solamente che il titolare raccogliesse il consenso, ma che questo fosse valido; che fosse dunque libero, informato e consapevole. Cfr., tra le ultime, Cass., 2.7.2018, n. 17278, in *Guida al dir.*, 2018, 20; Cass., 21.6.2018, n. 16358, *ivi*, 32; Cass., 16.5.2016, n. 9982, in *Dir. e Guis.*, 2016.

[540] La scarsa trasparenza del sistema non veniva reputata decisiva, sul rilievo che la validità della formula (elaborata dall'algoritmo e concernente la reputazione degli utenti) riguarderebbe il momento valutativo, «*a fronte del quale spetterebbe invece al mercato stabilire l'efficacia e la bontà del risultato ovvero del servizio prestato dalla piattaforma*», non incidendo, dunque, sul consenso prestato dagli utenti al momento dell'adesione al servizio. La Corte evidenzia, infatti, come «*non può logicamente affermarsi che l'adesione a una piattaforma da parte dei consociati comprenda anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo, per la valutazione oggettiva di dati personali, laddove non siano resi conoscibili lo schema esecutivo in cui l'algoritmo si esprime e gli elementi all'uopo considerati*». Cass., 25.5.2021, n. 14381, cit.

É stato sostenuto come il dovere di trasparenza che si delinea nei confronti del titolare sia in parte attenuato da una sorta di onere di autoresponsabilità che graverebbe sugli interessati. Si ritiene, infatti, ragionevole imputare all'utente, colpevolmente incurante dell'informativa, il rischio della inconsapevole circolazione dei propri dati. Nonostante un recente arresto giurisprudenziale, che ritiene il consenso in materia di privacy distinto sul piano del diritto rispetto a quello richiesto a fini negoziali[541], si è sostenuto che dal dettato normativo regolamentare emergerebbe la liceità dei trattamenti anche nel caso in cui l'interessato ignori con colpa l'informativa. Il fondamento di tale posizione viene fatto discendere proprio dalla lettura degli artt. 13 e 14, dai quali emerge la circostanza che il titolare non sia tenuto a fornire l'informativa allorché l'interessato già disponga delle informazioni ivi previste. Ne consegue, sul piano del diritto, che l'acquisizione delle informazioni nella propria sfera di disponibilità tenga luogo alla effettiva conoscenza[542].

Detta posizione non pare tuttavia condivisibile. Sebbene il Regolamento preveda in modo analitico i doveri informativi, quale espressione appunto di un obbligo di trasparenza, ciò di per sé non pare essere sufficiente a garantire quel coinvolgimento consapevole che è necessario affinché possa trovare effettiva espressione il diritto di disporre dei propri dati personali. Nemmeno la circostanza da ultimo citata, in merito al mancato obbligo di trasmissione di un'informativa già posseduta, pare sul punto dirimente[543]. Le disposizioni piuttosto si mostrano poco in linea con la prassi dei

[541] Si fa riferimento a Cass., 2.7.2018, n. 17278, cit.
[542] V. DI LORENZO, *op. cit.*, 245 s.
[543] Dal consenso non può farsi discendere un'automatica assunzione di rischio del soggetto, dovendo piuttosto compiersi una valutazione oggettiva delle posizioni e degli interessi delle parti. Deve essere, infatti, tenuta in considerazione l'utilità del rischio creato, la sua entità, quali interessi vengono messi in pericolo e la possibilità per il soggetto eventualmente danneggiato di sottrarsi a esso. Il fondamento dell'assunzione di rischio si basa sull'alternativa data al singolo, per cui questo può liberamente sottrarsi a esso o tutelarsene autonomamente. Tuttavia, non sempre questa alternativa è possibile, come nel caso di specie ove vi è una sostanziale sottovalutazione del rischio da parte degli interessati. Sul punto autorevole dottrina ricorda come «si tratterà di stabilire se e quando la particolare posizione del danneggiato di fronte al rischio possa modificare i su accennati elementi oggettivi fino a giustificare un'esclusione o una limitazione della responsabilità nei suoi confronti. La volontà di esporsi al rischio, ed eventualmente l'approvazione di esso (trascuriamo qui la volontà contrattuale di rinuncia ad ogni azione di responsabilità), possono valere a rendere lecita una condotta altrimenti illecita; e analogo effetto può avere una condotta del danneggiato, tale da far credere a una sua volontà di esporsi al rischio o di approvarlo. Ma questi non sono che alcuni degli elementi rilevanti: le ragioni per le quali il danneggiato si è esposto al rischio; l'utilità sociale della sua attività in rapporto a quella dell'attività rischiosa del danneggiante; il fatto che l'esposizione del danneggiato al rischio sia avvenuta nel corso di un rapporto contrattuale oneroso col danneggiante, oppure di un rapporto contrattuale gratuito, oppure sia stata consentita a titolo amichevole, o solo tollerata, o invece vietata dal danneggiante; il fatto che l'esposizione del danneggiato sia stata manifestazione di un fenomeno socialmente necessario, o

trattamenti moderni, rimanendo per molti versi, come già si è avuto modo di osservare, ancorate a una visione ormai superata della tecnologia e delle modalità di interazione con gli utenti. Il legislatore non tiene, infatti, in adeguata considerazione l'oggettiva difficoltà di comprendere, a prescindere dalle modalità espositive, le informazioni tecniche relative alle logiche sottese alle modalità di trattamento[544]. A fronte dunque delle obiettive difficoltà di comprensione che affliggono inevitabilmente il consenso, alla luce anche degli studi comportamentali sopra richiamati, non pare allora ragionevole che sugli utenti gravi il rischio di eventuali danni loro arrecati dal trattamento.

Diversamente nel caso in cui vi fosse un consenso effettivamente libero e informato, di tal che l'utente, soppesando rischi e benefici, abbia ritenuto di assumersi il rischio di subire un eventuale danno, quale esito di una valutazione quantomeno consapevole. Tuttavia, ciò appare sempre più difficile in ragione dell'uso pervasivo delle applicazioni digitali, il cui funzionamento risulta spesso essere opaco anche per gli stessi programmatori, dando luogo a quella che è stata efficacemente definita una *black box*[545].

4. Il diritto alla spiegazione, un dibattito ancora acceso

La questione in merito alle informazioni che il titolare del trattamento deve fornire al momento della raccolta del consenso si intreccia con la previsione del terzo comma dell'articolo in analisi. La disposizione statuisce che il titolare, nei casi in cui il trattamento si fondi sul consenso esplicito o sia necessario per la conclusione di un contratto, debba apprestare delle misure appropriate per tutelare i diritti e le libertà degli utenti; tra queste viene esplicitamente previsto l'intervento di un essere umano nel processo decisorio (*human in the loop*), il diritto di esprimere la propria opinione e di contestare la decisione automatizzata.

---

frequente, oppure no; il fatto che il danneggiato si sia esposto al pericolo come membro del pubblico, oppure in un rapporto individuale col danneggiante: questi sono tutti elementi che possono contribuire a determinare la soluzione del problema, insieme con le considerazioni sulla volontà del danneggiato e sulla sua consapevolezza del rischio». TRIMARCHI, *La responsabilità civile: atti illeciti, rischio, danno*, Milano, 2017, 94 s.

[544] Cfr. DI LORENZO, *ibidem*.

[545] PASQUALE, *The black box society*, cit.

Sul punto interessante la ricostruzione di parte della dottrina che ritiene l'intervento umano l'unico mezzo effettivamente idoneo a soddisfare il requisito dell'appropriatezza previsto dalla normativa[546]. Unicamente la presenza di un interlocutore, pur se non specificamente individuato, avente le necessarie capacità e autorità per modificare la decisione automatizzata, configurerebbe un effettivo presidio di garanzia a fronte di possibili esternalità negative. Detta posizione non è tuttavia condivisibile in quanto le misure appropriate, a cui fa riferimento il testo dell'articolo in commento, potrebbero ben consistere anche in sistemi automatizzati aventi lo scopo di controllare gli algoritmi, mediante revisioni periodiche, così da poterne verificare l'accuratezza e correggerne errori e inesattezze[547].

Se dunque possono essere diversi i mezzi che il titolare può legittimamente adottare per garantire i diritti degli interessati, appare tuttavia fin da subito evidente che la prerogativa per poter rendere effettivi i diritti sopra citati risieda nella comprensione dei meccanismi di funzionamento che hanno portato il sistema a una determinata soluzione. Se non fosse possibile comprendere la logica sottostante allo specifico *output* elaborato dalla macchina sarebbe, infatti, complesso un intervento umano diretto a modificarne i risultati; parimenti complesso appare l'esercizio del diritto di contestare la decisione automatizzata dal momento che di essa non è possibile conoscere la *ratio* ma solamente l'esito[548].

A fronte di queste considerazioni si è aperto un acceso dibattito in merito all'esistenza di un c.d. diritto alla spiegazione per coloro che sono soggetti a decisioni

---

[546] Si v. PELLECCHIA, *op. cit.*, 1220 ss., la quale riporta una disamina sulle "misure appropriate" previste dalla normativa. In argomento anche FALLETTI, *op. cit.*, 179 ss. Sul punto l'Autrice riporta la posizione della dottrina americana che si esprime nei termini di un "*right to a human decision*". Emergerebbe dunque un diritto a che un essere umano sia coinvolto nel processo decisorio, ciò in quanto solo così potrebbero avere ingresso la sensibilità e la capacità, tipicamente umana, di cogliere le sfumature tra le circostanze fattuali e, soprattutto, ciò permetterebbe l'utilizzo di una appropriata terminologia per qualificare i concetti giuridici.

[547] In argomento MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale*, cit., 863 ss.; PELLECCHIA, *op. cit.*, 1209 ss. Si vedano anche le linee guida emanate del Gruppo di Lavoro art. 29, le quali sembrano propendere proprio per una valorizzazione del ruolo degli strumenti tecnologici in chiave di controllo e di successivo intervento nel caso in cui vengano rilevati errori nei procedimenti automatizzati. *Guidelines on automated individual decision making and profiling for purposes of regulation 2016/679*, cit.

[548] Lo stesso Comitato europeo per la protezione dei dati ha, infatti, riconosciuto come la massima trasparenza, seppure garantita da standard informativi elevati, non può essere ritenuta sufficiente nel caso in cui le informazioni ricevute non siano comprensibili al destinatario. Detta circostanza, tuttavia, si verifica proprio in relazione a tutti quei trattamenti che si fondano sull'utilizzo di tecniche di *data mining* fondate sull'Intelligenza Artificiale. Si veda in argomento PELLECCHIA, *ibidem*; FALLETTI, *op. cit.*, 182 s.

automatizzate[549]. Sebbene il testo dell'art. 22 non preveda un espresso riferimento, ci si è chiesti se ad esso non potesse essere data un'interpretazione estensiva secondo quanto indicato dal Considerando n. 71[550], che sul punto precisa come l'interessato abbia il diritto di «*ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione*»[551].

---

[549] Diversi sono i contributi sul tema, si rimanda, senza pretesa di esaustività, a DE GREGORIO, TORINO, *op. cit.*, 469 ss.; PELLECCHIA, *op. cit.*, 1218 ss.; WACHTER, MITTELSTADT, FLORIDI, *ibidem*; MALGIERI, COMANDÈ, *op. cit.*, 243 ss.; FALLETTI, *ibidem*; MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale*, cit., 866 ss.; BRKAN, *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond* (2019) 27 *International Journal of Law and information technology* 91 ss.; SIMEONE, *op. cit.*, 284 ss.

[550] «*L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani. Tale trattamento comprende la «profilazione», che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona. Tuttavia, è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, se ciò è espressamente previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito. In ogni caso, tale trattamento dovrebbe essere subordinato a garanzie adeguate, che dovrebbero comprendere la specifica informazione all'interessato e 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. Tale misura non dovrebbe riguardare un minore.*

Al fine di garantire un trattamento corretto e trasparente nel rispetto dell'interessato, tenendo in considerazione le circostanze e il contesto specifici in cui i dati personali sono trattati, è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, metta in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori e al fine di garantire la sicurezza dei dati personali secondo una modalità che tenga conto dei potenziali rischi esistenti per gli interessi e i diritti dell'interessato e impedisca, tra l'altro, effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale, ovvero un trattamento che comporti misure aventi tali effetti. Il processo decisionale automatizzato e la profilazione basati su categorie particolari di dati personali dovrebbero essere consentiti solo a determinate condizioni». Considerando n. 71, reg. UE n. 679/2016.

[551] A sostegno di tale posizione interpretativa si rimandano, tra gli altri, a CAIA, *op. cit.*, 222; MESSINETTI, *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, cit., 188 ss.; ID., *La tutela della persona umana* versus *l'intelligenza artificiale*, *ibidem*; PELLECCHIA, *ibidem*; FALLETTI, *ibidem*; GOODMAN, FLAXMAN, *European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"* (2017) 38 *AI Magazine* 55 ss.; SELBST, POWLES, *Meaningful information and explanation* (2017) *International Data Privacy Law* 233 ss. BRKAN, *op. cit.*, 110 ss., ritiene che, indipendentemente da come lo si voglia chiamare, esiste un diritto a che gli interessati siano informati in merito a come funziona il sistema di decisione automatizzato. L'A. rileva, tuttavia, come l'effettività di tale diritto vada verificata nella pratica, in quanto i sistemi fondati su algoritmi di *deep learning* spesso non permettono di arrivare a

La posizione in dottrina non è pacifica. Parte dei commentatori ritiene che dal testo del GDPR non possa essere fatto discendere un diritto di tal fatta. Gli argomenti a favore di questa tesi sono molteplici e trovano fondamento tendenzialmente sul tenore letterale delle disposizioni regolamentari.

Si sostiene, innanzitutto, che a nulla varrebbe l'indicazione presente nel Considerando n. 71, dal momento che esso, avendo una funzione meramente esplicativa del testo di legge, non possiede una valenza normativa. A ciò si aggiunge come, pur essendo i considerando diretti a guidare l'opera degli interpreti, nel caso in esame esso non troverebbe applicazione, in quanto le norme sarebbero sufficientemente chiare e pertanto non richiederebbero alcuna precisazione interpretativa.

Nessuna rilevanza avrebbero, infine, le norme dirette a regolare il contenuto degli obblighi informativi previste agli articoli 13 e 14. Queste ultime – si sostiene – non possono trovare applicazione nel caso specifico delle decisioni automatizzate, in quanto sarebbero poste a presidio di una fase anteriore a quella della decisione e, precisamente, quella della raccolta dei dati. Inoltre, se anche fosse possibile dare alle norme sopra citate un'interpretazione estensiva, le informazioni richieste sarebbero comunque riferibili non alla singola decisione contestata, ma alla logica generale circa il funzionamento dell'algoritmo.

È interessante notare come nel testo della proposta di Regolamento fosse in realtà espressamente presente nel dettato normativo un diritto alla spiegazione; previsione poi espunta e lasciata unicamente nel considerando sopra citato[552]. Ne deriva, dunque, come sia stata una precisa scelta del legislatore quella di non prevedere un obbligo così delineato, forse anche in ragione dalla consapevolezza in merito alle crescenti difficoltà per il titolare di fornire una spiegazione confezionata sul singolo caso concreto; certamente più agevole si dimostra, infatti, l'obbligo di fornire indicazioni sulla generale logica sottesa al funzionamento dei sistemi informatici.

---

tale tipo di necessaria comprensione. Sul punto anche EDWARDS, VEALE, *Slave to the algorithm? Why a "right to an explanation" in probably not the remedy you are looking for* (2017) 16 *Duke Law & Technology review* 44, i quali evidenziano le difficoltà tecniche di esercizio di detto diritto in relazione agli algoritmi di *machine learning*.

[552] Si v. sul punto Moretti, il quale sostiene che dalla lettura della norma, così come oggi formulata, non sarebbe possibile far discendere un diritto alla spiegazione; questo potrebbe emergere solo da una prassi interpretativa che sia diretta a dare un'accezione maggiormente estesa alla normativa regolamentare. MORETTI, *Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679*, in *Dir. inform.*, 2018, 811 ss.; SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 260 ss. Tra i maggiori oppositori alla presenza di un diritto alla spiegazione all'interno del GDPR si v. WACHTER, MITTELSTADT, FLORIDI, *op. cit.*, 76 ss.

Guardando dunque unicamente al tenore letterale delle disposizioni, le informazioni "significative" richieste sembrerebbero effettivamente fare riferimento a una serie di indicazioni dirette sostanzialmente a specificare le modalità di funzionamento generale del processo automatizzato, e in che modo esso possa incidere sui diritti e le libertà degli interessati. Questo tipo di informazioni in alcuni casi può essere sufficiente a spiegare anche l'*output* del sistema; ciò in particolare per tutti quegli algoritmi che si fondano su di una logica lineare e deterministica. In essi, una volta chiarito il funzionamento generale, solitamente di natura *IF*/*THEN*, sarà allora intellegibile anche il risultato finale.

Diverso il discorso per quegli algoritmi non deterministici, quali sono quelli che si fondano su tecniche di *Deep Learning*, il cui funzionamento è particolarmente complesso perché interessato da un grande numero di variabili e di livelli di astrazione. In questi casi il funzionamento generale non permette di comprendere la *ratio* a fondamento delle singole decisioni. Ciò dunque comporterebbe per gli interessati, quanto meno per quei trattamenti automatizzati operati mediante algoritmi complessi, una mancanza di fatto di strumenti a tutela dei propri diritti, non rivelandosi utile una spiegazione generale al fine di efficacemente contestare un risultato specifico.

Se si accogliesse la ricostruzione dell'articolo in analisi quale espressione di un obbligo di fornire informazioni unicamente sulla generale logica del processo algoritmico, questi si dimostrerebbe gravemente lacunoso rendendo di fatto inefficaci le garanzie introdotte al terzo comma. Pertanto, alla posizione sopra ricordata si contrappone altra parte della dottrina, la quale ritiene come un diritto alla spiegazione emerga da una lettura sistematica delle disposizioni del GDPR, ivi compreso quanto previsto dal Considerando n. 71. All'espressione "informazioni significative sulla logica utilizzata" dovrebbe dunque essere data un'accezione più generale, nella quale andrebbero ricomprese tutte quelle informazioni che permettono all'interessato di comprendere le modalità di funzionamento del sistema, ivi compresa anche la logica sottesa al singolo risultato[553].

[553] Cfr. MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale*, *ibidem*; ID., *Trattamento dei dati per finalità di profilazione e decisioni automatizzate*, *ibidem*; PELLECCHIA, *ibidem*; FALLETTI, *ibidem*; SELBST, POWLES, *ibidem*. Interessante la posizione di questi ultimi che, in forte contrasto con la posizione espressa da Floridi, sottolineano come dal dettato normativo emerga un diritto alla spiegazione strettamente collegato alle informazioni significative, cioè strumentale a esercitare i

Il rilievo per cui gli articoli 13-14 non troverebbero applicazione nel caso di specie, riguardando una fase antecedente alla decisione, non pare essere pienamente convincente. Sul punto si evidenzia come il contenuto dell'obbligo informativo venga riportato pressoché integralmente anche nell'art. 15, dedicato al diritto di accesso, che ben potrebbe essere esercitato successivamente alla scoperta di essere stati oggetto di una decisione automatizzata. Ne discende allora come il diritto di ottenere informazioni significative operi durante tutto l'arco del trattamento, a nulla rilevando una pretesa differenziazione su base temporale.

Del pari – si specifica – poco incisiva si mostra la considerazione per cui i considerando non posseggano di per sé una valenza normativa; difatti, essi sono specificamente diretti a guidare l'interpretazione delle disposizioni regolamentari, rivestendo dunque un ruolo di rilievo nell'economia del testo legislativo, che dunque deve essere letto proprio alla luce delle specificazioni ivi previste. Poco fondato anche il rilievo per cui il considerando in parola nemmeno varrebbe come ausilio alla lettura dell'art. 22, rivelandosi questo già sufficientemente chiaro; questa critica si mostra, infatti, subito smentita dall'acceso dibattito, proprio in punto di interpretazione, che anima ancora oggi gli interpreti della materia.

Una particolare menzione merita infine la posizione espressa da autorevole dottrina, che ritiene debba essere fatto discendere dal dettato del GDPR un diritto non alla spiegazione, ma alla "leggibilità" dei dati e degli algoritmi[554]. L'obbligo di fornire informazioni significative avrebbe dunque quale oggetto tutte quelle informazioni necessarie a rendere comprensibile il funzionamento dell'algoritmo e che al contempo permettano di dare trasparenza al processo automatizzato, nell'ottica di rendere effettivo l'esercizio dei diritti riconosciuti agli interessati, senza tuttavia entrare nella specifica funzionalità tecnica del sistema.

Un diritto così elaborato – si specifica – sarebbe in grado di combinare la comprensibilità dell'architettura del sistema con la trasparenza sull'uso dello stesso, definita "implementazione". Questa posizione permetterebbe di superare le critiche, sopra riportate, in merito all'assenza di una previsione espressa di un diritto alla

---

diritti e le prerogative concesse agli interessati; ne discende, dunque, una necessaria lettura funzionale del diritto così delineato.

[554] A teorizzare un diritto alla leggibilità emergente da una lettura sistematica del testo del Regolamento MALGIERI, COMANDÈ, *ibidem*. In argomento v. anche PELLECCHIA, *op. cit.*, 1223 ss.; FALLETTI, *ibidem*.

spiegazione, sia le tensioni con le normative a tutela di eventuali segreti industriali su algoritmi e *dataset* utilizzati[555]. Le informazioni che permettono la leggibilità della decisione non coinciderebbero, infatti, con quanto necessario a spiegare nel dettaglio i singoli *output*, né obbligherebbero i titolari a svelare le tecniche di funzionamento degli algoritmi potenzialmente coperte da segreto; ciò che il titolare sarebbe tenuto a fornire dovrebbero essere unicamente quelle informazioni che permettano agli utenti di esercitare le prerogative loro concesse dal GDPR[556].

Gli autori, sul punto, presentano anche un c.d. test di leggibilità, diretto a chiarire, mediante una esemplificazione, quali informazioni i titolari debbano effettivamente fornire[557].

---

[555] Si tratta di quella che Burrell chiama opacità intenzionale. I maggiori sistemi algoritmici sono, come visto, proprietà di aziende private e, dunque, la presenza di un diritto alla spiegazione andrebbe a scontrarsi con la disciplina in materia di proprietà intellettuale e *trade seceret* (come è stato nel caso COMPAS). In argomento si v. TABARRINI, *op. cit.*, 573 ss.

[556] Gli Autori precisano che «legibility means the capability of individuals to autonomously understand the logic, the significance and the envisaged consequences of an algorithmic decision-making. It is different from mere readability of data or analytics because it includes more details about purposes, finalities, commercial significance and envisaged consequences; but it is also different from explanation/information because it is more 'proactive', tailored on individual understanding and concrete comprehensibility of the logic and consequences disclosed». MALGIERI, COMANDÈ, *op. cit.*, 245. Di diverso avviso Tabarrini, la quale ritiene che proprio in ragione dell'impossibilità di accertare il funzionamento delle applicazioni di *deep learning* nessuna delle due forme di *auditing* proposte da Malgieri e Comandè – tanto quella sull'architettura, quanto quella sull'implementazione dei dati – sarebbero allo stato attuale della tecnica sostenibili. V. TABARRINI, *op. cit.*, 570 ss.

[557] Gli Autori presentano un vero e proprio test di leggibilità che si fonda sull'analisi di elementi chiave in due distinte fasi: quella strettamente funzionale (legata all'architettura del sistema) e quella legata alla fase di implementazione dell'algoritmo. Gli Autori spiegano, infatti, che «Two key elements of a decision-making process must be highlighted from the outset: its inherent functionality (strict logic) and its contextual use, consequences, impact, etc. In other words, we need to distinguish the technical architecture of an algorithm from the contextual implementation of the decision-making in which that algorithm is employed. That is why we have elaborated a two-steps test: a prong for the Architecture and a prong for the Implementation. With regard to the Architecture auditing, three key elements need to be analysed:
a) the creation of the algorithm, i.e. how it was designed, which data have fed the machine-learning algorithm, which categories have been used, whether there are some feedback or correction mechanism.
b) its functioning/use, i.e. how the algorithm works, what (personal) data it needs, if any, which scoring parameters it has or, e.g., the weighting of features.
c) its expected outputs, i.e. what the algorithm can determine/decide, which kind of output is provided (predictive analytics, prescriptive analytics, inferences, etc.).
As for the Implementation auditing, other elements are relevant:
a) purposes for which algorithmic decision-making is employed (credit scoring, work assessment, behavioural advertisement)
b) level and tasks of eventual human intervention (setting the score, the parameters, etc.)
c) commercial / non-commercial nature of that decision-making;
d) statistical impacts on past costumers;
e) possibility to reconsider a decision after the algorithm has released its output;
f) environment in which it is deployed

Questa lettura proposta da Malgieri e Comandè possiede, come visto, il pregio di comporre alcune delle maggiori criticità avanzate dalla dottrina più critica. Rimane tuttavia da verificarne l'effettività anche per quegli algoritmi non deterministici[558]. È infatti opportuno evidenziare come il test di leggibilità proposto dagli autori paia ben conformarsi per gli algoritmi deterministici; per gli algoritmi basati sul *deep learning* appare invece meno agevole l'individuazione stessa di quali informazioni possano essere considerate significative alla luce del test sopra richiamato. Inoltre, pur ammettendo che il titolare possa avere accesso alle informazioni così delineate, ci si domanda se esse siano effettivamente capaci di chiarire in modo sufficientemente adeguato il funzionamento dei sistemi.

Queste riflessioni si innestano su di un tema di respiro più ampio e legato in generale all'opacità di funzionamento degli algoritmi.

Parte degli esperti della materia ha, infatti, sottolineato che se pure esistesse un diritto alla spiegazione esso non sarebbe comunque utile, ciò in quanto una spiegazione del funzionamento dell'algoritmo si dimostrerebbe troppo complessa perché gli interessati possano comprenderla. A questo rilievo si affianca anche la considerazione in merito alla impossibilità tecnica di risalire a una spiegazione, nella accezione che al termine viene data dal Regolamento. Difatti attualmente si mostra sempre più pervasivo l'impiego proprio di algoritmi dall'architettura sempre più complessa e tale da formare delle *black boxes*, da cui non è detto si possa risalire compiutamente a una vera e propria spiegazione degli *output* generati.

4.1 La *black box society*

L'espressione *black box society*, coniata da Frank Pasquale, fa riferimento alla diffusione sempre più pervasiva di algoritmi le cui modalità di funzionamento sono di

---

Moving from the just mentioned reflections, we have developed a test that can both convey legibility of the architecture and of its implementation and be the basis for auditing algorithms, empowering users in black–box scenarios». MALGIERI, COMANDÈ, *op. cit.*, 258 ss.

[558] In argomento MULA, *op. cit.*, 142 s. In particolare l'Autore, pur condividendo la ricostruzione della normativa dalla quale emergerebbe un diritto all'accessibilità e conoscibilità del *modus* con cui gli algoritmi trattano i dati, ritiene che un tale dettaglio di informazioni, tecnicamente molto difficili da rendere per il destinatario medio di servizi digitali, non sia comunque idonea a colmare il deficit informativo tra titolare e utenti.

difficile comprensibilità anche per gli stessi programmatori[559]. Questa condizione deriva, come visto in apertura del presente lavoro, dalla stessa architettura dei sistemi oggi più diffusi, tale da renderli delle c.d. scatole nere a cui è difficile accedere. A ciò deve aggiungersi come la presenza di un numero sempre più considerevole di variabili processate renda complesso fornire una spiegazione del perché il sistema abbia prodotto un determinato *output*. Solo per fare un esempio, l'algoritmo di funzionamento di Google, pur basandosi grossomodo sulla teoria dello sciame, rimane tuttavia segreto e poco comprensibile in ogni sua parte finanche dai suoi stessi programmatori[560].

L'utilizzo di algoritmi non è tuttavia limitato ai motori di ricerca, ma si è ormai diffuso a macchia d'olio; non si tratta solo di impieghi commerciali, anche gli Stati utilizzano forme più o meno invasive di vigilanza sulla popolazione, finendo per creare una vera e propria società del controllo.

Il problema sorge non tanto in relazione agli scopi per cui dette tecnologie sono impiegate, nessuno dubita che ne sia legittimo l'utilizzo per contrastare la criminalità o per scopi commerciali, quanto per la mancanza di trasparenza dell'intero processo. Fuori dai casi, parimenti allarmanti, di un uso all'insaputa degli utenti, ciò che più preoccupa è proprio l'opacità che circonda il funzionamento degli algoritmi, tale per cui diviene difficile prevederne e contestarne gli esiti.

In questo contesto è allora evidente come, laddove non sia possibile garantire un effettivo controllo sull'intero procedimento, l'opacità dei sistemi accresca il rischio che esternalità negative si propaghino a un numero potenzialmente indefinito di soggetti.

Differenti sono stati i casi di risultati errati, discriminatori, o di pratiche scorrette, a cui sono seguite istanze di trasparenza e di visibilità che tuttavia si sono scontrate con le disposizioni in materia di *intellectual property* e *trade secret*, invocate in relazione alla struttura dell'algoritmo e agli stessi *dataset* utilizzati per l'addestramento.

In questo senso si pensi alla sentenza della Corte Suprema del Wisconsin nel caso COMPAS, la quale, ritenendo l'algoritmo coperto da segreto, ha rigettato la richiesta di accesso al codice sorgente avanzata dalla difesa al fine di verificare le modalità di

[559] PASQUALE, *The black box society*, *ibidem*.
[560] In argomento Pariser sottolinea come anche chi ha programmato il motore di ricerca di Google non ne comprende a pieno i meccanismi di funzionamento. Il motore è, infatti, composto da centinaia di righe di codice che vengono continuamente messe a punto dai programmatori, i quali di fatto sono maggiormente interessati alla *performance* nei risultati, più che alla comprensione della logica sottesa agli *output* generati. PARISER, *op. cit.*, 151.

determinazione dei risultati. La Corte ha comunque ritenuto legittimo l'utilizzo del software, in quanto esso rappresenterebbe un mero strumento di ausilio per il giudice, al quale rimane imputata la decisione finale.

La sentenza della Corte ha il merito di aprire le porte all'uso delle applicazioni algoritmiche anche all'interno dei procedimenti giudiziali, tuttavia pare necessaria una attenta ponderazione in merito alle modalità di uso in determinati contesti.

Il problema non risiede, come già evidenziato, nell'utilizzo di per sé di tali sistemi, quanto piuttosto nella mancanza di consapevolezza circa le modalità di effettivo funzionamento. Non si dubita della necessaria presenza di un decisore umano, e dunque del ruolo di supporto a cui questi apparati sono destinati; il rischio latente è tuttavia quello dell'affidamento nei confronti dei risultati della macchina. Affidamento che si dimostra in parte cieco proprio in ragione della mancanza di conoscibilità della *ratio* a fondamento dei singoli *output*, oltre che dalla mancanza di accessibilità alla composizione dei dati di addestramento.

L'ambito giudiziario è certamente tra quelli più sensibili, facendo emergere problemi legati al diritto di difesa, ma non è il solo. Anche quello sanitario si dimostra particolarmente sensibile al tema. Le applicazioni di diagnosi medica fondate su algoritmi sono ad oggi tra gli sviluppi più promettenti della tecnologia. La possibilità di sviluppare una medicina personalizzata rappresenta uno dei grandi vantaggi che l'AI è in grado di portare nella scienza medica. Tuttavia, pur nella consapevolezza del ruolo necessariamente centrale che il medico deve continuare a rivestire nel rapporto di cura, ci si domanda quanto affidamento possa essere fatto dal sanitario sulla macchina algoritmica. Se di conforto sono le percentuali di successo nelle diagnosi, a queste tuttavia fanno da contraltare i casi – certamente possibili – di falsi positivi o negativi. A fronte di percentuali di accuratezza molto alte, la possibilità di un affidamento acritico sui risultati proposti dal sistema è certamente reale. Pare allora necessaria un'attenta riflessione giuridica, e ciò alla luce del rischio di tendenziale dereponsabilizzazione dei professionisti, i quali finirebbero col demandare la decisione al sistema, scaricando su di esso anche l'eventuale responsabilità in caso di errore[561]. È facile ipotizzare come la

[561] Si evidenza come l'algoritmo crei una situazione asimmetrica sul piano della responsabilità: se il decisore umano non ritiene corretta la soluzione data dalla macchina si assume la responsabilità di discostarsi dall'*output*, nel caso in cui il sistema avesse avuto ragione; se invece il professionista asseconda la macchina, per poi scoprire che ha commesso un errore, ben potrebbe scaricare su di essa la

scelta dell'operatore umano di discostarsi dagli *output* presentati dagli algoritmi diverrà sempre più complessa, dovendo egli fornire una difficile giustificazione alle proprie scelte, a fronte dell'impossibilità di conoscere i meccanismi utilizzati dai sistemi informatici per arrivare a una decisione[562]. Se, infatti, per gli esperti la comprensione della logica che ha portato a un determinato *output* risulta difficoltosa, è forte il rischio che essa si trasformi in una vera impossibilità di comprensione per coloro che non hanno competenze tecniche in materia.

Per tornare a un caso concreto, se è vero che il software COMPAS ha rivestito nelle Corti un mero ruolo strumentale, rimane insoluta la questione di quanto affidamento su di esso abbiano fatto i giudici. Il caso di specie risulta inoltre di particolare interesse in relazione a un'ulteriore criticità nascente dall'utilizzo di software proprietari. Difatti, in questo caso le istanze di trasparenza in merito alla logica seguita dalla macchina sono state disattese in ragione della prevalenza accordata alle norme a tutela dei *trade secret*. Questa circostanza viene definita da Burrell come opacità intenzionale, ciò in quanto deriva da una forma di protezione intenzionalmente diretta a tenere segrete le specifiche dei sistemi; così da permettere alle società, che hanno investito nella produzione e nello sviluppo, di mantenere un vantaggio competitivo.

Per far fronte a questa forma di opacità si è proposto l'utilizzo di algoritmi unicamente *open source*, dunque liberamente accessibili dai terzi, così ovviando a possibili rischi di perdite economiche o di competitività delle imprese[563].

---

responsabilità. A ciò dovrebbe aggiungersi anche il rischio di indebolire la stessa capacità di prendere decisioni del tutto umane. V. LONGO, SCORZA, *Intelligenza Artificiale*, Torino, 2020, 116.

[562] Sul punto si rimanda a Comandè. L'Autore, riferendosi all'ambito medico, evidenzia come «man mano che le AI diventeranno più capaci, i medici come altri professionisti saranno spinti a fare affidamento su di loro perdendo progressivamente una reale capacità critica sull'effettivo funzionamento e l'efficacia delle AI usate (*automation bias*). L'argomento può apparire estremo, ma è invero facile immaginare che man mano che le AI in campo medico arriveranno a svolgere atti medici a livelli uguali o superiori a quelli umani e ad essere massivamente usate si realizzerà un crollo degli incentivi a monte per i fornitori di formazione per gli stessi compiti: il risultato porterebbe ad una paradossale perdita di competenze che rimarrebbero interamente affidate ad una AI, magari senza possibilità di spiegare compiutamente come essa "ragioni"». COMANDÈ, *Intelligenza Artificiale e responsabilità tra* liability *e* accountability, cit., 183.

[563] V. SANDVIG *et al.*, *Auditing algorithms: Research methods for detecting discrimination on internet platforms* 2014 consultabile all'indrizzo: *http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf* (ultimo accesso 14 settembre 2021); BURRELL, *op. cit.*, 4, il quale evidenza come vi siano diversi modelli di business di successo che sono nati da un movimento *open source*. In tema di libera accessibilità al codice dell'algoritmo anche DIAKOPOULOS, *ibidem*; GRANDY, *Engaging rational discrimination: Exploring reasons for placing regulatory constraints on decision support systems* (2010)12 *Ethics and Information Technology* 29 ss.

Altra proposta interessante vede invece l'affidamento del compito di controllo a un soggetto terzo (di natura pubblica), che possa avere accesso all'algoritmo e ai dati di addestramento, avente l'obbligo di mantenere riservate le informazioni tecniche potenzialmente coperte da segreto[564]. Si tratterebbe di una sorta di *watchdog* avente il compito specifico di monitorare la correttezza del funzionamento delle applicazioni di AI, in particolare per quei settori dove vi sia un rischio elevato di danni per utenti e terzi[565]. L'istituzione di questa figura permetterebbe dunque di garantire una maggiore trasparenza, potendo l'autorità di controllo avere accesso alle specifiche di sistema, senza tuttavia comportare per le imprese un eccessivo sacrificio.

Le considerazioni fin qui viste in merito alla necessità di contemperare la tutela della proprietà intellettuale e i diritti di accesso e trasparenza ai sistemi[566], così come previsto dallo stesso GDPR nel Considerando n. 63[567], non sono di poco conto; tuttavia, esse non

[564] V. PASQUALE, *The black box society*, cit., 141 ss., secondo cui il compito di questo *auditor* pubblico sarebbe quello di assicurare che le classificazioni operate dagli algoritmi non si fondino su dati discriminatori.

[565] La proposta di una tale istituzione è stata avanzata anche per la Nuova Zelanda, sebbene gli strumenti di AI del governo vengano progettati per così dire *in-house*. Si rimanda sul punto a ZERILLI, GAVAGHAN, *Call for independent watchdog to monitor NZ government use of artificial intelligence*, 27 maggio 2019, consultabile all'indirizzo: *www.theconversation.com/call-for-independent-watchdog-to-monitor-nz-government-use-of-artificial-intelligence-117589* (ultimo accesso 9 giugno 2021).

[566] Difatti il titolare del trattamento potrebbe limitare il confine del diritto a una spiegazione invocando le disposizioni a tutela dei segreti commerciali, della proprietà intellettuale o, più in generale, la propria libertà di iniziativa economica che verrebbe frustrata da obblighi di trasparenza. In argomento v. DE GREGORIO, TORINO, *op. cit.*, 471 ss. Si rimanda anche a CELOTTO, *op. cit.*, 55, il quale evidenzia come una possibile soluzione alle difficoltà legate all'accesso agli algoritmi coperti dalle norme a tutela del diritto d'autore sarebbe quella di un investimento da parte dei Governi, diretto all'acquisto della proprietà intellettuale e allo sviluppo *ab origine* delle macchine. Si creerebbe, dunque, un sistema istituzionale svincolato da ogni necessità di tutela della proprietà intellettuale, potendo così garantire un'effettiva trasparenza nell'adozione delle decisioni algoritmiche. Sul punto anche MULA, *op. cit.*, 149. In particolare l'Autore evidenzia come il diritto di accesso concesso agli utenti non possa essere generale, ma debba trovare un limite nei diritti del titolare a non svelare tutti i passaggi computazionali dell'algoritmo. Ciò in quanto esso sarebbe coperto dalla normativa sui segreti commerciali, ritenuta la migliore protezione possibile anche rispetto alle forme di privative tradizionali del diritto d'autore e del brevetto, sia rispetto agli algoritmi che con riferimento ai loro prodotti. Conf. OTTOLIA, *op. cit.*, 70.

[567] «*Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni.*

rappresentano il nodo della questione. Difatti, pur se venisse concesso un accesso completo e trasparente ai codici sorgente delle macchine, ciò non porterebbe automaticamente alla comprensione delle logiche sottese alle singole decisioni.

Si pensi, per fare un ulteriore esempio, alle recenti sentenze del TAR e del Consiglio di Stato in relazione alla vicenda dell'assegnazione delle sedi di insegnamento del personale scolastico[568]. Instaurandosi la vicenda nel periodo di *vocatio legis* del GDPR, e dunque non potendo trovare applicazione l'art. 22, i ricorrenti avevano invocato il diritto di accesso all'atto amministrativo, considerando come tale il codice sorgente dell'algoritmo utilizzato dal MIUR[569].

A detta richiesta il Ministero opponeva due obiezioni. Innanzitutto, veniva contestata la qualifica del codice sorgente quale documento amministrativo; inoltre si sosteneva che i codici del software, classificabili come opere di ingegno, fossero tutelati dalla normativa in materia di proprietà intellettuale.

In prima battuta il TAR, dopo aver riconosciuto l'algoritmo quale atto amministrativo informatico, ha ritenuto che secondo il principio di trasparenza, discendente dal principio di buon andamento della Pubblica Amministrazione così come previsto dall'art. 97 Cost. e trasfuso nella l. n. 241/90, dovesse essere garantito il diritto di accesso degli interessati al codice sorgente, al fine di poter verificare le modalità e i criteri di esercizio del potere amministrativo[570]. Successivamente è intervenuto il

---

Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce». Considerando n. 63, reg. UE n. 679/2016.

[568] Il caso prende il nome dalla riforma detta della "Buona Scuola", attuata mediante la l. 13.7.2015, n. 107, la quale comprendeva un piano straordinario di assunzione per gli insegnanti. La normativa prevedeva la presentazione delle domande di assegnazione delle sedi del personale scolastico unicamente mediante l'utilizzo di un apposito portale telematico, predisposto dal MIUR. Chiusa la procedura l'algoritmo procedeva in modo automatico alle assegnazioni, senza tuttavia avere apparentemente preso in alcuna considerazione le preferenze espresse dai richiedenti. Gli insegnanti, e i loro sindacati, insoddisfatti dall'esito avevano, dunque, adito il giudice amministrativo, lamentando la mancanza di indicazione dei criteri adottati per l'assegnazione. La vicenda viene approfondita da SIMONINI, *Diritto costituzionale e decisioni algoritmiche*, cit., 48 ss.; COSTANTINI, *op. cit.*, 990 ss.

[569] Diritto di accesso evidentemente strumentale a conoscere le modalità di funzionamento dell'algoritmo, dunque i criteri da esso seguiti per la determinazione degli abbinamenti.

[570] Sia il TAR Lazio che il Consiglio di Stato hanno riconosciuto il pieno diritto alla conoscenza dell'algoritmo, poiché anche la decisione robotizzata, in quanto atto amministrativo informatico, «*deve essere 'conoscibile', secondo una declinazione rafforzata del principio di trasparenza, che implica anche quello della piena conoscibilità di una regola espressa in un linguaggio differente da quello giuridico*». Cons. Stato, VI sez., 8.4.2019, n. 2270, in *Foro it.*, 2019, III, 606; anche T.A.R. Lazio, 22.3.2017, n. 3769, in *Leggi d'Italia*. In argomento si v. CELOTTO, *op. cit.*, 48. Per un approfondimento in merito alla configurabilità dell'algoritmo quale atto amministrativo informatico e delle modalità di esercizio del diritto di accesso si rimanda a FALLETTI, *op. cit.*, 188 ss.; DE LEONARDIS, *Big Data, decisioni*

Consiglio di Stato il quale, coordinando il diritto di accesso con il diritto alla spiegazione, ha confermato quanto già precisato dal TAR. Il massimo organo amministrativo si spinge però oltre dichiarando come sia sempre necessario «*nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatica.* […] *è necessario che la macchina interagisca con l'essere umano*», ridimensionando così la portata e il ruolo svolto dai sistemi algoritmici all'interno del procedimento amministrativo[571]. Interessante, infine, la previsione, diretta a trovare un punto di equilibrio tra efficienza delle macchine e diritti degli interessati, di quattro criteri a cui l'algoritmo dovrebbe rispondere al fine di poterne accettare l'utilizzo, e il cui rispetto garantirebbe altresì una concreta applicazione del disposto dell'art. 22 GDPR[572].

La decisione pare dunque rispondere pienamente alle istanze di trasparenza, ritenendole prevalenti rispetto a possibili diritti del titolare del software. La logica sottesa risiede nella considerazione per cui garantendo l'accesso al codice sorgente sia possibile fornire una spiegazione certa in merito al funzionamento dei sistemi algoritmici. Questa concezione si dimostra tuttavia non pienamente fondata. Avere accesso a tali informazioni, infatti, non è sufficiente di per sé solo a spiegare il perché un algoritmo sia arrivato a un determinato *output*. Le variabili e la complessità della struttura rendono necessaria un'opera di *reverse engineering*, dispendiosa non solo in termini economici ma anche di tempo, a cui comunque non segue la certezza di riuscire a individuare la *ratio* dello specifico risultato elaborato dalla macchina.

Avere accesso al codice sorgente permetterebbe unicamente di comprendere il metodo di apprendimento automatico implementato nel sistema, nulla direbbe in merito alle specifiche regole sottese alla singola decisione, andando queste – quanto meno nelle

---

amministrative e "povertà" di risorse della pubblica amministrazione, in *La decisione nel prisma dell'intelligenza artificiale*, cit., 137 ss.; FERRARI, *La seducente perfezione di algoritmi e intelligenza artificiale nelle procedure amministrative alla luce dei modelli di responsabilità civile*, in *Diritto di Internet*, 2020, 177 ss.; CRISCI, *Evoluzione tecnologica e trasparenza nei procedimenti "algoritmici"*, *ivi*, 2019, 380 ss.; TRESCA, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale*, in *Medialaws – riv. dir. media*, 2018, 251 ss.

[571] Cons. Stato, VI sez., 13.12.2019, n. 8472, in *Foro it.*, 2020, III, 340.

[572] I principi elaborati dal Consiglio di Stato possono essere così riassunti: 1. l'algoritmo deve soggiacere ai principi generali di trasparenza, ragionevolezza e proporzionalità; 2. Non possono essere ammessi spazi applicativa discrezionali, essendo questa un'attività espressione del potere amministrativo e dunque necessariamente demandata a un essere umano; 3. l'amministrazione è chiamata a svolgere un ruolo compositivo degli interessi tra le parti coinvolte, così da poter raggiungere un equilibrio; 4. deve essere contemplato che il sia il giudice a svolgere la valutazione della correttezza del processo automatizzato in tutte le sue componenti. Cons. Stato n. 8472/2019, cit. In argomento si veda FALLETTI, *op. cit.*, 191.

applicazioni di *deep learning* – a determinarsi compiutamente mano a mano che le operazioni di analisi dei dati vengono svolte[573].

Ne discende allora come anche una piena trasparenza dei sistemi non sia sufficiente a garantire l'effettiva intellegibilità degli stessi, a maggior ragione nei confronti degli interessati che non sempre posseggono competenze tecniche. A volte la piena trasparenza non è neppure possibile né auspicabile, come nel caso dei sistemi utilizzati per ragioni di sicurezza pubblica o nel caso in cui ciò potrebbe mettere a rischio la protezione dei dati personali o segreti commerciali[574].

4.2 Quali possibili soluzioni all'opacità intrinseca dei sistemi

Prima dunque di chiedersi se esista un diritto alla spiegazione, sarebbe opportuno comprendere se una spiegazione sia tecnicamente possibile. Le istanze di trasparenza e comprensibilità hanno certamente rilievo, ma solo ove sia effettivamente possibile per il titolare del trattamento, come per i singoli interessati, arrivare a una effettiva comprensione delle modalità di funzionamento dell'algoritmo. Come si è già osservato questo diviene sempre più complesso per tutti quei sistemi che si fondano su di una AI non deterministica, tra quelli oggi più promettenti, che processano una mole di variabili sempre più consistente.

A fronte di questa "impossibilità" tecnica si sono allora avanzate alcune proposte dirette a rendere più trasparente e poter così più agevolmente controllare il funzionamento dei sistemi. Tra queste, per esempio, si propone la predisposizione di "*check point*" a cui poter accedere per visionare e ispezionare più facilmente le operazioni compiute dalla macchina.

La proposta si dimostra interessante, dal momento che permetterebbe di velocizzare le operazioni di controllo; in questi "punti" sarebbero infatti registrate informazioni sul sistema, e su come esso abbia fin lì operato, e ciò permetterebbe di far fronte alle criticità legate all'estensione dei collegamenti, guidando le operazioni di verifica degli operatori. Nella pratica, però, questa proposta incontra alcune difficoltà operative.

[573] La decifrazione del codice sorgente è, infatti, complessa anche per gli esperti; esso si limita a rilevare il metodo di apprendimento automatico utilizzato dal sistema, nulla dice invece in merito alla regola di decisione basata sui dati, in quanto essa viene a emergere automaticamente dai dati sottoposti ad analisi. Si v. PELLECCHIA, *op. cit.*, 1211 ss.
[574] PELLECCHIA, *ibidem*.

Similmente a quanto si vorrebbe implementare all'interno dell'algoritmo, sul mercato attuale sono già presenti degli *explanatory tools* a disposizione degli utilizzatori. Questi, tuttavia, si dimostrano inidonei all'identificazione di una vera e propria spiegazione degli *output* elaborati, essendo in realtà progettati per verificare l'efficienza dei sistemi e, *in primis*, l'affidabilità delle valutazioni predittive[575].

A questa considerazione se ne aggiungono altre di natura tecnica. La presenza di *check point*, il cui numero dovrà necessariamente variare in ragione dell'estensione e della complessità degli algoritmi, comporta un inevitabile rallentamento dell'intero processo. Per molti versi ciò potrebbe rivelarsi un buon compromesso per permettere una maggiore trasparenza, tuttavia il problema sorgerebbe per tutte quelle applicazioni che invece necessitano di tempi di risposta, se non immediati, molto veloci.

Si pensi alle auto a guida autonoma; per permetterne il funzionamento le vetture sono munite di differenti tecnologie e algoritmi, tra cui reti neurali artificiali, che interagiscono tra loro. Nella pratica, i sistemi compiono scelte e analizzano dati continuamente, e dunque dovrebbero provvedere a memorizzare molto frequentemente le informazioni nei *check point*, così, mano a mano, rallentando inevitabilmente il sistema. Nel settore *automotive* questa modalità potrebbe aumentare il rischio di incidenti; nell'esperienza di guida è necessario avere tempi di reazione molto ridotti e ciò vale anche per le auto a guida autonoma, chiamate a processare le innumerevoli variabili a cui sono esposte durante il movimento. Appare chiaro che un ritardo di reazione, pur se breve, potrebbe comportare il verificarsi di eventi dannosi anche gravi.

A ciò si aggiunga come il sistema di *check point* richiederebbe un certo spazio di stoccaggio delle informazioni per tutti quegli algoritmi adattivi, che dunque modificano la consistenza della struttura "imparando" di volta in volta, necessario per poter risalire agli specifici dati relativi all'evento in analisi. Se il sistema subisse un arresto al momento del verificarsi di un evento inatteso si potrebbe più facilmente risalire ai dati richiesti per l'analisi, tuttavia spesso ciò non accade e il sistema continua a operare e così a "imparare" dalla propria esperienza.

[575] MESSINETTI, *La tutela della persona umana* versus *l'intelligenza artificiale*, cit., 872 ss.; KROLL *et al*., *Accountable Algorithms* (2017) *Univeristy of Pennsylvania Law Review* 633 ss.; LIPTON, *The mythos of model interpretability*, 2017, consultabile all'indirizzo: *arxiv.org/pdf/1606.03490.pdf* (ultimo accesso 5 febbraio 2021).

Per poter risalire nel tempo ai dati di uno specifico momento "t" in cui si è verificato un danno, sarebbe allora necessario che la macchina archiviasse un salvataggio completo delle condizioni di sistema ogni volta che viene generato un *output*, non potendo sempre stabilirsi nell'immediato se quella determinata soluzione sia errata o discriminatoria.

Questa sembra una questione di poco conto; per meglio comprendere basta tuttavia pensare al funzionamento delle applicazioni di uso quotidiano, quale per esempio il pc. Il personal computer possiede una memoria entro cui vengono registrate le informazioni; si tratta di uno spazio finito e ciò comporta che le informazioni rutinarie vadano a riscrivere le precedenti. Potendo avere a disposizione dello spazio nell'hardware è possibile per l'utente salvare anche specifiche informazioni, fino a quando lo spazio non si esaurisce. Per quanto riguarda le applicazioni *data driven* una prima difficoltà risiede proprio nell'assenza di spazio fisico per poter salvare le informazioni; si pensi agli IoT, quali i *wearable things*, che non posseggono grandi spazi di memoria direttamente presenti nei dispositivi. Per ovviare a detto problema si è pensato di sfruttare i *Cloud*, dei server che permettono di allocare la memoria esternamente. É tuttavia bene ricordare che pur essendo dei servizi online anch'essi necessitano di uno spazio fisico in cui conservare i dati; ciò comporta, tra gli altri, anche un impatto ambientale importante, avendo un consumo di energie crescente in proporzione alla consistenza, problema questo che interessa anche i c.d. super-computer.

Si può dunque ben immaginare come un sistema del genere possa nel tempo divenire particolarmente farraginoso, per non parlare di possibili guasti ai server esterni o attacchi hacker[576]. Inoltre, si ricorda che un sistema, quale una sorta di scatola nera (analogamente a quella presente negli aerei), può essere utile nel caso in cui questo interrompa il proprio funzionamento, potendo così recuperare le informazioni che hanno provocato quella risposta. Poco utile sarebbe, invece, per quei sistemi che pur errando nelle risposte continuino a funzionare e dove queste ultime fungono anche da impulsi alla modifica del sistema stesso. In questi casi appare complesso poter andare a ritroso nella verifica di quale composizione di variabili abbia comportato un risultato errato o

[576] È per questo motivo che i luoghi ove sono posizionati i server non vengono resi pubblici.

discriminatorio, essendo nel frattempo mutata l'architettura del sistema che l'ha generato.

È bene notare, infine, come i sistemi formali (tra cui vanno annoverati i sistemi informatici) sono governati dal teorema dell'incompletezza di Gödel, secondo cui vi saranno sempre delle condizioni che portano la macchina a sbagliare[577], non potendo logicamente testare ogni possibile variabile e come essa vada a influenzare l'intero sistema. A ciò deve aggiungersi, come visto poc'anzi, come ad algoritmi sempre più complessi si accompagni una sempre maggiore difficoltà di verifica circa il singolo *output* prodotto. A fronte di queste considerazioni si è così proposto di limitare lo sviluppo della tecnologia nella direzione di quei sistemi che permettano di verificare le operazioni compiute. Parte della comunità scientifica ritiene che sia necessario giungere a un compromesso tra accuratezza e spiegabilità dei risultati, diminuendo la complessità degli algoritmi in favore di una maggiore trasparenza degli stessi[578]. Ciò sarebbe possibile grazie all'utilizzo di un numero più esiguo di variabili processate, tali dunque da poter essere controllate più facilmente, oltre che grazie alla progettazione di una architettura meno complessa, per esempio in una rete neurale ciò comporterebbe una limitazione del numero di *layer*.

Dall'altro lato questo tipo di limitazioni renderebbe i risultati elaborati dalle macchine meno affidabili, circostanza questa legata inevitabilmente alle stesse modalità di funzionamento degli algoritmi[579]; ridurre le variabili e la complessità della struttura non permette alla macchina di migliorare le proprie "capacità", limitandone l'esperienza[580].

---

[577] Il lavoro di Gödel, pur riguardando le proposizioni cosiddette indecidibili, ha portata generale e può essere esteso a tutti i sistemi formali (cioè sistemi finiti, quali sono ad oggi quelli informatici). Gödel dimostrò che è sempre possibile aggiungere assiomi all'interno di un sistema formale al fine di poter verificare la verità di una proposizione indecidibile. Tuttavia in questo sistema, arricchito dai nuovi assiomi aggiunti, esisterebbero comunque nuove proposizioni indecidibili. Il risultato raggiunto dal logico austriaco è generale, dunque è possibile affermare che per qualsiasi programma (sistema formale) esistono sempre affermazioni false che verranno interpretate come vere. Dunque ogni programma avrà sempre e inevitabilmente infinite istruzioni che non ne permettono il corretto funzionamento. Il teorema trova particolare espressione anche nell'ambito della sicurezza dei sistemi digitali; quando un programma riceve in ingresso delle informazioni non decidibili non è possibile prevedere il risultato dell'elaborazione, rendendo il sistema vulnerabile, in quanto soggetto a ogni tipo di potenziale incidente di sicurezza. In argomento D'ACQUISTO, NALDI, *op. cit.*, 180 ss.

[578] TABARRINI, *ibidem*; LISBOA, *ibidem*; VELLIDO, MARTIN-GUERRERO, LISBOA, *op. cit.*, 165 ss.

[579] Si rimanda alle considerazioni ivi svolte al capitolo 1.

[580] Sul punto Comandè evidenzia come la soluzione di imporre restrizioni generali abbia quale contraltare la limitazione di possibili soluzioni trovate dall'AI, diminuendone conseguentemente il valore intrinseco. Inoltre detta soluzione non si dimostra nemmeno risolutiva in quanto mitigare tutti i risultati indesiderati è

Per parte dei commentatori, come visto, ciò rappresenterebbe un giusto compromesso, non potendo rischiare di avere sistemi più accurati a cui tuttavia si finirebbe per fare un affidamento cieco, non potendo arrivare a una piena comprensione del loro operato[581].

La necessità di un maggiore controllo e di una effettiva trasparenza è diffusamente sentita, come dimostra il programma elaborato dall'agenzia DARPA dal titolo "*Explainable Artificial Intelligence*"[582]. L'obiettivo del progetto è appunto quello di incoraggiare la diffusione di applicazioni di Intelligenza Artificiale spiegabili, pur mantenendo un alto livello di accuratezza nelle *performance*; ciò premetterebbe al contempo di accrescere la fiducia degli utenti nell'utilizzo di tali applicazioni e dunque di aumentarne la diffusione nei diversi settori.

Questa proposta, più che la precedente, permetterebbe, infatti, di ovviare alle criticità legate alla fattibilità tecnica di una spiegazione dei risultati algoritmici, tuttavia non sembra ad oggi essere stata universalmente accolta dalla comunità scientifica[583]. Si assiste, piuttosto, allo sviluppo di sistemi di AI sempre più complessi, chiamati a gestire un numero sempre maggiore di variabili, senza che ne venga fatta alcuna selezione quantitativa. Sembra dunque trovare maggiore spazio la ricerca di una affidabilità dei risultati più elevata a discapito della trasparenza, ritenendo dunque i vantaggi di un impiego massiccio della tecnologia soverchiare i rischi derivanti dalla loro opacità.

Quale via mediana tra le due posizioni, attualmente una particolare attenzione viene prestata alle tecniche di *reverse engineering* aventi lo scopo di aprire la "scatola nera". Se non si intende rinunciare all'accuratezza delle macchine è allora necessario accrescere gli investimenti in quella branca di studi diretta a rivelarne, a posteriori, i meccanismi di funzionamento[584]. Diverse sono le tecniche usate[585], tra cui per esempio

---

semplicemente impossibile a causa della natura imprevedibile dei dati, spesso non strutturati ed eterogenei. V. COMANDÈ, *Intelligenza Artificiale e responsabilità tra* liability *e* accountability, cit., 171.

[581] TABARRINI, *op. cit.*, 593 s.

[582] Il progetto è consultabile all'indirizzo ufficiale: *www.darpa.mil/program/explainable-artificial-intelligence* (ultimo accesso 3 maggio 2021).

[583] In argomento si v. Burrell, il quale sottolinea come non sarebbe utile sviluppare unicamente algoritmi la cui logica sia completamente comprensibile. Difatti i modelli di *machine learning* che presentano qualche utilità, in termini di accuratezza delle classificazioni, possiedono un livello di complessità inevitabilmente alto; ciò perché si fondano sull'analisi dei Big Data, permettendo alla logica decisionale interna di cambiare mano a mano che apprende dai dati di addestramento. Limitare lo sviluppo di alcune tipologie di algoritmi ne pregiudicherebbe inevitabilmente l'utilizzo in quei settori dove si richiede una percentuale di accuratezza molto alta, quale può essere quello medico. BURRELL, *op. cit.*, 5.

[584] V. GOODMAN, FLAXMAN, *ibidem*.

quelle che si fondano su di un test controfattuale[586]. In quest'ultimo caso ai sistemi vengono proposte diverse variabili in modo da verificarne gli esiti e comprendere quale possa aver portato a un risultato non voluto.

Questa metodologia si avvicina alle valutazioni che vengono compiute al fine di trovare la causa di un determinato evento. Tuttavia è bene notare che tecniche di tal fatta difficilmente potranno portare a un'effettiva spiegazione, ciò in quanto gli *output* sono elaborati quale esito di una correlazione tra un numero molto alto di variabili, ma soprattutto da come essere interagiscono; elemento questo non spiegabile da un approccio che invece si fonda su di una analisi delle variabili singolarmente considerate[587].

---

[585] Lo stesso concetto di interpretabilità possiede diverse sfaccettature. Vi sono differenti approcci che possono essere applicati in modo complementare, ma non c'è un generale accordo sul modo in cui sia possibile rendere un modello predittivo interpretabile. Tra le maggiori criticità vi è, infatti, anche quella di rendere il modello algoritmico utilizzato generalizzabile; elemento questo, oltre che necessario nel metodo scientifico, in grado di aumentare l'affidabilità dei risultati operati dalla macchina e di migliorare la comprensibilità dello stesso. In argomento si rimanda a Lisboa il quale evidenzia le difficoltà in merito alla spiegabilità degli algoritmi anche nella prospettiva dei test di V&V (*verification and validation*) che normalmente vengono compiuti prima di immettere un prodotto sul mercato. V. LISBOA, *ibidem*. Per una panoramica sui metodi utilizzabili per rendere conoscibili, e dunque anche spiegabili, i risultati ottenuti da una AI, si rimanda a VELLIDO, MARTIN-GUERRERO, LISBOA, *op. cit.*, 163 ss.
In tema di auto *driverless*, dove la necessità di controllo in merito al corretto funzionamento del sistema sono particolarmente sentite, si rimanda a un interessante saggio in cui vengono riportati una serie di possibili test diretti a individuare gli eventuali errori compiuti dalla macchina. Cfr. YUCHI *et al.*, *DeepTest: Automated testing of Deep-Neural-Network-drive Autonomous Cars*, in *40th International Conference on Software Engineering*, May 27-June 3, New York, 2018, 12, consultabile all'indirizzo: *dl.acm.org/doi/pdf/10.1145/3180155.3180220* (ultimo accesso 15 maggio 2020). In tema di algoritmi di *reverse engineering*, diretti a rendere il processo maggiormente intellegibile, si rimanda a GOODMAN, FLAXMAN, *ibidem*.

[586] In argomento TABARRINI, *op. cit.*, 575 ss., la quale riporta tre metodi di spiegazione dei sistemi di *machine learning* che si fondano proprio su di una logica controfattuale: LOCO (*Leave One Column Out*), PI (*Premutation impact*) e LIME (*Local interpretable Model-Agnostic Explanations*). Tutti questi software permettono un'analisi esterna del processo decisionale; alcuni utilizzano anche dati reali per testare il modello e individuare le correlazioni *input-output*. È tuttavia necessario sottolineare come lo stesso funzionamento dei metodi citati rimane sempre indifferente alle particolarità del caso concreto, fondandosi su dati ipotetici creati appositamente per spiegare l'esito della decisione presa dalla macchina. Si pensi per esempio al funzionamento del software LOCO, questo premette di giungere a tre differenti tipi di spiegazione legate al soggetto interessato. Può, infatti, essere fornita all'utente una spiegazione per associazione, cioè diretta a indicare i fatti rilevanti che hanno portato alla specifica decisione attraverso la divulgazione delle caratteristiche che gli utenti condividono con altre persone che hanno ottenuto un esito analogo. È possibile ottenere anche una spiegazione, più legata alla logica seguita dalla macchina, nella quale si esplicita il tasso di errore dell'algoritmo indicando la percentuale di persone appartenenti alla stessa categoria che hanno ottenuto un risultato errato. Infine, è possibile avvalersi di un approccio casistico che fornirebbe una spiegazione consistente nella descrizione dei dati, utilizzati per programmare l'algoritmo, che più si avvicinano alla situazione specifica dell'interessato. In argomento di particolare interesse anche lo scritto di WACHTER, MITTELSTADT, RUSSELL, *Counterfactual explanations without opening the black box: automated decisions and the GDPR* (2018) 31 *Harvard Journal of Law & Technology* 842 ss., e, in relazione alla *compliance* con il GDPR, spec. 862 ss.

[587] Cfr. TABARRINI, *op. cit.*, 575 ss.

Strategie di *auditing* si dimostrano dunque non pienamente adeguate allo scopo, a prescindere dall'uso di logiche controfattuali, in ragione della generale impossibilità di garantire con un controllo a posteriori la funzionalità di un sistema, essendo il processo intrinsecamente incompleto[588]. Inoltre è necessario sottolineare come le operazioni di *auditing* hanno lo scopo di rivelare se siano state seguite le procedure appropriate e se il sistema sia stato eventualmente manomesso; ciò non permette di individuare con certezza le cause di eventuali cambiamenti, né consente di stabilire il perché essi siano stati considerati o meno significativi ai fini della decisione[589].

Ai rilievi di natura tecnica si accompagna, infine, una considerazione in merito anche all'effettiva possibilità di comprensione da parte dell'uomo. Il paradigma attraverso cui opera la macchina non risponde più al principio di causalità ma a quello di correlazione. É dunque lo stesso modo di concepire gli eventi a cambiare. La tendenza degli esseri umani alla ricerca di una logica causale sarebbe così di ostacolo a una effettiva comprensione delle scelte algoritmiche. Se anche si riuscisse a raggiungere una spiegazione certa di come la macchina sia arrivata a una determinata conclusione, a fronte dell'interazione di un numero elevatissimo di variabili, sarebbe egualmente complesso per un essere umano comprenderne effettivamente la *ratio*; si tratta di una vera incomunicabilità tra uomo e macchina.

Questo tipo di opacità è quella indicata da Burrell[590] come opacità intrinseca, intendendosi con questa espressione l'impossibilità di tradurre in una forma intellegibile agli esseri umani, compresi i programmatori, il complesso processo decisionale algoritmico[591]. Ne discende allora una particolare difficoltà per i titolari dei trattamenti a porre in essere sia un'analisi *ex ante* delle prevedibili conseguenze che possano

---

[588] Uno dei sette principi del *software testing* è proprio: "*Exhaustive testing is not possible*". Non sarà, infatti, mai possibile testare tutto il conoscibile; a logica nel reale le variabili sono infinite e dunque un test, per quanto esteso, si dimostrerà sempre a campione. Ne discende allora come non sia possibile garantire la funzionalità e l'affidabilità di un sistema nella totalità dei casi, ma solo per quelli che sono stati oggetto di test. Cfr. MEYER, *Seven Principles of Software Testing* (2008) 8 *IEEE transactions on Computers* 99 ss.

[589] PELLECCHIA, *ibidem*.

[590] Più specificamente Burrell sostiene che: «[…] *three distinct forms of opacity include: (1) opacity as intentional corporate or institutional self-protection and concealment and, along with it, the possibility for knowing deception; (2) opacity stemming from the current state of affairs where writing (and reading) code is a specialist skill and; (3) an opacity that stems from the mismatch between mathematical optimization in high-dimensionality characteristic of machine learning and the demands of human-scale reasoning and styles of semantic interpretation*». V. BURRELL, *op. cit.*, 1 s.

[591] TABARRINI, *op. cit.*, 575 ss.

discendere dall'impiego di dette tecniche, che, soprattutto, il confezionamento *ex post* di una spiegazione in merito alla specifica decisione presa dalla macchina.

Dalle considerazioni sopra svolte emerge con chiarezza come le proposte dirette all'implementazione di strumenti aventi lo scopo di aprire la "scatola nera", pur essendo pregevoli, si dimostrano nella pratica limitate. Certamente la scelta di aumentare gli investimenti per la progettazione di strumenti di *auditing* delle macchine, oltre che l'invito alla creazione di algoritmi *ab origine* spiegabili, riveste un ruolo importante nella costruzione di un ecosistema digitale più sicuro e diretto a garantire i diritti e le libertà fondamentali degli utenti. Attualmente, tuttavia, le soluzioni così proposte non sembrano ancora di per sé sufficienti a rispondere all'obiettivo.

Al fine di permettere una maggiore tutela degli interessati, a fronte della prassi di utilizzo di questi sistemi opachi, pare necessario prestare attenzione anche agli strumenti, oggi vigenti, che ascrivono la responsabilità in caso di danno a determinati soggetti. Infatti se lo sfruttamento sempre più pervasivo degli algoritmi sembra essere incoraggiato in ragione dei vantaggi che veicola, del pari non sembra corretto che i danni, che dall'uso di queste tecniche possono discendere, rimangano in capo agli utenti finali. La scelta operata dalle Istituzioni europee è allora ricaduta, per quanto qui interessa, sulla figura del titolare (e in alcuni casi del responsabile) del trattamento che sarà chiamato a rispondere per i danni da esso generati. Quest'ultimo viene dunque ritenuto il soggetto nella miglior posizione di sopportare il danno, secondo una logica per cui chi trae benefici da una determinata attività ne sopporta gli oneri (*cuius commoda eius et incommoda*). É opportuno allora verificare se tale scelta sia idonea a tutelare effettivamente gli utenti e rispondere efficacemente all'esigenza di ridurre gli eventi di danno, incentivando il soggetto ritenuto responsabile a porre in essere strategie di contenimento e riduzione dei rischi.

5. Le previsioni del GDPR a tutela degli interessati: l'*accountability*, la valutazione di impatto e la responsabilità per illecito trattamento dei dati personali

Alla luce delle considerazioni fin qui esposte appare evidente come i trattamenti operati mediante tecnologie *data driven* comportino particolari rischi in relazione alla protezione dei dati personali degli interessati. Alle difficoltà di applicazione dei principi

generali sanciti dal GDPR, legati a una parziale incompatibilità con il funzionamento stesso dei sistemi algoritmici, si accompagna una sostanziale inefficacia dello strumento del consenso quale base di legittimità del trattamento[592]. La mancanza di consapevolezza che discende dalla complessità tecnica delle applicazioni che trattano i dati non permette di ritenere l'istituto in parola nemmeno quale espressione di un'assunzione di rischio, finendo piuttosto una tale ricostruzione per acuire ulteriormente le asimmetrie tra titolari e interessati. Come visto, infatti, se in linea di principio si può pensare che l'utente possa liberamente sottrarsi al rischio, nell'attuale contesto sociale, ove la tecnologia e le sue comodità sono oramai di uso quotidiano, sarebbe difficile ipotizzare una totale disconnessione dell'interessato, tale da poterlo tenere in qualche modo al riparo dal rischio di danni derivanti dal trattamento dei propri dati.

A questi rilievi di carattere generale fanno eco specifiche criticità emerse in relazione alla sottoposizione degli utenti a decisioni automatizzate[593]. Sul punto si assiste attualmente a un acceso dibattito circa la presenza o meno di un diritto "alla spiegazione". Sebbene tra le posizioni esposte sia condivisibile quella che rinviene nel dettato normativo la presenza di un diritto alla leggibilità dell'algoritmo, che dunque sarebbe diretto a permetterne la comprensibilità per gli utilizzatori finali, pare tuttavia necessario sottolineare come anche questa interpretazione non sembra essere pienamente applicabile alle differenti modalità di trattamenti, quanto meno per quelli che si fondano sull'utilizzo di algoritmi di *deep learning*[594].

---

[592] V. FAINI, *Dati, algoritmi e Regolamento europeo 2016/679*, in *Regolare la tecnologia: il Reg. UE n. 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di MANTELERO, POLETTI, Pisa, 2018, 343 s. In relazione al mutamento di prospettiva derivante dall'avvento dei Big Data e dell'Intelligenza Artificiale, si v. MANTELERO, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di* Artificial Intelligence, *ivi*, 293 ss. In particolare interessanti le considerazioni di SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, *ivi*, 163. L'Autore ricorda come l'architettura del Regolamento, come già a suo tempo la Direttiva, rimanga basata sull'informativa, nonché sulla manifestazione del consenso. Tuttavia il legislatore non pare aver tenuto in considerazione come la fase dell'informativa il più delle volte si colora di un'asimmetria tra la capacità di cognizione del soggetto i cui dati si riferiscono e chi, invece, procede alla raccolta. Questa condizione di fatto svuota la tutela che il principio del consenso informato vorrebbe apprestare, finendo con l'essere solamente apparente ma privo di sostanza. L'Autore ricorda le parole di Guido Calabresi che già nel 1997 evidenziava che solo in apparenza il consenso informato si dimostra essere una regola efficiente. Da un'analisi dei casi concreti in cui esso viene applicato, come in materia dei trattamenti sanitari, si dimostra non essere un modello affidabile, realizzando spesso una tutela meramente apparente.

[593] Si v. *supra* §1 del presente capitolo.

[594] Per un approfondimento sul dibattito in tema di diritto "alla spiegazione" si rimanda *supra* al §4 del presente capitolo.

La comprensione della logica sottesa a una specifica decisione presa dal sistema di AI nei confronti di un individuo, come può essere per esempio la decisione di concedere un prestito o, come nel caso COMPAS, la classificazione di un soggetto come ad alto rischio di recidiva[595], è evidentemente il presupposto necessario per rendere effettive le garanzie concesse ai singoli dalla normativa sulla *data protection*, tra cui in particolare il diritto di poter contestare la decisione. Tuttavia, di ostacolo si dimostra proprio l'opacità intrinseca dei sistemi algoritmici, in quanto appare difficile contestare compiutamente una decisione di cui non si conosce la *ratio*. Ne discende allora una mancanza di strumenti effettivi a tutela degli interessati, a fronte di un concreto rischio di decisioni di fatto discriminatorie o errate nei confronti un numero potenzialmente molto esteso di soggetti, difficilmente contestabili.

Se è vero che non è possibile limitare il progresso scientifico-tecnologico, è allora necessario prestare attenzione all'intero trattamento nel suo complesso, dalla fase di progettazione degli algoritmi alla responsabilizzazione dei titolari, passando per una sensibilizzazione di tutti gli attori coinvolti. In questa prospettiva sarebbe auspicabile la predisposizione di strumenti che permettano di diminuire a priori il rischio di eventi avversi e *output* discriminatori, abbracciando una filosofia che si fonda sul principio di precauzione[596]. Ciò permetterebbe di non ostacolare eccessivamente il funzionamento del mercato e al contempo permetterebbe di garantire adeguate forme di tutela per gli interessati, mediante una diminuzione dei rischi di accesso e divulgazione dei dati non autorizzati, oltre che di loro perdita o distruzione, nell'attuale ambiente tecnologico[597].

In questa chiave va letto il principio di *accountability*[598], che informa l'intero *corpus* normativo[599] costituendo il fondamento dell'approccio fondato sul rischio, che

[595] Per alcuni esempi di decisioni automatizzate, oltre che per un approfondimento in merito al famoso caso COMPAS si rimanda *supra* §1 del presente capitolo.

[596] TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019, 40 ss.; GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, Napoli, 2018, 81 ss.; ID., *Responsabilità e risarcimento nel trattamento dei dati personali*, in *I dati personali nel diritto europeo*, cit., 1031 ss.; SIANO, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA, BELISARIO, I, Milano, 2018, *sub* art. 24, 238 ss.; GRECO, *I ruoli: titolare e responsabile*, in *Il nuovo Regolamento europeo sulla privacy*, cit., 254.

[597] Per un approfondimento in merito alle figure del titolare e del responsabile del trattamento si rimanda a FARACE, *Il titolare e il responsabile del trattamento*, in *I dati personali nel diritto europeo*, cit., 731 ss.

[598] Il concetto di *accountability* non è nuovo, un primo riconoscimento è rinvenibile nelle linee guida dell'OECD del 1980 a mente delle quali «*a data controller should be accountable for complying with measures which give effect to the material principles stated above*». Art. 14 "Accountable principle", OECD, *Guidelines on the protection of privacy and transborder flows of personal data*, entrate in vigore il 23 settembre 1980, consultabili all'indirizzo: *www.garanteprivacy.it/documents/10160/10704/1799578*

rappresenta la maggiore novità rispetto a quanto dettato dalla previgente Direttiva madre[600]. Quest'ultima, come è noto, era difatti incentrata prevalentemente sui diritti degli interessati, a differenza del Regolamento che invece sposta l'attenzione sul titolare e sugli obblighi su di esso gravanti.

Il principio in parola, comunemente tradotto come "responsabilizzazione"[601], riconosce dunque il titolare quale soggetto deputato a valutare le misure tecniche e organizzative più idonee in relazione alla natura dei dati, all'oggetto e alle finalità del trattamento; coloro che gestiscono i trattamenti sono chiamati non solo ad adottare tutti gli strumenti necessari a garantire il rispetto delle norme del Regolamento, ma su di questi grava anche un obbligo di provarne l'effettiva ed efficace adozione in misura adeguata al rischio creato.

La prova di aver posto in essere tutte le misure necessarie al rispetto del complesso delle disposizioni regolamentari non è semplice, dovendo il titolare dimostrarne anche

---

(ultimo accesso 9 giugno 2021). Queste sono poi state modificate nel 2013, dando un'effettiva consacrazione al principio, rendendolo principio fondamentale per la realizzazione pratica e internazionalmente condivisa della protezione della privacy.

[599] «*1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.*

2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento». Art. 24, reg. UE n. 679/2016. Oltre che all'art. 24, considerata la norma principale sull'*accountabilit*y, è possibile rinvenire alcuni espliciti richiami al principio nel Considerando n. 14 e negli artt. 5, comma 2°, e 32, reg. UE n. 679/2016.

[600] GAMBINO, BOMPREZZI, Blockchain *e* protezione *dei dati personali*, in *Dir. inform*., 2019, 619 ss.; SIANO, *op. cit.*, 236 ss.; GIANNONE CODIGLIONE, Riskbased approach *e trattamento dei dati personali*, in *La nuova disciplina europea della privacy*, a cura di SICA, D'ANTONIO e RICCIO, Padova, 2016, 71 ss.; FINOCCHIARO, *Privacy e protezione dei dati personali*, Torino, 2012, 289 ss.

[601] Il termine, che deriva dalla tradizione anglosassone, può essere tradotto in modi differenti tra cui "principio di rendicontazione" o di "responsabilità", componendosi nell'obbligo non solamente di conformarsi ai dettati del regolamento (responsabilità), ma anche di darne dimostrazione. Si v. FINOCCHIARO, *Il principio di* accountability, cit., 2778 ss.; ID., *Riflessioni su intelligenza artificiale e protezione dei dati personali*, cit., 246 s.; SIANO, *op. cit.*, 237. Sul punto è intervenuto anche il Gruppo di Lavoro art. 29 che, esaminando le questioni relative all'applicazione del principio in parola, nel parere n. 3/2010 ha evidenziato come il termine, che può essere tradotto in molti modi diversi, è espressione di un meccanismo che si fonda su due distinti livelli. Il primo livello è costituito dall'obbligo, vincolante per tutti i titolari, di attuare misure e procedure per la tutela dei dati personali, nel rispetto delle previsioni regolamentari, e di conservazione delle relative prove. Il secondo livello, non obbligatorio, includerebbe l'adozione di sistemi di responsabilità volontari ed eccedenti le norme di legge minime, in relazione ai principi fondamentali di protezione dei dati, così da poter garantire una maggiore efficacia delle misure predisposte, in ragione delle caratteristiche specifiche nascenti dal singolo trattamento posto in essere. V. Gruppo di Lavoro art. 29, *Parere 3/2010 sul principio di responsabilità*, 2010, consultabile all'indirizzo: *www.garanteprivacy.it* (ultimo accesso 20 maggio 2021).

l'efficacia in relazione alle caratteristiche proprie dello specifico trattamento. Al fine allora di facilitare la prova richiesta sono stati introdotti all'interno del testo normativo degli strumenti (c.d. *accountability tools*) agli artt. 40-43 del GDPR, regolanti le certificazioni e i codici di condotta. Si tratta di strumenti di autoregolamentazione la cui adozione viene incoraggiata anche al fine di permettere la creazione di fiducia negli utenti finali che si trovano a essere soggetti a molteplici trattamenti. Questa spinta "gentile" all'adozione di detti strumenti permetterebbe inoltre alle aziende di giovare di un vantaggio competitivo sul mercato, qualora al rispetto dei parametri qualitativi prefissati si associ anche l'operatività di meccanismi reputazionali[602], come già accade con i prodotti a marchio CE.

Tornando alla lettura dell'articolo 24, emerge con chiarezza una portata applicativa molto ampia; la formulazione della norma non prevede infatti un elenco esaustivo delle misure ritenute adeguate o degli obblighi del titolare, ma prevede piuttosto per quest'ultimo un ruolo pro-attivo durante tutto l'arco del trattamento, fin dalle sue fasi inziali[603]. Il titolare è chiamato a porre in essere misure tecniche e organizzative, ciò in quanto è solo una visione integrata dell'intero trattamento a permettere una corretta individuazione dei rischi da esso nascenti e quali interventi siano necessari per implementare di conseguenza le necessarie misure di sicurezza.

Nella formulazione della disposizione si richiede, dunque, che le misure adottate per garantire la conformità al Regolamento siano "adeguate" al contesto e alle specifiche circostanze del trattamento. La valutazione di adeguatezza va evidentemente fatta *ex ante* e deve avere ad oggetto: la natura, l'ambito di applicazione, le finalità dei trattamenti, oltre che i rischi per i diritti e le libertà delle persone fisiche[604].

Questo tipo di approccio si fonda sulla concessione di una maggiore libertà al titolare, a cui si accompagna una sua maggiore responsabilizzazione. La scelta compiuta

---

[602] POLETTI, CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in *Privacy digitale*, a cura di TOSI, Milano, 2019, 379 s., i quali sottolineano come manchino nel testo disposizioni dirette a perpetrare un "*accountability with the public*". Difatti non sembra rivenirsi alcuna effettiva previsione in merito a forme di partecipazione dei portatori di interesse, sia nella fase di adozione che in quella del loro monitoraggio ed *enforcement*; elemento questo che avrebbe permesso un incremento dello stesso livello di fiducia degli utenti, grazie a un loro coinvolgimento (attraverso anche solo un'audizione di alcuni rappresentati di categorie).

[603] Si pensi ai principi di *privacy by design* e *by default* che il titolare è chiamato a implementare fin dalla fase di sviluppo e progettazione dei trattamenti. V. CAPPARELLI, nel *Codice della Disciplina Privacy*, diretto da BOLOGNINI e PELINO, Milano, 2019, *sub* art. 24, 202. Si veda anche il parere del Gruppo di Lavoro art. 29, Parere 3/2010, cit.

[604] SIANO, *op. cit.*, 240; CAPPARELLI, *op. cit.*, 201.

dal legislatore europeo permette così di modulare caso per caso l'attuazione delle disposizioni previste dal GDPR, le quali per potere essere realmente efficaci necessitano di una declinazione concreta in relazione allo specifico trattamento posto in essere[605].

Lo stesso Gruppo di Lavoro art. 29 sul punto evidenzia come lo scopo della disposizione in parola sia proprio quello di promuovere l'adozione di misure concrete, così trasformando i principi generali sanciti dal Regolamento in *policy* e procedure efficaci; queste infatti vengono definite direttamente dal titolare e parametrate alle specifiche esigenze nascenti dai diversi trattamenti, fermo restando il rispetto delle leggi e dei regolamenti applicabili[606].

Ne discende allora come l'*accountability* possa essere considerata quale metodo per formalizzare e proceduralizzare l'autonomia concessa al titolare. Secondo un approccio tipicamente di *common law*, detta previsione permette di creare una procedura che i soggetti che trattano i dati sono chiamati a definire e rispettare; viene infatti richiesta l'adozione non solamente di misure di sicurezza, ma anche la prova della loro adeguatezza durante tutto l'arco del trattamento, in un contesto di assoluta autonomia decisionale[607].

Per il tema che qui ci occupa, il principio in analisi dimostra di avere un ruolo chiave declinandosi secondo una prospettiva che permette una maggiore trasparenza dell'intera architettura di sistema; ciò permetterebbe anche di garantire una più efficace tutela dei diritti degli interessati. Appare evidente, infatti, che per poter essere *compliant* con il Regolamento il titolare dovrà necessariamente porre in essere una serie di misure di diversa natura; queste dovranno essere dirette a rendere l'intero trattamento adeguato a garantire la protezione dei dati personali degli utenti. Ne discende allora come tra di esse debbano essere evidentemente annoverati anche quegli strumenti diretti a rendere il processo di analisi dei dati maggiormente comprensibile e trasparente proprio per gli utilizzatori finali. È bene tuttavia precisare che da una tale lettura del principio non discende in ogni caso una completa accessibilità, da parte dell'interessato, alle informazioni circa l'attività di un dato titolare. Il principio deve dunque essere inteso eminentemente quale strumento di garanzia che il trattamento posto in essere, pur se

[605] FINOCCHIARO, *Il principio di* accountability, cit., 2779; ID., *Privacy e protezione dei dati personali*, cit., 290 s.; POLETTI, CAUSARANO, *op. cit.*, 378; CAPPARELLI, *ibidem*.
[606] Gruppo di Lavoro art. 29, Parere 3/2010, cit.
[607] V. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, cit., 15; ID., *Privacy e protezione dei dati personali*, cit., 291 ss.

declinato secondo le specifiche esigenze fattuali, sia conforme alla disciplina normativa; conformità che il titolare deve essere in grado di dimostrare in ogni momento[608].

Il principio di *accountability* si dimostra centrale anche per le riflessioni in merito al regime di responsabilità civile applicabile in caso di danni discendenti dall'uso di applicazioni di AI. Difatti, quale che sia la regola responsabilità civile prescelta per la materia, essa potrà essere potenziata dal complesso degli strumenti regolanti il generale sistema di governo dell'utilizzo dei dati, essendo l'AI – come visto – una tra le maggiori tecnologie *data driven*.

La previsione di un'architettura nel complesso rispettosa delle norme previste dal GDPR, rendendo la *compliance* normativa il livello base di tutela, obbliga i titolari a porre in essere trattamenti che siano diretti fin dal principio al rispetto dei diritti fondamentali degli interessati, oltre che ad adottare tutte le misure necessarie a diminuire l'entità dei rischi per questi ultimi. È evidente allora come il principio in parola si rifletta positivamente nella generale disciplina dell'Intelligenza Artificiale, rappresentando al contempo un utile strumento volto a rafforzare la regola di responsabilità civile prescelta, in una prospettiva di diminuzione dei rischi di danno[609].

Dunque il Regolamento, come visto, introduce una maggiore autodeterminazione nei confronti del titolare, al quale è accordata un'ampia facoltà di scelta, a cui si accompagna anche una maggiore responsabilità, dovendo egli dimostrare in ogni momento l'adeguatezza delle misure apprestate al singolo contesto di riferimento. L'obiettivo perseguito dal legislatore è evidentemente quello di rendere più efficienti gli strumenti posti a protezione dei dati avvicinandoli, nel momento di concreta

---

[608] V. LUCCHINI GUASTALLA, Privacy *e* data protection: *principi generali*, in *Privacy digitale*, cit., 83. Sul punto si veda POLETTI, CAUSARANO, *op. cit.*, 379, secondo i quali la circostanza che il GDPR abbia strettamente legato i codici di condotta e certificazioni al principio di *accountability*, dovrebbe spingere a una loro diffusa adozione. Questi ultimi, difatti, rilevano come strumenti di agevolazione probatoria sia del rispetto degli obblighi del titolare, sia delle garanzie richieste in capo al responsabile del trattamento.

[609] Comandè sul punto sottolinea come «la centralità del ruolo dei dati nel ciclo di vita delle AI suggerisce di prendere in attenta considerazione la collocazione del principio di *accountability* al centro delle regole di responsabilità […]. Resta il fatto che la qualità, la quantità dei dati, il contesto di raccolta, le modalità di selezione rimangono centrali nella definizione di molti profili anche nuovi della responsabilità civile connessa alle IA. Il processo di apprendimento di una IA, come anticipato, analizza i dati, identifica in essi modelli sulla base delle correlazioni rinvenute e successivamente crea nuovi modelli, in modo ricorsivo, che vengono poi applicati ai nuovi ed ai "vecchi" dati che hanno generato i modelli». COMANDÈ, *Intelligenza Artificiale e responsabilità tra* liability *e* accountability, cit., 171. In arg. si veda anche ID., *Responsabilità ed* accountability *nell'era dell'Intelligenza Artificiale*, in *Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi*, a cura di DI CIOMMO e TROIANO, Piacenza, 2018, 1008 ss.

applicazione, a chi si trova nella migliore posizione per valutarne, caso per caso, la maggiore o minore opportunità.

Alla stessa *ratio* risponde l'introduzione nel testo anche delle disposizioni regolanti la valutazione preventiva di impatto, che diviene un obbligo per quei trattamenti che in sostanza possono comportare i maggiori rischi per i diritti e le libertà degli interessati.

5.1 La valutazione preventiva d'impatto

Oltre alle previsioni di una maggiore responsabilizzazione nei confronti del titolare del trattamento, di portata incisiva si dimostra la previsione dell'obbligo di una "valutazione di impatto", indicato all'art. 35 GDPR[610]. La disposizione prevede che qualora un trattamento possa comporta dei "rischi elevati" per i diritti e le libertà degli interessati, il titolare sia chiamato a svolgere detta valutazione preventiva.

La previsione di un'analisi dei rischi evidentemente risponde a una logica precauzionale, che, come visto, risulta pervadere tutto il dettato normativo[611]. Difatti il

---

[610] «*1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.*
2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. […]». Art. 35, reg. UE n. 679/2016.

[611] L'approccio che informa l'intero dettato normativo sembra fondato sul rischio che il trattamento dati genera nei confronti degli interessati. Vengono, infatti, previste misure e strumenti idonei a valutarne l'entità e diminuirne l'incidenza, graduando gli interventi a seconda che il trattamento stesso comporti rischi elevati per le persone fisiche. Sulla scorta di tali considerazioni vanno lette anche le disposizioni in merito alla previsione delle valutazioni preventive di impatto, sebbene queste abbiano rispetto alla previgente disciplina un carattere maggiormente flessibile. In argomento si rimanda a MANTELERO, *La gestione del rischio*, in *La protezione dei dati personali in Italia*, cit., 485 ss.; ID., *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in *Il nuovo regolamento europeo sulla privacy*, cit., 298 ss.; PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 64 ss.; TORINO, *La valutazione di impatto* (Data Protection Impact Assessment), in *I dati personali nel diritto europeo*, cit., 855 ss.; PIERUCCI, *op. cit.*, 445 ss.; FAINI, *op. cit.*, 337 ss.

legislatore, prendendo atto della dimensione che attualmente ricopre il fenomeno della circolazione dei dati e del loro trattamento mediante tecnologie *data driven*, nella consapevolezza dell'utilità economica e sociale che il progresso tecnologico può veicolare, persegue una strategia di limitazione del rischio prevedendo obblighi parametrati alla sua maggiore o minore intensità.

Solo ai rischi considerati elevati segue l'obbligo di effettuare una valutazione di impatto, nella quale andranno indicate le modalità di svolgimento del trattamento, ivi comprese la base giuridica di legittimità e le finalità perseguite, ma anche le misure che il titolare intende apprestare per diminuire le possibili esternalità negative per gli utenti[612].

Queste previsioni fanno emergere alcune considerazioni. Rimane incerta sia la nozione generale di "rischio" che di "alto rischio", non prevedendo il testo una specifica definizione di cosa debba intendersi con detti termini[613]. Sebbene in alcuni casi, elencati

[612] Il procedimento si suddivide in differenti fasi. Viene fatta un'iniziale e preliminare mappatura dei dati al fine di individuare le aree di rischio. A questa operazione segue la stima dell'entità e della gravità dei rischi così individuati. Solo successivamente verrà compiuta la vera e propria fase di valutazione, così come indentificata dal Regolamento, nella quale sono individuate le misure atte a ridurre o neutralizzare il rischio, o modificare l'intero processo in modo che esso sia *privacy-orientated* secondo il modello di *data protection by design*. In questa fase, dunque, il titolare è tenuto a compiere un'attenta opera di bilanciamento degli interessi in gioco; ciò in quanto essa comporta un'indagine in merito ai rischi per i diritti e le libertà delle persone che, tuttavia, va fatta congiuntamente alla disamina in punto di necessità e proporzionalità nel trattamento dei dati. Cfr. D'ACQUISTO, NALDI, *op. cit.*, 30 ss.; MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, in *Persona e mercato dei dati*, cit., 289; TORINO, *op. cit.*, 857 s.; MANTELERO, *La gestione del rischio*, cit., 504 ss.; ID., *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, cit., 307 ss.; PELLECCHIA, *op. cit.*, 1222 ss.; TARULLO, *La gestione del rischio nel trattamento dei dati personali*, in *La nuova "privacy europea"*, cit., 125 ss.; PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, *ibidem*.

[613] Una prima indicazione viene data nel Considerando n. 77, reg. UE n. 679/2016, che indica una serie di ordini e strumenti che permettono di individuare il rischio connesso al trattamento, la sua valutazione in temine di origine, natura, portabilità e gravità e l'individuazione delle migliori prassi per attenuare il rischio. Sul punto ha avuto modo di esprimenti anche il Gruppo di Lavoro art. 29, il quale, nel 2017, ha promulgato delle specifiche linee guida, poi adottate e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 e a cui rimanda anche la nostra Autorità Garante della privacy, che hanno individuato nove criteri di identificazione dei trattamenti rischiosi. Nello specifico un trattamento può presentare un rischio elevato qualora comporti: 1. valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di «*aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*»; 2. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone; 3. monitoraggio sistematico degli interessati; 4. dati sensibili o dati aventi carattere altamente personale; 5. trattamento di dati su larga scala; 6. creazione di corrispondenze o combinazione di insiemi di dati; 7. dati relativi a interessati vulnerabili; 8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative; 9. quando il trattamento in sé «*impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto*». Si v. Gruppo di Lavoro art. 29, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del Regolamento (UE) 2016/679*, 2017 (modificate il 4 ottobre 2017),

all'art. 35, la valutazione in merito all'elevata rischiosità venga già compiuta dal legislatore[614], questa generalmente rimane accordata all'autonomia del titolare.

Una previsione di tal fatta si dimostra in linea con l'affermato principio di *accountability*, lasciando anche in questo caso una maggiore libertà di scelta e di organizzazione, cui segue tuttavia una maggiore responsabilità. Si assiste, sotto questo profilo, a un complessivo alleggerimento degli oneri procedurali in capo al titolare, che nel loro complesso vanno a sostituire il previgente obbligo generale di notificare alle Autorità di controllo i trattamenti di dati personali[615].

L'impostazione adottata dal legislatore esclude, dunque, una valutazione preventiva e generalizzata ad opera delle Autorità di controllo, finendo per essere questa troppo onerosa e poco in linea con la velocità che caratterizza il mercato digitale. Il titolare diviene così un filtro rispetto all'attività di controllo pubblica, avendo costui autonomia nella valutazione dell'intensità del rischio dei trattamenti[616], anche se ciò in astratto potrebbe comportare sottostime da parte del titolare stesso[617].

Una presunzione di alto rischio viene però fatta direttamente dal legislatore europeo, il quale specificamente introduce un obbligo di valutazione d'impatto per tutti i trattamenti che prevedano «*una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione*». Detta previsione nasce evidentemente dalla consapevolezza delle particolari criticità legate all'utilizzo delle tecnologie *data driven*, introducendo così un obbligo di valutazione di impatto quale misura capace di rendere maggiormente trasparente l'intero procedimento automatizzato.

Il crescente impiego delle tecnologie algoritmiche basate sui dati ha fatto emergere, accanto ai profili di sicurezza, anche criticità non solamente circoscritte al singolo

---

WP 248 rev.01, consultabili all'indirizzo: *www.interlex.it/2testi/autorit/wp248dpia.pdf* (ultimo accesso 20 giugno 2021).

[614] All'interno del testo si rinvengono una serie di trattamenti per cui corre l'obbligo di una valutazione di impatto. In particolare essa è richiesta per quei trattamenti che: presentino una valutazione globale che involge aspetti personali e che siano basate su un trattamento automatizzato dei dati; effettuati su larga scala e comportanti una sorveglianza sistematica su larga scala in zone aperte accessibili al pubblico. Per un approfondimento in merito alle ipotesi in cui è obbligatorio effettuare una valutazione di impatto si rimanda a TORINO, *op. cit.*, 859 ss.

[615] Il modello di prevenzione di valutazione preventiva del rischio era, infatti, già presente all'art. 20 della Direttiva del 1995. All'articolo 18 si prevedeva un generale obbligo di notificare alle Autorità di controllo il trattamento dei dati personali.

[616] TORINO, *op. cit.*, 858; MOLLO, *op. cit.*, 290; TARULLO, *op. cit.*, 131 s.

[617] MOLLO, *ibidem*.

individuo ma, come visto, tali da ricomprendere nuove forme di pregiudizio nei confronti di gruppi e di alcune fasce della società. In questa prospettiva si è così proposto, oltre che di valorizzare il ruolo delle Autorità di controllo, di rendere la valutazione di impatto maggiormente articolata e tale da realizzare un modello di *Privacy, Ethical and Social Impact Assessment*; si ritiene, infatti, opportuno arricchire detto documento con delle valutazioni in merito alla congruenza dell'uso dei dati rispetto ai valori etici e sociali di riferimento[618]. Una previsione in tal senso introdurrebbe un maggior onere, in termini di costi e risorse, in capo ai titolari dei trattamenti. Tuttavia, si osserva come la complessità della valutazione sia legata alla natura del trattamento. Ove questo comporti bassi rischi per i diritti individuali e collettivi, una valutazione di impatto così articolata non richiederebbe un impegno di tempo e costi elevato; diverso il discorso per tutte quelle tipologie di utilizzo dei dati personali che in relazione alle modalità operative, o alla natura dei dati trattati, comportino un alto livello di rischio e a cui conseguentemente dovrà seguire una valutazione di impatto necessariamente più articolata. L'entità dei costi dovrà dunque rientrare nella valutazione circa la proporzionalità delle misure adottate e nella strategia di gestione dei rischi, purtuttavia non potendo rivestire una posizione tale da spingere verso una diminuzione del livello di tutela riconosciuto ai diritti e alle libertà fondamentali[619].

[618] MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, cit., 326 ss. L'Autore evidenzia come sarebbe possibile superare le difficoltà legate alla mancanza di modelli valoriali condivisi, e comunemente accettati, mediante una considerazione composita. Da una parte, dunque, dovrebbero essere tenuti in considerazioni i valori sanciti nelle carte internazionali dei diritti umani e delle libertà fondamentali, quali la Convezione europea dei diritti dell'uomo, a cui si dovrebbero affiancare i valori propri del singolo contesto in cui i dati vengono trattati e le finalità perseguite. Questi ultimi potrebbero trovare riferimenti formalizzati in dichiarazioni, od orientamenti giurisprudenziali, che fornirebbero un quadro ricognitivo degli stessi. Della medesima opinione anche Moretti, il quale, nel sottolineare l'importanza della valutazione preventiva d'impatto, ritiene necessario aggiungersi a essa anche valutazioni etiche e sociali, in modo da poter prevedere meglio l'impatto sull'utilizzo dei dati e la tutela dei diritti fondamentali della persona. MORETTI, *Algoritmi e diritti fondamentali della persona*, cit., 810 ss.

[619] Sul punto Mantelero ricorda che «come accade in altri contesti, si pensi alla tutela ambientale, mitigare l'impatto che la tecnologia e l'attività di impresa possono avere sui diritti fondamentali e la società ha un costo globale significativo, che può essere maggiore o minore in relazione ai casi specifici. Tuttavia, la preminenza dei diritti fondamentali sulle logiche economiche e dello sviluppo tecnologico comporta necessariamente che gli oneri finanziari della tutela di tali diritti non possano costituire un argomento sufficiente per giustificarne la compressione». MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati*, cit., 330.

Infine, l'elemento di preponderante novità che emerge dal combinato disposto degli articoli 35 e 36 è proprio il ruolo di controllo cui sono chiamate le Autorità garanti[620]. Qualora, infatti, le misure di sicurezza previste dalla valutazione di impatto non siano sufficienti ad attenuare i rischi derivanti dal trattamento, sul titolare grava l'ulteriore obbligo di consultazione preventiva dell'Autorità di controllo[621]; quest'ultima può avvalersi dei poteri concessi dall'art. 58[622], ivi compreso – se necessario – il divieto di trattamento[623].

---

[620] Per un approfondimento in merito al ruolo delle Autorità nella valutazione di impatto e, in particolare, per i casi in cui si prevedere l'obbligo di queste di attivare il meccanismo di coerenza (art. 63 GDPR) si rimanda a PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 69 ss.; ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, in *Il nuovo Regolamento europeo sulla privacy*, cit., 533 ss.

[621] «*1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.*

2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione. […]". Art. 36, reg. UE n. 679/2016.

[622] "*1. Ogni autorità di controllo ha tutti i poteri di indagine seguenti: a) ingiungere al titolare del trattamento e al responsabile del trattamento e, ove applicabile, al rappresentante del titolare del trattamento o del responsabile del trattamento, di fornirle ogni informazione di cui necessiti per l'esecuzione dei suoi compiti; b) condurre indagini sotto forma di attività di revisione sulla protezione dei dati; c) effettuare un riesame delle certificazioni rilasciate in conformità dell'articolo 42, paragrafo 7; d) notificare al titolare del trattamento o al responsabile del trattamento le presunte violazioni del presente regolamento; e) ottenere, dal titolare del trattamento o dal responsabile del trattamento, l'accesso a tutti i dati personali e a tutte le informazioni necessarie per l'esecuzione dei suoi compiti; e f) ottenere accesso a tutti i locali del titolare del trattamento e del responsabile del trattamento, compresi tutti gli strumenti e mezzi di trattamento dei dati, in conformità con il diritto dell'Unione o il diritto processuale degli Stati membri.*

2. Ogni autorità di controllo ha tutti i poteri correttivi seguenti: a) rivolgere avvertimenti al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono verosimilmente violare le disposizioni del presente regolamento; b) rivolgere ammonimenti al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del presente regolamento; c) ingiungere al titolare del trattamento o al responsabile del trattamento di soddisfare le richieste dell'interessato di esercitare i diritti loro derivanti dal presente regolamento; d) ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine; e) ingiungere al titolare del trattamento di comunicare all'interessato una violazione dei dati personali; f) imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento; g) ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento a norma degli articoli 16, 17 e 18 e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali ai sensi dell'articolo 17, paragrafo 2, e dell'articolo 19; h) revocare la certificazione o

Alla luce delle considerazioni sopra svolte in merito alla difficoltà di esercizio delle prerogative concesse all'interessato, la possibilità di un intervento preventivo di un'autorità pubblica, avente poteri incisivi di controllo e di intervento, si mostra particolarmente pregevole. Le Autorità garanti sono, infatti, soggetti dotati di comprovata competenza, tale da poter valutare la proporzionalità delle misure adottate dal titolare, il cui intervento è diretto alla verifica della presenza di opportune garanzie per i diritti e le libertà delle persone fisiche, prima che il trattamento abbia inizio. In questo modo il legislatore intende dare una effettiva espressione al principio di precauzione che in un contesto tecnologico, avente un impatto potenzialmente molto esteso, è di assoluta preminenza; così da premettere una tutela degli utenti idonea ed effettiva, prima del verificarsi di eventuali danni.

5.2 La responsabilità per illecito trattamento dei dati personali

A completamento della disciplina viene prevista, ai sensi dell'art. 82, una responsabilità particolarmente gravosa nei confronti dei titolari e, in alcune circostanze,

---

ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti; i) infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle misure di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso; e j) ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale.
3. Ogni autorità di controllo ha tutti i poteri autorizzativi e consultivi seguenti: a) fornire consulenza al titolare del trattamento, secondo la procedura di consultazione preventiva di cui all'articolo 36; b) rilasciare, di propria iniziativa o su richiesta, pareri destinati al parlamento nazionale, al governo dello Stato membro, oppure, conformemente al diritto degli Stati membri, ad altri organismi e istituzioni e al pubblico su questioni riguardanti la protezione dei dati personali; c) autorizzare il trattamento di cui all'articolo 36, paragrafo 5, se il diritto dello Stato membro richiede una siffatta autorizzazione preliminare; d) rilasciare un parere sui progetti di codici di condotta e approvarli, ai sensi dell'articolo 40, paragrafo 5; e) accreditare gli organismi di certificazione a norma dell'articolo 43; f) rilasciare certificazioni e approvare i criteri di certificazione conformemente all'articolo 42, paragrafo 5; g) adottare le clausole tipo di protezione dei dati di cui all'articolo 28, paragrafo 8, e all'articolo 46, paragrafo 2, lettera d); h) autorizzare le clausole contrattuali di cui all'articolo 46, paragrafo 3, lettera a); i) autorizzare gli accordi amministrativi di cui all'articolo 46, paragrafo 3, lettera b); j) approvare le norme vincolanti d'impresa ai sensi dell'articolo 47. […]». Art. 58, reg. UE n. 679/2016.

[623] Difatti alla richiesta di consultazione preventiva possono seguire differenti esiti. L'Autorità potrebbe ritenere la valutazione idonea a ridurre o contrastare i rischi: potrebbe altresì indicare degli specifici provvedimenti da adottare in seguito a un giudizio di inadeguatezza; infine potrebbe prevedere il divieto *tout court* di effettuare il trattamento. Quest'ultima eventualità si presenta qualora non sia possibile attenuare il rischio di impatto negativo, tenuto conto della tecnologia disponibile e dei costi di attuazione, sempre in una logica di proporzionalità tra mezzi e fini, come indicato dallo stesso Considerando n. 84, reg. UE n. 679/2016. Cfr. MOLLO, *op. cit.*, 291; TORINO, *op. cit.*, 874 ss.

dei responsabili del trattamento[624]. Il legislatore statuisce, infatti, che chiunque subisca un danno, materiale o immateriale, causato dalla violazione del trattamento dei dati ha diritto a un risarcimento.

La norma in parola introduce un modello di responsabilità che in molte parti riprende la formulazione del previgente articolo 23 della Direttiva 46/95 CE, pur ampliandone le previsioni fino a ricomprendere il responsabile del trattamento e disciplinando, infine, i rapporti interni tra eventuali corresponsabili[625]. Nel complesso la disposizione non sembra tuttavia presentare un contenuto innovativo; ciò rende dunque ancora attuali molte delle criticità e delle soluzioni interpretative proposte dalla dottrina in relazione alle disposizioni di attuazione della Direttiva Madre; nello specifico rispetto all'art. 18 della legge n. 675/1996 e al successivo art. 15 del d. lgs. n. 196/2003 (c.d. Codice Privacy)[626].

Da una prima lettura dell'art. 82 si conferma dunque come la condotta illecita, da cui discende l'obbligazione risarcitoria, debba essere configurata come un generico

---

[624] «*1. Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento.*
2. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il presente regolamento. Un responsabile del trattamento risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.
3. Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.
4. Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.
5. Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2.
6. Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto dello Stato membro di cui all'articolo 79, paragrafo 2». Art. 82, reg. UE n. 679/2016.

[625] SICA, *La responsabilità civile per trattamento illecito dei dati personali*, in *Regolare la tecnologia*, cit., 162 s. Per un approfondimento in merito alla declinazione del principio di responsabilità nella Direttiva Madre, e come esso sia stato trasposto nel testo del Regolamento, si rimanda a PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, cit., 275 ss.; FINOCCHIARO, *Privacy e protezione dei dati personali*, cit., 107 ss.

[626] GAMBINI, *Principio di responsabilità e tutela aquilina dei dati personali*, cit., 49; ID., *Responsabilità e risarcimento nel trattamento dei dati personali*, cit., 1017 ss.

mancato rispetto delle disposizioni presenti nel dettato normativo[627]. Una conferma di tale interpretazione viene dallo stesso Considerando n. 146, ove si precisa come debba essere ritenuto non conforme al Regolamento anche quel trattamento che non sia conforme ad atti delegati o di esecuzione adottati dagli Stati membri[628]. Ne discende, allora, come la valutazione circa la condotta causativa del danno debba essere compiuta avendo a riferimento tutte le disposizioni regolamentari; non pare infatti giustificata una limitazione del perimetro risarcitorio unicamente al caso di mancato rispetto degli obblighi di condotta da parte del titolare o del responsabile del trattamento, ben potendo derivare un danno anche qualora, pur tenendo la condotta richiesta, vengano violate altre disposizioni normative.

Quanto al riparto dell'onere della prova della violazione, limitandosi il primo comma dell'art. 82 a prevedere quest'ultima come elemento costitutivo della fattispecie, un'indicazione all'interprete viene data dalle disposizioni in tema di *accountability* sopra richiamate[629]. È necessario difatti dare una lettura dell'articolo in commento che sia coerente con l'intero testo del GDPR, ove appunto il principio sopra citato, nel prevedere una maggiore responsabilità in capo al titolare, statuisce per quest'ultimo un

---

[627] CATERINA, THOBANI, *Il diritto al risarcimento del danno*, *GDPR tra novità e discontinuità*, a cura di CATERINA, in *Giur. it*., 2019, 2805 ss.; POLICELLA, PELINO, nel *Codice della Disciplina Privacy*, diretto da BOLOGNINI e PELINO, Milano, 2019, *sub* art. 82, 441 ss.; BENVENUTO, COLAROCCO, *Le responsabilità del titolare e del responsabile connesse al trattamento dei dati personali*, in *Il diritto di internet nell'era digitale*, cit., 824 s.

[628] «*Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento*». Considerando n. 146, reg. UE n. 679/2016.

[629] CATERINA, THOBANI, *op. cit*., 2806 ss.; CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Jus civile*, 2020, 793.

obbligo di dimostrazione di aver posto in essere tutte le misure necessarie a rendere il trattamento *compliant* con la normativa.

Mal si concilierebbe allora un riparto dell'onere probatorio differente in caso di azione risarcitoria, facendo gravare la dimostrazione della violazione in capo al danneggiato. Una tale ricostruzione, oltre che in contrasto con i principi generali, comporterebbe un ingiustificato aggravio della posizione del singolo utente, finendo per favorire coloro che invece si trovano nella posizione migliore per fornire la prova richiesta, gravando già sul titolare e sul responsabile un obbligo di *compliance* così parametrato.

In caso di danni l'interessato sarà pertanto chiamato a provare la sussistenza di un trattamento dati, del danno e del nesso di causalità tra quest'ultimo e il primo, potendosi invece limitare ad allegare la violazione delle disposizioni previste Regolamento UE n. 679/2016 (nei termini sopra specificati). Infine, il danneggiato dovrà provare la riferibilità del trattamento al titolare o al responsabile; ciò in particolare qualora vi siano più soggetti responsabili, ovvero nel caso in cui l'interessato imputi a un titolare il danno derivante da un trattamento effettuato da terzi. Si pensi per esempio a messaggi pubblicitari indesiderati inviati da un soggetto a cui l'interessato non ha prestato il consenso. Il danneggiato potrebbe chiedere il risarcimento del danno a un terzo, titolare di un differente trattamento, invocandone la responsabilità per aver trasmesso i suoi dati personali senza il necessario consenso. In questo caso, evidentemente, graverà sull'attore l'onere di provare, anche per presunzioni, che la violazione sia imputabile al terzo per aver trasmesso, senza pervio consenso, i propri dati personali poi utilizzati per l'invio di materiale pubblicitario[630].

Nel contesto delle applicazioni digitali possono tuttavia sorgere alcune difficoltà proprio in merito all'individuazione dello specifico titolare del trattamento a cui imputare il danno subito; ciò in quanto si assiste sempre più a una vera e propria catena di trattamenti, di cui molto spesso l'interessato non ha effettiva contezza, avendo un diretto contato solo con "l'ultimo anello".

Questa condizione viene inoltre esacerbata dalla considerazione per cui spesso sono le stesse applicazioni di Intelligenza Artificiale, a contatto diretto con l'interessato, a

[630] In arg. CATERINA, THOBANI, *ibidem*.

raccogliere i dati per poi utilizzarli e trasmetterli per diverse finalità, come nel caso degli IoT o delle auto *driverless*.

Non pare possibile, seguendo la stessa definizione data dal GDPR, ritenere tutti i soggetti facenti parte della catena di trattamenti come co-titolari, in quanto nella realtà ognuno definisce in modo autonomo mezzi e fini del proprio trattamento, non avendo invece alcuna cognizione dei trattamenti altrui. Ne discende allora come per il danneggiato sia difficile individuare a quale tra i diversi titolari imputare il danno subito; inoltre, non avendo egli sempre effettiva contezza dei trattamenti posti in essere, si dimostra complessa anche l'individuazione del singolo trattamento da cui è disceca la violazione che ha determinato il danno subito.

Sul punto si è aperta una riflessione in merito alla possibilità di qualificare le stesse macchine autonome come responsabili, o finanche titolari, del trattamento che pongono in essere. Si è evidenziato come la stessa nozione di titolare del trattamento non sia legata necessariamente a una persona fisica, né giuridica, potendo detta carica essere rivestita anche da un'Autorità, un servizio o genericamente un organismo. L'unico discrimine risiede nel potere di determinare i mezzi e le finalità del trattamento. Se dunque un AI fosse in grado di determinare autonomamente mezzi e fini, ciò potrebbe rappresentare una condizione sufficiente per la nomina a titolare del trattamento, da cui tuttavia deriverebbe anche un obbligo di adempiere ai doveri previsti per tale figura dal GDPR, tra cui *in primis* quello di trasparenza[631].

Tale soluzione lascerebbe nondimeno impregiudicato il problema di chi debba rispondere economicamente delle violazioni e dei danni provocati dai trattamenti, rimanendo pur sempre l'AI un software/hardware non avente, per lo meno ad oggi, una personalità giuridica.

Forse più agevole potrebbe essere la nomina dell'AI quale responsabile del trattamento, rimanendo il produttore il titolare. Attualmente, infatti, è quest'ultimo – grazie ai programmatori suoi dipendenti – a definire gli algoritmi di funzionamento, vincolando anche lo spettro dei dati utilizzabili e delle decisioni che le macchine possono assumere. La nomina del sistema algoritmico quale responsabile del

[631] Cfr. PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 172 s., il quale evidenza come, a differenza di quanto emerso in merito alla concessione di una personalità elettronica ai robot, in questo caso sarebbe possibile procedere con l'attribuzione del ruolo direttamente alle macchine, non essendo la normativa in analisi ostativa.

trattamento lascerebbe inoltre in capo al titolare la responsabilità in merito alle istruzioni che impartisce alla macchina nella qualità di responsabile[632]. In questo caso evidentemente rimarrebbe un legame tra produttore e macchina, dovendo il primo sempre vigilare e controllare le modalità con cui gli algoritmi operano sui trattamenti. Tuttavia è bene sottolineare, come visto in precedenza, che proprio l'architettura dei sistemi informatici complessi non permette di operare questa tipologia di controllo, non potendo nemmeno il programmatore comprendere sempre le modalità di funzionamento dell'algoritmo.

Allo stato attuale dell'evoluzione tecnologica la concessione di ruoli decisori o di vertice nell'architettura dei trattamenti ai sistemi di Intelligenza Artificiale, per quanto possano essere considerati "autonomi", appare prematuro. Al di fuori di una prospettiva certamente evocativa per il futuro, detta proposta non sembra nemmeno essere risolutiva. Al fine di facilitare l'onere probatorio del danneggiato sarebbe forse maggiormente opportuno ritenere l'ultimo soggetto che tratta i dati, che entra direttamente in contatto con l'interessato, quale responsabile nei suoi confronti; ferma restando la possibilità per quest'ultimo di rivalersi sugli altri titolari facenti parte della catena di trattamenti in relazione alle responsabilità di ciascuno.

Per fare un esempio, si pensi alle auto a guida autonoma. Nel caso di violazione delle disposizioni a tutela dei dati personali ivi trattati, secondo un principio di vicinanza della prova oltre che di economia processuale, parrebbe più ragionevole che a rispondere nei confronti dell'utente danneggiato sia il produttore dell'auto, che per il tema che ci occupa rivestirebbe il ruolo anche di titolare del trattamento. È di tutta evidenza che in questo specifico frangente possano esserci diversi titolari in ragione dei singoli trattamenti operati dalla vettura, ma di cui l'utente finale è difficilmente consapevole[633]. Diversa invece la posizione della casa produttrice dei veicoli, la quale evidentemente si trova nella migliore posizione per conoscere tutti i soggetti che partecipano alle dotazioni della vettura; sarà dunque questa a rivalersi successivamente sugli altri titolari, in ragione delle rispettive responsabilità[634].

---

[632] PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, cit., 173 s.

[633] La stessa individuazione dei soggetti che rivestono il ruolo di titolari non pare pacifica. Il tema verrà affrontato *infra* nel capitolo 5 del presente lavoro.

[634] I soggetti potenzialmente coinvolti durate tutta la catena dei trattamenti sono molteplici. Oltre ai diversi titolari, di cui si è dato conto, ben potrebbero essere coinvolti anche diversi responsabili (sia interni che esterni all'organizzazione del titolare); questi ultimi potrebbero a loro volto nominare sub-

Se quanto fin qui richiamato in merito agli elementi costitutivi dell'illecito può dirsi sostanzialmente pacifico, un dibattito particolarmente acceso è invece sorto in merito al criterio di imputazione della responsabilità.

Così come già statuito dalla Direttiva madre, anche nel Regolamento il legislatore pare discostarsi dal regime ordinario di responsabilità per colpa *ex* art. 2043 c.c.[635], prevedendo una prova liberatoria consistente nella dimostrazione che l'evento dannoso non è in alcun modo imputabile al titolare o al responsabile.

Sul punto il legislatore italiano aveva introdotto un esplicito riferimento all'art. 2050 c.c.[636], aprendo così a un bibattito interpretativo in merito alla qualificazione dell'attività come pericolosa *ex lege*, e conseguentemente su quale regime di responsabilità dovesse essere applicato ai titolari dei trattamenti.

Pare necessario evidenziare come la qualifica dell'attività di trattamento dati fatta dal nostro legislatore non fosse basata su di una valutazione prognostica o statistica diretta a dimostrarne la pericolosità potenziale. Difatti, per poter essere considerata pericolosa

---

responsabili per porre in essere specifiche mansioni. È dunque evidente la complessità strutturale che coinvolge i trattamenti dati nel contesto digitale e, in particolar modo, nelle applicazioni di Intelligenza Artificiale. Se il Regolamento prevede espressamente nei confronti di titolari e responsabili una responsabilità solidale, si discute se sia possibile, ed entro quali limiti, una pattuizione contrattuale diretta stabilire una soglia oltre la quale il responsabile, in particolare quello esterno, non sia tenuto a rispondere. La normativa europea non prevede una tale possibilità, nemmeno da una lettura sistematica delle disposizioni e dei Considerando; il riferimento normativo, per il nostro ordinamento, rimangono dunque gli artt. 1229 e 1341 c.c., a mente dei quali è possibile una limitazione della responsabilità, che dovrà essere specificamente approvata, purché essa non preveda una limitazione anche nei casi di dolo o colpa grave, o qualora il fatto del debitore non costituisca violazione di obblighi derivanti da norme di ordine pubblico. Diversamente, come ha avuto modo di chiarire la Suprema Corte, dette clausole potranno considerarsi valide e non saranno soggette al regime previsto dall'art. 1341, non limitando (o escludendo) le conseguenze della colpa o dell'inadempimento, ma semplicemente specificando il rischio garantito (Cass., 11.9.2019, n. 15598, in *Guida al dir*., 2019, 60). In arg. si rimanda a BENVENUTO, COLAROCCO, *op. cit.*, 834 ss.

[635] BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in *Persona e mercato dei dati*, cit., 387 ss. L'Autore evidenzia come per parte della dottrina la previsione di una disposizione *ad hoc* in materia perseguisse lo scopo di introdurre una tipizzazione dell'illecito, così da consentire, sul fronte della tutela aquiliana, il risarcimento del danno non patrimoniale da violazione della privacy. L'A., tuttavia, ritiene che dalla mancanza di un esplicito riferimento alla responsabilità aquiliana, e dalla menzione di una necessaria violazione del Regolamento (causalmente collegata al danno), si debba desumere di essere in presenza di una responsabilità da inadempimento di prestazioni dovute, avente una natura "ancipite". La responsabilità così delineata dal legislatore comunitario si troverebbe, infatti, a cavallo tra responsabilità contrattuale ed extracontrattuale; pur se dalla stessa formulazione dell'articolo questa appia strutturalmente più vicina a una responsabilità contrattuale. In arg. si veda anche RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, in *Il nuovo Regolamento europeo sulla privacy*, cit., 624 ss.; ID., *La responsabilità da illecito trattamento dei dati personali*, in *La protezione dei dati personali in Italia*, cit., 786 ss.

[636] Il testo dell'art. 15 d. lgs. n. 196/2003, ora abrogato dal d. lgs. n. 101/2018, statuiva che: «*1. Chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile.*
2. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'articolo 11».

un'attività deve cagionare, secondo un modello di ricorrenza statistica, un alto numero di incidenti potenzialmente anche molto gravi, stante la particolare potenzialità offensiva dell'attività posta in essere[637]. Il legislatore italiano invece parrebbe aver posto a fondamento del rimando operato all'art. 2050 c.c., più che una valutazione circa il carattere pricoloso dell'attività, unicamente la previsione di esonero della responsabilità indicata al comma 2° dell'art. 23, Direttiva 46/95 CE, che statuiva: «*il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova che l'evento dannoso non gli è imputabil*e». Proprio la previsione di tale condizione di esonero aveva fatto propendere la migliore dottrina per ritenere corretto e coerente il richiamo, considerato più come un rinvio tecnico che come qualificazione dell'attività come pericolosa, fatto dal legislatore nostrano, dal momento che la prova della non imputabilità prevista dalla norma del 2050 c.c. è data dalla dimostrazione di aver adottato "*tutte le misure idonee ad evitare il danno*"[638].

La posizione dottrinale maggioritaria, cui ha aderito anche la giurisprudenza, tendeva dunque a ricostruire la fattispecie di responsabilità come oggettiva. Questo il senso del richiamo all'art. 2050 c.c., da cui discendeva l'obbligo per il titolare di porre in essere tutte le misure astrattamente possibili per evitare il danno; per andare esente da responsabilità il danneggiante era pertanto chiamato a provare l'interruzione del nesso di causalità, dimostrando come il danno fosse dipeso da caso fortuito o forza maggiore.

Come ricorda autorevole dottrina in merito alla responsabilità da attività pericolosa, la funzione della regola che vede l'esclusione della responsabilità qualora il danno discenda da un caso fortuito, dovrebbe essere quella di escludere l'attribuzione

---

[637] Cfr. MONATERI, *La responsabilità civile*, nel *Trattato Sacco*, Torino, 1998, 1019; POLICELLA, PELINO, *op. cit.*, 442.

[638] Cfr. sul punto RICCIO, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA, BELISARIO, I, Milano, 2018, *sub* art. 82, 598. Si veda inoltre FRANZONI, *Responsabilità derivante da trattamento dei dati personali*, in *Diritto dell'informatica*, a cura di FINOCCHIARO e DELFINI, Milano, 2014, 831.

Di diverso avviso invece parte dei commentatori che ritenevano la pericolosità intrinseca, non tanto nell'attività di trattamento, quanto nel dato personale stesso. Quest'ultimo difatti sarebbe al contempo informazione e fonte di informazione, e proprio da questa sua caratteristica, che permette di inferire ulteriori dati personali, ne discenderebbe la sua insita pericolosità. Pertanto la pericolosità sarebbe un attributo del dato e non del mezzo di trattamento. Sul punto si rimanda a COLIVA, *Prime valutazioni sulla responsabilità civile nella legge 675/96*, 20 aprile 1997, in *Interlex*, consultabile all'indirizzo: *www.interlex.it/675/coliva1.htm* (ultimo accesso 14 giugno 2021); G. RESTA, SALERNO, *La responsabilità civile per il trattamento dei dati personali*, in *La responsabilità d'impresa*, a cura di ALPA e CONTE, Milano, 2015, 643. In giurisprudenza, conforme a detta posizione in tema di dati personali Cass., 19.5.2014, n. 10947, in *Foro it.*, 2015, I, 120, con nota di PALMIERI. In argomento anche RATTI, *op. cit.*, 615 ss.

all'imprenditore (in questo caso il titolare) dei rischi che non siano da questo amministrabili economicamente. Ne discende allora che il caso fortuito debba comprendere quegli eventi che si siano verificati per il concorso o l'intervento di concause eccezionali, le quali abbiano determinato un danno la cui gravità eccede il rischio tipico, e ciò in quanto la loro incidenza non sarebbe prevedibile né calcolabile per l'imprenditore[639].

Le medesime considerazioni vengono poste in merito alla qualificazione dell'art. 82 GDPR; anch'esso dunque ritenuto espressione di una responsabilità di tipo oggettivo.

A sostegno di detta posizione, si evidenzia come questa interpretazione troverebbe conferma nel carattere pericoloso dell'attività di trattamento dati, la cui valutazione sarebbe stata compiuta dallo stesso legislatore europeo, così come dimostrato proprio dall'approccio basato sul rischio che informa tutta la normativa. Da questo punto di vista dunque l'art. 82 introdurrebbe un modello di responsabilità per rischio evitabile in capo al titolare[640].

Inoltre, la stessa prova liberatoria richiesta dalla norma condurrebbe a una tendenziale oggettivazione della responsabilità, risolvendosi in pratica in una *probatio diabolica*; infatti – si sostiene – se il titolare avesse adottato tutte le misure idonee, il danno non si sarebbe verificato[641]. Ne discende allora come il danneggiante possa

---

[639] Si evidenzia come questa ricostruzione sia coerente con la funzione stessa della responsabilità per attività pericolosa; accanto alla funzione reintegratoria del patrimonio del danneggiato vigerebbe una pressione economica su chi ha organizzato l'attività rischiosa, inducendolo a ridurre il rischio entro un limite economicamente giustificato. V. TRIMARCHI, *op. cit.*, 360 s.
Sul punto la Suprema Corte ha avuto modo di esprimersi recentemente e, ribadendo il consolidato orientamento, ha precisato che la «*la nozione di attività pericolosa, ai sensi e per gli effetti della norma suddetta, non deve essere limitata alle attività tipiche, già qualificate come tali da una norma di legge, ma deve essere estesa a tutte le attività che, per la loro stessa natura o per le caratteristiche dei mezzi adoperati, comportino una rilevante possibilità del verificarsi di un danno (Cass. 30/10/2002, n. 15288; Cass. 07/05/2007, n.10300; Cass. 16/01/2013, n.919; Cass. 29/07/2015, n. 16052). Il requisito della pericolosità, dunque, non va accertato in astratto ma in concreto, con valutazione che deve essere fatta caso per caso, tenendo presente che anche un'attività per natura non pericolosa può diventarlo in ragione delle modalità con cui viene esercitata o dei mezzi impiegati per espletarla (Cass. 05/06/2002, n. 8148). L'accertamento in concreto se una certa attività, non espressamente qualificata come pericolosa da una disposizione di legge, possa o meno essere considerata tale ai sensi dell'art. 2050 c.c., implica un accertamento di fatto, che il giudice del merito deve compiere secondo il criterio della prognosi postuma, in base alle circostanze esistenti al momento dell'esercizio dell'attività (Cass. 30/10/2002, n. 15288; Cass. 12/05/2005, n. 10027)* […]». Cass., 19.7.2018, n. 19180, in *Foro it*., 2018, I, 3968.

[640] In arg. CAMARDI, *op. cit.*, 795 s., la quale evidenzia come un'interpretazione delle norme nell'ottica di una dogmatica europea condurrebbe alle medesime conclusioni. L'A., infatti, ritiene la responsabilità oggettiva del responsabile un precipitato a valle di una visione a monte dell'attività del trattamento dati come attività libera ma vigilata. Dunque prima ancora che una responsabilità per danni, la responsabilità del titolare sarebbe di ordine organizzativo, specie quanto alla sicurezza dei dati.

[641] In arg. SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, cit., 168.

andare esente da responsabilità solo qualora provi l'interruzione del nesso eziologico tra l'attività da questi posta in essere e l'evento dannoso, così configurandosi un tipico esempio di responsabilità oggettiva[642].

Al fine di poter accertare l'interruzione del nesso di causalità dovranno essere valutati gli obblighi di condotta previsti dal GDPR con i parametri dell'adeguatezza tecnica e organizzativa, anch'essi ripresi a più voce dal legislatore europeo, secondo un giudizio valutativo in relazione al rischio tipico correlato al trattamento posto in essere. L'introduzione nel testo normativo di particolari obblighi di comportamento non sarebbe dunque diretta a verificare il grado di diligenza del titolare, quanto piuttosto a descriverne la condotta da tenere, la cui violazione configura un danno di per sé risarcibile.

In conclusione, secondo questa ricostruzione, la responsabilità per illecito trattamento dei dati personali, mutuando l'elaborazione della dottrina in merito alla responsabilità per esercizio di attività pericolose[643], dovrebbe essere qualificata quale oggettiva, ma limitata al rischio tipico, cioè a quello prevedibile e calcolabile dal titolare del trattamento[644].

---

[642] SPERA, *Profili di responsabilità civile nel trattamento dei dati*, in *Tecnologia e Diritto*, II, cit., 197 s.; TOSI, *Responsabilità civile per illecito trattamento dei dati personali*, cit., 32. Diversamente per Bravo, il quale ritiene che la prova liberatoria così delineata dal legislatore europeo riecheggi quella prevista dall'art. 1218 c.c.; ulteriore elemento, questo, a fondamento di una natura contrattuale della responsabilità da illecito trattamento dei dati personali. L'Autore, infatti, precisa come il paragrafo 3 della norma ravvisi l'evento dannoso, da cui deriva il danno-conseguenza, nel comportamento del titolare che si sostanzi in una violazione di una norma del regolamento; questa si concretizzerà sempre in una violazione di un obbligo previsto *ex lege* in favore dell'interessato, obbligo previsto per garantirgli uno strumento di protezione per i diritti e libertà a esso spettanti. Ne discende allora come la prova della non imputabilità in alcun modo dell'evento dannoso si sostanzi nella prova della non imputabilità dell'inadempimento all'obbligo previsto dalle disposizioni del GDPR; riprendendo così pienamente la dimostrazione della non imputabilità della prestazione dovuta prevista dall'art. 1218 c.c. V. BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, cit., 414 ss.

[643] Si rimanda a TRIMARCHI, *op. cit.*, 401 ss.

[644] Anche i rari incidenti potrebbero rientrare nei rischi tipici, proprio perché sebbene non evitabili possono essere calcolati e rientrare nel costo sociale dell'esercizio dell'attività d'impresa, dunque nel calcolo rischi-benefici. Ne discende che dovrebbero essere sottratti dalla responsabilità del titolare tutti quei rischi incalcolabili e imprevedibili (rischi atipici), che si ritiene socialmente, oltre che economicamente, accettabile non debbano essere posti a carico dell'imprenditore. Cfr. CAMARDI, *op. cit.*, 796; TOSI, *op. cit.*, 75 s., il quale sul punto si richiama Trimarchi che in merito alla responsabilità per rischio d'impresa sottolinea come sia necessariamente limitata al rischio tipico in quanto «occorre che si tratti di danni pertinenti a un rischio che abbia un'entità apprezzabile, tale da potersi pretendere che venga calcolata dall'imprenditore e coperto con l'assicurazione o con l'autoassicurazione». V. TRIMARCHI, *op. cit.*, 280.

Di diverso avviso altra parte dei commentatori, i quali ritengono che la responsabilità gravante sul titolare debba, sulla scorta di un'interpretazione sistematica dell'articolo in parola, essere qualificata come aggravata[645].

Questa ricostruzione – si sostiene – sarebbe quella più in linea con l'intero complesso normativo. Come visto, una maggiore e più intensa attenzione è posta sul ruolo del titolare, e sugli obblighi che su di esso gravano in forza della posizione di controllo rivestita nel trattamento; dall'altra parte proprio la specificazione di obblighi di condotta sembra essere indicativa di un rafforzamento dello standard tradizionale di valutazione della colpa, introducendo una diligenza maggiormente qualificata[646]. Difatti, quando all'agente viene imposta l'adozione di misure, normalmente richieste a un operatore del medesimo settore, necessarie a mantenere la sicurezza e prevenire possibili pregiudizi, l'imputazione del danno si sposta verso un regime di responsabilità per colpa[647].

Secondo questa lettura, dunque, il danno da violazione degli obblighi di tutela dei dati viene a configurarsi quale conseguenza colposa della mancata adozione delle misure organizzative, oltre che tecniche, necessarie a scongiuralo, tenuto conto anche dei rischi per i diritti degli interessati[648]. Proprio in ragione della specificità dell'attività di trattamento dei dati l'obbligo di prevenire ed evitare il danno diviene più rigoroso, ampliando e specificando il dovere di diligenza gravante sul titolare del trattamento.

---

[645] A questa posizione si affianca quella che in ragione di una linea di continuità con quanto previsto dalle previgenti normative ritiene il criterio di imputazione della responsabilità avente una natura semi-oggettiva. Da ciò discende un'inversione dell'onere della prova in merito all'elemento soggettivo, dunque il dolo o la colpa, rimanendo in capo al soggetto danneggiato l'onere di provare il danno subito e il nesso di causalità tra danno ed evento. Cfr. RICCIO, *op. cit.*, 600; GAMBINI, *Principio di responsabilità*, cit., 70 ss.; ID., *Responsabilità e risarcimento*, cit., 1048 ss.; SPERA, *op. cit.*, 195 ss.; CATERINA, THOBANI, *op. cit.*, 2805 ss.

[646] Gli obblighi di condotta previsti dal Regolamento si dimostrano certamente gravosi e intensi, essendo espressione dei principi di prevenzione e precauzione. Tuttavia questi sembrano collocarsi all'interno di un processo di aggravamento della colpa, ove dunque sempre meno spazio trovano le condizioni soggettive del titolare quanto piuttosto il rispetto di prerogative e obblighi applicabili all'intero settore, così venendo la categoria della colpa a subire una specificazione nell'ambito della protezione dei dati.

[647] GAMBINI, *Principio di responsabilità*, cit., 78.; ID., *Responsabilità e risarcimento*, cit., 1060 ss.

[648] Sul punto si rileva come la prova di aver adottato tutte le misure idonee per evitare il danno deve essere compiuta tenuto conto sia del progresso tecnologico che di quanto disposto dall'art. 32 del GDPR, il quale fa riferimento, tra le altre cose, alla capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi. A tale riguardo rileva il tema delle certificazioni, che potrebbero configurare un modello di riferimento adottabile dai titolari. Si pensi per esempio allo s*tandard* UNI EN ISO/IEC 27001:2017 che definisce il sistema di *best practices* per gestire i rischi legati alla protezione dei dati, andando a indicare un numero di misure predefinite e implementabili, anche ulteriori rispetto a quanto previsto dal Regolamento. In arg. v. BENVENUTO, COLAROCCO, *op. cit.*, 832.

A sostegno di detta posizione vi sarebbe inoltre il mancato riferimento, all'interno del testo, alle tradizionali cause oggettive e assolute di non punibilità, così facendo propendere per una ricostruzione che si fondi sulla colpa dell'agente[649].

Altra questione di interesse è se il danno discendente dalla violazione del regolamento sia *in re ipsa* o se piuttosto l'interessato ne debba provare la sussistenza e la quantificazione. Dalla violazione del trattamento possono, infatti, discendere differenti danni in capo agli interessati, di cui una elencazione viene data al Considerando n. 75[650]. Ci si è tuttavia domandati in dottrina se il risarcimento del danno non patrimoniale potesse discendere direttamente dalla stessa violazione delle disposizioni regolamentari, configurandosi dunque la violazione dei dati personali un danno-evento risarcibile[651].

Sul punto le posizioni dottrinarie si dividono nuovamente. Parte dei commentatori ritiene che dal tenore della norma in analisi possa essere fatto discendere un danno *in re ipsa* ogni volta che vengano violate le disposizioni del Regolamento, senza che sia necessario per il danneggiato provare nemmeno l'entità delle conseguenze dannose asseritamente subite. La normativa sulla tutela dei dati personali introdurrebbe, infatti, un'ipotesi speciale di responsabilità. Da ciò ne discende che ogni violazione dei precetti

---

[649] GAMBINI, *Principio di responsabilità*, cit., 83. L'A. inoltre, a sostegno di questa interpretazione, sottolinea come lo strumento della presunzione di colpa si dimostra, sul piano pratico, veicolo di soluzioni maggiormente eque ed efficienti, in relazione al bilanciamento delle esigenze di protezione della vittima e di promozione della libera circolazione dei dati. L'inversione dell'onere della prova permetterebbe, infatti, di responsabilizzare il titolare (o il responsabile, in determinati casi) il quale, per andare esente da responsabilità, avrà l'onere di dare la prova di aver impiegato tutte le misure di prevenzione e precauzione adeguate a evitare i pericoli, o limitare gli effetti pregiudizievoli degli illeciti trattamenti di dati personali.

[650] «*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*». Considerando n. 75, reg. UE n. 679/2016.

[651] TABARRINI, *op. cit.*, 555; PIERUCCI, *op. cit.*, 713 ss.; CATERINA, THOBANI, *op. cit.*, 2805 ss.; GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, cit., 107 ss.; CAMARDI, *op. cit.*, 794.; ESPOSITO, *Il risarcimento del danno non patrimoniale da illecito trattamento dei dati personali*, in *Corriere giur.*, 2019, 628 ss.

contenuti nel testo del Regolamento comporta un danno sempre risarcibile in quanto di per sé ingiusto; difatti la condotta tenuta dal danneggiante sarebbe lesiva del diritto alla tutela dei dati personali, diritto questo riconosciuto come fondamentale e a cui deve accompagnarsi, seguendo la ricostruzione del diritto alla salute, quanto meno una tutela risarcitoria[652].

Di converso, la posizione maggioritaria ritiene che, come da consolidato insegnamento della Suprema Corte, possono essere risarciti unicamente i danni-conseguenza, non potendo dunque trovare spazio una fattispecie di danno *in re ipsa*. Il danneggiato sarà chiamato a fornire la prova che dalla violazione delle disposizioni prevsite dal GDPR sia effettvamente disceso un danno. Alla mera violazione delle disposizioni del Regolamento, in assenza della dimostrazione di una lesione concreta, seguirà dunque una sanzione amministrativa – qualora ne ricorrano i presupposti – ma non un risarcimento del danno[653].

Tale ricostruzione trova fondamento anche nel dato testuale dell'articolo 82, il quale riporta l'espressione "danno causato" e "danno cagionato". Pertanto, ciò che va risarcito è quel danno-conseguenza che discenda dalla violazione delle disposizioni del Regolamento; non trova spazio, come da consolidato orientamento giurisprudenziale, nel regime di responsabilità il c.d. danno-evento, dovendo sempre essere dimostrata la sussistenza dello stesso, oltre che la sua gravità[654].

---

[652] Cfr. TOSI, *op. cit.*, 100 ss.

[653] Cfr. RATTI, *op. cit.*, 616 ss.; RICCIO, *op. cit.*, 600. La Cassazione ha infatti chiarito come «*pur in assenza di un trattamento illecito di dati personali, deve ritenersi erronea la condanna del relativo titolare al risarcimento del danno non patrimoniale allorché, per un verso, i pregiudizi all'immagine, all'onore e alla reputazione dell'interessato siano stati dalla stessa pronuncia ritenuti insussistenti o comunque indimostrati e, per altro verso, quest'ultimo non abbia allegato circostanze idonee a provare in che termini si fosse verificata una sofferenza ricollegabile al trattamento*». Cass., 5.9.2014, n. 18812, in *Foro it.*, 2015, I, 119, con nota di PALMIERI.

[654] V. GAMBINI, *Principio di responsabilità*, cit., 111; ID., *Responsabilità e risarcimento*, cit., 1067 ss.; RICCIO, *op. cit.*, 602.; CATERINA, THOBANI, *op. cit.*, 2807 ss.; SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, cit., 172. Se un obbligo risarcitorio discendesse dalla semplice violazione delle norme sul trattamento dei dati si rischierebbe di attribuire al risarcimento del danno una funzione preminentemente punitiva, pregiudicandone la duplice natura che guarda tanto al danneggiante quanto al danneggiato. BENVENUTO, COLAROCCO, *op. cit.*, 829. In arg. anche SPERA, *op. cit.*, 198 s. e 200 s., il quale riporta i criteri che il giudice è chiamato a seguire per la quantificazione del danno. L'A. riporta i criteri seguiti dalla Corte d'Appello di Milano (App. Milano, 22.7.2015, n. 3205, inedita), nello specifico «*gravità oggettiva delle intrusioni e loro tipologia* […]; *ambiti di vita esplorati; durata dell'intrusione; numero delle persone coinvolte nelle indagini e loro capacità e risorse professionali; modalità di trattamento dei dati e quindi maggiore o minore diffusione delle notizie riservate apprese; momento di conoscenza delle intrusioni da parte della vittima* […]; *relazione tra la vittima e l'autore delle intrusioni*. […] *ai fini della quantificazione del danno appaiono di primario rilievo gli aspetti concernenti la maggiore o minore penetrazione della sfera privata, la maggiore o minore diffusione delle notizie apprese*».

Sul punto l'orientamento della Superma Corte è costante e consolidato. Proprio in tema di risarcimento del danno da violazione della normativa sulla privacy gli ultimi arresti giurisprudenziali sembrano ancora una volta confermare la necessità per il danneggiato di fornire la prova, anche per presunzioni, di quali danni siano ad esso discesi dal comportamento illecito tenuto dal danneggiante.

I pregiudizi derivanti dalla violazione della privacy possono infatti essere differenti, potendo avere sia natura patrimoniale che non patrimoniale, pertanto graverà sull'attore l'onere di provarne la sussitenza. Si pensi, per fare un esempio, alla recente sentenza della Suprema Corte ove è stato riconosciuto a un avvocato un risarcimento pari a 8.500,00 euro a seguito della comunicazione di suoi dati personali, aventi ad oggetto giudizi disciplinari relativi al precedente impiego svolto e non pertitenti rispetto allo scopo per cui erano stati trattati.

Nel caso di specie è stato dunque risconosciuto un risarcimento non per il danno-evento (la divulgazione delle informazioni personali), ma per le conseguenze pregiudizievoli derivanti dalla comunicazione a terzi dei propri dati. Gli Ermellini hanno infatti ritenuto provato che dalla divulgazione illecita sia discesa una grave lesione per l'avvocato, configurandosi un serio pregiudizio non solamente alla sua sfera emotiva, ma anche alla sua immagine e reputazione sociale nel ristretto ambiente lavorativo in cui il danneggiato era da breve tempo entrato[655].

Affinché un danno derivante da un comportamento tenuto in violazione delle norme del Regolamento privacy possa essere risarcito, è inoltre necessario provarne anche la quantificazione. Si ricorda che, per giurisprudenza consolidata, è possibile risarcire unicamente quei danni che superano la normale soglia di tollerabilità[656].

---

[655] Il danneggiato difatti versava in una particolare condizione di fragilità. Essendo da poco iscritto all'Ordine forense egli si trova nella condizione di dover costruire la propria immagine e credibilità professionale, non solamente in relazione ai potenziali clienti, ma anche rispetto ai colleghi che possono certamente incidere sulla sua attività anche per il futuro. Pertanto la divulgazione illecita di precedenti azioni disciplinari nei suoi confronti, divulgazione per altro avvenuta in modo parziale e malizioso, occultando la circostanza che gli stessi erano stati archiviati e le sanzioni irrogate annullate, hanno dunque comportato un grave pregiudizio, quantificato in via equitativa in 8.500,00 euro. V. Cass., 26.4.2021, n. 11020, in *Mass. Giust. civ.*, 2021.

[656] Il riferimento è a quanto affermato nelle quattro sentenze di San Martino (sentt. n. 2697, 26973, 26974, 26975 dell'11 novembre 2008), ove appunto la Suprema Corte chiarisce come «*il risarcimento del danno non patrimoniale è dovuto sollo nel caso in cui sia superato il livello di tollerabilità ed il pregiudizio non sia futile*». Cass., sez. un., 11.11.2008, n. 26972, in *Resp. civ. e prev*., 2009, 38, con nota di MONATERI; in *Giust. civ.*, 2009, I, 913, con nota di ROSSETTI; in *Rass. dir. civ.*, 2009, 499 con nota di PERLINGIERI, TESCIONE; in *Guida al dir.*, 2008, 18, con nota di DALIA, COMANDÈ. Ne discende così l'esclusione dei c.d. danni bagatellari dal novero dei danni risarcibili, essendo questi meri fastidi o disagi che si collocano

Pur aderendo a una interpretazione in linea con la giurisprudenza europea, la quale ritiene risarcibile come danno morale anche i disagi, fastidi, disturbi, che possono essere generati a un interessato a seguito di un comportamento illecito[657], è tuttavia necessaria la dimostrazione che questi disagi superino una certa soglia di gravità, eccedendo i pregiudizi futili che sono tollerati in ragione di un dovere di convivenza sociale.

Sul punto ha avuto modo di esprimersi a più riprese la Corte di Cassazione che, nella vigenza del Codice Privacy, ha chiarito come: «*Il danno non patrimoniale, risarcibile ex art. 15 del Codice della privacy (d.lgs. n. 196/2003) non si sottrae alla verifica della "gravità" della lesione e della serietà del danno, atteso che anche per tale diritto opera il bilanciamento con il principio di solidarietà ex art. 2 Cost. Ne deriva che determina una lesione ingiustificabile del diritto non la mera violazione delle prescrizioni di cui all'art. 11 del predetto Codice ma solo quella che ne offende in modo sensibile la portata effettiva*»[658].

Così chiarito il perimetro del danno risarcibile è tuttavia necessario sottolineare un ulteriore aspetto critico legato ai trattamenti di dati operati mediante algoritmi. Si è già precisato come attualmente gran parte dei trattamenti viene posto in essere mediante una riconduzione dei soggetti all'interno di gruppi; questa categorizzazione è nella maggioranza dei casi alla base delle decisioni del sistema. Ciò fa sì che sebbene la decisione influenzi la sfera del singolo, essa viene presa in generale sul gruppo in cui l'individuo viene catalogato, comportando spesso per il danneggiato un danno di modesta entità[659]. Diviene così difficile la stessa stima del danno, avendo questo spesso natura non patrimoniale.

Proprio su tale considerazione si basa la tesi di coloro che ritengono il danno sempre, dunque indipendentemente dalla sua entità, risarcibile. Se così non fosse, per molti dei

---

al di sotto della soglia minima di apprezzabilità del danno. In argomento si rimanda tra gli altri a SCOGNAMIGLIO, *Il sistema del danno non patrimoniale dopo le decisioni delle sezioni unite*, in *Resp. civ. e prev.*, 2009, 261 ss.; ZIVIZ, *Lo spettro dei danni bagatellari*, *ivi*, 517 ss.; FRATI, MONTANARI VERGALLO, DI LUCA, *La giurisprudenza delle Sezioni unite sul danno alla persona:* et lux fruit?, in *Riv. it. med. leg.*, 2009, 277.

[657] Si fa riferimento all'orientamento europeo che vede riconosciuti i c.d. danni da vacanza rovinata, identificabili in disagi e fastidi che si ingenerano nel turista che non ha potuto godere della vacanza in ragione delle "sensazioni spiacevoli" suscitate dall'inadempimento del professionista. Sul punto Corte giust. UE, 12.3.2002, causa C-186/00, consultabile all'indirizzo: *eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62000CJ0168&from=HU* (ultimo accesso 20 giugno 2021).

[658] Cass., 11.1.2016, n. 222, in *Ri.da.re*, 2016, con nota di ZIVIZ; conf. Cass., 15.7.2014, n. 16133, in *Foro it.*, 2015, I, 120. Più di recente anche Cass., 20.8.2020, n. 17383, in *Mass. Giust. civ.*, 2020; Cass., 10.6.2021, n. 16402 in *DeJure*.

[659] In argomento INFANTINO, *ibidem*.

trattamenti che si fondano su tecnologie *data driven* si assisterebbe a una ingiustificata mancanza di tutela da parte dell'ordinamento, che finirebbe per non garantire una base di protezione a quei diritti, quali la privacy, che oggi vanno rivestendo una sempre maggiore importanza quali diritti fondamentali dell'uomo[660].

Nella prospettiva di garantire tutela anche per quei danni che per il singolo si rivelino di modesta entità, parte della dottrina ha sviluppato il concetto di *group privacy*, che si propone di estendere anche al gruppo in sé (non dunque in quanto somma dei singoli membri) la legittimazione a poter accedere a una tutela risarcitoria in relazione alla violazione del proprio diritto a un'identità infromazionale inviolata[661]. Ciò permetterebbe di apprestare tutela a tutte quelle posizioni che vedono una minima lesione dei diritti del singolo individuo, ma che essendo perpetrata nei confronti di una generalità di persone danno luogo a un danno particolarmente esteso e quantitativamente ingente[662].

Si è tuttavia già sottolineato come tale proposta necessiti di una specifica previsione normativa che introduca detta possibilità[663], non potendosi ritenere le azioni di classe egualmente idonee allo scopo; dal momento che spesso non vi è effettiva contezza del

[660] Il diritto alla protezione dei dati personali e alla riservatezza sono fatti rientrare tra i diritti fondamentali della personalità. Questi assumono, inoltre, una rilevanza meta-individuale, essendo precondizione per l'esercizio dei diritti civili, sociali e politici, e in ultima istanza per lo stesso funzionamento dell'ordine democratico. Cfr. TOSI, *op. cit.*, 24.

[661] Per un'analisi approfondita si rimanda a AA. VV., *Group Privacy. New Challanges of Data Technologies*, a cura di TAYLOR, FLORIDI, VAN DER SLOOT, Berlin, 2017; MITTELSTADT, *From individual to group privacy in Big Data Analytics* (2017) 30 *Philosophy & Technology* 475 ss. Si veda anche Moretti il quale evidenzia come «Dalla formulazione dei gruppi *ad hoc* e dal loro utilizzo attraverso processi decisionali automatizzati si possono dunque determinare trattamenti discriminatori di ampia portata che vadano ad incidere sul gruppo individuato e, in via indiretta, su quei soggetti che, anche se non identificati, vi sono ricompresi. Per tale ragione risulta opportuno elaborare nuovi modelli a tutela della privacy che non siano unicamente incardinati sulla protezione del singolo individuo e che tengano conto della classificazione in gruppi sempre più utilizzata all'interno dei processi automatizzati». MORETTI, *op. cit.*, 817.

[662] Cfr. INFANTINO, *op. cit.*, 1766 ss., secondo cui dovrebbe essere dedicata maggiore attenzione agli strumenti legati alle azioni collettive. L'A. sottolinea, infatti, come proprio nella materia che qui ci occupa sarebbe altamente probabile che su singoli attori possano ricadere danni di modesta entità, ma che se presi in considerazione nel loro complesso darebbero invece «volto e nome ad una considerevole dannosità arrecata alla società nel suo complesso». In argomento anche Moretti, che sottolinea come «L'impostazione atomistica adottata sin ora e ribadita all'interno del Regolamento può risultare talvolta riduttiva in considerazione delle innovative modalità di elaborazione dei dati. Ciò ha condotto parte della dottrina a sviluppare il concetto di group privacy che, parallelamente al riconoscimento di un diritto soggettivo individuale, valorizzi la dimensione collettiva della privacy». Secondo l'Autore infatti, ad assumere rilevanza non sarebbe più tanto l'identificabilità della singola persona, quanto l'individuazione degli aspetti che accumunano i deversi individui. Proprio dalla creazione di questi gruppi di utenti, e dal loro utilizzo attraverso processi decisionali automatizzati, deriverebbero possibili trattamenti discriminatori di ampia portata; questi, infatti andrebbero a incidere sul gruppo e, in via indiretta, su quei soggetti che, anche se non identificati, vi sono ricompresi. Cfr. MORETTI, *op. cit.*, 816 ss.

[663] Si rimanda *infra* alle considerazioni svolte nel § 7, capitolo 3, in tema di tutela collettiva.

singolo di appartenere a un determinato gruppo[664]. La prassi ha inoltre dimostrato come lo strumento delle azioni di classe abbia trovato scarsa applicazione negli ordinamenti di *civil law*, quali il nostro, a fronte della procedura in parte complessa e in parte in relazione alle criticità legate all'estensione dell'efficacia del giudicato anche nei confronti degli appartenenti alla medesima classe non intervenuti nel giudizio[665].

Si deve infine notare come lo strumento risarcitorio sembra rivestire un ruolo residuale nella materia. Ciò può discendere da una parte dalle sopra richiamate difficoltà relative alla prova dell'esitenza e della quantificazione del danno, e dall'altra dalla considerazione per cui nella prassi la funzione deterrente più che dalla responsabilità civile pare essere svolta dalle sanzioni pecuniarie particolarmente ingenti previste dalla normativa. A conferma di detta ricostruzione le poche, complice anche l'attualità del fenomeno, recenti pronunce legate alle tecnologie *data dirven*, nelle quali sono state irrogate sanzioni più o meno consistenti a fronte del mancato rispetto delle disposizioni previste dal GDPR. Si pensi alla recente sanzione comminata dall'Autotità Garante per la Privacy a Foodinho, dell'importo di 2,6 milioni di euro, per diverse violazioni tra cui: indaguatezza e insufficienza dell'informativa relativa al trattamento dei dati sulla posizione geografica dei lavoratori; mancanza di adegute informazioni in merito ai processi di decisione automatizzata che il software compiva per assegnare i punteggi; nonché la mancata previsione di strumenti a tutela dei diritti dei *riders*[666].

Anche un'altra azienda, anch'essa di *food delievery*, è stata recentemente oggetto di un'ordinanza del Tribunale di Bologna a causa dell'uso di un algoritmo discriminatorio atto ad assegnare in modo automatizzato un punteggio ai propri lavoratori. In questo caso la causa era stata intentata dalle associazioni sindacali, le quali lamentavano una violazione del diritto allo sciopero dal momento che l'algoritmo di fatto impediva la partecipazione dei lavoratori a forme di astensione collettiva. Nel caso di specie il Tribunale di Bologna ha ritenuto accertato come discrimantorio il funzionamento del

[664] MORETTI, *op. cit.*, 816.
[665] Cfr. CASAROSA, *La tutela aggregata dei dati personali nel Regolamento UE 2016/679: una base per l'introduzione di rimedi collettivi*, in *Regolare la tecnologia*, cit., 235 ss.; INFANTINO, *op. cit.*, 1770 ss. L'A. sottolinea come sia doveroso ripensare tali strumenti, oltre che per incentivare gli attori a porli in essere, anche sotto il profilo dell'incentivo di profitto per gli avvocati chiamati a patrocinare tali iniziative. Per motivi di brevità espositiva non è possibile approfondire le considerazioni in merito alle procedure di *class action*. Si rimanda all'interessante contributo avente un respiro anche comparatistico, e i riferimenti in nota ivi presenti, di CABRAL, *Procedure di risoluzione standard e conflitti di massa*, in *Riv. trim. dir. proc. civ*., 2020, 611 ss.
[666] Garante Privacy, Ordinanza di ingiunzione, 10.6.2021 [doc. web n. 9677521].

software e condannato l'azienda al pagamento in favore delle associazioni sindacali ricorrenti di un risarcimento del danno pari alla somma di 50.000,00 euro[667].

Diversa invece la situazione oltre oceano, ove vi è una maggiore diffusione e utilizzo di sistemi *data driven* e di algoritmi di Intelligenza Artificiale. L'ordinamento americano, come è noto, ha un approccio maggiormente libertario a cui non si sottrae la materia della *data protection*. Quanto ai danni generati da algoritmi di AI una sostanziosa *litigation* si rifà sostanzialmente ai danni generati dal malfunzionamento del robot "DaVinci", utilizzato per l'esecuzione di alcuni interventi chirurgici di precisione[668]. Non si dubita tuttavia che anche la diffusione di auto a guida autonoma generarà un aumento del contezioso in seguito a possibili sinistri, come dimostrano i casi di incidenti, anche mortali, verificatosi per esempio con il sistema *autopilot* di Tesla[669].

Tuttavia per quanto riguarda i danni derivanti da un illecito trattamento dei dati personali la *litigation* non sembra essere ancora particolarmente numerosa, complice forse anche la tendneza a trovare un accordo transattivo delle controversie. In argomento appare interessante la *class action* aperta contro il sito di incotri online Ashley Madison a seguito di un episodio di *data breach* verificatosi nel 2015. Gli attori, tra le varie accuse mosse, sostenevano che gli imputati stessero conducendo una condotta ingannevole e fraudolenta creando "*host*" e "*bot*" programmati per generare e inviare messaggi agli utenti di sesso maschile, fingendo di essere donne reali, inducendoli a fare acquisti sul sito web.

Per porre fine alla controversia è stato proposto un accordo di 11,2 milioni di dollari, prevedendo per ogni singolo ricorrente un risarcimento pari a un massimo di 3.500

---

[667] Trib. Bologna, 31.12.2020, cit. Per un approfondimento della vicenda si rimanda *supra* al § 1 del presente capitolo.

[668] Il robot "DaVinci", prodotto dalla società americana Intuitive surgical Inc., è un sistema composto da diversi bracci meccanici che possono essere comandati a distanza da un chirurgo, grazie a una consolle che gli fornisce una visione tridimensionale realistica del campo operatorio. In tema di *litigation* americana si rimanda all'interessante saggio di GUERRA, *Profili di responsabilità del produttore di robot chirurgico nell'ordinamento americano*, in *Riv. resp. medica*, 2020, 2015 ss. Sono diversi i procedimenti instaurati nelle corti americane, a seguito di un mal funzionamento della macchina, a mero titolo esemplificativo si v. O'Brien v. Intuitive Surgical, Inc., No. 10 C 3005, 2011 WL 304079, at *1 (N.D. Ill. Jul. 25, 2011); Mracek v. Bryn Mawr Hosp., 610 F. Supp. 2d 401, 402 (E.D. Pa. 2009), aff'd, 363 F. App'x 925 (3d Cir. 2010); Greenway v. St. Joseph's Hosp., No. 03-CA-011667 (Fla. Cir. Ct. 2003).

[669] Per un approfondimento si rimanda a CIAMPANELLI, *Da Uber a Tesla, tutti gli incidenti della auto a guida autonoma*, 20 aprile 2018, consultabile all'indirizzo: *corriereinnovazione.corriere.it* (ultimo accesso 5 luglio 2021).

dollari e destinando la somma eccedente a organizzazioni di beneficienza per la privacy digitale[670].

Sempre in relazione alla violazione dei dati personali si pensi anche allo scandalo Cambridge Anaytica che ha visto coinvolta la società Facebook, per aver dato accesso ai dati di circa 81 milioni di propri utenti, la quale ha versato l'enorme somma di 5 miliardi di dollari per risolvere la controversia transattivamente[671].

Da questi esempi si può facilmente ipotizzare come la sempre maggiore pervasività delle applicazioni digitali aventi a fondamento algoritmi di Intelligenza Artificiale porterà invitabilmente all'emersione di nuovo contenzioso, sia in relazione alla violazione della normativa sulla *data protection* che per i danni, potenzialmente anche fisici, causati dalla loro interazione con gli utenti finali[672]. Se da una parte la strategia posta in essere da legislatori e Istitutizioni è diretta, come visto, alla riduzione del rischio mediante una regolazione *ex ante*, che definisca i requisiti di sicurezza e affidabilità, il ruolo della responsabilità civile dovrebbe acquistare una sempre maggiore rilevanza nella chiusura del sistema, garantendo agli utenti il ristoro dei danni subiti.

6. Possibili prospettive di tutela

Sebbene la maggiore responsabilizzazione del titolare del trattamento e la valorizzazione del ruolo ricoperto dalle Autorità garanti rappresentino una buona base di partenza per una regolazione della materia digitale, di per sé non paiono sufficienti a

[670] V. Ashley Madison v. Customer Data Sec. Breach Litig., 148 F. Supp. 3d 1378, 1380 (JPML 2015).

[671] La sanzione è stata comminata dalla *Federal Trade Commission*. Si v. il comunicato presente all'indirizzo: *https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions* (ultimo accesso 10 settembre 2021).

[672] Si pensi al caso del software utilizzato, sempre negli Stati Uniti (ove questa tipologia di sistemi algoritmici è più diffuso), per valutare le prestazioni degli insegnanti. Dal 2009 in diversi distretti scolastici, generalmente quelli aventi a disposizione meno fondi, è stato utilizzato un software (IMPACT) avente lo scopo di individuare, a fronte del cattivo rendimento degli studenti, gli insegnanti meno competenti. Va da sé che il rendimento scolastico di un alunno dipende da diversi fattori, anche socio-economici, e non unicamente dalla preparazione e dalla bravura degli insegnanti; il software avrebbe, dunque, dovuto analizzare una pluralità di variabili per rispondere all'obiettivo prefissato. In ragione della valutazione compiuta dal software vennero licenziati nel 2010, nel distretto di Washington, circa 200 insegnanti che avevano totalizzato un punteggio inferiore alla media. Si è poi riscontrato come in realtà il software ritenesse predominanti gli esiti dei test nazionali compiuti dagli studenti alla fine dell'anno. Da questa evidenza è inoltre derivato un aumento di brogli nei test, dal momento che maggiori percentuali di promossi potevano garantire una relativa sicurezza anche agli insegnanti, così finendo per falsare ulteriormente le valutazioni operate dal sistema, che già di per sé si erano rivelate arbitrarie e inique. Per un approfondimento della vicenda si rimanda a O'NEIL, *op. cit.*, 10 ss.

tutelare concretamente i diritti e le libertà degli interessati. Alla luce delle criticità legate alle modalità di funzionamento degli algoritmi sarebbe auspicabile coniugare le previsioni del GDPR, sopra ricordate, con una maggiore attenzione alla stessa composizione dei *dataset*. Il rischio di errori determinati da dati poco rappresentativi o scorretti è infatti difficilmente arginabile a posteriori, mentre soluzioni che permettono di verificare la qualità dei dati di addestramento avrebbero quale immediato beneficio una minore probabilità di ricorrenza di detti eventi.

Questa esigenza si manifesta chiaramente anche in relazione alla raccolta e all'utilizzo di dati non personali, in ragione della capacità della tecnologia di inferire informazioni di natura personale anche da *dataset* così caratterizzati. Ben si comprende allora come il tema della qualità dei dati abbia acquistato una centralità sempre maggiore nel dibattito. Di detta necessità è consapevole lo stesso legislatore europeo, il quale, come già si è evidenziato, ricomprende il principio di esattezza tra quelli applicabili a tutti i trattamenti di dati personali.

Le previsioni regolamentari ricordate, pur rappresentando un mirabile punto di partenza, meriterebbero una maggiore implementazione. Il volume dei dati, e la considerazione per cui spesso chi li raccoglie non è lo stesso soggetto che poi li utilizza per l'addestramento degli algoritmi, sono elementi che rendono complessa l'indicazione specifica di attributi generalmente applicabili ai deversi ambiti di raccolta e di utilizzo.

Si è notato come il concetto stesso di qualità contenga differenti accezioni che tuttavia debbono essere necessariamente valutate in relazione agli scopi di utilizzo dei dati. La predisposizione di criteri unitari mal si concilierebbe, infatti, con le singole esigenze di settore; si pensi per esempio all'utilizzo di informazioni per finalità statistiche legate a un determinato fenomeno in un arco temporale definito, se fosse previsto un generale obbligo di aggiornamento ciò comporterebbe la perdita di utilità per quel trattamento.

Pare allora maggiormente auspicabile lo sviluppo di soluzioni, quali standard tecnici, in grado di regolare più dettagliatamente il settore in ragione delle singole specificità[673]. Il

[673] In argomento Moretti. L'Autore, dopo aver sottolineato l'inscindibilità tra algoritmi e dati, e dunque la necessità che questi ultimi siano di qualità affinché il procedimento matematico possa condurre a un risultato apprezzabile, pone l'attenzione sul ruolo dei *Data Scientists*. Essi sono, infatti, i soggetti preposti alla creazione dell'architettura del sistema, determinano gli obiettivi e le logiche seguite; si reputa allora opportuno un intervento che disciplini e vigili sul loro operato. L'Autore ipotizza l'adozione di codici di condotta che fissino regole condivise e omogenee. V. MORETTI, *op. cit.*, 815 ss.

legislatore europeo, come visto, aveva già auspicato la predisposizione di standard legati alla interoperabilità dei dati, nella prospettiva di renderne più agevole circolazione e permettere un completo sviluppo del mercato unico europeo. Del pari anche gli standard qualitativi ricoprirebbero un importate ruolo nella strategia di sviluppo del mercato, comportando una maggiore sicurezza dei sistemi e un rafforzamento anche dell'affidamento degli utenti; obiettivo anch'esso perseguito nella strategia europea sui dati.

Sul punto, attenzione meritano le normative della serie ISO/IEC 25000 dedicate proprio alla certificazione della qualità dei dati e dei software. Come visto poc'anzi il concetto di qualità non ha un'interpretazione univoca, dovendo essere parametrato agli scopi ai quali i dati sono diretti; da ciò discende una certa difficoltà nella verifica e nella misurazione della qualità dei *dataset*. Per ovviare a tali incertezze nel 2008 è stato emanato il primo Standard ISO/IEC diretto a individuare quali caratteristiche dei dati possono essere misurabili al fine di certificarne la qualità. Lo Standard ISO-25012 identifica dunque 15 caratteristiche[674], alcune delle quali inerenti agli stessi dati e altre dipendenti dal sistema a cui sono destinati, lasciando tuttavia ai singoli settori, in ragione del contesto d'uso, la definizione di soglie di accettabilità secondo cui le misurazioni potranno verificare la presenza o meno di qualità dei dati.

Successivamente, nel 2014, è stato emanato un nuovo Standard (ISO/IEC 25024) diretto adestendere il campo delle misurazioni, definendo 63 misure di qualità dei dati[675]. Elemento di particolare rilevanza è la presenza di caratteristiche quali la comprensibilità, la disponibilità, la portabilità, la sicurezza (in termini di privacy) e l'accessibilità, che se implementanti all'interno delle applicazioni di Intelligenza Artificiale permetterebbero la diffusione di sistemi maggiormente interoperabili, potendo questi ultimi operare su dati controllati, condivisi e di qualità.

---

[674] Le caratteristiche elencate dallo standard sono: Accuratezza, Completezza, Coerenza, Credibilità, Attualità, Accessibilità, Conformità, Riservatezza, Efficienza, Precisione, Tracciabilità, Comprensibilità, Disponibilità, Portabilità e Ripristinabilità. Come si nota le ultime tre sono direttamente dipendenti dalle caratteristiche del sistema in cui i dati sono utilizzati. ISO/IEC 25012/2008.

[675] Per un approfondimento in merito alle caratteristiche di qualità dei dati e un confronto con lo Standard ISO/IEC 9126-3, sulla qualità dei software, si rimanda a PINZON, SANABRIA, *Aplicación del estándar ISO/IEC 9126-3 en el modelo de datos conceptual entidad-relación*, in *Revista Facultad de Ingeniería*, 2013, 35, 113 ss.; NATALE, *Orientamenti sul modello di qualità dell'Intelligenza Artificiale*, 22 aprile 2020, consultabile all'indirizzo: *https://intelligenzartificiale.unisal.it/orientamenti-sul-modello-di-qualita-dellintelligenza-artificiale/* (ultimo accesso 28 maggio 2020).

Una maggiore qualità dei dati favorirebbe non solamente un miglior governo dei Big Data, ma anche l'incremento di dati riusabili, il miglioramento dei processi che causano dati errati, la stima dei costi di prodotti di non qualità, etc[676]. Evidentemente una diffusione di una prassi condivisa tra gli operatori comporterebbe altresì una maggiore possibilità di diffusione di *open data*[677], particolarmente importanti per esempio nel settore medicale ove lo sviluppo di soluzioni di Intelligenza Artificiale necessita di una sempre maggiore condivisione al fine di risolvere i problemi di replicabilità dei risultati; elemento del metodo scientifico necessario per permettere una sicura diffusione delle applicazioni all'interno della comunità scientifica.

Questa tipologia di strumenti si dimostra particolarmente utile. Così come i codici di condotta, anche gli Standard tecnici come gli ISO sono, infatti, elaborati a un livello più prossimo agli operatori, tenendo direttamente in considerazione le criticità e le prospettive tecniche di implementazione.

A differenza di un metodo normativo classico, gli standard, che potremmo qualificare come strumenti di *soft law*, permetterebbero una maggiore flessibilità, caratteristica necessaria per rispondere più velocemente alle evoluzioni tecnologiche di quanto farebbe un testo legislativo. Data la natura estremamente tecnica e la vocazione sovranazionale della stessa, la partita non può che essere giocata almeno a livello europeo; non è infatti pensabile la diffusione di standard differenziati legati a contesti territoriali, ciò renderebbe più farraginosa la circolazione dei dati compromettendo lo stesso funzionamento del mercato digitale. Attenzione dovrebbe essere prestata anche al ruolo svolo dagli organismi di certificazione, e alle procedure di accreditamento degli stessi.

Alla luce di queste considerazioni il ruolo delle Istituzioni europee ritrova centralità, esse infatti dovrebbero essere chiamate a regolare le procedure di accreditamento oltre che all'individuazione di un'Agenzia, avente il compito di controllare e valutare la compatibilità degli standard con le normative europee in materia di tutela dei dati e con

[676] Si veda l'interessate comunicato stampa dell'AGID in merito alla misurazione della qualità dei dati, che accompagna la pubblicazione dello Standard ISO nella versione in lingua italiana. Consultabile all'indirizzo:
www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/iso_25024_agid_misurazione_della_qualita_dei_dati.pdf (ultimo accesso 26 aprile 2021).

[677] V. FAINI, *op. cit.*, 344 ss. In argomento si rimanda anche all'interessante contributo di MARETTI, RUSSO, GOBBO, *Open data governance: civic hacking movement, topics and opinions in digital space* (2021) 55 *Quality & Quantity* 1133 ss., consultabile all'indirizzo: *https://doi.org/10.1007/s11135-020-01045-y* (ultimo accesso 26 aprile 2021).

i principi e le libertà fondamentali dell'uomo. Se da una parte ciò può sembrare una ingiustificata limitazione alla libertà di iniziativa economica, a fronte dei costi e dei tempi da affrontare per completare la procedura di controllo, al contempo l'apposizione di un eventuale marchio CE, a comprova della qualità dei dati utilizzati, avrebbe come immediata conseguenza una maggiore fiducia da parte non solamente degli utenti ma anche degli stessi titolari dei trattamenti. Questi ultimi infatti, dovendo rispondere per tutti i danni eventualmente occorsi, ben potrebbero privilegiare quegli algoritmi addestrati con dati dalla qualità certificata, così da ridurre il rischio di possibili *bias* comportanti esternalità negative per gli interessati e per i titolari stessi.

L'individuazione di un'Agenzia europea composta da esperti nelle diverse materie interessate dal fenomeno, compresi dunque esponenti delle Autorità Garanti della privacy, potrebbe rivestire importanza non solamente nelle procedure di accreditamento e di controllo degli standard, ma ad essa potrebbero essere demandate procedure di controllo aventi ad oggetto il rispetto delle normative europee a regolazione della materia.

Come visto, infatti, il quadro normativo di riferimento si dimostra oggi particolarmente complesso, essendo questo caratterizzato dal veloce avvicendarsi di Direttive e Regolamenti a disciplinare specificamente singoli settori, che tuttavia finiscono inevitabilmente per interagire e sovrapporsi. A ciò si aggiunga il contesto sempre più tecnologizzato della materia; appare allora evidente come l'individuazione di un soggetto che assommi in sé esperti delle diverse discipline interessante possa garantire, oltre che un controllo effettivo, anche, ove previsti poteri di intervento, una maggiore garanzia per gli individui soggetti ai trattamenti e in particolare per quelli operati mediante tecnologie di AI[678].

6.1 La *blockchain* quale possibile alleato nella filiera di dati di qualità

Oltre alla predisposizione di standard tecnici e l'individuazione di organismi di vigilanza, una proposta interessante introduce l'utilizzo delle stesse tecnologie digitali nella definizione di dati di qualità. In particolare, la tecnologia *blockchain* potrebbe

[678] In argomento Moretti. L'autore auspica la formazione di apposite figure di controllo e monitoraggio che abbiano il compito di svolgere attività di *audit* sull'utilizzo di algoritmi all'interno di processi decisionali. V. MORETTI, *ibidem*.

rispondere all'obiettivo di creare *dataset* di comprovata qualità; questi difatti potrebbero essere collazionati all'interno della catena unicamente se rispondenti a predeterminate caratteristiche e standard definiti. Una volta validati, dunque inseriti all'interno della *blockchain*, i dati sarebbero immodificabili, e ciò permetterebbe evidentemente una maggiore sicurezza circa la bontà delle informazioni raccolte.

Si è inoltre proposto l'utilizzo di detta tecnologia per contrastare l'accentramento delle capacità computazionali e l'eccessiva specializzazione degli algoritmi[679]. A questo obiettivo risponde il progetto *singularity.net* il quale è diretto alla creazione di un *marketplace* di Intelligenza Artificiale sfruttando appunto la *blockchain*[680]. Sarebbe infatti possibile per i produttori di AI attestare su un nodo della *blockchain* il proprio sistema di *machine learning*, o il proprio algoritmo, così consentendo ai partecipati al *network* di utilizzarlo, a fronte del versamento di un corrispettivo.

Grazie alla *blockchain* sarebbe dunque in astratto possibile eliminare posizioni dominanti sul mercato, mediante la predisposizione di registri distribuiti, non solamente di algoritmi di AI, ma anche di dati di addestramento, ove sarebbe possibile verificare in ogni momento le transazioni eseguite e la provenienza degli stessi[681].

A prima vista questa modalità tecnica si mostra particolarmente idonea a rispondere alle esigenze di trasparenza dei sistemi, grazie a una maggiore certezza e sicurezza anche in merito alla provenienza e conservazione di algoritmi e *dataset*. Tuttavia, nonostante questi indubitabili pregi, la *blockchain* presenta anche alcuni profili di criticità, sia giuridici che di natura tecnica, in merito ai quali pare necessaria un'attenta riflessione.

Per meglio comprendere le criticità è necessario preliminarmente chiarire cosa si intenda per *blockchain* e come essa funzioni.

Il termine ha avuto una risonanza mediatica molto forte a seguito della nascita e della diffusione delle valute digitali, quali il Bitcoin, che si fondano proprio su questa

[679] V. SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 119.
[680] Per un approfondimento in merito al progetto SingularityNET e alle applicazioni ad oggi sviluppate, si rimanda all'indirizzo: *https://singularitynet.io/* (ultimo accesso 24 aprile 2021).
[681] V. SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 120 s.; Così JESUS RODRIGUEZ, *Why Decentralized AI Matters Part I: Economics and Enablers*, 2018, consultabile all'indirizzo: *www.medium.com/datadriveninvestor/why-decentralized-ai-matters-part-i-economics-and-enablers-5576aeeb43d1* (ultimo accesso 5 settembre 2021).

tecnologia[682]. L'utilizzo della *blockchain* per le valute digitali è possibile dal momento che le sue stesse modalità di funzionamento permettono di instaurare un meccanismo di fiducia tra gli utenti e introducono il concetto di scarsità digitale, rendendo così le informazioni registrate nel sistema scambiabili e suscettibili di valutazione economica[683]. Ma la *blockchain* può essere impiegata in differenti settori[684], si pensi per esempio ai cosiddetti *smart contract*[685].

Sinteticamente questa tecnologia si basa su di un registro distribuito[686], ciò in quanto le informazioni presenti nel sistema vengono replicate in una serie di terminali, chiamati nodi, tra loro in posizione di parità. Questo sistema si pone in contrapposizione con il

[682] Quando si parla di *blockchain* si fanno risalire le sue origini al *paper* "*Bitcoin: A Peer-to-Peer Electronic Cash System*" pubblicato sotto lo pseudonimo di Satoshi Nakamoto nel 2008, nel quale ne viene descritto il funzionamento e a cui seguì, l'anno successivo, la creazione del blocco iniziale della *Blockchain* Bitcoin. Tuttavia l'idea di un sistema decentralizzato di pagamenti trova origine nei primi anni novanta nel movimento c.d. cyberpunk, che nel 1993 pubblicò un primo manifesto. Lo scopo del movimento era, infatti, quello di contrastare le restrizioni alle libertà e alla privacy derivanti dall'uso delle tecnologie informatiche, che avrebbero permesso a grandi società, oltre che ai governi, di monitorare e controllare le informazioni sugli utenti, finendo per inferire i loro stili di vita grazie alla raccolta di un considerevole numero da dati, tra cui quelli delle loro transazioni di consumo. Per un approfondimento si rimanda a SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 10 ss.; BELLINI, MARTINESCU, VASSALLI, *Digital Ledger Technologies*, in *Digital transformation and data management*, a cura di BELLINI e D'ASCENZO, Pisa, 2020, 138 ss.; PAROLA, MERATI, GAVOTTI, Blockchain *e* smart contract: *questioni giuridiche aperte*, in *Contratti*, 2018, 681 ss.; GIULIANO, *La* blockchain *e gli* smart contracts *nell'innovazione del diritto del terzo millennio*, in *Dir. inform.*, 2018, 993 ss.; CUCCURU, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, in *Nuova giur. civ.*, 2017, 107 s.; CAPACCIOLI, *Le criptovalute*, in *Tecnologia e Diritto*, II, cit., 385 ss.; GAMBINO, BOMPREZZI, *op. cit.*, 623 s.

[683] Nel contesto digitale, come è noto, ogni informazione è facilmente replicabile senza costi e oneri aggiuntivi. Il meccanismo della *blockchain* permette, invece, di rendere l'informazione scarsa, quindi ne permette una valutazione economica. Ciò è possibile grazie all'uso della crittografia, la cui applicazione rende il set di dati univocamente identificabile e tracciabile, potendo dunque distinguere gli originali dalle copie. Proprio questa caratteristica ha permesso la nascita delle valute digitali. Cfr. SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 18.

[684] GAMBINO, BOMPREZZI, *op. cit.*, 624 s. Lo stesso Parlamento europeo ha emanato un report ove vengono ipotizzati i possibili differenti utilizzi della tecnologia *blockchain*. Tra questi si ricorda, oltre alle valute virtuali e agli *smart contracts*, anche la possibilità di implementare piattaforme di voto elettronico, brevetti, catene di fornitura di prodotti etc. Si rimanda alla Risoluzione del Parlamento europeo del 3 ottobre 2018, *Tecnologie di registro distribuito e* blockchain*: creare fiducia attraverso la disintermediazione* (2017/2772(RSP)), consultabile all'indirizzo: *www.europarl.europa.eu/doceo/document/TA-8-2018-0373_IT.pdf* (ultimo accesso 15 maggio 2021).

[685] Per un approfondimento in merito agli *smart contract* si rimanda a: PAROLA, MERATI, GAVOTTI, *op. cit.*, 684 ss.; GIULIANO, *op. cit.*, 990 ss.; CUCCURU, *op. cit.*, 110 ss.; CASEY, NIBLETT, *Self-driving contracts* (2017) 43 *Journal of Corporation Law* 1 ss.; FIDOTTI, *Nuove forme contrattuali nell'era della* Blockchain *e del* Machine Learning. *Profili di responsabilità*, in *Diritto e Intelligenza Artificiale*, cit., 325 ss.; RINALDI, Smart contract: *meccanizzazione del contratto nel paradigma della* blockchain, *ivi*, 343 ss.; PASSAGNOLI, *Il diritto civile al tempo dell'intelligenza artificiale: spunti per una problematizzazione*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, cit., 75 ss.; SANTOSUOSSO, *Intelligenza artificiale e diritto*, cit., 121 ss. Interessanti le considerazioni in merito al rapporto tra *smart contract* e Intelligenza Artificiale in FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, 2018, 441 ss.

[686] Detta tecnologia fa, infatti, parte della categoria delle *Distributed Ledger Technology* – DLT.

classico modello centralizzato, ove le informazioni sono raccolte tutte in un server e si diramano mediante il download dei *clients*.

Entrando più nello specifico, le transazioni eseguite vengono ordinate cronologicamente (grazie a delle marcature temporali o *timestamps*) e divise in blocchi. I blocchi sono dotati di un *header*, utilizzato per organizzare il *database* distribuito, al cui interno è contenuto: un codice hash univoco (che si compone di una striscia alfanumerica)[687] di tutte le transazioni registrate nel blocco; la marcatura temporale e il codice hash del blocco precedente. Si forma così una vera e propria catena di blocchi, da cui deriva la stessa espressione[688]. Da ciò ne discende una particolare resistenza agli attacchi esterni; difatti qualora si forzasse il sistema ciò comporterebbe una modifica del codice hash, spezzando dunque la catena. Inoltre essendo un registro distribuito, in cui i nodi sono protetti da una crittografia asimmetrica[689], sarebbe difficile per un soggetto esterno individuare e modificare tutte le copie conservate nei nodi, rivelando dunque il tentativo di manomissione.

Per poter essere aggiunto alla catena, ciascun blocco deve essere validato. Solitamente questo compito viene affidato a nodi a ciò incaricati sulla base di regole prestabilite dal protocollo informatico e condivise dai partecipanti alla *blockchain*. La modalità di validazione più conosciuta è la c.d. *Proof of Work* – la stessa utilizzata per i Bitcoin – che consiste in una competizione tra validatori (*miners*) ove il primo che risolve un complesso problema matematico è legittimato a inserire un nuovo blocco e a ricevere una ricompensa per il lavoro svolto[690].

---

[687] La funzione di hash permette di comprimere i dati in un formato composto da una sequenza, avente lunghezza determinata, di cifre e lettere, assegnate mediante un algoritmo di calcolo. Per un approfondimento si rimanda a GIULIANO, *op. cit.*, 999 ss.; D'ACQUISTO, NALDI, *op. cit*., 136 ss.

[688] Cfr. BELLINI, MARTINESCU, VASSALLI, *op. cit.*, 127 ss.; TEROLLI, Blockchain *e* compliance (Regtech), in *Diritto e Intelligenza Artificiale*, cit., 378 ss.; SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 11 ss.; GAMBINO, BOMPREZZI, *op. cit.*, 620 ss.; FIORELLI, CASSANO, *La rivoluzione tecnologica della* blockchain, in *Il diritto di internet nell'era digitale*, cit., 253 ss.; CAPACCIOLI, *La blockchain*, in *Tecnologia e Diritto*, II, cit., 371 ss.

[689] La cifratura a chiavi asimmetriche si compone di una chiave pubblica, conosciuta nel *network*, e di una privata che invece è conosciuta solamente dall'utente. Questa tecnica permette di assicurare la paternità di un messaggio e la sua integrità. V. BELLINI, MARTINESCU, VASSALLI, *op. cit.*, 136 s.

[690] In questo modo non solamente vengono incentivati i partecipanti alla *blockchain* a mettere a disposizione risorse computazionali, ma con detto meccanismo si crea il consenso alla validazione delle transazioni; ciò in quanto ogni *miners* può riconoscere l'impiego delle risorse computazioni necessarie a risolvere l'algoritmo matematico per poter validare il blocco. Questa non è l'unica modalità di aggiunta di nuovi blocchi alla catena, la scelta varia tendenzialmente in ragione della tipologia di *blockchain* scelta. Cfr. sul punto GAMBINO, BOMPREZZI, *op. cit.*, 622 ss.; SARZANA DI S. IPPOLITO, NICOTRA, *op. cit*., 26 ss.; BELLINI, MARTINESCU, VASSALLI, *op. cit*., 133.; CUCCURU, *op. cit.*, 108 s.; CAPACCIOLI, *La blockchain*, cit., 374 ss.

Oltre a quella usata per i Bitcoin, ci sono diverse tipologie di *blockchain* che si distinguono a seconda dei premessi di lettura e scrittura delle transazioni, nonché nelle modalità di validazione e aggiunta dei blocchi al sistema. Sono per esempio presenti delle *blockchain* pubbliche, in cui le transazioni sono visibili a tutti, e *blockchain* private, in cui invece l'accesso è consentito solo a determinati soggetti. Possono esservi dei sistemi senza permessi (*permissionless*), in cui chiunque può effettuare transazioni e divenire un validatore, e sistemi più centralizzati ove invece dette prerogative sono autorizzate da una o più entità centrali, che si occupano di gestire il sistema, conoscendo l'identità dei singoli nodi[691]. In quest'ultimo caso, solitamente, si tratta di sistemi ad uso privato, potendo comunque essere resi visibili all'esterno (divenendo dunque pubblici) a seconda delle finalità per cui sono concepiti[692].

Alla luce delle modalità di funzionamento è emerso come il sistema, per quanto complesso, presenti delle caratteristiche che possano soddisfare parte delle previsioni del GDPR poste a tutela dei dati personali. La immodificabilità di fatto della *blockchain* permetterebbe di garantire certezza e sicurezza delle transazioni e dei dati in essa registrati.

Detta tecnologia, potrebbe inoltre permettere una maggiore consapevolezza da parte degli interessati, i quali potrebbero verificare tutte le transazioni eseguite, oltre che permettere l'accesso ai propri dati solo da parte dei soggetti da essi autorizzati. La crittografia asimmetrica permetterebbe di limitare l'accesso da parte dei titolari ai soli dati per cui gli utenti abbiano effettivamente dato il consenso, così inverando il principio di minimizzazione previsto all'art. 5 del GDPR. Questa caratteristica potrebbe rivelarsi particolarmente utile per rispondere ad alcune criticità legate agli IoT. Come già si è avuto modo di evidenziare, queste applicazioni raccolgono costantemente una grande mole di dati degli utenti, spesso senza che questi ne siano pienamente consapevoli. Una limitazione, consistente nella selezione dei soli dati per i quali gli interessati abbiano espresso il consenso, permetterebbe di rendere tecnicamente

[691] BELLINI, MARTINESCU, VASSALLI, *op. cit.*, 134 s.; GIULIANO, *op. cit*., 996 ss.; FIORELLI, CASSANO, *op. cit*., 259 ss.

[692] Le *blockchain* si differenziano in ragione degli scopi per cui sono create. Ci sono sistemi specializzati come IOTA, pensato per l'IoT, o Ripple, che facilita la conversione tra valute. Oggi inoltre iniziano a diffondersi dei servizi ideati dai grandi player mondiali che permettano di utilizzare la *blockchain as a service*, dunque consentendo agli utenti di attivare sulle piattaforme detta tecnologia, così da poterne usufruire per le proprie organizzazioni. Per un approfondimento sul tema si rimanda a SARZANA DI S. IPPOLITO, NICOTRA, *op. cit*., 16 ss.; BELLINI, MARTINESCU, VASSALLI, *op. cit*., 145 ss.

implementabile anche in dette applicazioni il principio di minimizzazione. Inoltre, ad oggi gli IoT sono necessariamente collegati a *cloud server* per la raccolta e la conservazione dei dati; così facendo essi sono più soggetti a rischi di attacchi esterni alla sicurezza, essendo i server centralizzati, a differenza di quanto invece accadrebbe se venisse implementata una *blockchain*.

Oltre a questi indubitabili vantaggi, come anticipato, sono altresì presenti alcuni elementi di criticità, anche dal punto di vista strettamente tecnico. Allo stato attuale della tecnologia, infatti, la stessa complessità di funzionamento rende le *blockchain* di grandi dimensioni piuttosto lente nel funzionamento. Questo elemento potrebbe essere un ostacolo quasi insormontabile, in considerazione dell'estrema velocità di creazione e conservazione dei Big Data e, soprattutto, di richieste di transazioni derivanti dalle molteplici applicazioni *data driven* che si appoggerebbero al singolo *network*, finendo per congestionare il sistema.

Per ovviare a tale condizione sono nati alcuni progetti diretti a creare un *network* di *blockchain* tra loro interoperabili, creando così delle applicazioni decentralizzate complesse. In questo modo le applicazioni potrebbero utilizzare la *blockchain* appartenente al *network* più performante, senza il rischio di congestioni e velocizzando le stesse operazioni di validazione[693].

A queste considerazioni di natura tecnica deve necessariamente osservarsi come l'intero processo abbia un costo, tendenzialmente legato ai soggetti – i *miners* – che permettono di tenere l'integrità della catena validandone i dati. La metodologia più usata è, come visto, la *Proof of Work*, la quale crea fiducia dal momento i *miners* sono economicamente disincentivati alla frode; ciò in quanto essa si basa sull'utilizzo di potere computazionale necessario a risolvere problemi di decriptazione complessi in cambio di valuta. Questa metodologia tuttavia si dimostra poco funzionale nella prospettiva di utilizzo della *blockchain* per le applicazioni di Intelligenza Artificiale. Difatti essa si basa sul consumo di GPU e conseguentemente di energia elettrica dei partecipanti; questa condizione tuttavia la rederebbe insostenibile in termini di impatto ambientale, oltre che di scalabiltà, richiedendo sempre più potere computazione ai

[693] Progetti come Polkadot, Cosmos e ICON sono diretti proprio a trovare soluzioni standardizzate per rendere le *blockchain* maggiormente interoperabili e, dunque, tra loro in comunicazione. Per un approfondimento si rimanda ai rispettivi siti internet. Per Polkadot: *https://polkadot.network/*. Per Cosmos: *https://cosmos.network/*. Per ICON: *https://icon.foundation/?lang=en* (ultimo accesso 24 aprile 2021).

validatori, dovendo il sistema costantemente aumentare la complessità dei problemi da risolvere.

Tra le possibili soluzioni è stata avanzata la proposta di utilizzare la stessa AI per la validazione delle transazioni all'interno dei *network*. L'addestramento di AI alla decriptazione permetterebbe sicuramente di abbassare i tempi di validazione, oltre che i costi, tra cui quelli legati all'energia necessaria ad alimentare la catena e allo spazio per allocare la memoria.

Oltre a questi rilievi alcune perplessità sorgono in merito alla compatibilità della tecnologia in analisi con le disposizioni del Regolamento 679/2016 UE. In particolare, il funzionamento dei registri distribuiti pare confliggere: con i principi di limitazione della conservazione; con l'individuazione del soggetto titolare; con l'effettiva esercitabilità dei diritti di accesso degli interessati, in special modo il diritto alla cancellazione e alla modifica dei dati errati o incompleti.

A queste criticità si contrappongono alcune obiezioni fondate sulla considerazione per cui l'intero sistema della *blockchain* sarebbe caratterizzato dall'anonimia sia dei dati che dei soggetti i cui terminali rappresentano i nodi della catena. Questo sarebbe possibile proprio grazie alle chiavi crittografiche utilizzate, le quali attribuirebbero ai singoli *accounts* dei partecipanti delle successioni casuali dei numeri e lettere; del pari dovrebbero essere considerati anonimi i dati contenuti nei blocchi, i quali sono normalmente criptati e identificabili unicamente mediante codice hash. Queste misure di sicurezza si ritiene siano sufficienti e rendere i dati trattati nel sistema anonimi e dunque a escludere l'applicazione della normativa dettata dal GDPR[694].

Questa ricostruzione non pare tuttavia convincente. Come visto le tecniche di crittografia, per quanto avanzate, non sono ancora in grado di rendere definitivamente anonimi i dati sottoposti a detto processo. Inoltre, nello specifico caso della *blockchain* lo stesso Gruppo di Lavoro art. 29 ha evidenziato come sia possibile non solo risalire all'identità dei soggetti i cui terminali fungono da nodo, grazie all'uso di informazioni aggiuntive in grado di rendere comprensibile il meccanismo di attribuzione della chiave pubblica, ma anche alla stessa decifrazione della funzione di hash[695]. A ciò deve

[694] CHANG, *Blockchain: Disrupting data protection?* (2017) 150 *Privacy Laws & Business International Report* 2; GAMBINO, BOMPREZZI, *op. cit.*, 632 ss.
[695] Gruppo di Lavoro art. 29, *Opinion 5/2014 on Anonymization techniques*, 2014, 0829/14/EN, 20. Sul punto anche GIULIANO, *op. cit.*, 1007 ss.

aggiungersi come sono presenti, e sempre più efficaci, tecniche di *blockchain analytics* che rendono possibile l'identificazione del proprietario della chiave pubblica, e di conseguenza permettono di risalire alla storia delle transazioni che lo riguardano[696]. Si tratterebbe dunque non di dati anonimi, come tali sottratti all'ambito di applicazione del GDPR, ma di dati pseudonimi e dunque pienamente soggetti alla normativa europea[697].

Così chiarita la natura delle informazioni e dei dati raccolti all'interno della *blockchain*, è opportuno vagliare le criticità sopra elencate al fine di verificare l'effettiva compatibilità della tecnologia in analisi con le disposizioni normative.

Innanzitutto un problema evidente sorge per tutte quelle tecniche che abbiamo definito *permissionless*, ove dunque chiunque può accedere e partecipare al *network*, senza alcun effettivo controllo da parte di alcuna entità centralizzata, come invece può accadere nel caso di sistemi *permissed*. Proprio le *blockchain permissionless* sono al centro di un acceso dibattito. Tra le maggiori preoccupazioni che discendono da questa architettura vi è l'impossibilità di individuare uno specifico titolare, o più titolari, del trattamento. Per risolvere questa tensione si è proposto di ritenere tutti i soggetti proprietari di un terminale che funge da nodo della catena contemporaneamente titolari per le proprie transazioni e responsabili del trattamento per tutte le altre transazioni che sono presenti nella catena[698].

Questa soluzione si dimostra risolutiva solo sulla carta, attribuendo una qualifica che tuttavia non rispecchia la realtà dei rapporti all'interno della tecnologia. Lo stesso GDPR fornisce una definizione di titolare individuandolo nel soggetto che definisce le finalità e i mezzi del trattamento. Per la tipologia *permissionless* appare evidente come nessun nodo possa essere qualificato come tale; infatti non solo tutti i nodi sono uguali tra loro, non essendoci limitazioni di accesso e pre-identificazioni, ma soprattutto

---

[696] Questo tipo di tecniche vengono spesso utilizzate per verificare la presenza di attività illecite da parte di indirizzi apparentemente anonimi, come per esempio in casi di riciclaggio di denaro. Cfr. sul punto GAMBINO, BOMPREZZI, *op. cit.*, 633; BARCELO, *User Privacy in the Public Bitcoin Blockchain* (2007) 1 *Journal of Latex Class Files* 3; DE FILIPPI, *The interplay between decentralization and privacy: the case of blockchain technologies* (2016) 7 *Journal of Peer Production* 12, consultabile all'indirizzo: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689* (ultimo accesso 15 maggio 2020).

[697] V. SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 68 ss.; GAMBINO, BOMPREZZI, *op. cit.*, 634 ss.

[698] Di questa opinione GIULIANO, *op. cit.*, 1010 ss.; FINCK, *Blockchain and data Protection in the european union* (2018*) European data protection law review* 27; MOSER, *The Application & Impact of the European General Data Protection Regulation on Blockchains*, *R3 Reports*, 2017, 10. Contra SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 76 ss. In arg. GAMBINO, BOMPREZZI, *op. cit.*, 638, i quali ritengono che il titolare del trattamento dovrebbe essere individuato nel soggetto che raccoglie i dati personali che tratta per una determinata finalità in una *blockchain permissionless*.

nessuno degli *users* o dei *miners* avrebbe contezza dell'interno trattamento, rappresentandone solamente un'unità, né potrebbe gestire e dominare l'intera catena non avendo potuto predefinire mezzi e scopi del trattamento. Da ciò discende come mancherebbero le condizioni affinché i singoli utenti possano assumersi qualsiasi responsabilità, né rispondere al principio di *accountability*, essendo sforniti di mezzi di controllo e di monitoraggio dell'uso dei dati replicati.

Questa criticità sarebbe facilmente superabile nel caso delle architetture *permissed*, o in quelle ibride; in esse è presente un'entità centrale, facilmente identificabile, la quale gestisce l'interno *network*, controllando le identità dei singoli nodi, definendo l'architettura e le prerogative dei singoli nel sistema.

Un'ulteriore tensione nascerebbe con i principi di limitazione della conservazione e i diritti di cancellazione e di rettifica dei dati. Come visto, le modalità tecniche di funzionamento della *blockchain* ne rappresentano un grande punto di forza in tema di sicurezza e affidabilità dei dati e delle transazioni, essendo i blocchi all'interno del sistema sostanzialmente immodificabili e stockati in modo definitivo e potenzialmente perpetuo. Queste stesse caratteristiche tuttavia entrano in tensione con i principi sopra elencati; appare evidente come la disponibilità imperitura di dati e informazioni presenti all'interno della catena violi uno dei principi generali dei trattamenti, quello di limitazione. Inoltre la sostanziale immodificabilità dei dati registrati non permetterebbe l'esercizio dei diritti fondamentali degli interessati previsti all'art. 17[699].

In merito alla violazione del principio di limitazione, parte dei commentatori sostiene come sia sufficiente un'interpretazione estensiva del canone in parola per rendere detta tecnologia con esso compatibile. Si afferma, infatti, che i dati possano essere conservati fintanto che siano necessari a conseguire le finalità per cui sono trattati. Proprio facendo leva sul tenore letterale della disposizione si è ritenuto che la finalità, richiamata dalla disposizione, non sarebbe limitata a quella inerente allo specifico trattamento, ma piuttosto al corretto e complessivo funzionamento del sistema[700]. Ne discenderebbe

[699] V. GAMBINO, BOMPREZZI, *op. cit.*, 626 ss.; SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 84 ss. Sul punto GIULIANO, *op. cit.*, 1013 ss., ritiene comunque detta tecnologia compatibile con le disposizioni del GDPR in quanto qualora un utente dovese operare in un tale sistema, secondo un principio di auto-responsabilità, avrebbe valutato i rischi che la *blockchain* comporta e accettato le limitazioni ad alcuni diritti che il Regolamento europeo gli attribuisce.

[700] BERBERICH, STEINER, *Blockchain technology and the GDPR – How to reconcile privacy and Distributed Ledgers?* (2106) *European Data protection Law Review* 426.

allora la compatibilità di una conservazione *sine die*, dal momento che tutti i dati all'interno della *blockchain* sono necessari al suo corretto funzionamento.

Questa interpretazione tuttavia pare in parte collidere con un principio di proporzionalità che impone il bilanciamento degli scopi e dei mezzi necessari al loro raggiungimento. Sarebbe invece più efficace una soluzione tecnica che vada ad impedire l'identificabilità degli interessati verso l'esterno, come per esempio la previsione della distruzione delle chiavi crittografiche dopo un determinato lasso di tempo.

Quanto ai diritti di accesso e di modifica concessi agli interessati, se la cancellazione dei dati non appare possibile, si potrebbe propendere anche qui per una soluzione tecnica che permetta la rettifica delle informazioni all'interno della catena. Per poter procedere a una modifica dei blocchi registrati, validati e poi distribuiti è necessario il consenso della maggioranza dei nodi; se ciò appare difficile per le *blockchain permissionless*, sarebbe invece fattibile per quelle catene *permissed*, ove sono note le identità di tutti i nodi, e dove dunque si può procedere a dare attuazione alle istanze di modifica da parte degli utenti.

Da tutto quanto sopra esposto emerge chiaramente come le potenzialità di detta tecnologia, nonostante le possibili tensioni evidenziate, se correttamente implementate possano rivelarsi strumenti utili a promuovere la trasparenza e la sicurezza dei trattamenti. Quanto ai problemi tecnici, da alcune parti sono state avanzate proposte volte a valorizzare lo sviluppo di *blockchain* realizzate su criteri di interoperabilità, quindi consentendo a singole *blockchain* di dialogare tra loro; in questo modo si favorirebbe lo scambio di dati, di sicura qualità, in una sorta di rete confederata di *blockchain*[701].

Consapevoli di dette potenzialità si sono dimostrate anche le istituzioni europee le quali fin dal 2018 hanno posto in essere alcune iniziative volte a incoraggiare lo sviluppo di detta tecnologia in armonia con le norme del GDPR. Si pensi all'istituzione di una *Blockchain Partnership* europea e allo stanziamento di fondi del programma Horizon 2020[702]. Quanto alle tensioni tra la tecnologia in parola e il GDPR la

[701] V. SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 25; LAGANA TOSCHI, *What's the next step in Blockchain technology?*, 2 agosto 2018, consultabile all'indirizzo: *https://medium.com/hackernoon* (ultimo accesso 24 aprile 2021).

[702] L'Unione Europea ha stanziato dei fondi a sostegno del progetto DECODE; progetto che si prefigge di utilizzare la tecnologia *blockchain* per la protezione dei dati personali. Per un approfondimento in merito

Commissione ha prima istituito un Osservatorio e Forum europeo, e in seguito il Parlamento ha pubblicato uno studio dal titolo "*Blockchain and the General Data Protection Regulation – can distributed ledgers be squared with European data protection law*?". Dallo studio è emersa la necessità di elaborare specifiche linee guida da parte dell'EDPB e codici di condotta che rendano possibile una maggiore collaborazione tra pubblico e settore privato, al fine di implementare soluzioni tecniche che permettano di rendere maggiormente *compliant* con il testo regolamentare queste tecnologie[703].

Si sono costituti inoltre tavoli di lavoro a livello internazionale, quale per esempio il gruppo di lavoro ISO/TC 307 *Blockchain and distributed ledger technologies*, diretti all'individuazione di regole standard uniformi per lo sviluppo delle *blockchain*; ciò permetterebbe una maggiore interoperabilità e qualità dei sistemi, dando al contempo impulso alla diffusione delle stesse[704].

La tecnologia *blockchain*, alla luce di quanto fin qui considerato, pur dimostrandosi particolarmente utile nella tutela dei diritti degli interessati, al contempo non pare pienamente in linea con le disposizioni sancite dal GDPR. Al fine di ovviare a tali possibili tensioni, come visto, potrebbero trovare spazio tecniche che permettano di implementare nella stessa *blockchain* soluzioni di *privacy by design* e *by default*. Dal punto di vista giuridico, sebbene ad oggi sia complesso dare una valutazione complessiva e unitaria del fenomeno, componendosi questo di differenti tipologie di *blockchain*, sarebbe forse auspicabile una maggiore diffusione, quanto meno in alcuni settori, delle tipologie *permissioned*. Queste difatti rappresenterebbero una via di mezzo che permetterebbe di rendere la tecnologia maggiormente in linea con le disposizioni del GDPR, pur dovendo necessariamente sacrificare parte di quelle caratteristiche legate alla sicurezza del sistema derivanti proprio dalla diffusione e decentralizzazione della *blockchain permissionless*.

---

agli obiettivi e alle sperimentazioni già avviate si rimanda all'indirizzo: *https://decodeproject.eu* (ultimo accesso 24 aprile 2021). Sul punto si veda anche GAMBINO, BOMPREZZI, *op. cit*., 630 ss.

[703] Per un approfondimento si rimanda a GAMBINO, BOMPREZZI, *ibidem*; PAROLA, MERATI, GAVOTTI, *op. cit.*, 682 ss.

[704] SARZANA DI S. IPPOLITO, NICOTRA, *op. cit.*, 21 ss.

7. Considerazioni conclusive

La diffusione di applicazioni di Intelligenza Artificiale in grado di raccogliere e processare ingenti moli di dati ha fatto emergere, come visto, l'esigenza di una maggiore tutela dei diritti degli utenti che si vedono, spesso inconsapevolmente, soggetti a trattamenti aventi le più differenti finalità.

Una particolare attenzione meritano quei sistemi che operano una profilazione delle persone, inferendo dati personali anche da *dataset* di diversa natura, e dirette a influenzare, in modo più o meno diretto, le abitudini di consumo. A ciò si aggiungono particolari rischi in relazione ai trattamenti che utilizzano forme di profilazione a fondamento di decisioni automatizzate. Si pensi, come già si è avuto modo di evidenziare, a quegli algoritmi utilizzati per la concessione di beni o servizi pubblici, agli algoritmi utilizzati per determinare la concessione di un mutuo, all'utilizzo fatto nelle Corti americane del software COMPAS, o all'utilizzo che ne può essere fatto in ambito medico.

I settori in cui la tecnologia di AI si sta diffondendo sono sempre più numerosi e può facilmente prevedersi una loro pervasività nei diversi settori socio-economici.

Appare allora necessaria una attenta valutazione in merito alle soluzioni tecnico-giuridiche necessarie a garantire il rispetto dei diritti e delle libertà delle persone fisiche, in una prospettiva di bilanciamento tra i diversi interessi in gioco.

Come visto, il diritto ad ottenere una spiegazione, o meglio il diritto alla leggibilità dei risultati algoritmici, emergente dal testo del GDPR, ove effettivamente possibile, si dimostra fondamentale presidio a tutela degli interessati; difatti, solo qualora la *ratio* a fondamento delle decisioni prese sia intellegibile agli utenti, potranno essere effettivamente esercitabili anche i diritti ad essi concessi, *in primis* quello alla contestazione del risultato.

Tuttavia, pur aderendo a una interpretazione estensiva del testo del GDPR, e dunque istitutiva di un siffatto diritto, alcune difficoltà tecniche sorgono proprio in relazione alla concreta possibilità di comprensione degli *output* della macchina. Oltre alle questioni legate alle c.d. opacità intenzionale dei sistemi, si è evidenziato come proprio la complessità dell'architettura degli algoritmi non deterministici, e la enorme mole di dati da questi processati, fungono da ostacolo alla comprensione non tanto della logica generale quanto piuttosto del risultato singolarmente raggiunto dalla macchina.

A questo rilievo si aggiunge anche la considerazione per cui tra esseri umani e macchine vi sarebbe una assoluta incomunicabilità (c.d. opacità intrinseca) derivante dalla diversità delle logiche utilizzate, fondandosi il sistema algoritmico su di un principio di correlazione in luogo di quello di causalità; a cambiare è dunque lo stesso modo di concepire gli eventi e di analizzare le informazioni, e ciò sarebbe di ostacolo a un'effettiva comprensione della *ratio* a fondamento dei singoli *output*.

Alla luce di queste considerazioni, non potendosi arrestare il progresso scientifico, pare allora opportuno valorizzare soluzioni non solamente tecniche, ma anche giuridiche, che siano dirette da un lato ad aprire la "scatola nera" e, dall'altro, che permettano di limitare *ab origine* il rischio di soluzioni errate e, di conseguenza, di danni.

Accanto alle proposte operative evidenziate nel testo, di grande rilevanza si dimostrano le disposizioni che accordano la responsabilità per eventuali danni in capo al titolare o al responsabile del trattamento, secondo una lettura del precetto normativo che vede l'instaurarsi di un regime di responsabilità c.d. "aggravata". Tale ricostruzione dell'istituto permetterebbe di avvicinarsi maggiormente agli obiettivi perseguiti dalla normativa europea, aumentando la fiducia degli utenti nelle tecnologie digitali e, conseguentemente, incrementandone la diffusione sul mercato, senza tuttavia scoraggiare gli investimenti nel settore.

Se la possibilità di sviluppo di algoritmi trasparenti e una maggiore responsabilità gravante sui titolari e responsabili rivestono un ruolo importante nella prospettiva di una regolazione dei sistemi *data driven* che sia rispettosa dei diritti fondamentali dell'uomo, una particolare rilevanza dovrebbero assumere, a parere di chi scrive, gli strumenti che permettano di verificare la qualità dei dati utilizzati.

Avuto riguardo proprio alla estrema difficoltà di controllo nell'utilizzo di una enorme quantità di dati, si dimostra necessario operare una selezione nei *dataset* utilizzati per addestrare le applicazioni di Intelligenza Artificiale. L'uso di dati di qualità certificata limiterebbe i rischi di *bias*, aumenterebbe la trasparenza del sistema (potendo gli operatori avere accesso ai *dataset* utilizzati) e permetterebbe inoltre di rendere i sistemi maggiormente interoperabili.

In questa prospettiva di particolare interesse si mostrano allora le proposte di utilizzo della tecnologia *blockchain*. Nonostante le possibili tensioni con il GDPR, detta

tecnologia, se correttamente implementata, permetterebbe, come visto, di garantire la qualità e la sicurezza dei sistemi e dei dati da questi utilizzati, oltre che una maggiore trasparenza, essendo i blocchi della catena accessibili unicamente ai soggetti in possesso delle chiavi di hash necessarie a svelarne il contenuto.

Dal punto di vista della valutazione circa l'effettività delle disposizioni normative sono dunque emerse differenti criticità legate al rapporto spesso conflittuale tra funzionamento delle applicazioni digitali e regolazione normativa. Per l'argomento che qui ci occupa, il testo del Regolamento n. 679/2016 UE, pur rappresentando un buon punto di partenza, non si mostra pienamente idoneo a regolare il fenomeno digitale, non assicurando una efficace tutela dei diritti degli interessati, a fronte invece dei particolari rischi che discendono proprio dall'utilizzo di tecnologie *data driven*.

Su queste considerazioni generali di sistema si innesta una conclusiva riflessione in merito alle criticità riscontrate in uno tra i settori maggiormente coinvolto nella sperimentazione di soluzioni di Intelligenza Artificiale quale è quello dell'*automotive*.

CAPITOLO 5

La regolazione dei dati nella mobilità connessa e autonoma

SOMMARIO: 1. Auto a guida autonoma. Una tassonomia. – 2. Il governo dei dati nelle *smart cars*. – 2.1. Quale base giuridica di legittimità dei trattamenti. – 3. La sicurezza delle vetture, un problema anche di privacy? – 4. Alcune questioni sui dati generati dalle vetture. – 4.1. Quale tutela giuridica per i dati grezzi non personali. – 5. Considerazioni conclusive.

1. Auto a guida autonoma. Una tassonomia

Chiarita la cornice regolatoria e le criticità emerse in relazione al contesto digitale nel suo complesso, e in special modo alle tecnologie *data driven*, una particolare attenzione deve essere prestata all'ambito della mobilità connessa e autonoma. Difatti tra le applicazioni più promettenti nel panorama delle tecnologie di Intelligenza Artificiale un posto di rilievo occupano le auto a guida autonoma (*driverless car*)[705].

Il settore *automotive* è da sempre un banco di prova per le evoluzioni tecnologiche; non stupisce che attualmente siano già disponibili sulle vetture soluzioni che assistono il conducente, permettendo di automatizzare alcune funzioni di guida. Si pensi al *cruise control*, al *lane assist*, ai dispositivi di frenata automatica etc. Si tratta di sistemi elettronici, detti ADAS (*Advanced Driver Assistance Systems*)[706], la cui implementazione sulle vetture, prevista dalla normativa di omologazione, è divenuta

[705] Il concetto di auto a guida autonoma (*driverless car*, o *self-driving vehicles*) non è inteso a indicare una specifica tecnologia, caratterizzata da determinati elementi tecnici, quanto piuttosto l'applicazione di una o più tecnologie dirette a rendere l'apporto umano nella guida sempre più marginale. Si può parlare di *driverless car* nel momento in cui il guidatore umano diverrà un mero fruitore, un passeggero non avente più alcun ruolo nella mobilità veicolare. V. VEDASCHI, NOBERASCO, *Gli autoveicoli a guida autonoma alla prova del diritto*, in *Dir. pub. comp. eur.*, 2019, 775.

[706] Rileva Simonini come questi dispositivi siano espressione di una tendenza che vede le vetture come dei contenitori di apparati altrui; condizione questa sostanzialmente ignorata dal proprietario del veicolo. I sistemi ADAS sono, infatti, a tutti gli effetti dei software la cui proprietà intellettuale appartiene al produttore; ne consegue – evidenzia l'autore – che qualora quest'ultimo decidesse di non rilasciare più aggiornamenti, la vettura diverrebbe di fatto obsoleta e, sotto certi versi, inutilizzabile. Cfr. SIMONINI, *L'autovettura e le applicazioni digitali (APP)*, in *Danno e resp.*, 2021, 307.

obbligatoria[707] nella prospettiva di migliorare la sicurezza e diminuire così il numero di sinistri stradali[708].

Già da qualche anno sono attive sperimentazioni dirette a rendere totalmente automatizzata l'esperienza di guida.

Le prospettive di sviluppo di questa tecnologia sono considerevoli oltre che in termini di rientri economici per le case produttrici, anche a livello di sicurezza stradale. La diffusione di auto a guida autonoma permetterebbe, infatti, di diminuire in modo considerevole l'inquinamento, avendo un sistema di trasporto più razionale e ottimizzato, ma soprattutto di diminuire il numero di incidenti.

Dalla relazione in tema di mobilità intelligente, presentata nel 2016 dalla Commissione europea, è emerso come il 95% dei sinistri stradali sia attualmente imputabile a un certo grado di errore umano; di questa percentuale il 75% è causato unicamente da fattori umani, quali eccessiva velocità, disattenzione e uso di sostanze alcoliche o stupefacenti[709].

A questo dato, già significativo, si aggiunge anche la considerazione per cui l'introduzione di sistemi tecnologici di assistenza alla guida ha già contribuito a diminuire il numero dei sinistri[710], che dunque verrebbero considerevolmente ridotti in uno scenario ove a circolare su strada fossero unicamente *driverless car*[711].

---

[707] Si v. il comunicato stampa del Parlamento Europeo*, Incidenti su strada: obbligo di tecnologie salvavita a bordo*, 16 aprile 2019, consultabile all'indirizzo: *www.europarl.europa.eu* (ultimo accesso 5 giugno 2021).

[708] Si pensi per esempio al dispositivo e-call. Si tratta di un sistema automatico che in caso di incidenti di particolare gravità chiama i soccorsi trasmettendo alcuni dati necessari all'individuazione del veicolo. Questo dispositivo è reso obbligatorio dal Regolamento UE n. 758/2015, del 29 aprile 2015, relativo ai requisiti di omologazione per lo sviluppo del sistema e-call di bordo. All'art. 3 questa applicazione viene definita come «*un sistema di emergenza, composto di un equipaggiamento di bordo e dei mezzi per attivare, gestire e attuare la trasmissione eCall, attivato automaticamente attraverso sensori di bordo oppure manualmente, che invia, per mezzo delle reti di comunicazione mobile senza fili, una serie minima di dati e apre un canale audio basato sul 112 tra gli occupanti del veicolo e uno PSAP per il servizio eCall*».

[709] Relazione della Commissione, *Salvare vite umane: migliorare la sicurezza dei veicoli nell'UE*, 12.12.2016, COM (2016) 787 final.

[710] La Commissione, nel 2010, ha difatti rilevato come nonostante il numero di vittime della strada sia elevato (nel 2018 circa 25 mila persone hanno perso la vita a seguito di un incidente) tra il 2001 e il 2010 si è riscontrata una riduzione di incidenti mortali del 43%. Comunicazione della Commissione, *Verso uno spazio europeo della sicurezza stradale: orientamenti 2011-2020 per la sicurezza stradale*, 20.7.2010, COM (2010) 389 final. Tra il 2010 e il 2018 detta percentuale si è ridotta di un ulteriore 21%. Sono progressi di un indiscusso rilievo. Rimane in ogni caso ferma la necessità di accrescere ulteriormente la sicurezza stradale. Interessanti alcuni documenti presentati dalle Istituzioni europee ove si prospettano interventi diretti a raggiungere l'obiettivo molto ambizioso di "zero vittime". Si v. Commissione Europea, *Documento di lavoro dei servizi della commissione. Quadro dell'UE 2021-2030 per la sicurezza stradale – Prossime tappe verso l'obiettivo "zero vittime" ("Vision Zero")*, 19.6.2019, SWD (2019) 283 draft;

La spinta verso l'automazione dei sistemi di guida e delle infrastrutture (fino ad arrivare alle c.d. *smart cities*[712]) potrebbe inoltre generare notevoli vantaggi anche dal punto di vista del benessere sociale, trovando così un fondamento nell'art. 41, comma 3°, Cost[713]. Si pensi per esempio alla possibilità per le persone con disabilità (ma anche agli anziani o ai minorenni) di poter usufruire dei servizi offerti dalla mobilità autonoma, così permettendone una maggiore inclusione sociale[714].

A queste prospettive di crescita si accompagnano alcune criticità, tra cui potenzialmente il peggioramento della situazione stradale e delle condizioni di guida. Potrebbe, infatti, aumentare il numero dei veicoli circolanti, a fronte dell'aumento dei soggetti che possono farne uso, a cui seguirebbe, almeno fintanto che non verranno potenziate le infrastrutture, un corrispettivo aumento del traffico stradale. Del pari

---

Comunicazione della Commissione, *L'Europa in movimento – Una mobilità sostenibile per l'Europa: sicura, interconnessa e pulita*, 17.5.2018, COM (2018) 293 final. Interessante anche il comunicato stampa *Auto a guida autonoma in UE: dalla fantascienza alla realtà*, 15 gennaio 2019, consultabile all'indirizzo: *www.europarl.europa.eu* (ultimo accesso 5 giugno 2021).

[711] Si v. in arg. lo studio del Parlamento europeo, *Research for TRAN Committee, Self-piloted cars: the future of road transport?*, 2016, consultabile all'indirizzo: *www.europarl.europa.eu* (ultimo accesso 5 giugno 2021). Alla luce di questi dati la Commissione si è dichiarata favorevole sia a programmi volontari di valutazione della sicurezza delle vetture, quali Euro NCAP, sia all'introduzione di regole che permettano la circolazione di vetture autonome; consentendo queste un risparmio di vite umane, oltre che una conseguente diminuzione dei premi assicurativi. V. SIMONINI, *L'intelligenza artificiale guida le nostre vetture. Profili di responsabilità*, Modena, 2018, 121 ss.

[712] Il termine "*smart city*" viene usato per indicare un sistema di connessione *high-tech* ubiquitario che permette di connettere persone, informazioni ed elementi della città, con l'obiettivo di ottimizzare le risorse, pianificare le attività di manutenzione, migliorare la sicurezza e massimizzare i servizi offerti ai cittadini. Tutto ciò sarà reso possibile solamente ove tutte le infrastrutture critiche (quali per esempio, strade, gallerie, ponti, ferrovie, aeroporti, grandi edifici etc.) saranno connesse, così da poterne monitorare le condizioni. In questa direzione si stanno sviluppando alcuni progetti, tra cui quello elaborato dall'Università di Firenze (REPLICATE), che mediante un'applicazione fornisce ai cittadini informazioni in tempo reale sui trasporti, sui beni culturali, sulle strutture ospedaliere etc. V. NAZZARO, Privacy, smart cities *e* smart cars, in *Privacy digitale*, cit., 330 s.

[713] «*L'iniziativa economica privata è libera.*
Non può svolgersi in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà, alla dignità umana.
La legge determina i programmi e i controlli opportuni perché l'attività economica pubblica e privata possa essere indirizzata e coordinata a fini sociali». Art. 41 Cost.

[714] Cfr. NAZZARO, Privacy, smart cities *e* smart cars, cit., 332. Per una riflessione in merito alle potenzialità sociali del fenomeno si rimanda in particolare a SCAGLIARINI, "Smart roads" *e* "driverless cars" *nella Legge di bilancio: opportunità e rischi di un'attività economica «indirizzata e coordinata a fini sociali»*, in *Quaderni costituzionali*, 2018, 497 ss.; LOSANO, *Verso l'auto a guida autonoma in Italia*, in *Dir. inform*., 2019, 425 ss. Le auto a guida autonoma potrebbero, infatti, migliorare e favorire gli spostamenti per quegli individui che, a causa delle proprie condizioni fisiche, ne erano prima preclusi. Si pensi alle persone disabili che vedrebbero aumentare le proprie capacità di spostamento e di movimento «nel solco di un rinnovato principio di autonomia. In questa prospettiva la tutela del diritto alla mobilità e allo spostamento può essere intesa come una condizione per l'accesso agli altri diritti, e dunque come un vettore che l'inclusione piena ed effettiva», VANTIN, *Automobili a guida autonoma: un'inedita opportunità per le persone con disabilità fisiche?*, in Smart Roads *e* Driverless cars*: tra diritto, tecnologie, etica pubblica*, a cura di SCAGLIARINI, Torino, 2019, 59 ss.

potrebbero verificarsi inefficienze di sistema, quali mancati segnali tra vetture e tra queste e l'infrastruttura, errori di progettazione, ma anche solo, nelle prime fasi di automazione, possibili sinistri derivanti dalla disattenzione dei conducenti (chiamati a dover gestire numerose informazioni e nuove applicazioni) o dalla circolazione su strada di vetture tradizionali e autonome[715].

Nonostante siano stati fatti grandi progressi nei sistemi di assistenza alla guida, l'avvento di una mobilità totalmente automatizzata sembra tuttavia ancora lontano da raggiungere. Prima di poter assistere a una sua diffusione su larga scala dovranno essere risolte alcune criticità tecniche, legate al funzionamento dei sistemi di AI, oltre che giuridiche. Sarà certamente necessario provvedere sia al ripensamento della cornice normativa che regola la circolazione stradale, ove ad oggi si fa ancora riferimento alla figura di un guidatore umano[716], sia al potenziamento e, dove manchino, alla creazione di infrastrutture con cui le vetture dovranno comunicare[717].

Alla fattibilità tecnica si accompagna anche la necessità di rispondere a interrogativi giuridici in merito al regime di responsabilità civile applicabile in caso di sinistri e, per l'argomento che qui ci occupa, in relazione al governo dei dati, sia raccolti che prodotti dalle *driverless car*[718].

---

[715] In arg. MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 79. L'A. ricorda, infatti, che nonostante la guida autonoma prometta di limitare l'errore umano, questo non può essere pienamente escluso, potendosi anche traslare a un momento precedente la circolazione delle vetture; dunque alla stessa fase ingegneristica e di progettazione, a cui possono evidentemente conseguire sinistri a causa dal malfunzionamento del veicolo.

[716] Per quanto riguarda il nostro ordinamento si fa evidentemente riferimento alle disposizioni del codice della strada. Tuttavia sarebbe necessario un intervento in questa direzione di stampo internazionale. Sarebbe, infatti, auspicabile una modifica della convenzione di Vienna, che regola la circolazione stradale, al fine di prevedere la possibile circolazione di vetture anche in caso di assenza di un vero e proprio guidatore. Oltre a queste, un intervento innovativo/integrativo sarà richiesto per la disciplina in tema di immatricolazione delle vetture, a fronte della necessità di garantire un livello di sicurezza adeguato in relazione alle componenti tecniche ed elettroniche, oltre che in ragione dei rischi di intrusioni esterne al sistema.

[717] L'esigenza di valorizzare e di adeguare il patrimonio infrastrutturale esistente allo sviluppo tecnologico dovrebbe svilupparsi e concretizzarsi in due differenti archi temporali: entro il 2025 dovrebbero essere realizzati interventi sulle infrastrutture appartenenti alla rete TEN-T *Trans European Transport* e su tutta la rete autostradale; entro il 2030 i servizi dovrebbero essere estesi a tutta la rete SNIT (Sistema Nazionale Integrato dei Trasporti). V. MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 83.

[718] Cfr. VEDASCHI, NOBERASCO, *op. cit.*, 772, i quali evidenziano come il settore *automotive* sia tra quelli maggiormente complessi, in quanto soggetto a una regolazione composita che deve tenere conto dei diversi aspetti che coinvolgono la circolazione stradale. Tra questi, si pensi alle normative: sull'immatricolazione dei veicoli, sulle patenti di guida, sulle responsabilità (civile, penale e amministrativa), sulla circolazione stradale, sulla tutela dei diritti personali. In questo quadro qualsiasi fenomeno che si collochi fuori dal perimetro delle norme vigenti, tra cui alcune aventi anche carattere tecnico, deve essere considerato in linea di principio contrario alla legge e dunque non consentito. Ne

Prima di procedere nell'analisi è tuttavia opportuno chiarire cosa si intenda precisamente per auto a guida autonoma, dovendo fare una necessaria differenziazione tra le nozioni di auto connesse, già presenti sul mercato da una decina d'anni, e auto autonome (entrambi sistemi che rientrano nella categoria delle *smart cars*). Le due nozioni vanno, infatti, tenute distinte.

Per veicolo "connesso" si intende un mezzo di trasporto dotato di una strumentazione che permetta lo scambio di dati direttamente con altri veicoli e con l'infrastruttura[719], mediante una connessione di rete[720]. Di solito questa tipologia di veicoli possiede anche connessioni senza fili a corto raggio, utilizzate per esempio per comunicare con i *device* personali dell'utilizzatore. Non si tratta di una prerogativa limitata alle vetture più moderne; molti dei veicoli in circolazione possono essere facilmente connessi mediante una semplice dotazione che si collega alla rete di bordo tramite l'interfaccia standard, in origine pensata per la manutenzione e la diagnostica (ODB-II, in Europa)[721].

Diversamente i veicoli a guida autonoma possono essere definiti come mezzi di trasporto nei quali un sistema automatizzato sostituisce parzialmente o totalmente l'apporto umano alla guida della vettura[722]. Si tratta di veicoli necessariamente connessi, in quanto le diverse componenti tecnologiche integrate nel sistema interagiscono raccogliendo ed elaborando i dati, al fine di permettere alla macchina di circolare senza l'apporto di un guidatore umano. Potremmo, infatti, idealmente suddividere il processo di guida autonoma in due momenti: una fase di *perception*, nella quale i dispositivi (sensori, telecamere etc.) raccolgono i dati e una fase di elaborazione, in cui questi vengono trasmessi a una piattaforma interna al veicolo che, tramite algoritmi, prende le decisioni necessarie a permettere la guida[723].

---

discende come l'inerzia del legislatore condizioni fortemente il mercato, in quanto nessuna innovazione potrà essere diffusa siano a quando non sia stata oggetto di regolazione.

[719] Lo scambio dei dati può avvenire per esempio anche con la casa produttrice della vettura o con il gestore dei servizi *cloud* implementati nella vettura.

[720] MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 77 s., descrive i veicoli connessi come «mezzi in grado di comunicare con l'infrastruttura e con gli altri veicoli in strada, idonei a cooperare nel traffico scambiandosi informazioni e decisioni». In arg. anche GUARINO, *I veicoli connessi: punto focale dell'internet delle cose*, 2017, 2 s., consultabile all'indirizzo: *www.studioag.pro* (ultimo accesso 24 gennaio 2020).

[721] GUARINO, *ibidem*.

[722] MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, *ibidem*.

[723] I dati vengono trasmessi sotto forma di messaggi, che si differenziano solitamente in CAM o DENM in relazione al contenuto o alla circostanza per cui sono generati e inviati. V. MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, in Smart Roads *e* Driverless cars: *tra diritto, tecnologie, etica pubblica*, cit., 31.

Possono essere individuati differenti gradi di autonomia dei sistemi di guida. Sul punto la *Society of Automotive Engineers* (SAE)[724] ha pubblicato uno standard internazionale, in larga parte condiviso, che descrive i "livelli di autonomia" di un veicolo[725].

Il documento identifica sei livelli di automazione partendo dal livello 0, che corrisponde alla mancanza completa di strumenti di assistenza alla guida, al livello 5 che invece corrisponde alle *driverless car*, ove l'essere umano riveste un ruolo passivo, divenendo un mero passeggero.

Andando con ordine, il livello 1 comprende veicoli forniti di alcuni sistemi di assistenza alla guida. In questo livello sulle vetture è previso solamente un software che analizza l'ambiente esterno e fornisce alert, per esempio segnali acustici o visivi, che indicano al guidatore situazioni di pericolo. Si pensi, per esempio, al *cruise control* adattivo o al *lane centering*.

L'utilizzatore deve dunque mantenere il controllo della marcia e le mani sul volante al fine di poter riprendere prontamente il governo del veicolo (*hands-on mode*) in caso di situazioni di pericolo.

Nel livello 2 si assiste a una prima forma di automazione parziale, in quanto in condizioni di segnaletica orizzontale ben visibile, la vettura può gestire alcuni compiti in modo parzialmente automatizzato. I veicoli sono, infatti, muniti di software che intervengono su sterzo, acceleratore e frenata (*hands-off mode*), pur sempre sotto il controllo vigile del guidatore. Quest'ultimo, sebbene non sia tenuto a mantenere il costante controllo del veicolo (come nel livello precedente), è comunque chiamato a prestare una continua attenzione alle condizioni di guida, così da poter intervenire in caso di necessità. Attualmente sono già in commercio automobili aventi questo grado di automazione e fornite, per esempio, di sistemi di *lane keeping assist*, *traffic jam assist*, *auto steer*, *highway assist*, *driver assist* (diversamente denominati dalle case automobilistiche) etc.

---

[724] SAE, International Standard j3016, *Levels of driving automation*, recentemente aggiornati con nuove precisazioni in merito ai livelli 3 e 4 di automazione. Il testo è accessibile all'indirizzo: *www.sae.org* (ultimo accesso 16 giugno 2021). In dottrina si v. GUARINO, *op. cit.*, 3 s.; NAZZARO, Privacy, smart cities *e* smart cars, in *Privacy digitale*, cit., 329; VEDASCHI, NOBERASCO, *op. cit.*, 776 s.

[725] La classificazione, elaborata da un operatore privato e poi successivamente riconosciuta dalla NHTSA, non fa riferimento a standard tecnologici propri di ciascun modello, ma si fonda sul livello di intervento richiesto al conducente del veicolo, a conferma di come nel settore della guida autonoma si debba necessariamente fare riferimento all'applicazione di più modelli tecnologici, e non irrigidirsi su eventuali standard tecnico-ingegneristici. V. VEDASCHI, NOBERASCO, *op. cit.*, 775.

Il livello 3 viene definito di automazione condizionata. Da questo livello si può effettivamente parlare di sistemi di guida automatica. Il sistema di assistenza viene qui integrato nella vettura affinché gestisca, in condizioni ambientali ordinarie, gli aspetti della dinamica di guida (accelerazione, frenata e direzione) senza il controllo di un guidatore. La presenza umana rimane tuttavia ancora necessaria, in quanto è sempre richiesto l'intervento dell'uomo in situazioni problematiche, sia in caso di esplicita richiesta del sistema sia se egli stesso verifichi la presenza condizioni di pericolo. A differenza di quanto avviene nei livelli precedenti, la capacità di gestione del sistema permette al conducente di distrarsi del tutto dalla guida (*eyes-off mode*), salvo che il veicolo stesso non richieda un intervento. Ciò presuppone, evidentemente, che il guidatore abbia le capacità di reagire a situazioni di emergenza con la necessaria tempestività. Questo tipo di automazione è attualmente implementata in un modello di Honda disponibile in Giappone (Honda Legend Hybrid EX).

Il livello 4 è definito di alta automazione. Il software della vettura è in grado di gestire qualsiasi evenienza, reagendo autonomamente a situazioni anomale in assenza di intervento umano (*mind-off mode*). È tuttavia necessaria la presenza di determinate caratteristiche di segnaletica stradale, avendo verificato durante le prime sperimentazioni alcuni problemi di riconoscimento degli ostacoli in caso di scarsa visibilità dovuta a condizioni di maltempo[726]. Pur non essendo ancora accessibili al pubblico, appartengono a questo livello i primi robotaxi senza conducente sperimentati in Europa per il trasporto locale[727].

Infine, il livello 5 è quello ove si può propriamente parlare di *driverless car*. Un veicolo così classificato è, infatti, completamente autonomo, dunque in grado di funzionare in qualsiasi condizione meteorologica e di traffico. In questo contesto non viene più richiesta la presenza di un guidatore umano; quest'ultimo rivestirà un ruolo per così dire passivo, limitandosi a essere un mero passeggero e dunque occupando il

[726] Si veda l'interessante resoconto degli incidenti stradali ove sono state coinvolte auto a guida autonoma e, in particolare, il sinistro che ha coinvolto un modello di auto Tesla dotato di *autopilot* nel 2015 e l'incidente avvenuto ad una vettura Uber che ha investito e ucciso un pedone nel 2018. CIAMPANELLI, *ibidem*.

[727] Negli ultimi anni sono state avviate sperimentazioni di robotaxi senza alcun conducente. Si v. *Renault avvia la sperimentazione pubblica del servizio di Zoe cab autonomi*, 16 ottobre 2019, consultabile all'indirizzo: *www.ilsole24ore.com* (ultimo accesso 5 luglio 2021); PINI, *Tesla, guida autonoma dal 2019 e robotaxi dal 2020. Fantascienza o realtà?*, 23 aprile 2019, *ivi*.

tempo del viaggio per differenti attività, non essendo più chiamato a vigilare sull'operato della macchina[728].

Da quanto riportato emerge un elemento comune ai differenti livelli di automazione: la connessione e l'analisi dei dati raccolti[729]. È, infatti, evidente che per poter effettivamente guidare in modo autonomo i veicoli dovranno essere necessariamente dotati di applicativi e software che processino gli *input* loro inviati dall'ambiente esterno. Sarà necessario riconoscere le segnaletiche orizzontali e verticali, verificare la presenza di ostacoli sulla carreggiata, gestire le condizioni stradali e atmosferiche per una guida sicura etc. I veicoli saranno dunque dotati di sensori che acquisiscano immagini, le quali verranno poi processate all'interno del software composto da differenti algoritmi deputati a diverse funzioni[730]. Le vetture dovranno inoltre ricevere e trasmettere messaggi (quindi dati) sia tra loro (V2V) che con l'infrastruttura (V2I) e, si auspica in futuro, anche con gli altri utenti della strada (V2X)[731].

Ne discende allora come le auto a guida autonoma saranno evidentemente macchine connesse, chiamate a processare un'ingente mole di dati, sia provenienti da fonti esterne che generati dal loro stesso funzionamento, rientrando così a pieno titolo tra gli IoT. Come gli altri oggetti *smart*, anche le vetture costituiranno sistemi sempre connessi alla rete, e tra loro, ricevendo *input* dall'ambiente e comunicando i dati acquisiti a un server[732]. Chiaramente, per poter comunicare in sicurezza è necessario che i veicoli

---

[728] Interessanti le considerazioni di Di Rosa che evidenzia come dal punto di vista giuridico dovrebbe assumere maggiore rilevanza il concesso di *dynamic driving task*. Con tale espressione si indicano le funzioni di guida dinamiche, che comprendono, oltre a quelle meramente operative (accelerare, decelerare, frenare, sterzare), anche quelle che permettono alla vettura di rispondere agli stimoli esterni e decidere come adattare il proprio comportamento. Fino al livello 3, rimane il conducente umano il responsabile di queste funzioni, eseguendole direttamente o monitorandole. Dal livello 4, invece, queste vengono demandate in gran parte al sistema di guida automatico, per poi essere totalmente eseguite da esso, nel livello 5 dove l'automazione è completa e non c'è più necessità di alcun intervento umano. DI ROSA, Autonomous driving *tra evoluzione tecnologia e questioni giuridiche*, in *Dir. e quest. pubbl.*, 2019, 129.

[729] NAZZARO, Privacy, smart cities *e* smart cars, cit., 333 s.

[730] Come visto nella parte inziale del presente lavoro, le tecniche di Intelligenza Artificiale sono molteplici e ognuna è impiegata in diversi contesti a seconda degli obiettivi da raggiungere. Per esempio, nel caso del riconoscimento di immagini saranno utilizzati degli algoritmi di *deep learning*, quali le reti neurali, essendo quelli che hanno *performance* migliori per questa tipologia di compiti. Per un approfondimento in merito al funzionamento degli algoritmi di AI si rimanda *supra* al capitolo 1 del presente lavoro.

[731] Per esempio le macchine potrebbero ricevere delle informazioni che segnalino un traffico intenso sul percorso scelto e conseguentemente cambiare direzione per evitarlo. Le comunicazioni tra vetture saranno comunque necessarie alla stessa circolazione stradale, difatti le macchine potranno trasmettere messaggi anche per indicare guasti o malfunzionamenti e prevenire possibili incidenti.

[732] Il termine internet delle cose si riferisce ad «infrastrutture nelle quali innumerevoli sensori sono progettati per registrare, processare, immagazzinare dati localmente o interagendo tra loro sia nel medio

siano muniti di un identificativo univoco, come per esempio un numero di serie che sia riconoscibile in radiofrequenza[733]. La sicurezza dei sistemi e delle comunicazioni si rende indispensabile nel momento in cui le vetture si troveranno a "dialogare" con l'infrastruttura pubblica, così da minimizzare possibili rischi di attacchi esterni[734].

Come si è già avuto modo di evidenziare, nonostante il veloce progresso tecnologico e ingegneristico, attualmente si stanno sperimentando vetture fino al quarto livello di automazione. Se dunque siamo ancora distanti da un'automazione completa, sono tuttavia già diffuse e circolanti su strada delle *smart cars*[735].

Negli ultimi decenni si è assistito a un accentuato potenziamento del sistema di *infotainment* dei veicoli[736] (dunque della telematica di bordo), al fine non solo di offrire

---

raggio, mediante l'utilizzo di tecnologie a radio frequenza (ad es. Rfid, Bluetooth), sia tramite una rete di comunicazione elettronica». MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 72.

[733] La tecnologia di Identificazione a Radio Frequenza (Rfid), secondo la definizione presente nella Raccomandazione 2009/387/CE, prevede «l'uso di onde elettromagnetiche o l'accoppiamento di un campo reattivo nella porzione di radiofrequenza dello spettro per comunicare a partire da, o verso, un'etichetta mediante una varietà di sistemi di modulazione e codifica allo scopo di leggere, in modo univoco, l'identità di un'etichetta di radiofrequenza o altri dati in essa registrati». L'Identificazione a Radio Frequenza necessita, pertanto, di dispositivi simili ai *microchip*, i quali contengano un identificativo riconoscibile attraverso un lettore funzionante in radiofrequenza. Tali tecnologie si basano, dunque, sull'utilizzo di microprocessori che fungono da etichette (c.d. etichette intelligenti) dal momento che permettono di trasmettere mediante onde radio segnali leggibili da lettori compatibili. Mediante questa tecnologia è possibile trattare, anche senza che l'interessato ne sia consapevole, diversi dati finanche di natura personale o sensibile. Gli oggetti intelligenti risultano, infatti, costantemente connessi alla rete, potendo così raccogliere e trasmettere dati in maniera continuata, anche quando l'utente non ne sta facendo uso. È chiaro come questi dati potrebbero essere in un secondo momento analizzati e aggregati insieme ad altri, così consentendo una insidiosa profilazione dell'interessato. MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 73; ID., *Privacy e informazione nell'era dei Big Data*, in *Riv. sc. com. arg. giur.*, 2019, 84 s.

[734] In linea di principio non è necessario che un veicolo autonomo sia costantemente connesso alla rete, tuttavia in pratica è prevedibile che nessun veicolo rimanga completamente isolato, sia per esigenze di sicurezza, sia per la necessità di trasmissione di alcuni dati per lo stesso corretto funzionamento della rete stradale. Si pensi per esempio alla trasmissione di dati che indichino i livelli di traffico oppure alle comunicazioni tra vetture (V2V). Oltre alle esigenze di funzionamento dei veicoli, anche altri attori sono interessati a una connessione permanente, tra questi gli operatori telefonici, che così potrebbero sfruttare le potenzialità economiche dei dati raccolti e trasmessi fornendo servizi personalizzati agli utenti. V. GUARINO, *op. cit.*, 3.

[735] La stessa Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione, nel 2017, ha fornito una definizione. Nel documento si fa riferimento alle *smart cars* come a sistemi che forniscono funzionalità connesse, a valore aggiunto, al fine di migliorare l'esperienza degli utenti di auto o migliorare la sicurezza delle auto. Comprende casi di utilizzo come la telematica, l'*infotainment* connessa o la comunicazione intra-veicolare. Definizione presente nella guida *Cyber security and resilience of smart cars*, pubblicata dalla European union agency for network and information security (Enisa), consultabile all'indirizzo: *www.enisa.europa.eu* (ultimo accesso 6 luglio 2021). Si veda in dottrina LOSANO, *Il progetto di legge tedesco sull'auto a guida automatizzata*, in *Dir. infrom.*, 2017, 1 ss.; NAZZARO, Privacy, smart cities *e* smart cars, *ibidem*.

[736] Rileva Simonini come le vetture stiano divenendo sempre più dei grandi *smartphone*. Queste sono state negli anni sempre più dotate di strumenti che non solo forniscono al guidatore assistenza durante la guida, ma che permettono, grazie alla connessione di rete, l'utilizzo di servizi di intrattenimento offerti dal fabbricante o da terzi. Cfr. SIMONINI, *L'autovettura e le applicazioni digitali*, cit., 307.

assistenza in caso di incidenti, come nel caso dei dispositivi che trasmettono alcuni dati direttamente alla polizia stradale, ma anche per fornire servizi, quali la ricerca di un parcheggio, o di controllo da remoto dello stato del veicolo; tutti servizi che necessitano una connessione di rete e che rappresentano un primo, fondamentale, passo verso sistemi di guida autonomi[737].

Dunque, attualmente sono già circolanti sistemi di guida intelligenti, seppure non autonomi (o per lo meno non totalmente), i quali, archiviando e processando i dati raccolti durante l'uso, non solo permettono di migliorare le performance di guida, ma anche di offrire nuovi servizi su misura per il singolo conducente. Basti pensare ai sistemi di tracciamento satellitare che permettono non più solamente il funzionamento del navigatore, ma anche di rilevare il traffico e le condizioni climatiche sul percorso. A questi si aggiungono strumenti che monitorano il funzionamento delle componenti del veicolo e memorizzano i dati da questo prodotti, quali la velocità, lo stato di frenata, l'angolo di sterzata, il posizionamento delle cinture di sicurezza, fino allo stile di guida, così da permettere interventi efficienti e mirati in caso di guasti o malfunzionamenti, sia una maggiore personalizzazione e potenziamento delle prestazioni.

Non si tratta di prospettive futuristiche, il controllo delle condizioni e dello stile di guida, mediante la raccolta di una serie di dati grazie a delle "scatole nere" installate sul veicolo, è già da qualche tempo utilizzato dalle compagnie assicurative per parametrare il premio annuale[738].

Alcuni passi sono dunque stati fatti, tuttavia la strada è ancora lunga.

È evidente che per raggiungere l'obiettivo di una mobilità completamente autonoma sia necessario primariamente rinforzare il sistema di connessione delle vetture, oltre che – naturalmente – creare un'infrastruttura digitale diffusa in tutto il territorio, quanto meno dell'Unione Europea, che permetta effettivamente ai veicoli connessi di circolare.

Sul punto la Commissione europea ha sottolineato l'importanza strategica del settore *automotive* per il rilancio dell'industria europea, auspicando lo sviluppo dei veicoli cooperativi, connessi e autonomi, e rilevando come la cooperazione, automazione e la

[737] Si assiste a una transizione dai sistemi di *infotainment* (composti, per esempio, da navigatori, sensori di parcheggio, chiavi intelligenti, comandi vocali, etc.) a sistemi di guida automatica, che naturalmente si fondano su di una estesa connessione. MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 76.
[738] NAZZARO, *Macchine intelligenti* (smart cars): *assicurazione e tutela della privacy*, in *Dir. merc. ass. fin.*, 2018, 77 ss.; ZHANG, *Who owns the data generated by your smart car?* (2018) 32 *Harvard J. L. & Tech.* 300.

connessione non siano da considerare delle tecnologie alternative, rinforzandosi reciprocamente, e prospettando uno scenario di collegamento funzionale[739].

In Italia i primi interventi nella prospettiva di una completa digitalizzazione prendono corpo nel 2016, con la presentazione del documento del Ministero delle Industrie e dei Trasporti dedicato alle *smart road*, dove vengono sintetizzati gli standard funzionali necessari a permettere un adeguamento tecnologico delle infrastrutture esistenti[740].

Alla discussione seguì la legge di Bilancio del 2018[741], nella quale sono stati stanziati due milioni di euro per la trasformazione digitale delle strade, al dichiarato scopo di promuovere le sperimentazioni di guida connessa a automatica[742]. Infine, nel 2018 è stato adottato il Decreto Smart Road recante "*modalità attuative e strumenti operativi della sperimentazione su strada delle soluzioni di smart road e di guida connessa e automatica*"[743].

Il documento si mostra particolarmente interessante. Oltre che alle disposizioni regolanti le richieste di autorizzazione alla sperimentazione su strada[744], esso rivolge una particolare attenzione proprio alle *smart road*, evidenziando la necessità di una trasformazione digitale delle strade al fine di dotarle di sistemi intelligenti in grado di monitorare il flusso stradale e dialogare (mediante lo scambio di dati) con le vetture[745].

---

[739] MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 78.

[740] MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 77. Si veda anche il comunicato ufficiale, modificato da ultimo il 1° agosto 2016, *Smart road, veicoli connessi e mobilità del futuro*, consultabile all'indirizzo: *www.mit.gov.it* (ultimo accesso 5 giugno 2021). Si rimanda anche al documento presentato dal ministero dei trasporti, *Standard funzionali per le Smart-Road*, 22 giugno 2016, *ivi*.

[741] Legge n. 205 del 27 dicembre 2017.

[742] All'Italia la Commissione europea ha destinato 6,5 miliardi di euro, dei circa 30 complessivi, per finanziare adeguamenti tecnologici della rete stradale. Cfr. *Smart road, veicoli connessi e mobilità del futuro*, cit.

[743] Decreto del Ministero delle Infrastrutture e dei trasporti del 28 febbraio 2018.

[744] Per un approfondimento in merito all'iter del procedimento autorizzatorio si rimanda a SCAGLIARINI, *La sperimentazione su strada pubblica dei veicoli autonomi: il "decreto* smart road*"*, in Smart Roads *e* driverless car: *tra diritto, tecnologie, etica pubblica*, cit., 18 ss.

[745] Evidentemente il potenziamento della rete stradale permetterebbe di migliorare l'efficienza dei trasporti e la sicurezza, oltre che essere strumentale alla circolazione delle *driverless car*. Il processo per così dire di "ammodernamento" della rete richiede ingenti investimenti, di cui i due milioni stanziati nella legge di bilancio non paiono sufficienti. Nel decreto viene, dunque, previsto come le spese di questo processo siano poste a carico del concessionario o dell'ente gestore, i quali le imputeranno, insieme a quelle di manutenzione delle infrastrutture, a costi di investimento di cui tenere conto in sede di convenzione. Cfr. SCAGLIARINI, *La sperimentazione su strada pubblica dei veicoli autonomi*, cit., 17; MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 77.

A livello europeo la Commissione ha avviato un progetto diretto allo sviluppo dei c.d. C-ITS (*Cooperative Intelligent Transport Systems*)[746]; si tratta di vetture, anch'esse qualificabili come *smart cars*, il cui sistema si fonda sullo scambio di dati e informazioni all'interno di un'architettura a chiave pubblica (*Public Key Infrastructure*, PKI).

Dal momento che i veicoli trasmetteranno e riceveranno dati, al fine di creare un sistema di comunicazione affidabile è subito parso necessario garantire l'autenticità dei messaggi, verificandone la provenienza e l'integrità. Per permettere questo livello di sicurezza delle comunicazioni, si prevede che ogni veicolo facente parte del sistema C-ITS dovrà essere identificato (mediante un'iscrizione gestita da un ente, *enrolment authority*) e autorizzato da un'autorità (*authorisation authority*) mediante l'attribuzione di un certo numero di certificati digitali con cui verranno firmati i messaggi inviati[747].

Per garantire la riservatezza degli utilizzatori questi messaggi dovranno evidentemente essere sottoposti a tecniche di crittografia che permettano la pseudonimizzazione del mittente e al contempo garantiscano la verifica dell'autenticità della fonte e del contenuto. In questo modo coloro che ricevono i messaggi ne potranno verificare la provenienza e l'integrità, controllando i certificati univocamente associati a un veicolo autorizzato, rimanendo allo stesso tempo garantito un certo livello di riservatezza per il guidatore.

2. Il governo dei dati nelle *smart cars*

Appare dunque chiara la necessità di operare un'attenta ponderazione in merito ai dati raccolti e trasmessi dalle vetture connesse e autonome[748]. Queste – come visto – sono composte da un insieme di *electronic control units* diretti a percepire l'ambiente

[746] NAZZARO, Privacy, smart cities *e* smart car, cit., 334; MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, cit., 30, ricorda come «i veicoli autonomi sono complessi sistemi su ruote, costituiti da un insieme di *electronic control units* (ECU), che hanno la capacità di percepire l'ambiente circostante e utilizzano tecnologie di guida che riducono l'interazione del guidatore, sino al livello di navigare senza l'intervento umano».

[747] MENEGHETTI, *La* privacy *del guidatore al tempo della mobilità intelligente*, in *Dir. mer. tec.*, 2017, 4 s.

[748] In arg. Miniscalco evidenzia come alcuni dati sono oggetto di trasmissione V2V o V2I, mentre altri sono immessi nel sistema mediante il collegamento con gli *smart devices* degli utilizzatori dei veicoli e, in futuro, degli altri utenti della strada. MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, *ibidem*.

esterno mediante sensori che raccolgono informazioni, le quali saranno oggetto di una pluralità di trattamenti, tra cui quelli posti in essere mediante algoritmi di Intelligenza Artificiale. Inoltre, ulteriori dati saranno trasmessi ai sistemi presenti nella vettura dai *device* degli utilizzatori e, in futuro, anche dagli utenti della strada.

Tutti questi dati sono arricchiti da quelli "generati" dalla vettura, cioè dati tecnici raccolti e anch'essi trasmessi[749]. Si stima che un veicolo autonomo possa generare più di un Terabytes di dati l'ora[750] e che entro il 2030 il valore di questi possa superare gli 1,5 trilioni di dollari[751].

Inoltre, per garantire un'adeguata sicurezza è necessario che i messaggi abbiano una provenienza certa e pertanto, pur se successivamente cifrati o sottoposti a procedimenti di pseudonimizzazione, essi potranno essere sempre collegabili alla vettura, identificata per esempio con una chiave PKI. Ne discende allora come anche i dati prettamente tecnici di funzionamento, se combinati con altri, possono portare all'identificazione specifica del veicolo e, grazie alla chiave PKI, alla persona fisica che utilizza lo stesso.

Nel 2015 un gruppo di ricercatori della University of Washington ha dimostrato come basandosi solamente su dati grezzi generati dai sensori di bordo sia possibile identificare in modo univoco la persona alla guida di una vettura. Sebbene l'esperimento sia stato compiuto su di un numero ristretto di variabili di soli quindici partecipanti (37 singoli dati prodotti da sedici sensori presenti su di una berlina prodotta nel 2009), l'analisi dei dati (tra cui l'angolo di sterzata, i giri del motore, coppia e

[749] Si tratta, come visto, di dati di differente natura, che potrebbero essere trattati per diversi usi, tra cui per esempio: finalità di marketing, profilazione degli utenti, miglioramento del trasposto pubblico mediante una gestione più razionale del traffico, miglioramento dei sistemi di AI, ricostruzione delle dinamiche incidentali ad uso giudiziario o per il settore assicurativo, ottimizzazione della manutenzione del veicolo etc. Cfr. l'interessate quadro delineato da ZHANG, *op. cit.*, 303 s. È evidente, dunque, che al crescere dei livelli di automazione crescerà anche il volume di dati, a cui diversi soggetti avranno accesso, prodotti e analizzati dalla vettura per poter funzionare correttamente. V. VEDASCHI, NOBERASCO, *op. cit.*, 794.

[750] Cfr. XU *et al.*, *Internet vehicles in Big Data Era* (2018) 1 *Journal of automatica Sinica* 19 ss. e spec. 28 in cui gli Autori evidenziano come «to make the self-driving come to life, a convergence of big data is required, including the data from on-board sensors, e.g., cameras, radar, Lidar, GPS, and information shared from other connected vehicles, e.g. road condition, traffic information etc. It is predicted that the self-driving vehicle can generate over 1 Tera Bytes data per hour. With all the data available, efficient learning schemes, and massive computing and storage power, the vehicles will be capable of perceiving the environments, and make actuation decisions to drive safely and efficiently».

[751] Si veda lo studio della McKinsey dal titolo *Car data: paving the way to value-creating mobility*, 2016, 5, consultabile all'indirizzo *www.the-digital-insurer.com* (ultimo accesso 5 luglio 2021).

potenza istantanea) mediante algoritmi di AI ha permesso di riconoscere gli stili di guida e, di conseguenza, il singolo guidatore con un'accuratezza del 100%[752].

Emerge allora chiaramente come grazie alle capacità di inferenza dimostrate dalle tecniche di *data mining*, anche da meri dati tecnici sia possibile profilare il singolo guidatore, portando a una forma di identificazione che potremmo quasi definire biometrica[753].

Oltre ai dati generati dal guidatore, o trasmessi dai propri *device*, non va dimenticato come i sistemi autonomi e connessi raccoglieranno anche ulteriori dati, quali ad esempio le immagini degli utenti che si trovano sulla strada e che sono captate delle telecamere intelligenti. Si tratta evidentemente di una mole considerevole di dati che darà origine a numerosi trattamenti, alcuni dei quali non strettamente legati al funzionamento della vettura, di cui gli utilizzatori potrebbero non essere pienamente consapevoli.

Sul punto, la FIA (Federazione Internazionale dell'Automobile) ha commissionato uno studio diretto a rivelare la quantità e la composizione dei dati scambiati dai veicoli in rete[754]. Sulla scorta dei risultati trovati è stato lanciato un progetto[755] diretto a

---

[752] Nell'esperimento è stato chiesto ai partecipanti di effettuare tre giri attorno a un parcheggio (chiuso e senza traffico), effettuare manovre di parcheggio e cambiare corsia. In un secondo momento gli è stato chiesto di percorre circa 80 chilometri in condizioni di guida normale; naturalmente tutti i partecipanti hanno effettuato lo stesso percorso a Seattle. In questo contesto il numero di persone tra cui individuare quella corretta era evidentemente piccolo, ma in proporzione lo era anche lo stesso *dataset* utilizzato. V. GUARINO, *op. cit.*, 7.

[753] GUARINO, *ibidem*.

[754] Lo studio è stato attuato mediante un sondaggio proposto agli utenti in dodici Paesi, oltre che di uno studio tecnico elaborato dall'ADAC (Automobil club tedesco) che ha dimostrato come sia i veicoli ad alimentazione tradizionale, sia quelli elettrici, possono trasmettere dati personali dei passeggeri, e dunque possono operare una profilazione degli stessi. I dati raccolti dalle vetture sono vari, tra cui le modalità di guida, le destinazioni (tramite le ricerche compiute dal GPS per i veicoli tradizionali), lo stato della vettura (tra cui la tensione delle cinture di sicurezza, lo stato delle luci, i chilometri percorsi etc.), i dati sincronizzati con il sistema di intrattenimento etc. È evidente che le informazioni raccolte sono particolarmente invasive. Sebbene questi studi abbiano confermato la quantità e la natura dei dati raccolti, l'elemento maggiormente significativo emerso sono le considerazioni degli utenti. Il 90% di questi ritiene che i dati siano di sua proprietà e vorrebbe poter attivare o disattivare la connessione del veicolo. Di poco inferiore (76%) risulta la percentuale di coloro che vorrebbero poter decidere quando, e per quanto tempo, condividere i propri dati. Significativa è infine la percentuale (95%) di coloro che ritengono sia necessaria una legislazione che protegga i propri dati personali trattati nelle vetture autonome e connesse. Cfr. *FIA reveals what data is being tracked and how the public reacts to connected cars*, 2015, consultabile all'indirizzo: *www.fia.com* (ultimo accesso 5 luglio 2021).

[755] Il progetto si chiama My Car My Data. Nel sito internet dedicato si afferma: «Data is the new currency. While users may not be shy about sharing data anymore, *we* believe that they should get the most out of it. By allowing various service providers to compete to offer added value to the connected car, we encourage innovation and ensure drivers can freely choose any application they wish over the lifetime of their vehicle – and opt-out whenever they want to. In a monopoly situation, the lone service provider would *be* able to dictate what services can be offered and for which price. Any application you

incrementare la consapevolezza degli utenti, da cui è altresì emersa la necessità di prevedere una normativa che regoli in modo puntuale il trattamento dei dati generati durante la guida delle vetture[756].

È evidente come sia necessaria una valutazione in merito al governo dei dati raccolti e trattati all'interno della *smart area*, a fronte dei rischi non solamente di una sorveglianza continua e di una profilazione particolarmente invasiva dei cittadini, ma anche dei danni derivanti da un loro uso illecito.

Il governo dei dati generati nel settore *automotive* è una questione ancora dibattuta e complessa a cui le Istituzioni dovranno dare risposta. Ad oggi, escludendo alcuni documenti programmatici e pareri di comitati consultivi, non sono infatti ancora state risolte le tensioni che la guida connessa mostra avere con le normative di riferimento, *in primi*s con il Regolamento n. 679/2016 UE[757].

È utile chiarire innanzitutto come, grazie alle tecniche di *data mining* e allo stesso funzionamento della trasmissione dei messaggi, gran parte dei dati raccolti e trattati dalle auto a guida autonoma dovrà essere considerata come dato personale, secondo quanto previsto dall'art. 4 GDPR. Come visto, infatti, la nozione di dato personale è molto ampia e presenta una natura relazionale; si va arricchendo nel tempo in ragione del progredire delle tecnologie, acquistando così significato[758]. Dunque, proprio la possibilità di identificazione di un soggetto grazie all'uso di algoritmi che processano differenti informazioni rende molti dei dati, anche tecnici, prodotti dalle automobili rientranti nella categoria dei dati personali[759]. Di conseguenza il loro trattamento per essere lecito richiede il rispetto delle diposizioni del Regolamento n. 679/2016 UE.

---

install would have to *be* either from the manufacturer or from a subcontractor they chose». Per un approfondimento si rimanda all'indirizzo: *www.mycarmydata.com* (ultimo accesso 10 luglio 2021).

[756] In argomento si veda GAETA, *op. cit.*, 156.

[757] Nonostante, per quanto riguarda le iniziative prese nel nostro ordinamento, il Decreto *smart road* preveda l'istituzione di un organo ("Osservatorio Smart Road") avente il compito di promuovere la sperimentazione nel settore, in tema di gestione dei dati trattati dai veicoli il documento non presenta in realtà alcun chiarimento. V. LOSANO, V*erso l'auto a guida autonoma*, cit., 425 ss.

[758] Per la nozione di dato personale si v. *supra* il capitolo 3 del presente lavoro.

[759] Si pensi per esempio ai dati di localizzazione di una vettura che mostrino una certa ricorrenza verso, per esempio, cliniche mediche specialistiche; questi dati, se combinati, possono dunque potenzialmente rivelare informazioni non solo personali, ma anche sensibili del guidatore o di altri soggetti che utilizzano la vettura. In arg. ZHANG, *op. cit.*, 304. Si veda anche JANEČEK, *Ownership of personal data in the Internet of Things* 2018 *Computer Law & Security Review* 1039 ss.

Sul punto lo stesso Gruppo di Lavoro art. 29 ha affermato come all'interno dei sistemi C-ITS vengono trattati dati personali degli automobilisti[760] e che pertanto deve trovare piena applicazione la normativa europea che impone il rispetto dei principi generali di trattamento (tra cui il principio di trasparenza, di minimizzazione, di finalità e di necessità), ma è altresì necessario individuare il titolare del trattamento e un'adeguata base giuridica che lo renda legittimo[761].

Sul tema della titolarità dei trattamenti il Gruppo di Lavoro ha avanzato la proposta di utilizzare il modello di contitolarità, così come previsto dall'art. 26 GDPR[762]. Pertanto, tutti gli attori coinvolti nella direzione, gestione e vigilanza dei dati richiesti dal sistema dovrebbero essere ritenuti titolari del trattamento. Questa interpretazione troverebbe fondamento sulla considerazione per cui tutti i trattamenti posti in essere, sebbene aventi una differente finalità, concorrano alla realizzazione di un fine ultimo rappresentato dal funzionamento del sistema di guida autonoma della vettura; pertanto i diversi attori della catena di trattamenti dovrebbero essere considerati contitolari essendo tutti animati da un fine comune.

Questa soluzione, tuttavia, non sembra pienamente convincente.

Una prima criticità emerge in relazione alla necessità di coordinare detto modello di titolarità con il più generale modello di *governance* scelto per il sistema di guida[763], operazione questa che non si dimostra agevole. Difatti, dal momento che difficilmente sarà possibile dettagliare *ex ante* i diversi scopi perseguiti dai singoli attori facenti parte della lunga catena di trattamenti, non sarà sempre possibile individuare con certezza i

[760] Si fa riferimento all'Opinion pubblicata nel 2017. Si v. Gruppo di Lavoro art. 29, *Opinion 3/2017 on processing personal data in context of cooperative intelligent transport systems (C-ITS)*, 4 ottobre 2017, 4, consultabile all'indirizzo: *ec.europa.eu* (ultimo accesso 5 luglio 2021).

[761] MENEGHETTI, *op. cit.*, 6; NAZZARO, Privacy, smart cities *e* smart cars, cit., 334.

[762] Art. 26, reg. UE n. 679/2016, "Contitolari del trattamento": «*1. Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente 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, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.*
2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento».

[763] MENEGHETTI, *op. cit.*, 10.

diversi ruoli e le conseguenti responsabilità[764]. Si ricorda che la complessità dell'architettura del sistema, da un lato, e l'ampiezza dei dati trattati, dall'altro, rende complesso, così come per ogni sistema di *machine learning*, determinare a priori le finalità di tutte le operazioni di trattamento.

Proprio l'eterogeneità dei possibili usi dei dati raccolti non sembra dunque compatibile con un regime di contitolarità, non potendo il titolare di un singolo segmento della catena avere un'effettiva conoscenza, né controllo, dell'intero sistema[765].

In secondo luogo, pur ammettendo che tutti gli attori condividano un obiettivo finale, non sembra questo un elemento sufficiente a poter ritenere applicabile la disposizione dell'art. 26 GDPR. La stessa previsione normativa non sembra conciliabile con una tale considerazione; difatti ogni singolo attore pone in essere un autonomo trattamento per un proprio fine e non ha accesso ai trattamenti altrui, né può concorrere in alcun modo a determinarne le finalità e i mezzi per perseguirli.

Lo schema della contitolarità non sembra dunque rispondere in modo adeguato ai rapporti esistenti tra i diversi attori coinvolti nella mobilità autonoma. Autorità pubbliche, produttori di veicoli, programmatori di software, società di telecomunicazioni etc. dovranno piuttosto essere considerati ognuno titolare di un trattamento distinto e autonomo, di cui saranno evidentemente chiamati a rispondere[766].

2.1 Quale base giuridica di legittimità dei trattamenti

Complessa appare inoltre l'individuazione di un'idonea base giuridica di legittimità per i trattamenti, così come previso dall'art. 6 GDPR.

---

[764] Interessante il riferimento compiuto da Miniscalco alla "*smart area*" modenese. Per comprendere quanti attori differenti entrino in gioco si pensi che «il titolare dei trattamenti dei dati personali oggetto di raccolta, elaborazione e ogni altra operazione posta in essere nell'ambito del processo di sperimentazione della guida autonoma è l'Università degli studi di Modena e Reggio Emilia, per i dati raccolti e comunicati dalle infrastrutture installate nella *smart area* modenese […] è il Comune di Modena; quest'ultimo, peraltro condivide i dati raccolti con l'Università che, per tale ragione, potrebbe qualificarsi come responsabile esterno del trattamento, ovvero, qualora determini essa stessa le finalità e i mezzi del trattamento, di co-titolare o, al più, di (autonomo) titolare». V. MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, cit., 33.

[765] MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, cit., 34.

[766] MENEGHETTI, *op. cit.*, 11.

Quanto al consenso dell'interessato si è già avuto modo di evidenziare le criticità legate alla mancanza di effettiva consapevolezza degli utenti, finendo questo col divenire un mero simulacro che non ne assicura più un'effettiva autodeterminazione. Dagli studi comportamentali si è visto, infatti, come il consenso sia prestato inconsapevolmente per diverse ragioni: perché l'informativa è predisposta in modo eccessivamente tecnico e complesso; perché l'utente si trova sovraesposto a richieste continue; perché dal punto di vista cognitivo non è agevole valutare con cognizione probabili conseguenze future negative, dando preferenza ai vantaggi immediati, etc[767].

Nel contesto attuale, inoltre, il consenso non pare nemmeno libero. A fronte della pervasività dei dispositivi elettronici/digitali e alle comodità di uso ormai quotidiano, non sembra realistica l'ipotesi di una libera e completa rinuncia da parte degli utenti nell'usufruire di un servizio, pur a costo della messa a disposizione dei propri dati personali[768].

Tutte queste considerazioni sembrano in parte esacerbarsi se rapportate ai trattamenti posti in essere nelle vetture connesse e autonome. Se anche si volesse ritenere il consenso quale base di legittimità, una prima tensione sorge nell'individuazione del momento in cui dovrebbe essere richiesto, oltre che, naturalmente, in relazione a quale dovrà essere il contenuto delle informative sottoposte all'interessato.

Non pare idoneo ad assicurare un'effettiva autodeterminazione dell'utente un consenso espresso al momento del primo utilizzo della vettura, presumibilmente in occasione dell'acquisto della stessa, e valevole per ogni raccolta e utilizzo futuro dei dati. Un consenso così delineato non potrebbe, infatti, dirsi realmente "informato", in quanto avrebbe a oggetto trattamenti che in realtà ancora non si conoscono. Inoltre è necessario ricordare come la grande varietà dei dati prodotti e trattati all'interno di una vettura connessa permetta di rilevare le abitudini di guida dell'utilizzatore, informazioni queste raccolte e scambiate tra gli operatori e che rispondono a finalità in tutto differenti da quelle individuate al momento del primo utilizzo della vettura (e per le quali si ipotizza sia stato prestato il consenso).

[767] Per un approfondimento in merito all'istituto del consenso e alla sua perdita di centralità nei trattamenti operati mediante tecnologie *data driven* si rimanda *supra* al capitolo 4 del presente lavoro.
[768] MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, cit., 35 s.

Così tracciato, l'istituto non potrebbe nemmeno dirsi libero, in quanto necessario allo stesso utilizzo dei servizi, siano essi legati al funzionamento dell'automobile, che a una delle altre funzionalità offerte nel contesto delle future *smart cities*[769].

Neppure la previsione di informative molto dettagliate in merito ai possibili futuri utilizzi dei dati raccolti sarebbe sufficiente a rendere il consenso effettivo e consapevole. Come visto, un maggior livello di dettaglio genererebbe piuttosto una ancora maggiore avversione da parte degli utenti[770]; ciò in particolar modo quando sarebbe necessario, come in questo caso, provvedere a fornire informative che diano conto di complessi trattamenti, aventi differenti finalità, di cui non tutte strettamente legate al funzionamento della vettura.

Se dunque un consenso preventivo non si mostra idoneo, del pari difficile appare anche una sua richiesta ogniqualvolta vengano utilizzate le applicazioni che raccolgono e trattano i dati [771]. Difatti, a fronte della moltitudine di titolari è complesso ipotizzare che ognuno debba richiedere un consenso specifico e distinto; come invece richiederebbe il GDPR in ragione delle differenti finalità da questi perseguite[772].

Rimane, infine, impregiudicato il problema dell'uso secondario di questi dati, della difficoltà di una sua previsione al momento della raccolta e di conseguenza di una relativa richiesta di consenso[773]. Si ricorda che le vetture saranno chiamate a trattare una

---

[769] NAZZARO, Privacy, smart cities *e* smart cars, cit., 337.

[770] Per un approfondimento si rimanda *supra* al capitolo 4 del presente lavoro.

[771] Si è già evidenziato come la vettura sarà connessa in modo continuato, dunque a prescindere dal suo impiego per uno specifico servizio. Ne discende che ogni utilizzo comporti la raccolta e la trasmissione di un numero considerevole di dati, di cui l'utilizzatore spesso è inconsapevole. V. NAZZARO, Privacy, smart cities *e* smart cars, *ibidem*.

[772] MENEGHETTI, *op. cit.*, 8. Interessanti anche le considerazioni di Miniscalco secondo cui l'acquisizione del consenso potrebbe risultare operazione complessa poiché i titolari dei trattamenti potrebbero non entrare in contatto diretto con gli interessati. Nemmeno può dirsi sostitutivo dell'obbligo di acquisizione del consenso l'obbligo previsto per i gestori delle tratte stradali, in cui verranno sperimentate le soluzioni di guida connessa e autonoma, di divulgare, mediante segnaletica presente sul percorso, informazioni per gli utenti della strada. V. MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, cit., 36.

[773] Oltre alla perdita di controllo informativo legata a un inconsapevole trattamento operato dalle applicazioni che forniscono servizi sulla vettura, criticità emergono in relazione all'esistenza di *second* (o *sub-sequential*) *uses* sui propri dati, come anche in merito alle s*econdary information* che vengono inferite da dati grezzi (*raw data*). In questi casi le informazioni estratte sono diverse rispetto a quanto oggetto del trattamento iniziale e potenzialmente utilizzate per finalità ulteriori non sempre espressamente autorizzate dall'interessato. Proprio in relazione a dette tensioni legate al funzionamento degli IoT, il Gruppo di Lavoro art. 29 ha precisato che affinché il trattamento possa dirsi lecito è necessario che l'utilizzatore possa esercitare il pieno controllo dei propri dati per tutto il ciclo di vita dei dispositivi. Per quanto riguarda i *second uses* dei dati personali sarà pertanto necessario che l'utente presti un consenso specifico, espressione di una sua piena consapevolezza e autorizzazione ai trattamenti. Gruppo di Lavoro art. 29, *Opinion 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti*, 1471/14/IT WP 223,

mole considerevole di dati, alcuni anche direttamente forniti dagli utenti nel momento della connessione dei propri *smartphone*.

Grazie alle potenzialità delle tecnologie algoritmiche l'analisi di tutte queste informazioni, comprese quelle di natura prettamente tecnica, può comportare una profilazione particolarmente invasiva. Dell'uso secondario di questi profili il più delle volte l'utilizzatore del veicolo non è pienamente consapevole; spesso nemmeno coloro che raccolgono e processano i dati hanno infatti contezza di tutti i possibili utilizzi secondari a cui le informazioni raccolte potranno essere destinate[774]. Non si vede dunque come sia possibile l'indicazione di trattamenti futuri di cui non si ha contezza, né sarebbe sufficiente una generica e indeterminata richiesta di consenso per eventuali utilizzi secondari dei dati raccolti.

Critici si mostrano infine gli scenari di *data retention*. Nel momento in cui la vettura non viene più utilizzata, per esempio perché venduta, l'assenza di consapevolezza in merito al tipo e alla quantità di dati conservati poterebbe comportarne la mancata cancellazione, oltre che a volte l'impossibilità di potervi accedere da parte dell'utente[775].

Interessante, allora, la proposta avanzata dalla Commissione europea di introdurre un dispositivo di bordo che possa interrompere lo scambio dei dati, fornendo al conducente le necessarie informazioni in merito alle conseguenze disfunzionali in termini di sicurezza e di efficienza tecnica del veicolo; ciò permetterebbe, a opinione della Commissione, di garantire l'espressione di una consapevole autodeterminazione del

---

2014. In dottrina cfr. MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 87 s. Per un approfondimento in merito ai c.d. usi secondari si v. *supra* il capitolo 3 del presente lavoro.

[774] Sul punto interessante la considerazione di Cantone. L'Autore, prendendo in considerazione la prassi del settore assicurativo che negli ultimi anni spinge per soluzioni parametrate sullo stile di guida degli assicurati, evidenza che se l'attività di profilazione posta in essere può trovare fondamento nel legittimo interesse del titolare, tale tipo di trattamento potrebbe essere fondato anche, in virtù del considerando n. 47, sulla necessità di prevenzione delle frodi. Si pensi al controllo circa i falsi sinistri, finalità per cui originariamente erano state pensate le *black boxes* installate sulle vetture. Rimane fermo l'obbligo per il titolare di fornire tutte le informazioni necessarie a rendere trasparente il processo e, in particolare, nel caso in cui vengano poste in essere decisioni automatizzate. Tuttavia – evidenzia l'Autore – spesso i dati raccolti e profilati vengono poi ceduti a soggetti terzi, operanti in altri settori (*in primis* quello finanziario e delle telecomunicazioni), per finalità che spesso non sono realmente conosciute dall'interessato; in questi contesti, infatti, i dati non verranno evidentemente utilizzati per individuare un equo premio alla base del contratto di RCA, quanto piuttosto per finalità di marketing. Ne discende come la condizione di legittimità del trattamento (il legittimo interesse) non possa più essere a fondamento anche di questi trattamenti ulteriori; sarà necessario individuare una nuova base di legittimità, quale per esempio un contratto o il consenso dell'interessato, a cui dovrà seguire una informativa chiara e intellegibile, delle cui criticità tuttavia si è già detto *supra* al capitolo 4. Si v. CANTONE, *L'IoT nel settore* automotive: *problematiche* privacy on board *e* on road, in *Dir. merc. tec.*, 2018, 12 ss.

[775] GUARINO, *op. cit.*, 10.

conducente, che così verrebbe messo nelle condizioni di apprestare un consenso effettivo e libero al trattamento dei propri dati[776].

La proposta presenta certamente dei pregi, tuttavia non sembra sciogliere le tensioni sopra evidenziate, introducendo, piuttosto, un'ulteriore richiesta di consenso a cui l'interessato verrebbe esposto.

Inoltre, fuori dai casi in cui detto dispositivo venga utilizzato al momento della vendita della vettura, non è chiaro quali dati potrebbero essere oggetto di cancellazione; non pare ipotizzabile la cancellazione di quelli strettamente legati al funzionamento della vettura, funzionamento che chiaramente deve mantenere uno standard di sicurezza. Potrebbe allora la cancellazione essere limitata a quei dati forniti ai gestori di servizi *cloud* collegati al sistema *infotainment* del veicolo, generati anche dal collegamento dei propri *device*, per esempio per gestire le preferenze musicali, per individuare gli indirizzi in agenda, la posizione della vettura (sebbene quest'ultimo dato potrebbe rientrare tra quelli necessari).

Se, dunque, in alcuni casi il dispositivo proposto potrebbe avere un'effettiva utilità, è bene ricordare, come si è già evidenziato, che difficilmente nella pratica un utente sceglierà di limitare pienamente i trattamenti, precludendosi così la comodità di servizi di uso ormai quotidiano. Rimane inoltre poco chiaro il destino dei dati trattati prima della richiesta di cancellazione, dell'uso che di questi viene fatto e, presumibilmente, del profilo dell'utente creato.

Inoltre, le informazioni inviate dal veicolo mittente sono trasmesse nell'ambiente circostante senza sapere se o chi riceverà il messaggio; gli attori del sistema non sono, infatti, tra loro in un rapporto di comunicazione biunivoca e quindi l'interessato non potrebbe essere adeguatamente informato in merito all'identità di tutti coloro che

[776] La C-ITS *Platform* ha indicato cinque principi basilari per il corretto accesso informativo: il consenso dell'interessato al trattamento dei dati personali, identificato con il proprietario del veicolo; la libera competizione tra prestatori di servizi; la protezione dei dati privati; la sicurezza informatica e la responsabilità; l'economicità. Si v. sul punto Maceratini, *Dall'*Internet of Things *alle* Smart Roads, cit., 90. Chiaramente il titolare rimane tenuto al rispetto dei principi generali elencati dal GDPR e, in particolare, il principio di necessità e di finalità del trattamento. Difatti non sempre è necessario l'utilizzo dei dati personali, ne discende che per alcuni utilizzi, una volta raccolti, questi debbano essere sottoposti a procedimenti anonimizzazione (o pseudonimizzazione) e utilizzati nei limiti delle finalità dichiarate. Nel caso della mobilità autonoma, come visto, il trattamento di alcuni dati è indispensabile al funzionamento del sistema, pertanto è possibile immaginare un *dataset* minimo di dati costituito dalla localizzazione del veicolo, dalla velocità di movimento e dalla direzione di viaggio. Così come per i dispositivi e-call installati nelle vetture che raccolgono determinate informazioni legate alla prestazione del servizio di assistenza in caso di incidenti. In arg. si v. MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 90.

ricevono e utilizzano i propri dati. Da questa considerazione discende anche una evidente difficoltà di esercizio dei diritti garantiti agli interessati, tra cui, appunto, quello di revocare il consenso in qualsiasi momento[777].

Sebbene la scelta di fondare il trattamento sul consenso possa in astratto assicurare una maggiore autodeterminazione degli interessati, alla luce delle considerazioni sopra svolte la sua utilizzabilità nel contesto della guida autonoma sembra di difficile realizzazione.

Sotto certi aspetti una scelta più adeguata potrebbe allora essere quella di ritenere il trattamento necessario ai fini dell'esecuzione di un contratto[778].

Detta base di legittimità potrebbe essere adeguata per quei trattamenti in cui l'interessato partecipi alle trattative o stipuli effettivamente un contratto[779], come nel caso del rapporto che si instaura tra proprietario e casa produttrice del veicolo. Se, come visto, il funzionamento delle vetture autonome richiede necessariamente il trattamento di alcuni dati, si potrebbe allora ipotizzare quale base di legittimità di questo tipo di trattamenti il contratto di compravendita, o altro differente quale una locazione, stipulato tra il futuro proprietario/conducente/conduttore e la casa produttrice o altra società che mette a disposizione la vettura autonoma. Più complesso si mostra invece il caso dei servizi forniti dai dispositivi installati sul veicolo e che non sono necessariamente legati allo stretto funzionamento dello stesso. Il trattamento di questa tipologia di dati non sembra, infatti, essere necessaria all'esecuzione del contratto, ben potendo il veicolo autonomo funzionare anche senza questi servizi aggiuntivi.

Si ricorda inoltre che i titolari di questi trattamenti spesso non corrispondono alle case produttrici delle vetture, ma sono soggetti terzi, estranei dunque al rapporto contrattuale che si instaura al momento dell'acquisto o della locazione di una vettura. Per fare un esempio si pensi all'uso di servizi di navigazione satellitare, in questo caso il titolare dei dati immessi nel sistema non sarà l'azienda produttrice della vettura, quanto piuttosto quella che fornisce il servizio. Appare anche difficile qualificare i diversi

[777] Difatti non sarebbe agevole ripercorrere a ritroso le trasmissioni di dati effettuati e individuare i vari soggetti a cui sono stati inviati. In arg. si v. MENEGHETTI, *op. cit.*, 8 ss.
[778] GAETA, *op. cit.*, 175.; MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, cit., 36.
[779] In argomento anche il Gruppo di Lavoro art. 29 ha chiarito come «the applicability of this legal basis might not be general. The reliance on this legal ground may be possible in specific scenarios, for instance when the data subject actually does have a contract with a private road operator to be able to drive on the road». *Opinion* 3/2017, cit., 5.

soggetti che raccolgono e trattano i dati per fornire servizi aggiuntivi sulle vetture come responsabili esterni. Difatti non pare possibile ritenere la casa produttrice della vettura, che stipula un contratto di compravendita, unico titolare dei trattamenti, dal momento che, come si è già avuto modo di evidenziare, questa non avrebbe in realtà alcun controllo sulla scelta delle finalità e dei mezzi per il trattamento posto in essere dai gestori dei servizi. Inoltre, se non sempre l'interessato ha contezza della diversità di trattamenti e di titolari che si susseguono, del pari difficilmente si può immaginare che questi possa aver stipulato differenti contratti con ciascuno dei soggetti che raccoglie e analizza i dati generati nell'utilizzo della vettura.

Peraltro, se pure ritenessimo lecito il trattamento effettuato dalla casa produttrice, avente a fondamento, per esempio, un contratto di compravendita della vettura, difficilmente potrebbero essere così giustificati anche i trattamenti dei dati di un utilizzatore diverso dal proprietario, ovvero degli altri passeggeri che potrebbero trasmettere informazioni personali connettendosi al sistema di *infotainment*[780]. In questi casi non potremmo considerare legittimo nei confronti di terzi un contratto stipulato tra l'acquirente del veicolo e il produttore; non avendo inoltre gli utilizzatori alcun contatto diretto con quest'ultimo si mostra complesso anche sottoporre loro un'adeguata informativa circa gli usi a cui verranno destinati i dati condivisi con il sistema.

Nemmeno pare convincente porre a fondamento dei trattamenti il legittimo interesse del titolare. Oltre alla necessità di compiere differenti valutazioni in merito ai distinti trattamenti, è bene ricordare come l'art. 6 GDPR preveda che l'interesse del titolare sia tale da prevalere sui diritti degli interessati.

Certamente la libertà di iniziativa economica assume importanza nel generale quadro di *governance* dei dati, non trovandosi in una posizione subordinata rispetto al diritto alla loro protezione, come espressamente ricordato anche dal legislatore europeo[781]. A detto interesse, tuttavia, non può essere concessa una assoluta primazia; non pare infatti possibile ritenere a priori come prevalente l'interesse del titolare, a fronte di una indeterminatezza delle specifiche finalità a cui verranno destinati i dati raccolti e trattati.

[780] MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, cit., 37.
[781] L'art. 1 prevede espressamente che: «*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*», art. 1, n. 3, reg. UE n. 679/2016.

A ciò è necessario aggiungere la considerazione per cui detta valutazione dovrebbe essere compiuta singolarmente, in merito a tutti i differenti titolari che operano lungo la catena di trattamenti, potendo ciò comportare risultati confliggenti[782].

Pertanto, alla luce delle complessità sopra richiamate sia in merito all'architettura dei sistemi connessi, che alle difficoltà di determinazione *ex ante* dei c.d. usi secondari, il legittimo interesse non pare essere una base idonea dei trattamenti operati nelle vetture. Alle stesse conclusioni giunge anche il Gruppo di Lavoro art. 29, che si dimostra contrario a ritenere lecito un trattamento che su di esso si fondi[783].

Per alcuni trattamenti si potrebbe immaginare quale fondamento un obbligo legale o l'esecuzione di un compito di interesse pubblico[784].

Questa lettura potrebbe trovare un fondamento in ragione delle prospettive di accrescimento del benessere sociale che l'introduzione della guida autonoma potrebbe generare. Oltre alla diminuzione del numero di sinistri, si è già sottolineato come la possibilità di accesso alla mobilità veicolare anche per quei soggetti che ora non possano accedervi concorrerebbe a rendere la società maggiormente inclusiva, apportando dunque benefici non solo economici ma anche sociali.

Così come richiesto dall'art. 6, n. 3, GDPR, la previsione di un obbligo di trattamento, stabilito in base al diritto dell'Unione o di uno Stato membro, dovrebbe contenere disposizioni specifiche in merito: al rispetto dei principi generali applicabili, di cui all'art. 5 GDPR; alle tipologie di dati trattati; alle misure previste a garanzia dei diritti degli interessati; alle limitazioni delle finalità e ai tempi di conservazione dei dati.

Una previsione di tal fatta potrebbe tuttavia incorrere nelle difficoltà sopra ricordate e legate alla complessità di funzionamento dei sistemi *data driven*. Difficilmente poi potrebbero essere considerati essenziali al perseguimento di un legittimo interesse quei dati raccolti da alcuni servizi *cloud* presenti nella vettura e non legati allo stretto funzionamento della stessa.

---

[782] MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, *ibidem*.
[783] Gruppo di Lavoro art. 29, *Opinion 3/2017*, cit.
[784] Si pensi per esempio ai dispositivi e-call. Il trattamento posto in essere qui non si fonda su di un consenso esplicito, né espresso, del fornitore del servizio e-call ai servizi di pronto intervento, che riveste il ruolo di titolare, nonostante si tratti di dati certamente personali, e potenzialmente anche sensibili. In particolare a fondamento del trattamento vengono posti motivi di tutela della sicurezza, ritenuti prevalente e per cui si ritiene dunque possibile prescindere da una manifestazione esplicita del consenso. V. GAETA, *ibidem*.

Allo stato attuale, dunque, nessuna delle basi giuridiche, singolarmente considerata, sembra poter rispondere adeguatamente al vaglio di liceità dei trattamenti; conclusione questa a cui giunge anche il Gruppo di Lavoro art. 29[785]. Da quanto sopra evidenziato, tuttavia, più convincente sembra un intervento legislativo che fissi un obbligo di trattamento o determini un legittimo interesse, quanto meno per quei dati che sono strettamente necessari al funzionamento delle *driverless car*; ciò, infatti, permetterebbe di determinare a priori i trattamenti leciti e al contempo di tutelare adeguatamente i diritti degli interessati.

Gli altri trattamenti dovranno invece trovare fondamento in una differente base giuridica; alcuni potrebbero fondarsi su di un contratto di fornitura di servizi, quali per esempio quelli effettuati dai servizi *cloud* collegati alla vettura. Si potrebbe pensare anche a una "stratificazione" del consenso, prevedendo una prima specifica richiesta di manifestazione del consenso per il trattamento di quei dati strettamente necessari alla fruizione del servizio; per quanto riguarda gli usi secondari, fatta salva la necessità di identificarne le finalità, potrebbe essere prevista una seconda specifica richiesta, e ciò in particolare qualora i dati vengano utilizzati per la profilazione degli interessati. Si è consapevoli che un'informativa troppo particolareggiata e tecnica, dunque particolarmente complessa, potrebbe divenire quasi un deterrente per l'interessato, spingendolo a prestare un consenso senza tuttavia aver preso visione delle informazioni sottopostegli; tuttavia, per alcuni tipi di servizi, quali quelli *cloud* di cui sopra, dunque non legati strettamente al funzionamento della vettura, detto istituto, pur se in parte ripensato, potrebbe trovare ancora spazio quale base giuridica.

Al fine di risolvere alcune delle criticità sopra richiamate, una possibile soluzione potrebbe risiedere nella progettazione di una forma che potremmo definire *user friendly*, grazie alla quale sarebbero mostrate succintamente solo le informazioni strettamente necessarie, quali per esempio le finalità perseguite, lasciando invece un maggior livello di dettaglio a disposizione dell'utente, mediante un collegamento diretto facilmente accessibile[786].

Una formulazione più intuitiva potrebbe aiutare gli interessati a comprendere in modo veloce gli usi che delle loro informazioni vengono fatti. A questo scopo si

[785] MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, cit., 36 s.; LOSANO, *Verso l'auto a guida autonoma*, cit., 429 ss.; MENEGHETTI, *op. cit.*, 9 s.
[786] AULINO, *op. cit.*, 309 ss.

potrebbero prendere in prestito alcune tecniche di *content design* usate nel neuromarketing; l'uso sapiente di grassetti, corsivi, immagini[787], ma anche degli stessi font, viene, infatti, già usato per migliorare la leggibilità di testi e attirare l'attenzione degli utenti, ciò soprattutto per scopi commerciali. Non si vede allora perché non estendere queste tecniche anche alle informative sulla privacy, rendendole così maggiormente intellegibili e, soprattutto, più accessibili. Inoltre, nella consapevolezza che sovente si finisce per assentire a ogni tipo di finalità, anche non strettamente necessaria al funzionamento del bene o del servizio prestato, una seconda e distinta richiesta di manifestazione del consenso potrebbe rivelarsi utile per rendere l'utente maggiormente consapevole. Questa seconda richiesta, anch'essa pensata per essere facilmente intellegibile, sarebbe dunque destinata a chiedere l'assenso per tutti e soli quegli usi secondari, e di trasmissione dei dati a terzi. Questa stratificazione permetterebbe così agli utenti una maggiore consapevolezza delle finalità distinte cui si sta acconsentendo.

Si avrebbe pertanto una prima richiesta di consenso destinata unicamente a quei trattamenti necessari al funzionamento del bene o alla fruizione del servizio, a cui ne seguirebbe una seconda, distinta anche visivamente mediante l'uso di finestre successive, invece destinata a raccogliere l'assenso per tutti gli usi che non sono strettamente necessari. Del pari, a fronte della pratica attuale di prevedere delle spunte in chiusura di lunghe finestre poco leggibili, anche la previsione di un *design* più intuitivo, che renda ben visibile la distinzione di usi e di finalità, si ritiene potrebbe concorrere a rendere il consenso prestato maggiormente consapevole e libero.

[787] Nella consapevolezza che gli studi comportamentali hanno dimostrato come l'attenzione sia maggiormente attratta da simboli e immagini, meglio se colorate e a contrasto con lo sfondo, piuttosto di un testo scritto, di recente anche il Garante della Privacy ha lanciato un *contest* diretto a individuare delle icone e/o dei simboli che rappresentino la totalità degli elementi che dovrebbero essere contenuti nelle informative privacy ai sensi degli artt. 13 e 14, reg. UE n. 679/2016. Grazie all'utilizzo di immagini e icone, o altre soluzioni grafiche, si vorrebbe rendere le informative più chiare e immediatamente comprensibili per tutti gli utenti. Si veda il comunicato stampa del 15 marzo 2021 dal titolo *Informative privacy più chiare grazie alle icone? È possibil*e. *Il Garante lancia un contest facendo appello alla creatività collettiva*, consultabile all'indirizzo: *www.garanteprivacy.it* (ultimo accesso 10 settembre 2021).

3. La sicurezza delle vetture, un problema anche di privacy?

Alcune considerazioni devono essere svolte anche in merito al profilo della sicurezza delle vetture, facendo una necessaria differenza tra la sicurezza del sistema, con possibili ricadute sull'incolumità degli occupanti il veicolo, e la sicurezza delle comunicazioni e dei dati raccolti.

La possibilità di una connessione costante, se da un lato può generare alcuni vantaggi, tra cui, per esempio, l'accesso a dati rilevanti per la *vehicle forensics* in caso di incidenti, dall'altro potrebbe comportare un considerevole aumento dei rischi di attacchi informatici al sistema.

Attualmente nelle vetture coesistono una pluralità di reti connesse tra loro e con l'esterno, lo stesso protocollo CAN (il più diffuso) permette di connettere tutti gli elementi critici del veicolo, tra cui per esempio il motore e la trasmissione, ma anche diverse applicazioni destinate a fornire servizi all'utente. Se inizialmente questa rete era accessibile solo fisicamente, in modalità cablata tramite la porta OBD (*On-board diagnostic*), oggi è possibile avervi accesso anche da remoto, così evidentemente estendendo la superficie sensibile a possibili attacchi[788].

Un sistema connesso è, infatti, necessariamente aperto; aperto alla trasmissione, ma anche alla ricezione di messaggi. Questo comporta che ognuna delle connessioni che viene instaurata potrebbe divenire una possibile porta d'accesso per coloro i quali intendano alterare i sistemi di controllo del veicolo o sottrarre i dati ivi raccolti[789]. Per esempio, un hacker potrebbe avere accesso dal sistema di *infotainment* e generare dei messaggi diretti ad alterare il sistema di frenata, lo sterzo o l'acceleratore; potrebbe anche alterare i messaggi diretti ai rilevatori *radar* di ostacoli, magari generando un

[788] Le vetture autonome e connesse sono dotate di numerosi microprocessori collegati tra loro, e con la rete mediante protocolli standard, che permettono al sistema di guida di comunicare con i diversi sensori destinati a rilevare dati sullo stato del veicolo (per esempio il regime di rotazione del motore, i livelli di usura dei componenti, la posizione dei pedali etc.). Inoltre i sensori installati sulle vetture (si parla di automobili per comodità ma nella gamma dei veicoli connessi rientrano anche veicoli agricoli e industriali) permettono anche la registrazione di *input* quali riprese video da telecamere (interne ed esterne alla vettura), localizzazione, *radar* o sensori laser (LIDAR). A tutti questi dati oggi è possibile accedere non solamente dall'interfaccia dedicata alla diagnostica mediante USB, ma anche mediante reti wireless, Bluetooth o infrarossi e reti a corto raggio, via WiFi e si prevede anche mediante reti a banda larga 4/5G; la moltiplicazione dei punti di accesso evidentemente aumenta il rischio di possibili intrusioni esterne dirette a sottrarre o compromettere i dati oltre che a manomettere le vetture. Cfr. GUARINO, *op. cit*., 4 s.

[789] LOSANO, *Verso l'auto a guida autonoma*, cit., 433 ss.; COSTANTINI, MONTEROSSO, *Il problema della sicurezza tra informatica e diritto: una prospettiva emergente dalle "Smart Cars"*, in *Inf. e dir*., 2016, 95 ss.

allarme per un ostacolo inesistente o, peggio, cancellare l'allarme per un ostacolo esistente[790].

Non si tratta di scenari futuristici.

Grande risonanza hanno avuto alcuni episodi di intrusioni che hanno intaccato i sistemi di sicurezza e finanche "pilotato" da remoto le vetture; gli hacker sono infatti riusciti a prendere il controllo del volante e dei sistemi di accelerazione e frenata dei veicoli. Il caso forse più noto è quello della Jeep Cherokee[791]. Qualche anno prima, nel 2013, la società Enter Berla aveva dichiarato di essere riuscita a *hackerare* diversi modelli di auto, contando fino a 4.600 vetture nel 2017. I ricercatori erano difatti riusciti a sfruttare la vulnerabilità riscontrata in un modello per accedere anche ai diversi sistemi di gestione di altri veicoli della stessa casa costruttrice[792].

Questi episodi evidenziano la necessità di migliorare la solidità dei sistemi informatici presenti nelle vetture. I veicoli sono sempre più connessi e informatizzati e così si trovano soggetti alle medesime criticità in tema di *cybersecurity* che affliggono i classici terminali (telefoni, computer, *server* etc.)[793].

---

[790] LOSANO, *Verso l'auto a guida autonoma*, cit., 431 ss.

[791] L'episodio risale al 2015 quando due ricercatori di sicurezza informatica sono riusciti ad attaccare da remoto i sistemi elettrici della Jeep Cherokee; una volta avuto accesso hanno potuto controllare via wireless la vettura, accedendo al sistema di *infotainment*, alle funzioni del cruscotto e controllando freni, sterzo e trasmissione, causandone l'uscita di strada. A seguito di questo episodio la FCA è stata costretta a richiamare 1,4 milioni di veicoli.
Diversi sono stati gli episodi di intrusioni esterne. È stato possibile accedere all'ibrido Outlander PHEV di Mitsubishi tramite rete WiFi. In questo caso i ricercatori hanno scoperto che la password di accesso era la medesima per tutti i veicoli prodotti e riportata nel manuale; è stato dunque facile per gli studiosi ricostruire il protocollo di comunicazione interno al sistema e, per esempio, disabilitare l'antifurto.
Altro caso è quello della Nissan Leaf. La vettura era dotata di un'applicazione per il controllo da remoto a cui si poteva accedere immettendo il numero di telaio, questo però, come è noto, è visibile sui cristalli dall'esterno, così permettendo a chiunque di utilizzare l'applicazione per controllare la vettura. Per un approfondimento si v. GUARINO, *op. cit.*, 9.

[792] Si v. CANTONE, *op. cit.*, 4.

[793] Si pensi, per esempio, alle difficoltà di aggiornamento dei software quando è necessario rimediare a qualche vulnerabilità del sistema, così come accade per i terminali quali computer e *smartphone*. Nel contesto delle auto autonome la questione diviene delicata. Non è certo che qualunque utente sia in grado o anche solo sia disposto ad aggiornare periodicamente il software della vettura. Così come per i mancati aggiornamenti del proprio computer, la spiegazione risiede nella difficoltà per gli utenti di rendersi effettivamente conto dei rischi legati alle vulnerabilità dei sistemi informatici. L'unica alternativa per avere la sicurezza di vedere installato l'aggiornamento sarebbe, dunque, quella di procedere da remoto; questa opzione, tuttavia, comporterebbe ugualmente alcuni rischi, tra cui quello di interferenza con le necessità dell'utente e con il rischio di procedere a un aggiornamento quando la vettura è in uso. Sul punto interessanti le considerazioni di Guarino il quale evidenzia come «La facilità d'uso per gli utenti normalmente fa perno sul livello di sicurezza, difficilmente percepibile, e i fornitori ne tengono conto. La poca consapevolezza dei principi della sicurezza informativa da parte dei costruttori dipende non solo dalla carenza di competenze specifiche ma anche da pressioni e meccanismi economici: la necessità di portare sul mercato i nuovi prodotti in tempi brevi porta a non investire in sicurezza, che è una

Una maggiore attenzione dovrà dunque essere posta nella predisposizione di sistemi di protezione, nonostante un inevitabile appesantimento dei programmi e un aggravamento dei costi di produzione dei veicoli. Inoltre, sarebbe auspicabile l'introduzione di un processo di certificazione diretto ad assicurare lo sviluppo di prodotti con elevate garanzie di sicurezza non solamente delle componenti fisiche delle vetture, ma anche dei software[794].

La necessità di interventi diretti a rendere i veicoli più sicuri da attacchi esterni trova evidentemente fondamento nell'esigenza di garantire l'incolumità degli utenti; la possibilità di intaccare e controllare i sistemi di guida ha infatti mostrato l'impellenza per le case costruttrici di investire in sicurezza.

I rischi derivanti da un accesso non autorizzato non si limitano tuttavia al perimetro della sicurezza fisica degli utenti, ma interessano anche la sottrazione e l'utilizzo illecito dei dati raccolti dal sistema[795].

Come visto, i trattamenti posti in essere durante l'utilizzo dei veicoli connessi saranno numerosi e dall'analisi dei dati, quali per esempio quelli di posizionamento o le abitudini di guida, potrebbero emergere informazioni finanche sensibili. Oltre alla perdita di controllo da parte degli interessati, un'intrusione illecita potrebbe dunque ledere la privacy, intesa come riservatezza, degli utenti.

Criticità sorgono anche in merito all'utilizzo dei dati "scambiati" con le infrastrutture. In particolare, la conservazione di dati che riguardino la posizione, il tempo, la marca e il modello della vettura, se da un lato fa sorgere un effettivo rischio di un ingiustificato monitoraggio continuo dei cittadini, dall'altro aumenta sensibilmente i rischi derivanti da possibili *data breach* al sistema di controllo pubblico.

La soluzione più semplice sarebbe allora quella di impedire completamente la trasmissione di informazioni, bloccando ogni comunicazione; tuttavia questa soluzione non è praticabile. Per permettere il corretto funzionamento della vettura connessa, e in futuro autonoma, è necessario che alcuni dati di posizionamento siano tracciati e

---

caratteristica non percepita dai consumatori a causa di enormi asimmetrie informative». GUARINO, *op. cit.*, 8 s.

[794] LOSANO, *Verso l'auto a guida autonoma*, cit., 425 ss.

[795] Sottolinea Maceratini come dall'utilizzo degli oggetti connessi derivino nuove forme di minaccia alla privacy degli utenti «rese possibili da un anonimato difficile da mantenere, come avviene usualmente nel web, e dalla pressoché automatica identificazione dei profili individuali, determinata dalla proliferazione e dall'incrocio dei dati anonimi che, se correttamente interpretati, conducono alla delineazione di profili individuali». MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 75.

condivisi sia con gli altri veicoli che con l'infrastruttura[796]. La loro raccolta e utilizzo risponde evidentemente a un'esigenza di sicurezza e incolumità pubblica nella circolazione stradale, e ciò ne legittima il trattamento.

Non si dubita della prevalenza dell'interesse pubblico alla sicurezza rispetto alla tutela della riservatezza dei guidatori *tout court* considerata[797], nondimeno appare necessario un attento bilanciamento, rispettoso dei principi generali sanciti dal GDPR e, in particolare, di quello di minimizzazione e di limitazione anche temporale dell'utilizzo e della conservazione dei dati[798].

Si conferma quindi necessario un intervento legislativo che limiti la quantità di dati raccolti ai soli effettivamente necessari per permettere il funzionamento delle vetture in sicurezza, similmente a quanto già viene previsto per i dispositivi *e-call*. Per limitare i rischi di un controllo ingiustificato e pervasivo degli utenti sarebbe inoltre auspicabile la definizione di un termine alle attività di trattamento e una successiva cancellazione dei dati, così da limitare possibili abusi e garantire quantomeno un perimetro minimo di sicurezza per gli interessati.

Si auspica inoltre una maggiore valorizzazione di quegli interventi di c.d. tecno-regolamentazione.

La complessità tecnica dei sistemi *data driven*, come visto, rende particolarmente complessa la previsione di disposizioni legislative che siano efficaci a regolare anche le evoluzioni tecnologiche. Rilievo assumono allora previsioni tecniche che permettano *ex ante* di incorporare nei sistemi digitali soluzioni rispettose delle disposizioni normative a tutela degli utenti, ma anche *ex post* che siano dirette a controllare l'operato dei sistemi e che permettano di intervenire in caso di errori o malfunzionamenti[799].

Una particolare influenza potrebbero allora ricoprire quei principi di *privacy by design* e *by default* che, andando a operare in una fase precedente al trattamento, permetterebbero di sviluppare applicazioni maggiormente *compliant* con il

[796] Per esempio le informazioni in merito a un incidente potranno essere trasmesse a una vettura che si trovi in prossimità di questo, ma solo se si ha accesso ai dati di posizionamento.
[797] Si v. DI ROSA, *op. cit.*, 132.
[798] L'associazione nazionale fra imprese assicuratrici ha evidenziato come il sistema dovrebbe garantire un libero accesso a tutti i portatori di interessi legittimi, pur al contempo prevedendo soluzioni dirette a migliorare la sicurezza informatica e a permettere una libera scelta nell'individuazione del *provider*. Ciò sarà possibile solo grazie a un adeguato coinvolgimento degli operatori del settore, tra i quali dunque dovranno essere ripartiti i costi di implementazione del sistema. Cfr. MACERATINI, *Dall'*Internet of Things *alle* Smart Roads, cit., 83.
[799] GAETA, *op. cit.*, 176.

Regolamento GDPR e minimizzare i rischi di possibili esternalità negative per gli interessati.

Si pensi all'utilizzo di tecniche di pseudonimizzazione per rendere difficilmente ricollegabili all'interessato i dati raccolti.

Si potrebbe inoltre prevedere l'eliminazione dopo un lasso di tempo predeterminato delle chiavi di decifrazione; previsione, questa, che permetterebbe di rendere ulteriormente complessa, e dunque spesso non economicamente conveniente, la decifratura e la conseguente ricollegabilità delle informazioni al singolo utente della vettura. Ne discenderebbe anche una maggiore garanzia per gli interessanti nel caso in cui dati pseudonimizzati dovessero essere trasmessi per usi secondari.

Si è già avuto modo di ricordare come le tecniche di anonimizzazione e, a maggior ragione, di pseudonimizzazione non permettano di recidere definitivamente il collegamento con la persona fisica a cui i dati si riferiscono[800]; pertanto rimane necessaria, fintanto che questi rimangono conservati e utilizzati dal titolare, un'opera di controllo e di ammodernamento delle misure di sicurezza, in ragione della veloce evoluzione delle tecniche di *data mining*.

Nel contesto delle auto *driverless* il Gruppo di Lavoro art. 29 ha avanzato la proposta di criptare i dati[801] al fine di prevenire attacchi diretti alla loro sottrazione, oltre che di utilizzare una localizzazione a corto raggio, così da realizzare una stretta connessione causale tra viabilità e veicoli presenti nelle differenti zone. Per rendere più difficoltose le attività di decifrazione si è inoltre proposta la frequente modifica dei titoli di autorizzazione (come gli pseudonimi) che identificano i veicoli[802].

A fronte delle problematiche nascenti tanto dalla raccolta quanto dal trattamento dei dati, appare utile un confronto con le soluzioni proposte oltreoceano, in una prospettiva di necessario coordinamento tra ordinamenti, avendo la circolazione dei dati una naturale vocazione sovranazionale.

---

[800] Si v. *supra* § 5.1, capitolo 3.

[801] Evidenzia Di Rosa come tuttavia questo tipo di misure potrebbe in alcuni casi influire negativamente sulla possibilità di utilizzare i dati prodotti dalle vetture per fini di sicurezza, come per esempio in caso di accertamento di responsabilità da reato. DI ROSA, *ibidem*.

[802] Gruppo di Lavoro art. 29, *Opinion 3/2017*, cit. In dottrina cfr. CANTONE, *op. cit.*, 21, il quale evidenzia come sarebbe auspicabile una modifica per tutti i veicoli che attraversano una determinata zona, così da rendere più complesso tenere tracciata una singola vettura. Si v. anche AA. VV., S*ecurity and privacy for next generation wireless networks*, Berlin, 2018, 111 ss.

Nell'esperienza americana, sebbene proprio qui si sia radicato il diritto alla privacy, la protezione dei dati personali è sempre stata considerata in un'ottica prevalentemente di mercato, dando in un certo senso poco rilievo al loro coinvolgimento nell'esercizio dei diritti fondamentali. La *ratio* può essere individuata nell'approccio tradizionalmente liberale nella regolazione degli interessi tra privati[803], in luogo di quello paternalistico che invece caratterizza in vario modo e in diversa entità gli ordinamenti di *civil law*.

Nel tempo, per far fronte all'esigenza di contemperare diritti contrapposti, la giurisprudenza statunitense ha elaborato il principio della *reasonable expectation of privacy* secondo cui le violazioni della privacy dovrebbero essere rapportate al livello di riservatezza che sarebbe ragionevolmente esigibile nel caso concreto; si richiede dunque di esaminare caso per caso il potenziale di invadenza dei trattamenti nelle relazioni umane[804].

In seguito a scandali come "*Datagate*", come pure a fronte delle capacità di analisi delle tecnologie sempre più pervasive, diviene tuttavia complesso stabilire sino a che punto possa ragionevolmente spingersi l'aspettativa di privacy, divenendo così necessario un intervento normativo che fissi limiti alla raccolta e all'utilizzo dei dati da parte di enti, sia privati che pubblici.

Nel contesto sanitario, per esempio, in ragione dell'estrema sensibilità dei dati trattati, il principio sopra citato viene ad affiancarsi a un generale divieto di trattamento senza il consenso degli interessati; requisito che può essere limitato solo in determinate circostanze[805].

Anche nel settore della mobilità connessa e autonoma sono emerse preoccupazioni proprio in merito all'esigenza di tutelare gli utenti da possibili abusi, a fronte di un rischio elevato di controllo degli stessi[806]. Il Congresso si è così impegnato a emanare un atto legislativo avente lo scopo di tutelare la privacy degli individui nell'uso delle tecnologie a guida automatica[807].

---

[803] Si v. *supra* il capitolo 3 del presente lavoro.
[804] MACERATINI, Privacy *e informazione nell'era dei* Big Data, cit., 76 e spec. 86.
[805] Per un approfondimento si v. TAYLOR, WILSON, *Reasonable expectations of privacy and disclosure for health data* (2019) 3 *Medical Law Review* 432 ss.
[806] GLANCY, *Privacy in autonomous vehicles* (2012) 52 *Santa Clara law review* 1216 ss.
[807] Si fa riferimento all'*Autonomous Vehicle Privacy Protection Act*, sottotitolato *To protect consumer privacy during the development and use of autonomous vehicle technologies*. A questo atto dovrebbe seguire l'emanazione, da parte del *Controller General* degli Stati Uniti, di un report che certifichi la preparzione del Dipartimento dei Trasporti a far fronte alle sfide derivanti dall'introduzione dei veicoli a guida automatica nella circolazione stradale. Si v. DI ROSA, *op. cit.*, 141. Nell'ordinamento americano era

L'esperienza americana, pur muovendo da un approccio differente, sembra dunque approdare anch'essa verso soluzioni che prevedano un intervento normativo, non potendo lasciare agli operatori, sia privati che pubblici, un'eccessiva libertà nella definizione delle modalità di collezione e di utilizzo dei dati.

La previsione di limiti e di condizioni per il trattamento, permetterebbe non solamente di accrescere la fiducia degli utenti, garantendo il rispetto quantomeno di un perimetro minimo di tutela, ma anche di concedere agli operatori nel mercato un certo spazio di libertà che permetta uno sfruttamento economico dei dati raccolti, oltre che di quelli generati e di cui essi vorrebbero essere considerati titolari.

Il settore *automotive* si dimostra uno tra i più paradigmatici terreni di scontro tra l'esigenza di tutela della riservatezza e dei dati degli interessati, da un lato, e la libertà di iniziativa economica, dall'altro. Appare allora necessaria un'attenta ponderazione tra interessi confliggenti, dal momento che una regolazione troppo restrittiva potrebbe comportare un pregiudizio per il mercato stesso. Già si è detto circa il valore economico dei dati e la necessità di una loro libera circolazione al fine di permetterne lo sfruttamento e non pregiudicare il mercato digitale[808].

Alla luce delle criticità sopra evidenziate in relazione ai rischi legati non solamente a un utilizzo illegittimo dei dati, ma anche a possibili attività di profilazione degli interessati, si ritiene dunque auspicabile l'utilizzo di soluzioni tecniche che rendano il rispetto della normativa sulla *data protection* un necessario requisito di sistema. L'adozione di codici di condotta e di standard sembra, infatti, ben adattarsi all'attuale contesto tecnologico, ove è alto il rischio che una regolazione troppo specifica divenga velocemente obsoleta. Diversamente una previsione normativa che rimandi all'adozione di questi strumenti, evidentemente declinati nello specifico contesto di utilizzo, si mostra più adeguata a garantire misure che, tenendo conto dello stato dell'arte, possano tutelare adeguatamente i diritti degli interessati durante tutto l'arco di funzionamento dei sistemi.

---

stato già emanato nel 2015 il *Driver Privacy Act* nel quale si prevedeva per i costruttori di vetture la possibilità di inserire "scatole nere" sulle vetture, attenendosi alla normativa federale di riferimento. Secondo queste disposizioni i dati raccolti appartengono ai proprietari dei veicoli; per tanto non possono essere prelevati senza il loro consenso. Questa posizione è stata accolta anche dall'Agenzia governativa (N.H.T.S.A) che regola il traffico. Si v. SIMONINI, *L'intelligenza artificiale guida le nostre vetture*, cit., 130.

[808] Per un approfondimento si v. *supra* il capitolo 2 del presente lavoro.

Del pari un ruolo chiave dovrebbero assumere le tecniche di pseudonimizzazione e, ove possibile, quelle di anonimizzazione. Queste misure di sicurezza, periodicamente aggiornate, permetterebbero di garantire una tutela preventiva degli interessati non limitando eccessivamente le possibilità di sfruttamento economico dei dati da parte dei titolari[809].

4. Alcune questioni sui dati generati dalle vetture

Come visto, affinché sia possibile il funzionamento dei veicoli autonomi sarà necessaria la creazione, trasmissione e ricezione di un numero considerevole di dati di differente natura. A quelli personali si affiancheranno quelli tecnici di funzionamento delle componenti delle vetture che, se pure non strettamente personali, possono ugualmente, mediante il collegamento con altre informazioni raccolte, portare all'identificazione degli utenti.

Evidente è dunque l'esigenza di porre in essere una strategia preventiva di tutela dei diritti degli individui; questo, tuttavia, non è l'unico profilo critico su cui è necessario soffermarsi. A fronte delle potenzialità nascenti da un loro sfruttamento si è acceso un dibattito in merito a quale soggetto possano "appartenere", avendo questi un ingente valore economico[810] sia per la casa produttrice del veicolo che, in generale, per i fornitori di servizi digitali[811].

Si pensi sul punto a quanto dichiarato nel 2014, in occasione del congresso dell'associazione tedesca dei produttori (VDA), dell'allora CEO del gruppo Volkswagen. L'amministratore delegato ha precisato che la casa automobilistica da un lato cercherà di connettersi ai sistemi di Google, evidentemente per poter fornire ulteriori servizi personalizzati ai propri clienti, dall'altro intende essere considerata

[809] GAETA, *op. cit.*, 177 s.
[810] L'uso delle virgolette è d'obbligo, in quanto non è pacifico – come vedremo – che su di questi si possa esercitare un diritto di proprietà classico, in ragione della immaterialità, della non esclusività e non rivalità degli stessi.
[811] I dati raccolti potrebbero infatti essere utilizzati per fornire differenti servizi, per esempio di supporto alla guida o sistemi di assistenza in caso di emergenza. Potrebbero essere presenti nelle vetture come dotazioni opzionali scelti dall'utente, ma in futuro potrebbero essere oggetto anche di servizi in abbonamento. Oltre a questi si stima che con il miglioramento delle connessioni potranno essere estesi anche i servizi di intrattenimento, quali per esempio lo *streaming* di contenuti, *social network*, servizi di *car-sharing*, raccomandazioni commerciali etc.

"padrona" di dati generati dalle proprie vetture[812]. Da queste parole ben si comprende come già sette anni fa fosse chiaro il valore economico delle informazioni raccolte e prodotte dalle vetture; non stupisce che diversi attori se ne contendano la proprietà.

Appare allora necessario chiarire se i dati possano essere soggetti a un regime proprietario e a quale dei diversi soggetti possano essere attribuiti. La questione non è di poco conto, dal momento che evidentemente va a incidere sul potere di sfruttamento di questi veri e propri "giacimenti".

Prima di vedere quale può essere il regime applicabile in particolare ai dati generati dai veicoli autonomi è necessario fare una distinzione.

Per quanto riguarda i dati di natura personale la Commissione europea ha precisato come essi appartengano all'interessato, sia esso il conducente che, eventualmente, i passeggeri[813]. Ne discende l'applicabilità della normativa GDPR, con la necessità di individuare la base giuridica di legittimità dei trattamenti, l'individuazione del titolare e, naturalmente, il rispetto degli obblighi previsti per il titolare e dei i diritti concessi agli interessati.

Diverso invece il caso di dati grezzi di natura tecnica non attribuibili a una specifica persona fisica e quindi non soggetti alla normativa sulla *data protection*.

Sebbene si sia evidenziata la difficoltà di individuazione di *dataset* totalmente non personali, oltre che la stessa complessità di individuazione di dati così qualificati[814], rimane tuttavia necessaria una riflessione giuridica sul punto.

---

[812] Si v. GUARINO, *op. cit.*, 6.

[813] Comunicazione della Commissione, *Una strategia europea per i sistemi di trasporto intelligenti cooperativi, prima tappa verso una mobilità cooperativa, connessa e automatizzata*, COM (2016) 766 final, 2016, 9. Più di recente è stata emanata una nuova Comunicazione, *Strategia per una mobilità sostenibile e intelligente: mettere i trasporti europei sulla buona strada per il futuro*, COM (2020) 789 final, 2020, 15 ss. Nel documento da ultimo citato, la Commissione, dopo aver chiarito come il futuro dell'*automotive* risiede nei sistemi di trasporto intelligente, richiama la necessità di garantire una maggiore disponibilità, accesso e scambio di dati, creando uno spazio comune europeo dei dati sulla mobilità. Emerge, dunque, la consapevolezza del ruolo chiave rivestito dall'analisi dei dati nel settore; un ostacolo alla circolazione degli stessi, quale per esempio una normativa troppo rigida e una mancanza di interoperabilità tra i sistemi, potrebbe comportare un serio pregiudizio all'economia di mercato e così incidere negativamente anche sulle strategie di mobilità sostenibile e intelligente. Nella consapevolezza, pertanto, che l'accesso ai dati sarà funzionale alla condivisione degli stessi e alla mobilità intelligente, si prevede che la Commissione proponga una nuova iniziativa sul punto, nella quale verrà presentato un quadro equilibrato che garantisca un accesso equo ed efficace ai dati da parte dei fornitori di servizi di mobilità; fermo il rispetto della privacy degli utenti. Cfr. SIMONINI, *L'intelligenza artificiale guida le nostre vetture*, cit., 149.

[814] Per un approfondimento circa le difficoltà legate ai dati non personali e, in particolare, ai *dataset* misti v. *supra* § 3, capitolo 2, del presente lavoro.

Non sembra, infatti, facile stabilire se questi dati "appartengano" al soggetto che li genera, al titolare del software/hardware che li registra (come nel caso delle scatole nere), oppure alla casa automobilistica che li raccoglie e/o li elabora[815] o, ancora, al proprietario del veicolo che, avendolo acquistato, potrebbe dirsi proprietario anche di tutte le sue componenti, compresi i software utilizzati, e dei dati da queste generati.

Alla luce della crescente importanza che stanno rivestendo i software (in futuro si stima che rappresenteranno circa il 20/30% delle componenti di una vettura di lusso) è necessaria una ulteriore considerazione preliminare.

A differenza delle componenti brevettate e implementate nella vettura, che vengono pacificamente considerate appartenere al proprietario del veicolo (rimanendo il costruttore titolare del brevetto), in relazione ai software dei sistemi elettronici la questione è invece più sfumata[816].

Secondo l'impostazione tradizionale il costruttore della vettura deve considerarsi anche il proprietario dei software, i quali sono tutelati dal diritto d'autore di cui egli è titolare. Ne consegue che l'uso dei software viene concesso in licenza al soggetto che acquista la vettura; licenza che potrebbe essere a tempo determinato, con rinnovo automatico, oppure a tempo indeterminato[817].

Questa interpretazione trova conferma nell'obbligo gravante sul costruttore di rilasciare continui aggiornamenti, oltre che di sostituzione delle parti rivelatisi inefficienti sotto il profilo progettuale, come previsto dalla Direttiva 95/20015 CE. Ciò fa dunque propendere per la fornitura di un servizio, più che per una vendita di un prodotto (il software) di cui l'acquirente diverrebbe proprietario. Inoltre, il costruttore al momento della vendita della vettura non rilascia i c.d. programmi sorgente, ma solo delle copie, coperte da misure di sicurezza che non ne permettono la modifica,

---

[815] ZENO ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Medialaws – riv. dir. media*, 2018, 33; DETERNMANN, *No one owns data* (2019) 70 *Hasting law journal* 29 ss.

[816] In merito alla questione circa la proprietà dei software presenti nella vettura si rimanda a ZHANG, *op. cit.*, 307 s. L'A. evidenzia che nella pratica ai proprietari delle vetture viene concesso l'uso dei software mediante contratti di licenza, nei quali vengono indicati i limiti e le modalità d'uso; si esclude così la possibilità che questi appartengano ai proprietari delle vetture. Se così non fosse non si spiegherebbero gli obblighi per il costruttore sia di tenere aggiornati i software di cui le proprie vetture sono dotati, che di sostituzione in caso in cui siano emerse inefficienze sotto il profilo progettuale, come nei casi previsti dalla Direttiva 95/2001 CE.

[817] In arg. Simonini ritiene che il termine finale del contratto di licenza potrebbe identificarsi nella pubblicazione di un nuovo aggiornamento. SIMONINI, *L'intelligenza artificiale guida le nostre vetture*, cit., 138 s.

concedendo all'acquirente solo un diritto di utilizzazione; diritto questo che poi si trasmette tacitamente in caso di successive vendite del veicolo[818].

Secondo altra interpretazione, invece, l'acquisto di una vettura comporterebbe l'acquisto di tutte le componenti, ivi compresi i software in essa installati. Questa ricostruzione non è convincente. Difatti se anche si decidesse di aderire a tale interpretazione i diritti esercitabili dal proprietario del veicolo sarebbero comunque limitati, essendo il software tutelato dal diritto d'autore. Egli avrebbe unicamente il diritto a un suo pieno utilizzo e a rivedere lo stesso, per effetto del diritto di esaurimento[819]. Non potrebbe invece modificare il programma né crearne delle nuove copie, dal momento che così facendo lederebbe appunto il diritto d'autore.

Più convincenti appaiono dunque gli argomenti a sostegno della tesi che vede il costruttore della vettura proprietario dei software, e sottoscrittore un contratto di licenza con l'acquirente del veicolo.

Precisato a chi appartengano i software installati nei veicoli, rimangono da chiarire alcune criticità legate ai dati generati dai sensori. In particolare, una prima tensione emerge in relazione alla loro stessa qualificazione. Dal momento che questi genererebbero informazioni eminentemente tecniche, si è ritenuto che i dati così prodotti non dovessero essere qualificati come personali.

Secondo tale ricostruzione, infatti, per permettere l'identificabilità di un individuo sarebbe necessario accedere a ulteriori informazioni (non sempre facilmente reperibili) che permettano, prima, di ricollegare il dato alla vettura e, poi, la singola vettura a una determinata persona fisica. Alcune di queste informazioni sarebbero inoltre coperte da misure di anonimizzazione tali da non rendere ragionevolmente possibile compiere questo collegamento finale con l'interessato.

Ne discenderebbe la non applicabilità della normativa sulla *data protection*; si tratterebbe infatti di dati non personali di proprietà del soggetto che ha investito nella loro generazione e che dunque può disporne liberamente. Si noti inoltre come la raccolta

---

[818] SIMONINI, *L'intelligenza artificiale guida le nostre vetture*, cit., 134 s.

[819] La normativa chiarisce che la tutela è accordata se il programma è originale. Per «*programma per elaboratore si intende anche il materiale preparatorio per la progettazione del programma*». Art. 1, dir. CE n. 24/2009.
Inoltre l'art. 4 prescrive che il titolare del diritto d'autore può autorizzare forme di distribuzione al pubblico del programma, compresa la locazione. Se si effettua una compravendita, la prima vendita della copia del programma esaurisce il diritto di distribuzione, pertanto il primo proprietario dovrebbe eventualmente distruggere tutte le copie in suo possesso, non essendone consentita dalla normativa la duplicazione.

e l'analisi di questi dati comporti un investimento considerevole da parte di un soggetto che, dunque, necessita di essere tutelato; si comprende così la posizione dei produttori dei veicoli che, ritenendo questi dati come diffusi, dunque non riferibili direttamente a un soggetto, escludono che essi possano appartenere agli utilizzatori della vettura[820].

Attenzione merita anche la posizione di chi ritiene che i dati tecnici grezzi non debbano essere considerati come beni economici proprietari, ma come esternalità appropriabili fuori da un esplicito scambio di mercato[821]. Questa interpretazione si fonda sulla qualificazione operata da Calabresi e Melamed circa le possibili forme di tutela che possono essere applicate ai beni economici in ragione delle loro caratteristiche giuridiche[822]. Escludendo la massima tutela concessa dalla *inalienability rule* (che individua un bene proprietario non negoziabile), i dati che vengono generati dai sensori, quali per esempio quelli relativi al traffico stradale, possono essere considerati delle esternalità, intese come beni economici pubblici, generati indirettamente da altre transazioni, privi di tutela giuridica e dunque come tali appropriabili[823].

---

[820] Si veda anche la Comunicazione della commissione, COM (2017) 9 final, ove si sancisce il principio della libera circolazione dei dati. La commissione chiarisce che «i fabbricanti o i fornitori di servizi possono divenire di fatto "proprietari" dei dati generati dalle loro macchine o processi anche quando i dispositivi stessi sono di proprietà dell'utilizzatore». In dottrina si v. ALPA, *La proprietà dei dati personali*, in *Persona e mercato dei dati*, cit., 19; CAMPBELL, *UK urged to clarify data rules from Connected cars*, Financial Times, 3 luglio 2017, consultabile all'indirizzo: *www.ft.com* (ultimo accesso 5 giugno 2021); SIMONINI, *L'intelligenza artificiale guida le nostre vetture*, cit., 149.

[821] NICITA, *op. cit.*, 1171.

[822] Si rimanda a CALABRESI, MELAMED, *Property rules, liability rules, and inalienability: one view of the cathedral* (1972) 6 *Harvard Law Review* 1089 ss.

[823] Si individuano 4 categorie: *property rule*; *liability rule; inalienability rule* e le *externalities*. La "*property rule*" si applica a quei beni proprietari che possono essere oggetto di disposizione da parte del titolare («An entitlement is protected by a property rule to the extent that someone who wishes to remove the entitlement from its holder must buy it from him in a voluntary transaction in which the value of the entitlement is agreed upon by the seller»). La "*liability rule*", invece, determina una regola di responsabilità per cui il terzo sarà chiamato a corrispondere un prezzo al titolare del bene in caso se ne appropri o lo danneggi («Whenever someone may destroy the initial entitlement if he is willing to pay an objectively determined value for it, an entitlement is protected by a liability rule»). Quanto alla "*inalienability rule*" essa individua un perimetro di indisponibilità di beni e diritti, che dunque non possono essere trasferiti dal titolare a terzi («An entitlement is inalienable to the extent that its transfer is not permitted between a willing buyer and a willing seller»). Infine, si parla di "*externalities*" facendo riferimento a quei beni o diritti che discendono indirettamente da altre transazioni, privi dunque di tutela giuridica e appropriabili («[…] a transaction would create significant externalities […] to a third parties. For instance, if Taney were allowed to sell his land to Chase, a polluter, he would injure his neighbour Marshall by lowering the value of Marshall's land. Conceivably, Marshall could pay Taney not to sell his land; but, because there are many injured Marshalls, freeloader and information costs make such transactions practically impossible. The state could protect the Marshalls and yet facilitate the sale of the land by giving the Marshalls an entitlement to prevent Taney's sale to Chase but only protecting the entitlement by a liability rule. It might, for instance, charge an excise tax on all sales of land to polluters equal to its estimate of the external cost to the Marshalls of the sale. But where there are so many injured

Tuttavia, a fronte dell'estrema varietà dei dati, della loro provenienza e dei diversi utilizzi a cui sono soggetti, una categorizzazione generale mal si concilierebbe con una tutela effettiva delle posizioni confliggenti degli interessati da una parte e dai titolari dall'altra.

Per garantire una *governance* che sia adattabile alle diverse esigenze e alle evoluzioni delle tecniche di *data analysis* è dunque necessario contemperare meccanismi di mercato con situazioni nelle quali invece i dati non possano essere considerati beni negoziabili.

Tenendo a mente la classificazione operata da Calabresi e Melamed, dunque, per quanto riguarda i dati non personali se ne potrebbe favorire la circolazione restituendo al titolare[824] il diritto al controllo sull'uso che ne viene fatto, o il reddito che deriva dalla sua commercializzazione o valorizzazione (secondo rispettivamente una *property rule* e una *liability rule*).

Differenti considerazioni dovrebbero valere invece per quei dati che siano espressione della dimensione più strettamente intima e personale dell'individuo e la cui commercializzazione inciderebbe su di una dimensione di dignità della persona, connotato che fonda la stessa idea di identità digitale e di *homo dignus*[825], e che dunque non dovrebbero essere considerati beni negoziabili (secondo una *inalienability rule*).

Quanto infine ai dati grezzi, non strutturati, generati dai sensori, questi potrebbero essere ritenuti esternalità e come tali dunque appropriabili da parte delle imprese, a fronte del fatto che esse hanno operato un investimento nella produzione e/o raccolta di questi dati, la cui disponibilità in via esclusiva rappresenta per esse un valore.

Questa interpretazione potrebbe conciliare differenti istanze, *in primis* quella di individuare una classe di dati di natura non personale di cui permettere una più agevole e libera circolazione; inoltre la possibilità per l'impresa che ha investito nella loro generazione e/o raccolta di appropriarsene e, di conseguenza, di poterne sfruttare il potenziale economico, consentirebbe il buon funzionamento del mercato. Non privando

---

Marshalls that the price required under the liability rule is likely to be high enough so that no one would be willing to pay it, then setting up the machinery for collective valuation will be wasteful. Barring the sale to polluters will be the most efficient result because it is clear that avoiding pollution is cheaper than paying its costs - including its costs to the Marshalls»). V. CALABRESI, MELAMED, *op. cit.*, 1092 s. e 1111. In arg. anche NICITA, *ibidem*.

[824] Potremmo ritenere titolare il soggetto che ha compiuto un investimento rilevante nella generazione o nella raccolta dei dati grezzi.

[825] Sul punto si rimanda ad ALPA, *La proprietà dei dati personali*, cit., 14; RODOTÀ, *Il diritto di avere diritti*, cit.; quanto al diritto all'*habeas data*, ID., *Il mondo nella rete*, cit.

le imprese del vantaggio competitivo raggiunto queste sarebbero infatti maggiormente incentivate nell'investire nel settore. A maggiori investimenti segue solitamente una maggiore offerta di servizi di qualità, così portando un vantaggio anche per i consumatori finali.

Alla luce delle considerazioni sopra svolte, per quanto riguarda i dati generati dalle componenti della vettura, potremmo dunque ritenere la casa costruttrice quale "proprietario"[826], avendo questa compiuto un investimento economico rilevante per la raccolta e l'analisi degli stessi, secondo uno schema che ricalca la *ratio* a fondamento delle normative a tutela della proprietà intellettuale e dei *database*[827]. Difatti si noti che spesso non sono i dati di per sé ad avere valore; questi acquistano valore solo grazie agli strumenti di *data analytics* utilizzati per estrarre informazioni (queste sì aventi un valore economico)[828]. Si tratta di un'attività sofisticata che comporta dei costi; pertanto non si dubita che chi abbia svolto questo tipo di investimento rivesta una posizione meritevole di tutela[829].

Seguendo questa considerazione e dunque ritenendo "proprietario" il soggetto che ha investito nella creazione di un sistema che raccolga e analizzi i dati, rimane da chiarire quale regime giuridico possa efficacemente tutelarne gli interessi.

---

[826] Da questa considerazione si escludono quei dati che permettano l'identificazione di una specifica persona fisica. In questo caso di fronte a dati di natura personale e come tali "appartenenti" alla persona fisica a cui si riferiscono. Si v. Comunicazione della Commissione, *Una strategia europea per i sistemi di trasporto intelligenti cooperativi, prima tappa verso una mobilità cooperativa, connessa e automatizzata*, cit.

[827] Contra la posizione espressa nel documento elaborato nel 2016dal Texas A & M Transport Institute, *Data ownership issues in a connected car environment*, consultabile all'indirizzo: *https://static.tti.tamu.edu/tti.tamu.edu/documents/165604-1.pdf* (ultimo accesso 5 giugno 2021), ove si rileva che per proprietario dai dati generati dal veicolo si deve intendere il proprietario della vettura. Il concetto di proprietà, quando è riferito a beni immateriali, non è evidentemente legato alla "fisicità" de1 dato, quanto alla possibilità di controllarlo. Se il proprietario dei dati è il proprietario del veicolo, è tuttavia evidente che non li può controllare, ma deve delegare il controllo al costruttore del mezzo. Del pari quest'ultimo deve raggiungere un accordo con il proprietario del mezzo per estrarli e usarli.

[828] Sul punto ricorda Zeno Zencovich come «We are shifting the legal framework from ownership to service provision. Whether the latter is provided by the data holder, or the third party is granted a license to extract certain results from the data, we have moved from property to contract». ZENO ZENCOVICH, *Ten legal perspectives on the "big data revolution"*, in *Conc. merc.*, 2016, 34.

[829] ALPA, *La proprietà dei dati personali*, cit., 31.

4.1 Quale tutela giuridica per i dati grezzi non personali

Alcune considerazioni devono essere infine svolte in merito a quale tutela giuridica sia possibile accordare ai dati grezzi, dunque non strutturati, di natura non personale, tra cui possono essere fatti rientrare anche quelli generati da un sistema algoritmico[830].

Il regime classico della proprietà, intesa in senso romanistico, non sembra essere in linea con la natura stessa dei dati e con il loro modo di circolazione.

L'istituto della proprietà ha una struttura complessa che ha visto per lungo tempo la dottrina civilistica interrogarsi nella ricerca di una sua definizione. La difficoltà di approdare a una concezione unitaria dell'istituto può essere fatta discendere in parte dalle molteplicità degli "statuti proprietari"[831], che rifuggono da una definizione comune, in parte dalla diffusione tra gli interpreti di un approccio "antiformalista", ispirato alla dogmatica tedesca. La faticosa ricerca definitoria ha così lasciato spazio a una riflessione avente a oggetto la struttura dell'istituto e le sue caratteristiche[832].

Potremmo pertanto descrivere la proprietà secondo quelle che sono, nel nostro ordinamento, le caratteristiche principali che ne definiscono la sostanza: il diritto di escludere i terzi dal godimento e il potere assoluto che il titolare può esercitare sull'oggetto.

Sebbene dunque venga garantita dall'ordinamento una forma di tutela molto intensa per il proprietario, le stesse caratteristiche dei dati e le esigenze di sfruttamento economico degli stessi sembrano ostare all'applicazione di un regime proprietario[833]. Si ricorda, infatti, come l'istituto sia nato per rispondere all'esigenza di allocare risorse scarse, frenando possibili situazioni di abuso[834], permettendo lo sfruttamento pieno ed

[830] Non si fa riferimento al caso in cui i dati siano inventati, rappresentati artisticamente, rielaborati o creati dall'interessato. In queste circostanze, ricorda Alpa, questi potrebbero infatti essere qualificati come opere d'arte o invenzioni ed essere dunque tutelati secondo le relative normative di settore. ALPA, *La proprietà dei dati personali*, cit., 27 ss.

[831] MATTEI, voce «proprietà», nel *Digesto, Disc. priv*., *sez. civ.*, XV, Torino, 1997, 433 ss.

[832] Si rimanda per un approfondimento a MATTEI, voce «proprietà», cit.

[833] ZENO ZENCOVICH, *Dati, grandi dati, dati granulari*, cit., 33 s.; FIA, *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in *Nuovo not. giur.*, 2019, 92 ss.

[834] Ricorda Mattei come l'istituzione della proprietà privata si giustifica come rimedio alla c.d. tragedia dei beni comuni. «Si tratta del ben noto problema per cui in mancanza di disciplina giuridica dell'appartenenza, tutti gli individui sono portati ineluttabilmente verso la catastrofe ingenerata dall'appropriazione selvaggia di risorse scarse (e.g. balene) non disciplinate come tali. La ragione di ciò è che ciascun individuo tenderà ad appropriarsi del maggior numero possibile di risorse perché i benefici di tale appropriazione ricadranno interamente su di lui mentre i costi verranno divisi fra tutti i consociati. Un esempio assai banale si ha nello sfruttamento selvaggio della Foresta Amazzonica laddove i benefici

esclusivo dei beni di cui un soggetto è proprietario, senza limiti temporali. Tuttavia, come visto, i dati sembrano avvicinarsi maggiormente ai beni pubblici; questi non sono beni scarsi, consumabili, né rivali; dunque, l'uso non ne comporta un esaurimento né interferisce con l'uso altrui, potendo uno stesso dato essere usato contemporaneamente da diversi soggetti [835] (si pensi ai dati personali che vengono richiesti continuamente agli utenti nella navigazione web).

Inoltre, i dati sono per vocazione naturale destinati a circolare fuori dai confini di un determinato territorio; pertanto, mancando ancora una base comune per un vero e proprio diritto privato europeo, il riconoscimento di un regime proprietario finirebbe col generare conflitti tra i diversi ordinamenti, così finendo di fatto per ostacolarne la circolazione e lo sfruttamento[836].

Nemmeno in relazione ai dati personali sembra trovare fondamento un approccio di tipo proprietario. Le stesse disposizioni del GDPR, più che un diritto dominicale, prevedono un potere di controllo sull'uso che ne viene fatto, un diritto di opposizione al trattamento e di cancellazione dai dati illegittimamente trattati[837]. Né il consenso dell'interessato sembra essere espressivo di uno schema contrattuale avente ad oggetto la vendita dei dati personali, ma piuttosto di una delega all'impiego esclusivo,

economici ed i costi sociali del disboscamento sono allocati in modo del tutto divaricato». V. MATTEI, voce «proprietà», cit., 435 ss.; ID., *La proprietà*, nel *Trattato Sacco*, II, Torino, 2015, 145.

[835] V. ZENO ZENCOVICH, *Dati, grandi dati, dati granulari*, *ibidem*; ID., *Ten legal perspectives*, cit., 29 s.; ZENO ZENCOVICH, GIANNONE CODIGLIONE, *op. cit.*, 36; FIA, *op. cit.*, 98 s.; STAZI, CORRADO, *op. cit.*, 445 ss. In arg. anche RUOTOLO, *ibidem*, il quale richiama Stiglitz che già negli anni '80, sebbene non in riferimento ai Big Data, interpretava le informazioni come beni pubblici, essedo questi beni aventi le caratteristiche di non rivalità e non esclusività.

[836] ZENO ZENCOVICH, *Dati, grandi dati, dati granulari*, *ibidem*.

[837] Evidenzia ancora Zeno Zencovich come la prassi di uso dei dati abbia piuttosto fatto emergere come i diritti concessi agli interessati siano quasi illusori, dal momento che una volta acquisiti i dati questi sono utilizzati, trasferiti, elaborati, ceduti e duplicati spesso all'insaputa dell'interessato. V. ZENO ZENCOVICH, *Dati, grandi dati, dati granulari*, cit., 35. Della stessa opinione STAZI, CORRADO, *op. cit.*, 460 ss. Dette criticità emergono anche nel contesto dei dati relativi alla salute, ai quali spesso hanno accesso differenti soggetti per differenti finalità. Cfr. EVANS, *Much ado about data ownership* (2011) 25 *Harvard law review* 77 ss. *Contra* Janeček, il quale ritiene che vi siano alcuni dati aventi una intrinseca natura personale, che li rende espressione della personalità del soggetto e, dunque, come ogni espressione dell'identità personale, non possono essere considerati beni appropriabili e commerciabili; tuttavia, a esclusione di questi la forma che sembra meglio adattarsi alle esigenze di controllo e tutela dei dati appare proprio quella della classica proprietà. L'A. ritiene compatibili le disposizioni del GDPR con detto regime, dal momento che una effettiva autodeterminazione dell'interessato nel controllo dei propri dati, come emerge dalla normativa europea, è pienamente possibile allorquando a quest'ultimo sia riconosciuto una proprietà piena, secondo una concezione classica dell'istituto. Cfr. JANEČEK, *op. cit.*, 1041 ss.

funzionale a erogare un servizio determinato secondo i fini dichiarati nell'informativa[838].

Maggiormente compatibile si dimostra un regime di titolarità, quale quello vigente per i beni immateriali, che permetterebbe di garantire alcuni diritti di esclusiva e di sfruttamento economico, prevedendo al contempo limiti e rimedi[839]. È tuttavia bene notare come anche detta soluzione presenti alcune criticità: autorevole dottrina ricorda, infatti, come l'affermazione di pretese giuridiche sui beni immateriali sia possibile a fronte di un loro espresso riconoscimento normativo, essendo questi un *numerus clausus*[840] che, per quanto riguarda i dati, sembrerebbe invece ancora difettare[841]. Questi godrebbero di una tutela indiretta attraverso la disciplina della concorrenza sleale, della responsabilità civile, dei segreti d'impresa, ma non di per sé[842] (con l'esclusione di dati personali e dei *database*). Inoltre, in ragione delle caratteristiche proprie dei dati, come sopra richiamate, secondo una prospettiva di efficienza di mercato, una volta che il bene

---

[838] Differente è la consapevolezza di prestare un consenso all'utilizzo dei propri dati e quella che invece deve presiedere la partecipazione a una transazione economica avente a oggetto questi ultimi; consapevolezza che manca sia nel primo caso, che a maggior ragione nel secondo ove spesso i servizi vengono percepiti come gratuiti dagli utenti. V. MACERATINI, Privacy *e informazione nell'era dei Big Data*, cit., 87. Si pensi sul punto ai recenti arresti giurisprudenziali ove le Corti hanno rilevato come ingannevoli le informative presentate da Facebook. La società, infatti, presentava il servizio come gratuito e non avente, invece, quale corrispettivo la raccolta e l'utilizzo dei dati personali degli utenti. Si v. T.A.R. Lazio, 10.1.2020, in *Dir. internet*, 2020, consultabile all'indirizzo: *https://dirittodiinternet.it* (ultimo accesso 4 maggio 2021).

[839] STAZI, CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. inform.*, 2019, 451 ss.; ZENO ZENCOVICH, *Dati, grandi dati, dati granulari*, cit., 32 ss.; G. RESTA, I *diritti della personalità*, cit., 569.

[840] Per un approfondimento in merito ai beni immateriali e alla loro tutela giuridica si rimanda a G. RESTA, *Nuovi beni immateriali e* numerus clausus *dei diritti esclusivi*, in *Diritti esclusivi e nuovi beni immateriali*, a cura di ID., Milano, 2010, 11 ss.; ID., *I diritti della personalità*, cit., 552 ss.

[841] V. ZENO ZENCOVICH, GIANNONE CODIGLIONE, *Ten legal perspectives on the "big data revolution"*, cit., 30 s.; ZENO ZENCOVICH, *Dati, grandi dati, dati granulari*, cit., 33 ss.; STAZI, CORRADO, *op. cit.*, 452 ss.

Se si aderisse alla ricostruzione che vede l'estensione di un regime di titolarità per i dati, ricorda Resta, ne discenderebbe come la menzione del diritto alla protezione dei dati da parte del legislatore dovrebbe intendersi come costitutiva di un nuovo bene immateriale, rappresentato appunto dai dati personali. Difatti, «non a caso, potrebbe osservarsi, si è adottata l'espressione "protezione dei dati" a preferenza dell'omologa "autodeterminazione informativa", intendendosi con ciò rimarcare che sono le informazioni, e non la persona, a costituire il termine di riferimento oggettivo della tutela». G. RESTA, *I diritti della personalità*, cit., 570.

[842] ZENO ZENCOVICH, *Dati, grandi dati, dati granulari*, cit., 34. Evidenzia l'A. come la stessa pretesa appropriativa rischia di apparire utopistica di fronte una mole di dati sempre più estesa. Difatti a fronte del volume di dati la cui circolazione e duplicazione non presenta particolari costi, «schemi generali di titolarità risultano di scarsa utilità ai fini pratici, ovverosia quello di assicurare ad un soggetto – e solo a quel soggetto – il diritto di trarre un vantaggio economico dalla sua posizione». L'A. conclude evidenziando come la tutela dei diritti individuali si presti a essere tutelata non tanto mediante istituti privatistici, quanto piuttosto mediante più penetranti poteri di controllo di natura pubblicistica, di cui sono titolari gli Organi quali i Garanti per la protezione dei dati personali.

"informazione" è stato prodotto dovrebbe essere reso accessibile a tutti coloro che vi abbiano interesse.

Tuttavia, la considerazione dei dati come beni liberamente accessibili a tutti non sarebbe compatibile con quei casi in cui il bene non sarebbe stato prodotto perché svantaggioso dal punto di vista economico, non potendo il produttore ricavarne un vantaggio competitivo. In questi contesti allora potrebbe trovare spazio una temporanea "privatizzazione del bene", applicando per esempio la normativa sul diritto d'autore[843]. Nemmeno questa soluzione sembra però essere pienamente compatibile con le caratteristiche dei *dataset* prodotti dagli IoT, in particolare di quelli aventi natura non personale.

La tutela accordata dal diritto d'autore difatti si fonda sul requisito dell'originalità dell'opera, quale espressione/creazione dell'autore. Pur dando un'interpretazione estensiva al concetto di "originalità" non sembra comunque possibile estenderne la nozione a una mera raccolta di dati non strutturati, effettuata mediante processi automatizzati[844], diversamente da quanto previsto per i software, i quali sono invece espressione di un'opera creativa e originale del programmatore[845].

---

[843] A fronte anche della considerazione per cui il costo marginale di riproduzione è pari a zero, si ritiene che una volta remunerato il produttore (mediante una forma di privatizzazione temporanea), il bene dovrebbe successivamente essere allocato a tutti i soggetti che lo richiedano. Sul punto precisa Nicita come «Anche quando l'informazione è un bene privato, e quindi escludibile, – ad esempio in quanto protetta da un brevetto – l'efficienza di mercato richiede che il diritto di proprietà sul bene informazione sia comunque limitato nel tempo, per una durata sufficiente a far recuperare al titolare i costi di investimento necessari a generare l'informazione e dunque idoneo ad allineare in via ottimale gli incentivi ad investire, almeno secondo la tradizionale impostazione microeconomica». V. NICITA, *op. cit*., 1165 e spec. 1167. In arg. si veda anche PRETA, ZOBOLI, *Intelligenza artificiale ed economia dei dati*, cit., 213 ss. Gli A. ritengono, infatti, che una privatizzazione potrebbe scoraggiare gli investimenti nel settore, per tanto sarebbe maggiormente auspicabile un approccio che valuti, caso per caso, in quale settore i dati possano di per sé rappresentare un *essential facility* e, quindi, quando l'accesso agli stessi debba essere esteso a tutti gli attori economici, evitando così barriere all'ingresso nei mercati.

[844] FARKAS, *Data created by the Internet of Things: The new gold without ownership* (2017) 23 *Revista la propiedad inmaterial* 7 ss.; DETERMANN, *op. cit.*, 13 ss.

[845] Il dibattito circa la protezione da accordare ai programmi per gli elaboratori elettronici ha interessato gli interpreti fin dagli anni '80, momento in cui si sono iniziati a diffondere i computer e sono nate alcune aziende produttrici di software. Dibattuta era la questione se il software, in quanto bene immateriale, potesse essere soggetto alla tutela brevettuale o del diritto d'autore. Nel nostro ordinamento è stata accolta questa seconda interpretazione. Dunque, ai sensi della l. n. 633/1941 i programmi per elaboratore sono tutelati dalla legge sul diritto d'autore come opere letterarie «*in qualsiasi forma espressi, purché originali quale risultato della creazione intellettuale dell'autore*». L'art. 2, n. 8, chiarisce, inoltre, che oggetto di tutela è anche il materiale preparatorio necessario alla progettazione del programma. Rimangono esclusi dalla tutela così accordata «*le idee e i principi che stanno alla base di qualsiasi elemento di un programma, comprese quelli alla base delle sue interfacce*». Tuttavia, col passare del tempo e con il progresso e la diffusione delle tecnologie, sono stati concessi anche brevetti per invenzioni attuate per mezzo di programmi per elaboratore, purché – come chiarito dall'Ufficio Brevetti Europeo con decisione T1173/97 (consultabile all'indirizzo: *www.epo.org*, ultimo accesso 15 luglio2021) – queste costituiscano

Difficile anche individuare chi possa essere considerato autore dei dati generati dagli IoT, dal momento che, secondo la normativa, solo una persona fisica può essere considerata autore, escludendo dalla tutela così riconosciuta quelle creazioni che sono unicamente state prodotte da algoritmi[846].

Nemmeno la normativa regolante i *database*[847], Direttiva 9/96 CE, recepita nel nostro ordinamento nella legge sul diritto d'autore (l. 22 aprile 1941, n. 633, agli artt. 2 e 102 bis), pare essere applicabile nel caso che ci occupa.

La normativa europea instaura un doppio binario di tutela per i *database*: «*le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione dell'ingegno propria del loro autore*»[848] sono tutelate dal diritto d'autore; tutela che tuttavia «*non si estende al loro contenuto e lascia impregiudicati i diritti esistenti su tale contenuto*»[849] . Nel caso in cui la banca dati non possa invece dirsi una "creazione

---

un contributo tecnico, o contribuiscano allo stato dell'arte in un settore tecnico, giudicato non ovvio da una persona competente in materia. In argomento si rimanda tra i molti a GRANIERI, PARDOLESI, *Il software*, in *AIDA*, 2007, 288 ss.; RANIELI, *Cronache in tema di brevettabilità delle invenzioni* software related*, con particolare riguardo al ruolo dell'EPO e alla più recente giurisprudenza del regno unito*, in *Riv. dir. ind.*, 2009, 233 ss.

[846] FARKAS, *op. cit.*, 8. Considerazioni simili sono emerse anche in relazione alla regolazione vigente negli Stati Uniti, v. sul punto ZHANG, *op. cit.*, 305 ss. Sul tema del riconoscimento del diritto d'autore per le opere prodotte da una AI si rimanda, tra i tanti, a SPEDICATO, *Creatività artificiale, mercato e proprietà intellettuale*, in *Riv. dir. ind.*, 2019, 253 ss.; FRANZOSI, Copyright*: chi è l'autore delle opere generate a computer?*, in *Dir. aut.*, 2018, 168 ss.

[847] Una definizione di banca dati si rinviene all'art. 1 della Direttiva CE n. 9/96, secondo cui essa viene definita come «*una raccolta di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili grazie a mezzi elettronici o in altro modo*». A chiarire la portata piuttosto ampia della definizione il Considerando n. 17, dir. CE n. 9/96, precisa che: «*con il termine 'banca di dati' si intende definire una raccolta di opere, siano esse letterarie, artistiche, musicali o di altro genere, oppure di materiale quali testi, suoni, immagini, numeri, fatti e dati; che deve trattarsi di raccolte di opere, di dati o di altri elementi indipendenti, disposti in maniera sistematica o metodica e individualmente accessibili*».

La definizione similmente a quanto accaduto per il concetto di dato personale, ha subito un notevole ampliamento in via ermeneutica grazie all'opera della Corte di Giustizia. Si v. a titolo di esempio Corte giust. CE, grande sezione, 9.11.2004, C-444/2002, in *Dir. aut.*, 2005, 574; Corte giust. UE, 29.10.2015, C-490/2014, in *Dir. inform*., 2016, 185.

[848] Art. 3., dir. CE n. 9/96.

[849] La Corte di Giustizia ha chiarito che una banca dati può essere tutelata dal diritto d'autore «*se la scelta o la disposizione del contenuto costituisca una creazione intellettuale del proprio autore*». Viene dunque in rilievo la nozione di "creazione intellettuale" che necessita, quale requisito essenziale, del carattere di originalità. La Corte continua precisando che «*tale criterio è soddisfatto quando, mediante la scelta o la disposizione dei dati in essa contenuti, il suo autore esprima la sua capacità creativa con originalità, effettuando scelte libere e creative*». Corte giust. UE, 1.3.2012, C-604/2010, in *Dir. com. scamb. int.*, 2012, 269. Lo stesso Considerando n. 15, dir. CE n. 9/96, precisa che: «*i criteri da applicare per stabilire se una banca dati sia protetta dal diritto d'autore dovranno limitarsi al fatto che la scelta o la disposizione del contenuto della banca di dati costituisce una creazione intellettuale, propria dell'autore; che questa protezione riguarda la struttura della banca di dati*" e "*non dovranno essere applicati altri criteri diversi da quello di originalità, nel senso di creazione intellettuale, per stabilire se una banca di*

dell'ingegno", ma sia il risultato di un rilevante investimento qualitativo e/o quantitativo[850], questa potrà essere tutelata unicamente secondo il c.d. "diritto *sui generis*".

Le considerazioni sopra svolte in relazione all'applicabilità delle disposizioni a tutela del diritto d'autore possono estendersi anche a questo contesto, così escludendo la qualificazione dei dati generati e raccolti dai sistemi algoritmici come *database* coperti dal diritto d'autore. A ciò si aggiunga come i dati raccolti non solamente non sono tra loro omogenei, ma non vengono – come visto – né selezionati né organizzati, come invece viene fatto nella creazione di una banca dati; non possono dunque dirsi espressione di una creazione intellettuale, e ciò anche perché la raccolta viene effettuata in modo automatico durante l'utilizzo delle applicazioni digitali[851].

Sotto certi aspetti potrebbe essere più aderente al contesto tecnologico in analisi la tutela accordata dal c.d. diritto *sui generis*, in quanto la raccolta e la conservazione dei dati, oltre che la loro analisi, richiede un investimento in termini sia economici che di dotazioni strumentali[852].

Affinché possa trovare applicazione la tutela sopra richiamata è necessario che l'investimento sia rilevante. Sulla portata del requisito si è più volte espressa la Corte di Giustizia, la quale ha chiarito che può dirsi rilevante un investimento: che insista sui mezzi destinati alla ricerca e alla raccolta dei dati; che sia diretto all'impiego di mezzi volti al controllo e all'esattezza degli elementi ricercati e, infine, quello diretto alla

---

dati sia tutelabile o meno in base al diritto d'autore, e in particolare non dovrà essere effettuata alcuna valutazione della qualità o del valore estetico della banca di dati».

[850] V. MORO VISCONTI, *La valutazione economica dei database (banche dati)*, in *Dir. ind.*, 2017, 359 ss.; CIANI, *Property rights model v. contractual approach: how protection non-personal data in cyberspace?*, in *Dir. comm. int.*, 2017, 838 ss.; OTTOLIA, *op. cit.*, 73 ss.

[851] OTTOLIA, *op. cit.*, 84 ss.; BOGNI, DEFANT, *Big Data: Diritti IP e problemi della* privacy, in *Dir. ind.*, 2015, 117 ss. Le Autrici evidenziano come potrebbe forse sostenersi che l'opera di disposizione dei dati che compie l'algoritmo possa essere in certi casi considerata come una creazione intellettuale; ciò in quanto la grande mole di dati raccolta e conservata viene successivamente analizzata spesso con il fine di clusterizzare i dati. Tuttavia questa posizione non sembra pienamente coerente con la *ratio* della tutela accordata dalla normativa sul diritto d'autore, che pare riferirsi al fatto che l'opera creativa sia espressiva della personalità – dell'ingegno – dell'autore, presupponendo la presenza di una persona fisica che possa dirsi tale. In argomento anche MACERATINI, Privacy *e informazione nell'era dei Big Data*, cit., 83, ricorda, giustamente, come la maggior parte dei Big Data raccolti risulti in genere non strutturata, ciò in quanto viene acquisita e memorizzata secondo criteri differenti da quelli che regolano l'organizzazione dei tradizionali archivi elettronici.

[852] Art. 7, dir. CE n. 9/96.

creazione di un'architettura della banca dati che permetta un'organizzazione sistematica del materiale e l'accessibilità agli utenti[853].

Parte dei commentatori ritiene, tuttavia, che, per quanto riguarda i dati raccolti dai sistemi digitali, mancherebbe proprio l'elemento costitutivo della rilevanza dell'investimento. Le grandi imprese raccoglierebbero dati come sottoprodotto di altre attività produttive, non affrontando dunque costi elevati per la raccolta e conservazione e non superando, conseguentemente, la soglia della rilevanza prevista dalla Direttiva 9/96 CE[854].

L'argomento non sembra pienamente convincente.

Le imprese che operano nel mercato digitale devono necessariamente effettuare investimenti rilevanti, se non nella raccolta, nei sistemi algoritmici in grado di trovare correlazioni ed estrarre valore dai dati. In linea di principio potremmo dunque ritenere applicabile ai *dataset* così raccolti il diritto c.d. *sui generis*. Si dubita, tuttavia, che anche tale soluzione possa apprestare una tutela adeguata agli interessi economici dei titolari.

La tutela accordata al titolare si mostra meno intesa, limitandosi la normativa a regolare le possibilità di utilizzo in modo lecito del *database* da parte di terzi. Il diritto *sui generis* è rivolto, infatti, a «*impedire l'estrazione e/o il riutilizzo dell'intero o di una parte sostanziale, valutato qualitativamente del contenuto della banca dati*»[855], non accordando quindi un vero e proprio diritto di sfruttamento esclusivo al soggetto che ha investito nella raccolta.

Tenendo a mente il funzionamento degli algoritmi di *data analysis*, non sembra possibile garantire nemmeno il minimo di tutela accordata. Si ricorda, infatti, come l'estrema varietà dei dati raccolti e la capacità di trovare correlazioni a cui dare significato sia di ostacolo all'identificazione di una "parte sostanziale" [856] dei Big Data

---

[853] La nozione di investimento significativo è anch'esso frutto di un'opera ermeneutica della Corte di Giustizia. In particolare si v. Corte guist. CE, 9.11.2004, C-203/2002, in *Eur. dir. priv.*, 2006, 319; Corte giust. CE, 9.11.2004, C-444/2002, cit.

[854] In argomento TUCKER, WELLFORD, *Big mistakes regarding big data* (2014) *The antitrust source* 3; FIA, *op. cit.*, 78.

[855] Sul punto Bogni e Defant chiariscono come il divieto di estrazione e reimpiego colpisca non solamente le operazioni aventi fini commerciali, ma più in generale tutte quelle attività che posseggano un carattere "parassitario", tali dunque da poter limitare gli interessi di stampo economico di colui che ha elaborato il *database*. Cfr. BOGNI, DEFANT, *op. cit.*, 119 ss.

[856] Quanto alla nozione di "parte sostanziale", la Corte di Giustizia ha chiarito come la stessa sia legata ad una valutazione «*sotto il profilo quantitativo dovendosi intendere il volume dei dati estratti e/o reimpiegati in relazione al volume del contenuto totale della banca e, sotto il profilo qualitativo,*

sottoposti al trattamento. Il singolo dato di per sé non ha valore, ma lo acquista nel complesso dell'analisi a cui viene sottoposto. Pertanto non è possibile fornire a priori una valutazione circa l'essenzialità o meno dei dati presi in considerazione[857]. Anche una grande quantità di dati, ove non analizzati con algoritmi adeguati, potrebbe non corrispondere a una parte sostanziale; del pari, una piccola parte di dati estratti, grazie all'analisi effettuata mediante algoritmi efficienti, potrebbe essere considerata una parte sostanziale dell'intero *dataset*[858].

A questi rilievi deve inoltre aggiungersi come il diritto esclusivo del costitutore sorga al momento del completamento della banca dati[859]. Una previsione di tal fatta evidentemente stride con lo stesso funzionamento dei sistemi *data driven*, e delle vetture connesse e autonome in particolare, che sono invece destinate a generare e raccogliere dati in modo continuativo, secondo un processo dinamico.

Difficoltà sorgono in merito all'applicazione della normativa in analisi anche per i c.d. *single-source database*, cioè quelle banche dati a cui può avere accesso unicamente il creatore. Evidentemente una tutela giuridica di stampo proprietario potrebbe generare distorsioni della concorrenza e situazioni di monopolio, impedendo totalmente la circolazione dei dati raccolti e conservati[860]. Nella consapevolezza di tali rischi la Corte di Giustizia ha così chiarito che «*il fine della tutela, conferita dal diritto sui generis, introdotta dalla direttiva, è infatti di incentivare la creazione di sistemi di memorizzazione e di gestione di informazioni esistenti, e non la creazione di elementi che possano essere successivamente raccolti in una banca dati*»[861]. Ne discende come la Direttiva 9/96 CE non sia dunque applicabile nel caso in cui gli investimenti del

---

dovendosi invece fare riferimento alla rilevanza dell'investimento collegato al conseguimento, verifica o presentazione relativa a quella parte del contenuto che è stata estratta o reimpiegata, indipendentemente dal fatto che tale parte rappresenti una parte quantitativamente sostanziale del contenuto complessivo della banca di dati». Corte giust. CE, 9.11.2004, C-203/2002, cit. Il riferimento a una valutazione qualitativa potrebbe essere più in linea con la prassi applicativa legata all'elaborazione dei Big Data, tuttavia appare complessa una verifica in tale senso proprio in ragione della estrema varietà dei dati raccolti e delle stesse tecniche di analisi utilizzate.

[857] PRETA, ZOBOLI, *IA ed economia dei dati*, cit., 219 s., i quali sottolineano come appaia impossibile individuare *ex ante* quali tra le tante informazioni siano essenziali nel *dataset*.

[858] ZENO ZENCOVICH, *Ten legal perspectives*, cit., 33 ss.

[859] Art. 102 *bis*, comma 6°, l. 22 aprile 1941, n. 633.

[860] Per un approfondimento in merito alle *single-source database* si rimanda a BORGHI, KARAPAPA, *Contractual restrictions on lawful use of information: sole-source databases protected by the back door?* (2015) 8 *European intellectual property review* 505 ss.

[861] Corte giust. CE, 9.11.2004, C-203/2002, cit., par. 31. In dottrina v. FARKAS, *op. cit.*, 9.

creatore si limitano alla produzione dei singoli elementi, che poi verranno conservati nella banca dati da lui unicamente accessibile.

Le disposizioni normative richiamate non sembrano allora sufficienti a garantire un'effettiva protezione del diritto di sfruttamento economico del soggetto che ha effettato un investimento per la raccolta e la conservazione dei dati e che dunque rischierebbe di vedersi privato del vantaggio competitivo così raggiunto.

Parte dei commentatori ritiene applicabile alla materia che ci occupa la normativa sui *trade secrets*[862], prevista dalla Direttiva 943/2006 UE[863], considerando i dati come un insieme di asset, replicabili e non, ripetibili e non, profilati attraverso altre risorse proprietarie, quali i processi algoritmici, le cui caratteristiche restano segrete[864]. Per valutarne l'effettiva applicabilità è necessario chiarire innanzitutto cosa si intenda per segreto commerciale e se tale nozione possa ricomprendere anche le raccolte di dati generati dagli IoT.

Sul punto, la Direttiva all'art. 2 prevede alcuni requisiti a cui devono rispondere le informazioni raccolte affinché possano essere considerate "segrete" e come tali soggette alle misure di protezione ivi previste. Si precisa che esse: «*a) sono segrete nel senso che non sono, nel loro insieme o nella precisa configurazione e combinazione dei loro elementi, generalmente note o facilmente accessibili a persone che normalmente si occupano del tipo di informazioni in questione; b) hanno valore commerciale in quanto segrete; c) sono state sottoposte a misure ragionevoli, secondo le circostanze, da parte della persona al cui legittimo controllo sono soggette, a mantenerle segrete*»[865].

È bene specificare che le informazioni sono coperte da segreto fintanto che esse siano accessibili solo a un numero ristretto di persone, che ne hanno il legittimo controllo. La tutela così accordata non è inoltre soggetta a un termine, come per gli altri diritti di proprietà intellettuale, ma si estingue qualora le informazioni siano in qualche modo svelate, divenendo così di pubblico dominio.

---

[862] In arg. OTTOLIA il quale ritiene la normativa a tutela del segreto industriale efficace nella regolazione non solamente dei dati quali "giacimenti", ma anche del codice sorgente del software e, infine, degli strumenti di analisi dei dati che vengono incorporati. V. OTTOLIA, *op. cit.*, 43 ss.

[863] BOGNI, DEFANT, *op. cit.*, 118 ss.

[864] NICITA, *op. cit.*, 1174; OTTOLIA, *ibidem*

[865] Art. 2, dir. UE n. 943/2016. Il testo continua definendo la persona fisica o giuridica che controlla legittimamente il segreto come «*detentore del segreto commerciale*». Il testo della Direttiva è ripresto pressoché integralmente agli artt. 98 e 99 c.p.i., i quali disciplinano il diritto di proprietà industriale sulle informazioni riservate.

Dalla lettura della disposizione non sembra in prima istanza pacifica l'estensione applicativa di tutti i requisiti previsti anche al contesto che ci occupa.

Detta normativi potrebbe ben adattarsi al fenomeno digitale nella dimensione in cui la tutela prevista si accorda sia ai singoli dati che all'intero *dataset*; inoltre, non sono necessari requisiti di originalità, ma i dati possono semplicemente riguardare un'attività commerciale la cui raccolta e archivio facciano parte di dette attività. Tuttavia, le maggiori criticità fanno ancora una volta perno sul valore attribuibile ai dati raccolti. Alcuni commentatori ritengono, infatti, che non sia conciliabile il requisito del valore commerciale delle informazioni[866], facendo leva sul Considerando n. 14 il quale prescrive che la definizione di segreto commerciale esclude le informazioni trascurabili[867]. Dal momento che non sono i dati ad avere valore, quanto piuttosto il processo di analisi a cui sono sottoposti, ne discende come questi non possano avere di per sé un valore commerciale rilevante, come invece richiederebbe la normativa[868].

Tuttavia a questa lettura può essere contrapposta la considerazione per cui non potendo definire a priori quali dati nell'insieme abbiano rilevanza per un determinato trattamento, potrebbero essere tutti considerati rilevanti. Pertanto, nessun dato

[866] FIA, *op. cit.*, 82 ss. Contra BOGNI, DEFANT, *ibidem*. Le Autrici ritengono che il valore economico sussista non solo quando sia positivamente noto che i dati consentono, ad esempio, di ricavare una profilazione di un numero di utenti tali da rivestire interesse economico, oppure di dare in modo attendibile informazioni sulla correlazione fra fatti, ma anche quando si possa comunque ritenere che un operatore economico sarebbe interessato ad acquistarli nella prospettiva di processarli, avendo una ragionevole aspettativa di trarne delle informazioni utili per la sua attività. Conf. Ottolia, il quale ritiene che il requisito della significatività dell'investimento, a differenza che nella disciplina sui *database*, non dovrebbe rilevare nell'ambito della fattispecie costitutiva del diritto. Anche un investimento minimo potrebbe essere ritenuto idoneo a creare un giacimento di dati oggetto della protezione del diritto. Quanto alla precisazione per cui l'informazione non debba essere di "poca importanza", l'A. sottolinea come l'importanza a cui il considerando fa riferimento dovrebbe attenere «all'idoneità di questa a servire gli interessi del titolare non riguarda invece l'investimento effettuato a monte per ottenerla». OTTOLIA, *op. cit.*, 56 ss. e spec. 57.

[867] «*È importante stabilire una definizione omogenea di segreto commerciale, senza imporre restrizioni sull'oggetto da proteggere contro l'appropriazione illecita. Detta definizione dovrebbe pertanto essere costruita in modo da comprendere il know-how, le informazioni commerciali e le informazioni tecnologiche quando esiste un legittimo interesse a mantenere la riservatezza nonché una legittima aspettativa circa la tutela di tale riservatezza. Inoltre, tali know-how o informazioni dovrebbero avere un valore commerciale, sia esso effettivo o potenziale. Tali know-how o informazioni dovrebbero considerarsi come aventi un valore commerciale, ad esempio, laddove l'acquisizione, l'utilizzo o la divulgazione non autorizzati degli stessi rischino di recare danno agli interessi della persona che li controlla lecitamente, poiché pregiudicano il potenziale scientifico e tecnico, gli interessi commerciali o finanziari, le posizioni strategiche o la capacità di competere di detta persona. La definizione di segreto commerciale esclude le informazioni trascurabili, l'esperienza e le competenze acquisite dai dipendenti nel normale svolgimento del loro lavoro, ed esclude altresì le informazioni che sono generalmente note o facilmente accessibili alle persone all'interno delle cerchie che normalmente si occupano del tipo di informazioni in questione*». Considerando n. 14, dir. UE n. 973/2016.

[868] ZECH, *Data as a tradeable commodity* (2016) *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution* 63; FIA, *op. cit.*, 88 s.; FARKAS, *op. cit.*, 10 ss.

all'interno dei *dataset* può dirsi in linea di massima trascurabile, dal momento che non si ha una precisa conoscenza di quale sia il peso che esso potrà rivestire nei futuri trattamenti.

Più condivisibili sono invece le perplessità in merito al requisito della segretezza, il quale non sembra essere pienamente applicabile nel contesto dei dati generati e raccolti dalle auto connesse. Basti pensare come ai dati di posizionamento delle vetture debbano avere liberamente accesso oltre che l'infrastruttura anche le altre vetture connesse circolanti. Si tratta di un numero molto elevato di soggetti, non tutti conoscibili a priori; condizione questa che rendere difficile poter considerare osservato il requisito della segretezza[869]. Sarebbe inoltre difficile la determinazione delle misure ragionevoli che il detentore deve porre in essere per soddisfare detto requisito, ciò in quanto alcuni dati devono necessariamente essere condivisi e accessibili al fine di permettere lo stesso funzionamento delle vetture.

Infine, anche la protezione offerta dal segreto non sembra rispondere pienamente alle esigenze degli operatori economici, non prevedendo la normativa un diritto esclusivo in capo al detentore. Quest'ultimo viene invece tutelato mediante una regolazione dei modi di acquisizione, uso e divulgazione dei segreti ritenuti leciti, la cui violazione dà luogo a responsabilità.

Il detentore del segreto ha dunque un mero potere di fatto sulle informazioni; potere in parte equiparabile a quello del possessore, da cui tuttavia si differenzia in quanto il detentore del segreto può essere tale solo se ne è entrato in possesso legittimamente. Proprio in relazione a tale ultimo requisito emergono ulteriori tensioni. Per i *dataset* di grandi dimensioni non è agevole verificare se ogni singolo dato sia stato acquisito legittimamente. Complessa si mostra anche l'identificazione del soggetto da ritenere detentore, qualora ai dati prodotti possano avere accesso differenti figure, quali per esempio il costruttore dell'oggetto che raccoglie i dati, l'utilizzatore dell'applicativo o il soggetto che gestisce servizi *cloud* ove i dati vengono conservati[870].

---

[869] FARKAS, *ibidem*.

[870] Cfr. FIA, *op. cit.*, 90; DREXL, *Economic Efficiency versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics*, in *Max Planck Institute for Innovation and Competition Research Paper n. 16-16*, 2016, 8.

Alla luce delle criticità riscontrate è stato allora proposto un intervento normativo volto a riconoscere uno specifico diritto esclusivo sui dati non personali, a prescindere dalle modalità con cui essi siano stati prodotti.

Tale prospettiva è accolta anche dalla Commissione europa, la quale in un recente documento chiarisce che, tenendo conto degli investimenti allocati nel settore, il titolare di questo diritto di utilizzo esclusivo dovrebbe essere il produttore del *dataset*, cioè il responsabile dei dispositivi che generano i dati[871]. A quest'ultimo sarebbe inoltre concessa la facoltà di concedere in licenza o trasferire detto diritto di esclusiva a un'altra persona fisica o giuridica[872].

A ben vedere tuttavia l'introduzione di diritti di proprietà sui dati non personali, per quanto possano essere contenuti nel tempo, potrebbe comportare una limitazione eccessiva alla loro circolazione e, di conseguenza, allo stesso mercato digitale, diminuendo così gli investimenti economici nel settore.

Tra le varie possibili soluzioni quella preferibile sembra allora essere una tutela contrattuale che lascerebbe agli operatori maggiore libertà di autoregolamentazione mediante, per esempio, clausole contrattuali tipo. Si pensi a clausole penali (in caso di divulgazioni non autorizzate) o protezioni di natura tecnica che limitano la possibilità di copia e di accesso alle informazioni.

Questa soluzione permetterebbe alle imprese di esercitare una forma di controllo sui *dataset*, pur non limitandone la libertà di circolazione, e di sfruttamento degli stessi[873]. Lo strumento contrattuale possiede, infatti, una natura flessibile che ne permette un maggior adattamento ai diversi settori dell'economia dei dati, che, come visto, si mostrano particolarmente dinamici e caratterizzati da diverse esigenze. Quanto ai diritti di sfruttamento economico, già oggi vengono regolati mediante contratti di licenza, a prescindere dunque dalla presenza di una privativa sui dati oggetto del contratto.

Rimanendo nell'ambito contrattuale, per alcune categorie di dati, parte dei commentatori ritiene più opportuno fare riferimento a contratti di compravendita non dei dati ma dei servizi che su di essi basano. In questo modo troverebbe un'estesa

---

[871] Cfr. Commissione Europea, *Final Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*, 2017, 30 ss.; ZECH, *op. cit.*, 75; FARKAS, *op. cit.*, 11 ss.; FIA, *ibidem*.

[872] FIA, *op. cit.*, 100 ss.

[873] In arg. CAVO, *op. cit.*, 217; CIANI, *op. cit.*, 830 ss.; FIA, *op. cit.*, 109 ss.; DREXL, *op. cit.*, 40 s.; ZHANG, *op. cit.*, 316 ss.

applicazione la Direttiva 770/2019 UE, relativa ai contratti di fornitura di contenuto digitale e di servizi digitali, nella quale si prevede anche un'adeguata protezione per gli utenti[874].

Da queste considerazioni rimane impregiudicata la questione circa l'accesso alle risorse nella cornice di un mercato ove queste sono controllate *de facto* da poche grandi imprese. Più che una tutela dei dati ci si muove qui verso politiche di governance a cui è necessario guardare secondo un approccio forse maggiormente settoriale, in ragione della differente estrazione delle informazioni, dell'uso che di queste viene fatto e, di conseguenza, delle differenti criticità nascenti[875]. Se gli strumenti di autoregolazione, di stampo contrattuale, da una parte si mostrano tra quelli più efficaci a regolare la circolazione dei dati tra operatori privati, permettendo al contempo di garantire la possibilità di sfruttamento economico, dall'altro è necessario, come visto, un intervento attento e diretto a consentire un efficiente sviluppo del mercato unico digitale, che permetta l'ingresso di nuove imprese e un'effettiva concorrenza. Si è, infatti, già evidenziato come dall'osservazione del mercato emerga l'esigenza di imporre regole di controllo che possano prevenire possibili illeciti lesivi della concorrenza da parte delle imprese [876].

L'opera di bilanciamento tra diritti e interessi confliggenti non pare semplice, né immediata. In conclusione, si ritiene allora fondamentale prestare una continua attenzione al processo di trattamento dei dati, a come essi vengano raccolti, alle finalità a cui sono destinati, evitando una incontrollata liberalizzazione e concedendo alle imprese diritti di proprietà o di esclusiva sui dati. Autorevole dottrina, che si ritiene di condividere, ricorda, infatti, come la prospettiva di analisi della materia trascende le esigenze del singolo, poiché coinvolge l'intera comunità; pertanto una maggiore attenzione deve essere data a come viene costruita l'identità degli utenti, grazie

[874] CAVO, *ibidem*. Per un approfondimento in merito al trattamento dei dati personali e al coordinamento con il GDPR si rimanda a DE FRANCESCHI, *La circolazione dei dati personali nella proposta di Direttiva UE sulla fornitura di contenuti digitali*, in *Regolare la tecnologia*, cit., 203 ss.
[875] V. ZENO ZENCOVICH, *Ten legal perspectives*, cit., 39 ss.; STAZI, CORRADO, *op. cit.*, 473 ss.; OTTOLIA, *op. cit.*, 297 ss. Una regolazione efficace non può escludere dall'analisi gli strumenti previsti dal diritto della concorrenza, per un approfondimento in merito alle prospettive di fallimento di mercato si rimanda *supra* al capitolo 2 del presente lavoro. Diverso il caso dei dati destinati alla ricerca scientifica, a cui evidentemente deve essere dato libero accesso secondo una strategia *open data*, già avviata nel settore pubblico, che dovrebbe coinvolgere maggiormente anche i dati raccolti da operatori privati.
[876] OTTOLIA, *op. cit.*, 311 ss. Per un approfondimento si rimanda *supra* §1.1 del capitolo 2.

all'opera di continuo monitoraggio e analisi dei dati a cui sta seguendo una vera e propria appropriazione commerciale dell'identità degli individui[877].

5. Considerazioni conclusive

La diffusione delle tecnologie *data driven* e la conseguente necessità di tutela per gli individui, che si vedono sempre più soggetti a trattamenti di cui non hanno effettiva contezza, sta interessando pressoché la totalità dei settori di mercato. Tra questi una particolare attenzione merita il comparto *automotive*, ove negli ultimi anni si è assistito a una veloce trasformazione della mobilità verso soluzioni sempre più automatiche.

La prospettiva di una vettura a guida completamente autonoma, il cui livello di autonomia dunque corrisponde al quinto previsto dello Standard SAE, seppure ancora lontana da raggiungere, fa emergere interrogativi in merito al sistema di governance dei dati. Le auto a guida autonoma, come visto, saranno necessariamente vetture connesse e dovranno trattare un'ingente mole di dati, ricevendo – ma anche trasmettendo – "messaggi", sia tra loro (V2V), sia con le infrastrutture (quali reti stradali intelligenti: V2I), nonché, in generale, nei confronti di tutti gli utenti della strada (V2X).

Svariati sono i profili critici che emergono, tra cui quelli legati alla sicurezza dei sistemi di guida.

Tralasciando i dettagli tecnici, l'esperienza quotidiana insegna che ogni sistema connesso alla rete può essere oggetto di un attacco esterno; la connessione rende, infatti, il sistema inevitabilmente aperto, dovendo questo comunicare all'interno della rete, e proprio questa "apertura" lo rende sensibile a possibili attacchi.

I veicoli autonomi non fanno eccezione. Si sono già verificati episodi che hanno visto intrusioni non autorizzate e che hanno permesso finanche di "pilotare" la vettura da remoto[878]. Per garantire, dunque, la sicurezza, sia dei sistemi che dei messaggi, appare evidente che i veicoli dovranno essere identificati univocamente mediante chiavi pubbliche che certifichino la provenienza e l'autenticità dei messaggi trasmessi. Tuttavia, pur se queste misure di sicurezza appaiono necessarie, è chiaro che ogni possibile dato trasmesso, per quanto criptato, potrebbe essere ricondotto a una singola

[877] ALPA, *La proprietà dei dati personali*, cit., 33.
[878] Si v. *supra* § 3 del presente capitolo.

vettura e, andando a ritroso, al singolo utente a cui inerisce. Ne discende che tutti i dati raccolti e trasmessi nell'ambito della mobilità connessa e autonoma possano astrattamente ricondursi a una persona fisica e dunque, secondo la definizione prevista all'art. 4 GDPR, debbano essere considerati dati personali.

La sicurezza da attacchi esterni non è dunque circoscritta alla, seppur vitale, limitazione di rischi per l'incolumità fisica degli occupanti del veicolo, ma deve riguardare altresì i dati raccolti e generati. L'accesso e l'utilizzo non consentito di questi potrebbe, infatti, comportare non solo una violazione della privacy degli utenti, ma anche danni derivanti dall'utilizzo illecito di dati che, in alcuni casi, possono avere una natura sensibile.

Nella generale analisi circa la diffusione e l'utilizzo di vetture autonome non può dunque essere trascurato anche un vaglio di compatibilità con le disposizioni previste dalla normativa sulla *data protection*.

Dall'analisi svolta sono emerse fin da subito alcune tensioni, sia in relazione al regime di titolarità o contitolarità, sia alla stessa individuazione di una base di legittimità applicabile ai trattamenti. Difatti, proprio l'architettura del sistema di guida autonoma sembra non permettere una piena applicabilità delle disposizioni del GDPR.

Si è pertanto evidenziata la necessità di un intervento normativo da parte del legislatore, quantomeno europeo, che possa fungere da base di legittimità dei trattamenti e che al contempo detti anche dei limiti agli utilizzi, soprattutto di natura secondaria, dei dati raccolti e generati. A questo deve aggiungersi anche la necessità di prevedere specifici obblighi di trasparenza per i titolari, nella prospettiva di instaurare un perimetro minimo di garanzie per gli interessati.

Se, infatti, la guida autonoma può portare differenti vantaggi, sia per le imprese che per la società nel suo complesso, ad essa si accompagnano rilevanti rischi per gli individui. Il grande numero dei dati raccolti, come visto, potrebbe facilmente essere utilizzato per una profilazione particolarmente invasiva dei guidatori o per un ingiustificato e costante controllo della popolazione, per tacere di possibili utilizzi illeciti in danno degli interessati. Ben si comprende allora l'esigenza di un intervento normativo, a cui però dovrebbe anche affiancarsi una maggiore valorizzazione dell'utilizzo di soluzioni tecniche.

Come già si è avuto modo di notare in relazione al generale funzionamento dei sistemi di AI[879], anche per le vetture autonome si ritiene necessario un approccio preventivo che minimizzi il rischio di possibili danni.

Maggiore spazio dovranno trovare soluzioni che siano espressive dei principi di *privacy by design* e *by default*, che permettano per esempio di rendere particolarmente complessa, e così poco attrattiva, la possibilità di ricollegare i dati a un singolo individuo. Del pari sarà necessario incoraggiare l'adozione di standard e di codici di condotta che siano espressione di un approccio di regolazione preventiva, che tenga conto anche delle istanze etiche emerse; questi strumenti, indirizzandosi a chi progetta i sistemi algoritmici, si mostrano infatti idonei a fornire a monte una maggiore sensibilità circa le possibili deformazioni che un uso non controllato dell'AI potrebbe comportare per i singoli e per l'intera società.

A queste importanti considerazioni fanno eco anche le questioni in merito alla titolarità e al regime giuridico applicabile ai dati tecnici generati dalle vetture, che non siano qualificabili come dati personali.

Si è detto della difficoltà di identificazione certa di tali dati, grazie al sempre maggiore perfezionamento delle tecniche di *data analysis*[880], in ragione delle innegabili potenzialità di sfruttamento economico di questi veri e propri "giacimenti" di dati; proprio per ciò si ritiene opportuna un'attenta riflessione giuridica sul punto.

Il tema è complesso, mostrandosi ancora una volta le normative vigenti non pienamente adeguate a regolare la materia.

Chiarito, infatti, come tra i diversi attori operanti nella catena di trattamenti il titolare dei dati grezzi generati dalla vettura potrebbe essere identificato in colui che ha effettuato un investimento nello sviluppo delle tecnologie dirette alla raccolta e all'analisi (si può ipotizzare la casa costruttrice del veicolo), rimane tuttavia difficoltoso individuare con certezza quale regime giuridico possa essere ad essi applicato.

Dall'analisi svolta, lo strumento che si dimostra maggiormente duttile rimane quello contrattuale, in ragione della sua natura flessibile, per quanto anch'esso non possa dirsi pienamente compatibile con le finalità di tutela del diritto di sfruttamento economico dei dati, di una loro libera circolazione, di tutela del mercato, oltre che dei diritti degli interessati.

[879] V. *supra* § 6, capitolo 4.
[880] Si v. *supra* §3, capitolo 2.

L'opera di bilanciamento tra diritti e interessi confliggenti non si mostra mai semplice, né immediata, e ciò in particolare in un contesto in continua evoluzione quale è quello delle tecnologie *data driven*. A floride prospettive di sviluppo e di crescita, sia economica che sociale, si affiancano concreti rischi per i diritti degli individui. Autorevole dottrina, che si ritiene di condividere, ricorda, inoltre, come la prospettiva di analisi della materia trascenda le esigenze del singolo, coinvolgendo l'intera comunità. Proprio per tale ragione una maggiore attenzione dovrebbe essere data a come viene costruita l'identità degli utenti, mediante un continuo monitoraggio e analisi dei dati a cui sta seguendo una vera e propria appropriazione commerciale[881].

Come si è cercato di evidenziare, proprio la complessità tecnica di funzionamento delle tecnologie di AI in generale, così come nel *leading case* delle auto *driverless*, sembra in parte mal conciliarsi con le disposizioni normative poste a tutela degli individui. Se fermare il progresso non sembra possibile, né a dire il vero auspicabile, la soluzione sembra risiedere in un approccio che, più che *ex post* e di tipo rimediale, che pure deve essere ripensato in ragione delle specificità dell'attuale contesto tecnologico, deve essere *ex ante*, e si presti, dunque, a una continua verifica dell'intero processo di trattamento dei dati, di come essi vengano raccolti e delle finalità a cui sono destinati.

Un approccio così pensato non sarebbe espressione di un atteggiamento "di sospetto" nei confronti del progresso, ma si dimostra invece idoneo a rispondere alle numerose istanze sollevate dai diversi *stakeholders*, tra cui anche dagli stessi produttori e sviluppatori di soluzioni di Intelligenza Artificiale[882]; il dato che emerge in modo chiaro è difatti proprio l'esigenza condivisa di provvedere a uno sviluppo controllato delle soluzioni di AI.

---

[881] Il riferimento è alle parole di ALPA, *La proprietà dei dati personali*, cit., 33, il quale evidenzia anche un'apparente contraddizione: «la persona ha una identità digitale con la quale si identifica o è identificata, ma appunto per questo non dovrebbe "possederla"; per contro, i terzi se ne possono appropriare, e possono esercitare un diritto proprietario su di essa: ed in effetti la disciplina (anche europea) delle banche di dati protegge la proprietà di chi ha raccolto dati altrui». Su quest'ultimo punto si veda anche Nicita, «[…] i nostri «comportamenti digitali» sono, a un tempo, figli della nostra libertà di espressione e, in quanto elementi dei Big Data, oggetto di appropriazione esclusiva da parte di terzi. In altri termini, più aumentiamo la nostra libertà digitale e l'intensità della nostra dimensione su Internet, più ricco è l'insieme di dati di cui altri si appropriano. La libertà digitale genera nuove forme di proprietà privata digitale, che non appartengono più a chi le ha generate, né possono da questi essere controllate, indirizzate, modificate». NICITA, *op. cit.*, 1169.

[882] Si pensi all'*Advanced technology external advisory council* creato da Google per fornire pareri in merito alle maggiori questioni etiche nascenti dallo sviluppo delle tecnologie di AI. Le numerose carte etiche proposte negli ultimi anni, il cui ruolo dovrebbe tuttavia essere in parte ridimensionato, sono espressione proprio di queste sentite istanze di regolazione della materia.

Una regolazione attenta a garantire uno standard di sicurezza dei dispositivi di Intelligenza Artificiale, nella quale attenzione dovrà essere necessariamente rivolta anche alla qualità dei dati raccolti e analizzati, potrebbe difatti permettere una diminuzione dei rischi di danni, legati come visto in larga parte alla dimesione tecnica di funzionamento delle macchine.

In conclusione, questo tipo di approccio *ex ante* permetterebbe non solamente di garantire quanto meno un perimetro di sicurezza minimo per gli utenti che si trovino ad interagire con detti sistemi, ma anche di non limitare eccessivamente lo sviluppo dell'intero settore tecnologico.

Indice Bibliografico

Articoli, monografie, volumi collettanei

A.A. V.V., *Group Privacy. New Challenges of Data Technologies*, a cura di TAYLOR, FLORIDI, VAN DER SLOOT, Berlin, 2017.

A.A. V.V., *Macchine che pensano*, Bari, 2018.

A.A. V.V., *Security and privacy for next generation wireless networks*, Berlin, 2018.

ADINOLFI, *L'Unione europea dinanzi allo sviluppo dell'intelligenza artificiale*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, DORIGO, Pisa, 2020, 13 ss.

ALPA, *I diritti della personalità*, *Le persone e la famiglia*, *1*, *Le persone fisiche e i diritti della personalità*, a cura di ALPA e G. RESTA, nel *Trattato Sacco*, Torino, 2006, 145 ss.

ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessioni*, in *Contr. imp.*, 2017, 723 ss.

ALPA, *La proprietà dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di ZORZI GALGANO, Milano, 2019, 11 ss.

AMATO MANGIAMELI, *Algoritmi e "big data". Dalla carta sulla robotica*, in *Riv. fil. dir.*, 2019, 107 ss.

AMIDEI, *Intelligenza artificiale e* "product liability": *sviluppo del diritto dell'Unione europea*, in *Giur. it.*, 2019, 1715 ss.

AMIDEI, *Intelligenza artificiale e responsabilità da prodotto*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di RUFFOLO, Milano, 2020, 125 ss.

AMRAM, *L'Ulisse* Accountable. *Ricerca e protezione dei dati personali concernenti la salute: il tentativo di armonizzazione a livello europeo post GDPR e le interpretazioni offerte dai sistemi irlandese, belga, spagnolo e italiano*, in *Riv. it. med. leg.*, 2019, 209 ss.

ANDREOLA, Fake news *e danno da false informazioni in internet. I parte*, in *Resp. civ. e prev.*, 2020, 1064 ss.

ANDREOLA, Fake news *e danno da false informazioni in internet. II parte*, in *Resp. civ. e prev.*, 2020, 2000 ss.

ANGELINI, *Intelligenza Artificiale e* governance. *Alcune riflessioni di sistema*, in *Intelligenza Artificiale, protezione dei dati personali e regolazione*, a cura di PIZZETTI, Torino, 2018, 293 ss.

ASCIONE, *Il futuro della salute. Come la tecnologia digitale sta rivoluzionando la medicina (e la nostra vita)*, Milano, 2018.

ASIMOV, *Circolo vizioso* (or. Runaround), *Io, Robot*, Milano, 1973, rist. 2016.

AULINO, *Il consenso al trattamento dei dati e carenza di consapevolezza: il* legal design *come un rimedio* ex ante, in *Dir. inform.*, 2020, 303 ss.

BAKSHY, MESSING, ADAMIE, *Exposure to ideologically diverse news and opinion on Facebook*, 2015 (*https://education.biu.ac.il/sites/education/files/shared/science-2015-bakshy-1130-2.pdf*, ultimo accesso 13 maggio 2021).

BALLO, *Dalla macchina di Turing ai calcolatori digitali*, in *L'eredità di Alan Turing. 50 anni di Intelligenza Artificiale*, a cura di CAPPUCCIO, Milano, 2005, 15 ss.

BARBARESCHI, GIUBILEI, *L'equilibrio tra la tutela dei dati personali e la manifestazione del pensiero*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 453 ss.

BARCELO, *User Privacy in the Public Bitcoin Blockchain* (2007) 1 *Journal of Latex Class Files* 3.

BELLINI, MARTINESCU, VASSALLI, *Digital Ledger Technologies*, in *Digital transformation and data management*, a cura di BELLINI e D'ASCENZO, Pisa, 2020, 127 ss.

BENEDETTI, *IA e (in)sicurezza*, in *Intelligenza Artificiale, protezione dei dati personali e regolazione*, a cura di PIZZETTI, Torino, 2018, 239 ss.

BENGIO, *Learning Deep Architectures for AI* (2019) 2 *Foundations and Trends® in Machine Learning* 1 ss.

BENVENUTO, COLAROCCO, *Le responsabilità del titolare e del responsabile connesse al trattamento dei dati personali*, in *Il diritto di internet nell'era digitale*, a cura di CASSANO e PREVITI, Milano, 2020, 821 ss.

BERBERICH, STEINER, *Blockchain technology and the GDPR – How to reconcile privacy and Distributed Ledgers?* (2016) *European Data protection Law Review* 422 ss.

BIANCA C.M., *Diritto Civile*, *5*, *La Responsabilità*, Milano, II, 2019, 704 ss.

BIANCA M., *La* filter bubble *e il problema dell'identità digitale*, in *MediaLaws – riv. dir. media*, Milano, 2019, 39 ss.

BIANCHI, D'ACQUISTO, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA e BELISARIO, Milano, 2018, *sub* art. 25, 245 ss.

BOCCACCINI, *Le origini della privacy e della protezione dei dati*, in *Tecnologia e Diritto*, 2, a cura di ZICCARDI e PERRI, Milano, 2019, 37 ss.

BODEN, *L'Intelligenza Artificiale*, Bologna, 2019.

BOGNI, DEFANT, *Big Data: Diritti IP e problemi della privacy*, in *Dir. ind.*, 2015, 117 ss.

BOLOGNINI, PELINO, BISTOLFI, *Il regolamento privacy europeo*, Milano, 2016.

BONAVITA, *La profilazione*, Cambridge analytica *e il* micro-targeting, in *Tecnologia e Diritto*, 3, a cura di ZICCARDI e PERRI, Milano, 2019, 65 ss.

BONAVITA, *La profilazione e il* micro-targeting, in *Il diritto di internet nell'era digitale*, a cura di CASSANO e PREVITI, Milano, 2020, 391 ss.

BORGHI, KARAPAPA, *Contractual restrictions on lawful use of information: sole-source databases protected by the back door?* (2018) 5 *European intellectual property review* 505 ss.

BOYD, CRAWFORD, C*ritical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon* (2015) 15 *Information Communication and Society* 662 ss.

BOZDAG, VAN DEN HOVEN, *Breaking the filter bubble: Democracy and design* (2017) 4 *Ethics and Information Technology* 249 ss.

BRAVO, *Il consenso e le altre condizioni di liceità*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO, Torino, 2017, 101 ss.

BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 775 ss.

BRAVO, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito di dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di ZORZI GALGANO, Milano, 2019, 383 ss.

BRAVO, *La «compravendita» di dati personali?*, in *Diritto di Internet*, 2020, 521 ss.

BRKAN, *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond* (2019) 27 *International Journal of Law and information technology* 91 ss.

BURRELL, *How the machine 'thinks': Understanding opacity in machine learning algorithms* (2016) 1 *Big Data & Society* 1 ss.

BUSNELLI, *Nota introduttiva al commento della l. 31 dicembre 1996, n. 675. Spunti per un inquadramento sistematico, Tutela della privacy (l. 31 dicembre 1996 n. 675)*, in *Nuove leggi civ. comm*., a cura di BIANCA *et al*., 1999, 228 ss.

BUTTI, *Principio di precauzione, Codice dell'ambiente e giurisprudenza delle Corti comunitarie e della Corte Costituzionale*, in *Riv. giur. amb*., 2006, 809 ss.

BUTTOLO, *Introduzione alla Robotica*, Albino, 2017.

BYGRAVE, *Minding the machine: Article 15 of the data protection directive and automated profiling* (2001) 17 *Computer Law and Security Rev*iew 17 ss.

CABRAL, *Procedure di risoluzione standard e conflitti di massa*, in *Riv. trim. dir. proc. civ.*, 2020, 611 ss.

CACACE, *Autodeterminazione in salute*, Milano, 2017.

CAGGIA, *Libertà ed espressione del consenso*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 249 ss.

CAGGIANO, *Il consenso al trattamento dei dati personali nel nuovo Regolamento europeo. Analisi, giuridica e studi comportamentali*, in *Oss. dir. civ. comm.*, 2018, 67 ss.

CAIA, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA e BELISARIO, Milano, 2018, *sub* art. 22, 219 ss.

CALABRESI, BOBBIT, *Scelte Tragiche*, Milano, 2006.

CALABRESI, MELAMED, *Property rules, liability rules, and inalienability: one view of the cathedral* (1972) 6 *Harvard Law Review* 1089 ss.

CALISAI, *I diritti dell'interessato*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 327 ss.

CALZOLAIO, voce «protezione dei dati personali», nel *Digesto VII ed.*, *Disc. pubbl.*, a cura di BIFULCO, CELOTTO, OLIVETTI, diretto da SACCO, Milano, 2017, 594 ss.

CAMARDI, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Jus civile*, 2020, 786 ss.

CANTONE, *L'IoT nel settore* automotive: *problematiche privacy* on board *e* on road, in *Dir. merc. tec.*, 2018, 1 ss.

CAPACCIOLI, *Le criptovalute*, in *Tecnologia e Diritto*, 2, a cura di ZICCARDI e PERRI, Milano, 2019, 385 ss.

CAPACCIOLI, *La blockchain*, in *Tecnologia e Diritto*, 2, a cura di ZICCARDI e PERRI, Milano, 2019, 371 ss.

CAPILLI, *Responsabilità e robot*, in *Nuova giur. civ. comm.*, 2019, 621 ss.

CAPPARELLI, nel *Codice della Disciplina Privacy*, a cura di BOLOGNINI e PELINO, Milano, 2019, *sub* art. 24, 201 ss.

CAPPELLETTI, GOLATO, *Medicina di Laboratorio 4.0*, in *Riv. it. med. leg.*, 2018, 192 ss.

CAROCCIA, *Soggettività giuridica dei robot?*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 213 ss.

CASAROSA, *La tutela aggregata dei dati personali nel Regolamento UE 2016/679: una base per l'introduzione di rimedi collettivi*, in *Regolare la tecnologia: il Reg. UE n. 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di MANTELERO e POLETTI, Pisa, 2018, 235 ss.

CASEY, NIBLETT, *Self-driving contracts* (2017) 43 *Journal of Corporation Law* 1 ss.

CASINI, *Lo stato nell'era di Google*, in *Riv. trim. dir. pubb.*, 2019, 1111 ss.

CATALETA, *Categorie particolari di dati: le regole generali e i trattamenti specifici*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di FINOCCHIARO, Torino, 2019, 204 ss.

CATERINA, THOBANI, *GDPR tra novità e discontinuità. Il diritto al risarcimento del danno*, in *Giur. it.*, 2019, 2805 ss.

CAVO, *Il Regolamento europeo sulla libera circolazione dei dati non personali tra benefici e criticità*, in *Diritto di Internet*, 2020, 207 ss.

CELOTTO, *Come regolare gli algoritmi. Il difficile bilanciamento fra scienza, etica e diritto*, in *Analisi giur. econ.*, 2019, 47 ss.

CEROCCHI, COLAROCCO, *I dati personali e la tutela della persona*, in *Il diritto di internet nell'era digitale*, a cura di CASSANO e PREVITI, Milano, 2020, 379 ss.

CHANG, *Blockchain: Disrupting data protection?* (2017) 150 *Privacy Laws & Business International Report* 1 ss.

CHENG *et al.*, *The Rise of Robots in China* (2019) 33 *Journal of Economic Perspectives* 71 ss.

CIANI, *Property rights model v. contractual approach: how protection non-personal data in cyberspace?*, in *Dir. comm. int.*, 2017, 831 ss.

CICORIA, *Quale danno in materia di* privacy*?*, in *Giust. civ.*, 2007, 39 ss.

CINGOLANI, *L'altra specie. Otto domande su noi e loro*, Bologna, 2019.

CINGOLANI, ANDRESCIANI, *Robot, macchine intelligenti e sistemi autonomi: analisi della situazione e prospettive*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 23 ss.

CIRONE, *Big Data e tutela dei diritti fondamentali: la ricerca di un (difficile) equilibrio nell'ambito delle iniziative europee*, in *Il ragionamento giuridico nell'era dell'Intelligenza Artificiale*, a cura di DORIGO, Pisa, 2020, 143 ss.

COLIVA, *Prime valutazioni sulla responsabilità civile nella legge 675/96*, in *Interlex*, 1997 (*www.interlex.it/675/coliva1.htm*, ultimo accesso 14 giugno 2021).

COMANDÈ, *Privacy informatica: prospettive e problemi*, in *Danno e resp.*, 1997, 147.

COMANDÈ, *Responsabilità ed* accountability *nell'era dell'Intelligenza Artificiale*, in *Giurisprudenza e autorità indipendenti nell'epoca del diritto liquido. Studi in onore di Roberto Pardolesi*, a cura di DI CIOMMO e TROIANO, Piacenza, 2018, 1001 ss.

COMANDÈ, *Ricerca in sanità e* data protection *un puzzle… risolvibile*, in *Riv. it. med. leg.*, 2019, 187 ss.

COMANDÈ, *Intelligenza artificiale e responsabilità tra* liability *e* accountability. *Il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi giur. econ.*, 2019, 169 ss.

COMELLA, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza* "safe harbor" *della corte di giustizia dell'unione europea*, in *Dir. inform.*, 2015, 719 ss.

CONSULICH, *Il nastro di* Möbius. *Intelligenza artificiale e imputazione penale nelle nuove forme di abuso del mercato*, in *Banca borsa tit. cred.*, 2018, 195 ss.

CONTALDO, PELUSO, *Cybersecurity*, Pisa, 2018.

COOLEY, *A treatise on the Law of Torts. Or the Wrongs which arise independent of contract*, Chicago, 1888.

COPPINI, *Diritti del paziente e consenso informato*, in *La nuova responsabilità medica*, a cura di RUFFOLO, Milano, 2018, 167 ss.

CORDESCHI, *L'intelligenza artificiale. Logica, paradossi e intelligenza artificiale*, in *La Scienza*, Roma, 2005, 667 ss.

CORONA, DEL PIZZO, *IA: l'approccio europeo è basato sull'eccellenza e la fiducia*, in *Diritto di Internet*, nota di aggiornamento 5 giugno 2020 (*https://dirittodiinternet.it/ia-lapproccio-europeo-basato-sulleccellenza-la-fiducia/*).

COSTANTINI, *Profilazione e* "automated decision making" *in ambito lavorativo nella giurisprudenza italiana*, in *Lavoro nella giur*., 2016, 984 ss.

COSTANTINI, MONTEROSSO, *Il problema della sicurezza tra informatica e diritto: una prospettiva emergente dalle "Smart Cars"*, in *Inf. e dir*., 2016, 95 ss.

COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, in *Giur. it.*, 2019, 1686 ss.

CRISCI, *Intelligenza artificiale ed etica dell'algoritmo*, in *Foro amm*., 2018, 1787 ss.

CRISCI, *Evoluzione tecnologica e trasparenza nei procedimenti "algoritmici"*, in *Diritto di Internet*, 2019, 380 ss.

CUCCURU, *Blockchain ed automazione contrattuale. Riflessioni sugli* smart contract, in *Nuova giur. civ. comm.*, 2017, 107 ss.

CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 3 ss.

D'ACQUISTO, NALDI, *Big Data e Privacy by Design*, Torino, 2017.

D'ACQUISTO, PIZZETTI, *Regolamentazione dell'economia dei dati e protezione dei dati personali*, in *Analisi giur. econ.*, 2019, 89 ss.

D'ALESSANDRO, *Dal miraggio dell'Intelligenza Artificiale alla simulazione di un sistema vivente*, in *L'eredità di Alan Turing. 50 anni di Intelligenza Artificiale*, a cura di CAPPUCCIO, Milano, 2005, 245 ss.

D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inform*., 2020, 635 ss.

D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 61 ss.

DALMASTRO, NICITA, *Big Data. Come stanno cambiando il nostro mondo*, Bologna, 2019.

DE ANNA, *Automi, responsabilità e diritto*, in *Riv. fil. dir.*, 2019, 125 ss.

DE CUPIS, *I diritti della personalità*, nel *Trattato Cicu-Messineo*, 4, II ed., Milano, 1982, 93 ss.

DE FILIPPI, *The interplay between decentralization and privacy: the case of blockchain technologies* (2016) 7 *Journal of Peer Production* 1 ss. (*https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852689*, ultimo accesso 15 maggio 2020).

DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017.

DE FRANCESCHI, *La circolazione dei dati personali nella proposta di Direttiva UE sulla fornitura di contenuti digitali*, in *Regolare la tecnologia: il Reg. UE n. 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di MANTELERO, POLETTI, Pisa, 2018, 203 ss.

DE FRANCESCHI, *Il "pagamento" mediante dati personali*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 1381 ss.

DE GAUDIO *et al.*, *Consenso informato*, in *Governo clinico e medicina perioperatoria*, a cura di GULLO e MURABITO, Milano, 2016, 163 ss.

DE GREGORIO, TORINO, *Privacy, tutela dei dati personali e Big Data*, in *Privacy digitale, Riservatezza e protezione dei dati e nuovo Codice Privacy*, a cura di TOSI, Milano, 2019, 447 ss.

DE LEONARDIS, *Big Data, decisioni amministrative e "povertà" di risorse della pubblica amministrazione*, in *La decisione nel prisma dell'intelligenza artificiale*, a cura di CALZOLAIO, Milano, 2020, 137 ss.

DEL FEDERICO, POPOLI, *Disposizioni generali*, in *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO, Torino, 2017, 57 ss.

DEL PIZZO, *Trattamento dei dati non personali: punti di contatto tra il Regolamento (UE) 2018/1807 e il GDPR*, in *Diritto di Internet*, nota di aggiornamento 18 febbraio 2020 (*https://dirittodiinternet.it/trattamento-dei-dati-non-personali-punti-contatto-regolamento-ue-20181807-gdpr/*).

DELFINI, *Il commercio elettronico: inquadramento generale*, in *Diritto dell'Informatica*, a cura di FINOCCHIARO e DELFINI, Milano, 2014, 351 ss.

DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 179 ss.

DENG, YU, *Deep Learning: Methods and Applications* (2014) 7 *Foundations and Trends in Signal Processing* 197 ss.

DENOZZA, *Logica dello scambio e "contrattualità": la società per azioni di fronte alla crisi*, in *Giur. comm.*, 2015, 5 ss.

DETERNMANN, *No one owns data* (2019) 70 *Hasting law journal* 1 ss.

DI BENEDETTO, *La funzione interpretativa del principio di precauzione nel diritto internazionale*, in *Dir. comm. int.*, 2006, 321 ss.

DI LORENZO, *Spunti di riflessione su taluni "diritti dell'interessato"*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di ZORZI GALGANO, Milano, 2019, 237 ss.

DI PORTO, *La rivoluzione Big Data. Un'introduzione*, in *Con. merc.*, 2016, 5 ss.

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

DI ROSA, Autonomous driving *tra evoluzione tecnologia e questioni giuridiche*, in *Dir. e quest. pubbl.*, 2019, 34 ss.

DIAKOPOULOS, *Algorithmic accountability reporting: on the investigation of black boxes* (2014) *Two Center for Digital Journalism* 1 ss. (*https://academiccommons.columbia.edu/doi/10.7916/D8ZK5TW2*, ultimo accesso 30 maggio 2021).

DIMITRAKOPOULOU, voce «Digital literacy», in *Encyclopedia of Big Data*, a cura di SCHINTLER, MCNEELY, Berlin, 2018.

DREXL, *Economic Efficiency versus Democracy: On the Potential Role of Competition Policy in Regulating Digital Markets in Times of Post-Truth Politics*

(2016) 16 *Max Planck Institute for Innovation and Competition Research Paper n. 16-16* 1 ss.

DRIGO, *Sistemi emergenti di intelligenza artificiale e personalità giuridica: un contributo interdisciplinare alla tematica*, in *Il ragionamento giudico nell'era dell'intelligenza artificiale*, a cura di DORIGO, Pisa, 2020, 179 ss.

EDWARDS, VEALE, *Slave to the algorithm? Why a "right to an explanation" in probably not the remedy you are looking for* (2017) 16 *Duke Law & Technology review* 18 ss.

ELIA, *Il* Digital single market, *il commercio elettronico e la tutela del consumatore*, in *Tecnologia e Diritto*, 2, a cura di ZICCARDI e PERRI, Milano, 2019, 327 ss.

ELVY, *Paying for privacy and the personal data economy* (2017) 117 *Columbia Law Review* 1369 ss.

ESPOSITO, *Il principio di coerenza e i meccanismi volti ad assicurare l'uniforme applicazione della disciplina in materia di protezione dei dati personali*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO, Torino, 2017, 533 ss.

ESPOSITO, *Il risarcimento del danno non patrimoniale da illecito trattamento dei dati personali*, in *Corr. giur.*, 2019, 628 ss.

EVANS, *Much ado about data ownership* (2011) 25 *Harvard law review* 69 ss.

FAINI, *Dati, algoritmi e Regolamento europeo 2016/679*, in *Regolare la tecnologia: il Reg. UE n. 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di MANTELERO, POLETTI, Pisa, 2018, 333 ss.

FARACE, *I titolare e il responsabile del trattamento*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 731 ss.

FARALLI, *Il diritto alla privacy profili storico-filosofici*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di ZORZI GALGANO, Milano, 2019, 1 ss.

FARINA, *Il* cloud computing *e i big data*, in *Tecnologia e Diritto*, 1, a cura di ZICCARDI e PERRI, Milano, 2019, 55 ss.

FARKAS, *Data created by the Internet of Things: The new gold without ownership*, in *Revista la propiedad inmaterial*, 2017, 5 ss.

FASAN, *Intelligenza artificiale e pluralismo: uso delle tecniche di profilazione nello spazio pubblico democratico*, in *Biolaw Journal – Rivista di BioDiritto*, 2019, 107 ss.

FERRARI, *La seducente perfezione di algoritmi e intelligenza artificiale nelle procedure amministrative alla luce dei modelli di responsabilità civile*, in *Diritto di Internet*, 2020, 177 ss.

FIA, *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in *Nuovo not. giur.*, 2019, 60 ss.

FICI, PELLECCHIA, *Il consenso al trattamento*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di PARDOLESI, 1, Milano, 2003, 469 ss.

FIDOTTI, *Nuove forme contrattuali nell'era della* Blockchain *e del* Machine Learning*. Profili di responsabilità*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 325 ss.

FINCK, *Blockchain and data Protection in the european union* (2018) 4 *European data protection law review* 17 ss.

FINOCCHIARO, *Privacy e protezione dei dati personali*, Torino, 2012.

FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO, Torino, 2017, 1 ss.

FINOCCHIARO, *Il contratto nell'era dell'intelligenza artificiale*, in *Riv. trim. dir. proc. civ.*, 2018, 441 ss.

FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, 1670 ss.

FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di FINOCCHIARO, Torino, 2019, 1 ss.

FINOCCHIARO, *Il principio di* accountability, *GDPR tra novità e discontinuità*, a cura di CATERINA, in *Giur. it.*, 2019, 2777 ss.

FINOCCHIARO, *Riflessioni su intelligenza artificiale e protezione dei dati personali*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di RUFFOLO, Milano, 2020, 237 ss.

FIORELLI, CASSANO, *La rivoluzione tecnologica della* blockchain, in *Il diritto di internet nell'era digitale*, a cura di CASSANO e PREVITI, Milano, 2020, 253 ss.

FLEXMAN, GOEL, RAO, *Filter Bubbles, Echo Chambers, and Online News Consumption* (2016) 80 *Public Opinion Quarterly* 298 ss.

FLORIDI, *Infosfera. Etica e filosofia nell'età dell'informazione*, Torino, 2009.

FRANSMAN, *The New ICT Ecosystem: Implications for Policy and Regulation*, Cambridge, 2010.

FRANZONI, *Responsabilità derivante da trattamento dei dati personali*, in *Diritto dell'informatica*, FINOCCHIARO e DELFINI, Milano, 2014, 829 ss.

FRANZOSI, Copyright: *chi è l'autore delle opere generate a computer?*, in *Dir. aut.*, 2018, 168 ss.

FRATI, MONTANARI VERGALLO, DI LUCA, *La giurisprudenza delle Sezioni unite sul danno alla persona:* et lux fruit?, in *Riv. it. med. leg.*, 2009, 277 ss.

FRIXIONE, *Il ruolo delle macchine di Turing nelle scienze cognitive*, in *L'eredità di Alan Turing. 50 anni di Intelligenza Artificiale*, a cura di CAPPUCCIO, Milano, 2005, 161 ss.

FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. inform.*, 2020, 465 ss.

RUOTOLO, *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2018, 97 ss.

GAETA, *La protezione dei dati personali nell'*Internet of Things: *l'esempio dei veicoli autonomi*, in *Dir. inform.*, 2018, 147 ss.

GALGANO, *Trattato di diritto civile*, a cura di ZORZI, 1, III ed., Padova, 2015.

GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço Jurídico*, 2013, 149 ss.

GAMBINI, *Principio di responsabilità e tutela aquiliana dei dati personali*, Napoli, 2018.

GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 1017 ss.

GAMBINO, BOMPREZZI, Blockchain *e* protezione *dei dati personali*, in *Dir. inform.*, 2019, 619 ss.

GAMBINO, MULA, *Diritti fondamentali, protezione dei dati e* cybersecurity, in *La circolazione dei dati. Titolarità, strumenti negoziali, diritti*, a cura di GAMBINO e STANZI, Pisa, 2020, 23 ss.

GATT, MONTANARI, CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Pol. dir.*, 2017, 363 ss.

GIANNONE CODIGLIONE, Riskbased approach *e trattamento dei dati personali*, in *La nuova disciplina europea della privacy*, a cura di SICA, D'ANTONIO e RICCIO, Padova, 2016, 55 ss.

GIANNONE CODIGLIONE, *Internet e tutele di diritto civile. Dati – persona – mercato: un'analisi comparata*, Torino, 2020.

GIOLITO, *Turing e la filosofia della mente*, in *L'eredità di Alan Turing. 50 anni di Intelligenza Artificiale*, a cura di CAPPUCCIO, Milano, 2005, 153 ss.

GIOVANELLA, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 1213 ss.

GIULIANO, *La* blockchain *e gli* smart contracts *nell'innovazione del diritto del terzo millennio*, in *Dir. inform.*, 2018, 989 ss.

GIUSTI, *Intelligenza artificiale e sistema sanitario*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di DORIGO, Pisa, 2020, 309 ss.

GLANCY, *Privacy in autonomous vehicles* (2012) 52 *Santa Clara law review* 1171 ss.

GOODFELLOW, BENGIO, COURVILLE, *Deep Learning*, Cambridge, 2016.

GOODMAN, FLAXMAN, *European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"* (2017) 38 *AI Magazine*, 2017, 50 ss.

GRANDY, *Engaging rational discrimination: Exploring reasons for placing regulatory constraints on decision support systems* (2010) 12 *Ethics and Information Technology* 29 ss.

GRANIERI, PARDOLESI, *Il software*, in *AIDA*, 2007, 288 ss.

GRECO, *I ruoli: titolare e responsabile*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO, Torino, 2017, 251 ss.

GRECO, MANTELERO, *Industria 4.0, robotica e* privacy-by-design, in *Dir. inform*., 2018, 875 ss.

GUARINO, *I veicoli connessi: punto focale dell'internet delle cose*, 2017, 1 ss. (*www.studioag.pro*, ultimo accesso 24 gennaio 2020).

GUGGINO, BANORRI, *L'*advertising *ai tempi dell'Intelligenza Artificiale: algoritmi e* marketing *personalizzato*, in *Intelligenza Artificiale. Il diritto, i diritti, l'etica*, a cura di RUFFOLO, Milano, 2020, 625 ss.

HILDEBRANDT, *Learning as a machine: Crossovers between Humans and Machines* (2017) 4 *Journal of Learning Analytics* 6 ss.

HILDEBRANDT, *The Dawn of Critical Transparency right for the profiling era*, in *Digital Enlightment Yearbook*, a cura di HILDEBRANDT *et al*., Amsterdam, 2012.

HOBERG, voce «Supply Chain and Big Data», in *Encyclopedia of Big Data*, a cura di SCHINTLER, MCNEELY, Berlin, 2020.

INFANTINO, *La responsabilità per danni algoritmici: prospettive europeo-continentali*, in *Resp. civ. e prev.*, 2019, 1762 ss.

IPPOLITI MARTINI, *Comitato europeo per la protezione dei dati*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di FINOCCHIARO, Torino, 2019, 725 ss.

IPPOLITI MARTINI, *Comitato europeo per la protezione dei dati*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO, Torino, 2017, 552 ss.

ISRANI, *Algorithmic due process: mistaken accountability and attribution in State v. Loomis*, 2017 (*https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1*, ultimo accesso 14 settembre 2021).

ITALIANO, *Le sfide interdisciplinari dell'intelligenza artificiale*, in *Analisi giur. econ.*, 2019, 9 ss.

IULIANI, *Note minime in tema di trattamento dei dati personali*, in *Eur. e dir. priv.*, 2018, 293 ss.

JAIN, GYANCHANDANI, KHARE, *Big Data privacy: a Technological Perspective and Review* (2016) 3 *Journal of Big Data* 1ss.

JANEČEK, *Ownership of personal data in the Internet of Things* (2018) 34 *Computer Law & Security Review* 1039 ss.

JORGENSEN, RIKKE, *Human rights in the global information society*, Cambridge, 2019.

KISZL, FODOR, *The "Collage Effect" – against filter bubbles: interdisciplinary approaches to combating the pitfalls of information technology* (2018) 44 *The Journal of Academic Librarianship* 753 ss.

KITCHENS, JHONSON, GRAY, *Understanding echo chambers and filter bubbles: the impact of social media on diversification and partisan shifts in news consumption* (2020) 44 *Mis Quarterly* 1619 ss.

KLABBERS, *International Law*, Cambridge, 2017.

KLITOU, *A solution, but not a panacea for defending privacy: The challenges, criticism and limitations of privacy by design*, in *Privacy Technologies and Policy: First Annual Privacy forum*, Berlin, 2014.

KROLL *et al*., *Accountable Algorithms* (2017) 165 *University of Pennsylvania Law Review* 633 ss.

KULESZA, voce «Privacy», in *Encyclopedia of Big Data*, a cura di SCHINTLER, MCNEELY, Berlin, 2017.

LANIER, *You are not a gadget: a manifesto*, London, 2011.

LECUN, BENGIO, HINTON, *Deep Learning* (2015) 521 *Nature* 436 ss.

LEXCELLENT, *Artificial intelligence versus human intelligence: are humans going to be hacked?*, Switzerland, 2019.

LIPTON, *The mythos of model interpretability*, 2017 (*https://arxiv.org/pdf/1606.03490.pdf*, ultimo accesso 5 febbraio 2021).

LISBOA, *Interpretability in Machine Learning – Principles and Practice*, in *Fuzzy Logic and Applications 10th International Workshop*, Berlin, 2013, 15 ss.

LOLLI, *Turing: il coraggio dell'ingenuità*, in *L'eredità di Alan Turing. 50 anni di Intelligenza Artificiale*, a cura di CAPPUCCIO, Milano, 2005, 23 ss.

LONGO, SCORZA, *Intelligenza Artificiale*, Torino, 2020.

LOSANO, *Il progetto di legge tedesco sull'auto a guida automatizzata*, in *Dir. infrom.*, 2017, 1 ss.

LOSANO, *Verso l'auto a guida autonoma in Italia*, in *Dir. inform.*, 2019, 423 ss.

LUCCHINI GUASTALLA, *Privacy e* data protection: *principi generali*, in *Privacy digitale, Riservatezza e protezione dei dati e nuovo Codice Privacy*, a cura di TOSI, Milano, 2019, 55 ss.

MONTAGNANI, *La libera circolazione dei dati al bivio: tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Merc. conc. reg.*, 2019, 293 ss.

MACERATINI, *Dall'*Internet of Things *alle* Smart Roads. *Riflessioni informatico-giuridiche su strade intelligenti, veicoli automatici e connessi*, in *Riv. elet. dir. econ. management*, 2019, 71 ss.

MACERATINI, *Privacy e informazione nell'era dei Big Data*, in *Riv. sc. com. arg. giur.*, 2019, 79 ss.

MAGGIANO, CICERCHIA, *Algoritmi, etica e diritto*, in *Dir. inform.*, 2019, 1161 ss.

MALGIERI, COMANDÈ, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation* (2017) 7 *International Data Privacy Law* 243 ss.

MALGIERI, CUSTERS, *Pricing privacy: the right to know the value of your personal data* (2018) 34 *Computer Law & Security Review* 289 ss.

MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO, Torino, 2017, 287 ss.

MANTELERO, *La gestione del rischio nel GDPR: limiti e sfide nel contesto dei Big Data e delle applicazioni di Artificial Intelligence*, in *Regolare la tecnologia: il Reg. UE n. 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di MANTELERO, POLETTI, Pisa, 2018, 289 ss.

MANTELERO, *La privacy all'epoca dei Big Data*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 1181 ss.

MANTELERO, *La gestione del rischio*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101a*, a cura di FINOCCHIARO, Torino, 2019, 473 ss.

MARCHINI, *Intelligenza Artificiale e responsabilità civile: dal* "Responsibility Gap" *alla personalità elettronica dei robot*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di DORIGO, Pisa, 2020, 231 ss.

MARETTI, RUSSO, GOBBO, *Open data governance: civic hacking movement, topics and opinions in digital space* (2021) 55 *Quality & Quantity* 1133 ss. (*https://doi.org/10.1007/s11135-020-01045-y*, ultimo accesso 26 aprile 2021).

MASTRELIA, *Gestione dei Big Data in una prospettiva orientata alla tutela della privacy degli individui*, in *Dir. ind*., 2018, 364 ss.

MATTEI, voce «proprietà», nel *Digesto, Disc. priv., sez. civ.*, 15, XV, Torino, 1996, 433.

MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in *Libera circolazione e protezione dei dati personali*, a cura di PANETTA, Milano, 2006, 993 ss.

MCCARTHY *et al*., *A proposal for the Dartmouth Summer Research Project on Artificial Intelligence,* August 31, 1955, (2006) 27 *AI magazine* 12 ss.

MENDOZA, BYGRAVE, *The right not to be subject to automated decisions based on profiling*, in *EU Internet Law: Regulation and Enforcement*, a cura di SYNODINOU *et al.*, Berlin, 2017, 77 ss.

MENEGHETTI, *La privacy del guidatore al tempo della mobilità intelligente*, in *Dir. mer. tec.*, 2017, 1 ss.

MESSINA, *Le linee guida in materia di Intelligenza Artificiale: alla ricerca di un* "etica by design" *nel nuovo scenario digitale*, in *De Iustitia. riv. giur.*, 2019, 87 ss.

MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. piv.*, 1998, 339 ss.

MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione della decisione automatizzata*, in *Contr. impr.*, 2019, 861 ss.

MEYER, *Seven Principles of Software Testing* (2008) 8 I*EEE transactions on Computers* 99 ss.

MINISCALCO, Smart area, *circolazione dei veicoli autonomi e protezione dei dati personali*, in Smart Roads *e* Driverless cars: *tra diritto, tecnologie, etica pubblica*, a cura di SCAGLIARINI, Torino, 2019, 27 ss.

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

MITTELSTADT, *From individual to group privacy in Big Data Analytics* (2017) 30 *Philosophy & Technology* 475 ss.

MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, in *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di ZORZI GALGANO, Milano, 2019, 255 ss.

MONATERI, *La responsabilità civile*, nel *Trattato Sacco*, Torino, 1998.

MONTEROSSI, *Estrazione e (ri)utilizzo di informazioni digitali all'interno della rete internet. Il fenomeno del c.d.* web scraping, in *Dir. inform.*, 2020, 327 ss.

MORETTI, *Algoritmi e diritti fondamentali della persona. Il contributo del Regolamento (UE) 2016/679*, in *Dir. inform.*, 2018, 799 ss.

MORO VISCONTI, *La valutazione economica dei database (banche dati)*, in *Dir. ind.*, 2017, 358 ss.

MOSER, *The Application & Impact of the European General Data Protection Regulation on Blockchains*, in *R3 Reports*, 15 febbraio 2017 (*https://www.r3.com/wp-content/uploads/2018/04/GDPR_Blockchains_R3.pdf*, ultimo accesso 14 settembre 2021).

MULA, *Elaborazione e sfruttamento dei dati mediante algoritmi*, in *La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele*, a cura di GAMBINO e STANZI, Pisa, 2020, 127 ss.

NARAYANAN, SHMATIKOV, *Robust De-anonymization of Large Sparse Datasets* (2008) *IEEE Symposium on Security and Privacy* 111 ss.

NAZZARO, *Macchine intelligenti* (smart cars): *assicurazione e tutela della privacy*, in *Dir. merc. ass. fin.*, 2018, 77 ss.

NAZZARO, *Privacy*, smart cities *e* smart cars, in *Privacy digitale, Riservatezza e protezione dei dati e nuovo Codice Privacy*, a cura di TOSI, Milano, 2019, 325 ss.

NEGROPONTE, *Being Digital*, New York, 1995.

NERVI, *Il perimetro europeo: portata applicativa e definizioni*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 161 ss.

NICITA, *Il dato profilato nella prospettiva economica tra* privacy, propertization, secrecy, in I *dati nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 1163 ss.

NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006.

O'NEIL, *Armi di distruzione matematica*, Milano, 2017.

OGRISEG, *Le basi giuridiche del trattamento dati*, in *Tecnologia e Diritto*, 2, a cura di ZICCARDI e PERRI, Milano, 2019, 75 ss.

OKKA, SADASIVAM, *Deep Learning Model for Detection of Attacks in the Internet of Things Based Smart Home Environment*, in *Proceedings of International Conference on recent trends in machine learning, IoT, Smart Cities and Applications*, Singapore, 2005, 727 ss.

ORFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *MediaLaws – riv. dir. media*, 2018, 82 ss.

OTTOLIA, *Big Data e innovazione computazionale*, Torino, 2017.

PACE, *Informazione: valori e situazioni soggettive*, in *Dir. soc.*, 2014, 735 ss.

PAGALLO, *Intelligenza artificiale e diritto. Linee guida per un oculato intervento normativo*, in *Sistemi int.*, 2017, 615 ss.

PALAZZANI, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Roma, 2020.

PALMERINI, *Robotica e diritto: suggestioni, intersezioni, sviluppi a margine di una ricerca europea*, in *Resp. civ. e prev.*, 2016, 1816 ss.

PALMIERI, *Trattamento dei dati personali e giornalismo: alla ricerca di un equilibrio stabile*, in *Diritto alla riservatezza e circolazione dei dati personali*, a cura di PARDOLESI, 2, Milano, 2003, 337 ss.

PARISER, *The filter bubble. What the Internet is hiding from you*, Milano, 2011, trd. 2012.

PAROLA, MERATI, GAVOTTI, Blockchain *e* smart contract: *questioni giuridiche aperte*, in *Contratti*, 2018, 681 ss.

PASQUALE, *The black box society: The Secret Algorithms that control money and information*, Cambridge, 2015.

PASQUALE, *New Laws of robotics. Defending human expertise in the age of AI*, Cambridge, 2020.

PASSAGLIA, *Il sistema delle fonti normative in materia di tutela dei dati personali*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 85 ss.

PASSAGNOLI, *Il diritto civile al tempo dell'intelligenza artificiale: spunti per una problematizzazione*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di DORIGO, Pisa, 2020, 67 ss.

PATTI, *La protezione dei dati personali*, nel *Commentario al D. lgs. 30 giugno 2003, n. 196 ("codice privacy")*, a cura di C.M. BIANCA e BUSNELLI, Padova, 2007, *sub* art. 23, 541 ss.

PELLECCHIA, *Profilazione e decisioni automatizzate al tempo della Black Box Society: quale leggibilità dell'algoritmo nella cornice della* responsible research and innovation, in *Nuove leggi civ. comm.*, 2018, 1209 ss.

PERRI, *Sicurezza giuridica e sicurezza informativa dal d.lgs. 196/03 al Regolamento generale sulla protezione dei dati*, in *Tecnologia e diritto*, 2, a cura di ZICCARDI e PERRI, Milano, 2019, 3 ss.

PERRUCCI, *Dai "Big Data" all'ecosistema digitale. Dinamiche tecnologiche e di mercato e ruolo delle politiche pubbliche*, in *Analisi guir. econ.*, 2019, 61 ss.

PIERUCCI, *Elaborazione dei dati e profilazione delle persone*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 413 ss.

PINZON, SANABRIA, *Aplicación del estándar ISO/IEC 9126-3 en el modelo de datos conceptual entidad-relación*, in *Revista Facultad de Ingeniería*, 2013, 113 ss.

PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in N*uove leggi civ. comm*., 2017, 369 ss.

PIRODDI, *I trasferimenti di dati personali verso paesi terzi dopo la sentenza schrems e nel nuovo regolamento generale sulla protezione dei dati*, in *Dir. inform*., 2015, 827 ss.

PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016.

PIZZETTI, *La protezione dei dati personali e la sfida dell'Intelligenza Artificiale*, in *Intelligenza Artificiale, protezione dei dati personali e regolazione*, a cura di PIZZETTI, Torino, 2018, 5 ss.

POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, *GDPR tra novità e discontinuità*, a cura di CATERINA, in *Giur. it.*, 2019, 2783 ss.

POLETTI, CAUSARANO, *Autoregolamentazione privata e tutela dei dati personali: tra codici di condotta e meccanismi di certificazione*, in *Privacy digitale*, a cura di TOSI, Milano, 2019, 369 ss.

POLICELLA, PELINO, nel *Codice della Disciplina Privacy*, a cura di BOLOGNINI e PELINO, Milano, 2019, *sub* art. 82, 440 ss.

PRETA, ZOBOLI, *Intelligenza Artificiale ed economia dei dati. Profili regolatori e concorrenziali in tema di accesso e condivisione dei dati*, in *Analisi giur. econ.*, 2019, 213 ss.

PRINS, *Property and Privacy: European Perspectives and the Commodification of our Identity*, in *The Future of the Public Domain, Identifying the Commons in Information Law*, The Hague, 2006, 223 ss.

PROIETTI, *La responsabilità nell'Intelligenza Artificiale e nella robotica*, Milano, 2020.

PUCELLA, *Autodeterminazione e responsabilità nella relazione di cura*, Milano, 2010.

QUAGLIARELLO, FIN, *Il consenso informato in ambito medico: un'indagine antropologica e giuridica*, Bologna, 2016.

RABAI, *I «big data» nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in Amministrare, 2017, 405 ss.

RANIELI, *Cronache in tema di brevettabilità delle invenzioni* software related, *con particolare riguardo al ruolo dell'EPO e alla più recente giurisprudenza del regno unito*, in *Riv. dir. ind.*, 2009, 233 ss.

RATTI, *La responsabilità da illecito trattamento dei dati personali nel nuovo regolamento*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO, Torino, 2017, 615 ss.

RATTI, *La responsabilità da illecito trattamento dei dati personali*, in *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, a cura di FINOCCHIARO, Torino, 2019, 773 ss.

RESTA F., nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA e BELISARIO, Milano, 2018, *sub* art. 5, 49.

RESTA G., *Nuovi beni immateriali e* numerus clausus *dei diritti esclusivi*, in *Diritti esclusivi e nuovi beni immateriali*, a cura di RESTA G., Milano, 2010, 3 ss.

RESTA G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in *Dir. inform.*, 2015, 697.

RESTA G., *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019 /770 e il Regolamento (UE) 2016/ 679*, in *La circolazione dei dati. Titolarità, strumenti negoziali, diritti e tutele*, a cura di GAMBINO e STANZI, Pisa, 2020, 55 ss.

RESTA G., SALERNO, *La responsabilità civile per il trattamento dei dati personali*, in *La responsabilità d'impresa*, a cura di ALPA e CONTE, 2015, 643 ss.

RICCIO, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA e BELISARIO, Milano, 2018, *sub* art. 82, 596 ss.

RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *Dir. inform*., 2018, 689 ss.

RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 23 ss.

RICOTTI, *Dati sanitari e gli altri profili etici nella bioingegneria*, in *Riv. it. med. leg.*, 2019, 251 ss.

RINALDI, Smart contract: *meccanizzazione del contratto nel paradigma della* blockchain, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 343 ss.

RIZZUTI, *Il* peculium *del robot. Spunti sul problema della soggettivizzazione dell'intelligenza artificiale*, in *Il ragionamento giuridico nell'era dell'Intelligenza Artificiale*, a cura di DORIGO, Pisa, 2020, 283 ss.

RODOLFI, *La fuga di dati e la minaccia dei* data breach, in *Tecnologia e Diritto*, 2, a cura di ZICCARDI e PERRI, Milano, 2019, 139 ss.

RODOTÀ, *La privacy tra individuo e collettività*, in *Pol. dir.*, 1974, 545 ss.

RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012.

RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Roma-Bari, 2014.

RODOTÀ, *Elaboratori elettronici e controllo sociale*, 1973, Ristampa anastatica, a cura di ALPA, Napoli, 2018.

ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 103 ss.

ROMEO, *Il governo giuridico delle tecniche dell'informazione e della comunicazione*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 1243 ss.

ROSSI DAL POZZO, *Alcune riflessioni a margine della nuova disciplina in materia di protezione dei dati personali di cui al Regolamento (UE) 2016/679/UE*, in *Eurojus*, 1 ss.

ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (da*l safe harbour *al* privacy shield*)*, in *Riv. dir. int.*, 2016, 690.

ROTOLO, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA e BELISARIO, Milano, 2018, *sub* art. 32, 293 ss.

RUFFOLO, *Per i fondamenti di un diritto della robotica* self-learning: *dalla* machinery *produttiva all'auto* driverless: *verso una "responsabilità da algoritmo"?*, in *Intelligenza artificiale e responsabilità: responsabilità da algoritmo?, A.I. e automobili* self-driving, *automazione produttiva, robotizzazione medico-farmaceutica, A.I. e attività contrattuali, le tendenze e discipline unionali*, a cura di RUFFOLO, Milano, 2017, 1 ss.

RUFFOLO, *Intelligenza artificiale,* machine learning e *responsabilità da algoritmo*, in *Giur. it*., 2019, 1689 ss.

RUFFOLO, *Le responsabilità da* artificial intelligence*, algoritmo e* smart product*: per i fondamenti di un diritto dell'intelligenza artificiale* self-learning, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di RUFFOLO, Milano, 2020, 93 ss.

RUFFOLO, *La personalità elettronica*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di RUFFOLO, Milano, 2020, 213 ss.

RUSSELL, NORVIG, *Intelligenza Artificiale. Un approccio moderno*, 1, II ed., Milano, 2005.

RUSSELL, NORVIG, *Intelligenza Artificiale. Un approccio moderno*, 2, II ed., Milano, 2005.

SAMMARCO, *L'attività di* web scraping *nelle banche dati ed il riuso delle informazioni*, in *Dir. inform.*, 2020, 219 ss.

SANDVIG *et al.*, *Auditing algorithms: Research methods for detecting discrimination on internet platforms*, 2014 (*http://www-personal.umich.edu/~csandvig/research/Auditing%20Algorithms%20--%20Sandvig%20--%20ICA%202014%20Data%20and%20Discrimination%20Preconference.pdf*, ultimo accesso 14 settembre 2021).

SANTOSUOSSO, *Diritto, Scienza, Nuove Tecnologie*, Padova, 2016.

SANTOSUOSSO, *Questioni definitorie*, in *Biolaw Journal – Rivista di Biodiritto*, 2020, 469 ss.

SANTOSUOSSO, *Intelligenza artificiale e diritto. Perché le tecnologie di IA sono una grande opportunità per il diritto*, Firenze, 2020.

SARRA, Business Intelligence *ed esigenze di tutela: criticità del c.d.* Data Mining, in *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, a cura di MORO e SARRA, Milano, 2019, 41 ss.

SARZANA DI SANT'IPPOLITO, NICOTRA, *Diritto della* Blockchain, *intelligenza artificiale e IoT*, Milano, 2018.

SCAGLIARINI, "Smart roads" *e* "driverless cars" *nella Legge di bilancio: opportunità e rischi di un'attività economica «indirizzata e coordinata a fini sociali»*, in *Quaderni cost.*, 2018, 497 ss.

SCAGLIARINI, *La sperimentazione su strada pubblica dei veicoli autonomi: il "decreto smart road"*, in Smart Roads *e* Driverless cars: *tra diritto, tecnologie, etica pubblica*, a cura di SCAGLIARINI, Torino, 2019, 15 ss.

SCALZINI, *Alcune questioni a proposito di algoritmi, dati, etica e ricerca*, in *Riv. it. med. leg.*, 2019, 169 ss.

SCOGNAMIGLIO, *Il sistema del danno non patrimoniale dopo le decisioni delle sezioni unite*, in *Resp. civ. e prev.*, 2009, 261 ss.

SCORZA, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA e BELISARIO, Milano, 2018, *sub* art. 2, 10 ss.

SELBST, POWLES, *Meaningful information and explanation* (2017) 7 *International Data Privacy Law* 233 ss.

SIANO, nel *Commentario GDPR e normativa privacy*, a cura di RICCIO, SCORZA e BELISARIO, Milano, 2018, *sub* art. 24, 236 ss.

SIANO, MONTUORI, *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in *Le nuove frontiere della privacy nelle tecnologie digitali*, a cura di BUSIA, LIGUORI e POLLICINO, Roma, 2016, 101 ss.

SICA, *Il consenso al trattamento dei dati: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.*, 2001, 621 ss.

SICA, *La responsabilità civile per il trattamento illecito dei dati personali*, in *Regolare la tecnologia: il Reg. UE n. 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, a cura di MANTELERO e POLETTI, Pisa, 2018, 161 ss.

SIMEONE, Machine Learning *e tutela della Privacy alla luce del GDPR*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 275 ss.

SIMONCINI, *Diritto costituzionale e decisioni algoritmiche*, in *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, a cura di DORIGO, Pisa, 2020, 37 ss.

SIMONINI, *L'intelligenza artificiale guida le nostre vetture. Profili di responsabilità*, Modena, 2018.

SIMONINI, *L'autovettura e le applicazioni digitali (APP)*, in *Danno e resp.*, 2021, 305 ss.

SORO, *La protezione dei dati personali nell'era digitale*, in *Nuova giur. civ. comm.*, 2019, II, 343 ss.

SPAGNARO, *L'ambito di riferimento materiale del nuovo regolamento*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di FINOCCHIARO, Torino, 2017, 23 ss.

SPEDICATO, *Creatività artificiale, mercato e proprietà intellettuale*, in *Riv. dir. ind.*, 2019, 253 ss.

SPERA, *Profili di responsabilità civile nel trattamento dei dati*, in *Tecnologia e Diritto*, 2, a cura di ZICCARDI e PERRI, Milano, 2019, 191 ss.

STAZI, CORRADO, *Datificazione dei rapporti socio-economici e questioni giuridiche: profili evolutivi in prospettiva comparatistica*, in *Dir. inform.*, 2019, 442 ss.

STIANO, *Il diritto alla privacy alla prova della sorveglianza di massa e dell'*intelligence sharing: l*a prospettiva della corte europea dei diritti dell'uomo*, in *Riv. dir. int*., 2020, 511 ss.

STRAMPELLI, *L'informazione societaria a quindici anni dal T.U.F.: profili evolutivi e problemi*, in *Riv. soc.*, 2014, 991 ss.

TADDEI ELMI, *Soggettività e responsabilità dei sistemi di IA*, in *Il diritto di Internet nell'era digitale*, a cura di CASSANO e PREVITI, Milano, 2020, 847 ss.

TARULLO, *La gestione del rischio nel trattamento dei dati personali*, in *La nuova "privacy europea". I principali adempimenti del regolamento UE 2016/679 e profili risarcitori*, a cura di DI RESTA, Torino, 2018, 113 ss.

TAYLOR, WILSON, *Reasonable expectations of privacy and disclosure for health data* (2019) 27 *Medical Law Review* 432 ss.

TEROLLI, Blockchain *e* compliance (Regtech), in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 377 ss.

TEUBNER, *Soggetti giuridici digitali?: sullo status privatistico degli agenti software autonomi*, a cura di FEMIA, Napoli, 2019.

TEUBNER, *Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten* (tr. *Digital personhood? the status of autonomous software agents in private law*), in *Ancilla Iuris*, 2018, 36 ss.

THOBANI, *Il consenso al trattamento dei dati come condizione per la fruizione di servizi on-line*, in *Internet e diritto civile*, a cura di C. PERLINGIERI e RUGGERI, Napoli, 2015, 459 ss.

THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e dir. priv.*, 2016, 513 ss.

THOBANI, *Il mercato dei dati personali: tra tutela dell'interessato e tutela dell'utente*, in *MediaLaws – riv. dir. media*, 2019, 131 ss.

TORINO, *La valutazione di impatto* (Data Protection Impact Assessment), in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 855 ss.

TOSI, *Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale*, Milano, 2019.

TRAVAGLIA, *Big data e Regolamento europeo sulla protezione dei dati personali*, in *academia.edu*, 2017, 1 ss.

TRESCA, *I primi passi verso l'Intelligenza Artificiale al servizio del cittadino: brevi note sul Libro Bianco dell'Agenzia per l'Italia digitale*, in *MediaLaws – riv. dir. media*, 2018, 240 ss.

TREVISI, *La Regolamentazione in materia di intelligenza artificiale, robot, automazione: a che punto siamo*, in *MediaLaws – riv. dir. media*, 2018, 447 ss.

TRIMARCHI, *La responsabilità civile: atti illeciti, rischio, danno*, Milano, 2017.

TUCKER, WELLFORD, *Big mistakes regarding big data* (2014) *The antitrust source* 1 ss.

TURANO, *Robotica e roboetica: questioni e prospettive nazionali ed europee*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 125 ss.

TURING, *Computing Machinery and intelligence* (1950) 59 *Mind* 433 ss.

ULISSI, *I profili di responsabilità della macchina dell'apprendimento nell'interazione con l'utente*, in *Diritto e Intelligenza Artificiale*, a cura di ALPA, Pisa, 2020, 435 ss.

VADARIYA, JADAV, *A survey on phishing URL detection using Artificial Intelligence*, in *Proceedings of International Conference on recent trends in machine learning, IoT, Smart Cities and Applications*, Berlin, 2021, 9 ss.

VAGNI, *The role of human judge in judicial decisions, preliminary remarks on legal interpretation in the age of artificial intelligence*, in *La decisione nel prisma dell'intelligenza artificiale*, a cura di CALZOLAIO, Milano, 2020, 185 ss.

VANTIN, *Automobili a guida autonoma: un'inedita opportunità per le persone con disabilità fisiche?*, in Smart Roads *e* Driverless cars: *tra diritto, tecnologie, etica pubblic*a, a cura di SCAGLIARINI, Torino, 2019, 55 ss.

VEDASCHI, NOBERASCO, *Gli autoveicoli a guida autonoma alla prova del diritto*, in *Dir. pub. comp. eur.*, 2019, 769 ss.

VELLIDO, MARTIN-GUERRERO, LISBOA, *Making machine learning models interpretable*, in *European Symposium on Artificial Neural Networks*, *Computational Intelligence and Machine Learning*, Burges, 2012, 163 ss.

VESPIGNANI, RIJTANO, *L'algoritmo e l'oracolo. Come la scienza predice il futuro e ci aiuta a cambiarlo*, Milano, 2019.

VITTAL, *Phishing, Pharming, and other Scams* (2005) 22 *GP Solo – Privacy and security* 26 ss.

VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale. Sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019.

WABER, *People Analytics: How social sensing Technology will transform business and what It tells Us about the New World of Work*, New York, 2013.

WACHTER, MITTELSTADT, FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation* (2017) 7 *International Data Privacy Law* 76 ss.

WACHTER, MITTELSTADT, RUSSELL, *Counterfactual explanations without opening the black box: automated decisions and the GDPR* (2018) 31 *Harvard Journal of Law & Technology* 842 ss.

WARREN, BRANDEIS, *The right to privacy* (1890) 4 *Harvard Law Review* 193 ss.

WARWICK, *Intelligenza Artificiale. Le basi*, Palermo, 2012, tr. 2015.

XU *et al*., *Internet vehicles in Big Data Era* (2018) 5 *Journal of automatica Sinica* 19 ss.

YUCHI *et al*., *DeepTest: Automated testing of Deep-Neural-Network-drive Autonomous Cars*, in 4*0th International Conference on Software Engineering*, May 27-June 3, New York, 2018, 303 ss. (*dl.acm.org/doi/pdf/10.1145/3180155.3180220*, ultimo accesso 14 settembre 2021).

ZAMBRANO, *Il Comitato europeo per la protezione dei dati*, in *I dati personali nel diritto europeo*, a cura di CUFFARO, D'ORAZIO e RICCIUTO, Torino, 2019, 983 ss.

ZANUZZI, *Internet of Things e privacy. Sicurezza e autodeterminazione informativa*, in *Tecnodiritto. Temi e problemi di informatica e robotica giuridica*, a cura di MORO e SARRA, 2019, 99 ss.

ZECH, *Data as a tradeable commodity*, in *European Contract Law and the Digital Single Market. The Implications of the Digital Revolution*, Cambridge, 2016, 51 ss.

ZENO ZENCOVICH, *Una lettura comparatistica della l. 675/96 sul trattamento dei dati personali*, in *La disciplina del trattamento dei dati personali*, a cura di CUFFARO, RICCIUTO e ZENO ZENCOVICH, Torino, 1997, 733 ss.

ZENO ZENCOVICH, *Ten legal perspectives on the "big data revolution"*, in *Conc. merc.*, 2016, 29 ss.

ZENO ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws – riv. dir. media*, 2018, 32 ss.

ZHANG, *Who owns the data generated by your smart car?* (2018) 32 *Harvard Journal of Law & Technology* 299 ss.

ZHAO, voce «Web Scraping», in *Encyclopedia of Big Data*, a cura di SCHINTLER, MCNEELY, Berlin, 2017.

ZIVIZ, *Lo spettro dei danni bagatellari*, in *Resp. civ. e prev.*, 2009, 571 ss.

Documenti

AGID, Comunicato stampa *Misurazione della qualità dei dati*, 2015 (*www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/iso_25024_agid_misurazione_della_qualita_dei_dati.pdf*, ultimo accesso 26 aprile 2021).

AGCOM, *Big data Interim report nell'ambito dell'indagine conoscitiva di cui alla delibera 217/17/CON*, 2018 (*https://www.agcom.it/documents/10179/10875949/Studio-Ricerca+08-06-2018/c72b5230-354d-444f-9e3f-5467ca450714?version=1.0*, ultimo accesso 30 dicembre 2020).

AGCOM, *Indagine conoscitiva sui Big Data di cui alla delibera 458/19/CONS*, 2020 (*https://www.agcom.it/documents/10179/17633816/Documento+generico+10-02-2020+1581346981452/39c08bbe-1c02-43dc-bb8e-6d1cc9ec0fcf?version=1.0*, ultimo accesso 30 dicembre 2020).

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO, provvedimento n. 24432, Facebook – condivisione dati con terzi, 2018.

COMITATO CONSULTIVO DELLA CONVEZIONE 108, *Linee guida in materia di intelligenza artificiale e protezione dei dati*, 2019.

COMITATO CONSULTIVO DELLA CONVENZIONE 108, *Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big data*, 2017.

COMMISSIONE EUROPEA, *Orientamenti per l'attuazione/applicazione della direttiva 2005/29/CE relativa alle pratiche commerciali sleali*, 2016.

COMMISSIONE EUROPEA, Comunicato stampa *Riforma della protezione dei dati nell'UE – Più tutele per i singoli, meno costi per le imprese*, 2012 (*https://ec.europa.eu/commission/presscorner/detail/it/IP_12_46*, ultimo accesso 14 settembre 2021).

COMMISSIONE EUROPEA, Comunicato stampa *Ethics Guidelines for Trustworthy AI*, 2019 *(https://ec.europa.eu/futurium/en/ai-alliance-consultation.1.html*, ultimo accesso 15 dicembre 2020).

COMMISSIONE EUROPEA, Comunicato stampa *Orientamenti etici sull'intelligenza artificiale: proseguono i lavori della Commissione*, 2019 (*https://ec.europa.eu/commission/presscorner/detail/it/IP_19_1893* ultimo accesso 20 dicembre 2020).

CONSIGLIO D'EUROPA, *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*, 2019.

CONSIGLIO EUROPEO, *Programma di Stoccolma – Un'Europa aperta e sicura al servizio e a tutela dei cittadini*, 2010.

Dichiarazione dei Diritti di Internet, 14 luglio 2015, (*https://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf*, ultimo accesso 14 settembre 2021).

EUROPEAN DATA PROTECTION BOARD, *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of COVID-19*, 2020.

EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data*, 2016.

EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, 2017.

EUROPEAN UNION AGENCY FOR CYBERSECURITY, *Cyber security and resilience of smart cars*, 2017 (*www.enisa.europa.eu*, ultimo accesso 6 luglio 2021).

FIA, Comunicato stampa *FIA reveals what data is being tracked and how the public reacts to connected cars*, 25 novembre 2015 (*www.fia.com*, ultimo accesso 5 luglio 2021).

FEDERAL TRADE COMMISSION, Comunicato stampa *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, 24 luglio 2019

(*https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions*, ultimo accesso 14 settembre 2021).

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Marketing: necessario il consenso per l´invio di comunicazioni promozionali via e-mail, 2010.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Linee guida in materia di attività promozionale e contrasto allo spam, 2013.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Ordinanza di ingiunzione nei confronti di Telecom Italia S.p.A., 2018.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid-19 - App Immuni, 2020.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Scheda informativa *Deepfake. Il falso che ti «ruba» la faccia (e la privacy)*, 2020 (*https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9512278*, ultimo accesso 30 maggio 2021).

GRUPPO DI LAVORO ART. 29, *Parere 4/2007 sul concetto di dati personali*, 2007.

GRUPPO DI LAVORO ART. 29, *Parere 3/2010 sul principio di responsabilità*, 2010.

GRUPPO DI LAVORO ART. 29, *Opinion 3/2013 on purpose limitation*, 2013.

GRUPPO DI LAVORO ART. 29, *Parere 5/2014 sulle tecniche di anonimizzazione*, 2014.

GRUPPO DI LAVORO ART. 29, *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet degli oggetti*, 2014.

GRUPPO DI LAVORO ART. 29, *Guidelines on automated individual decision-making and profiling for the purposes of regulation* 2016/679, 2017.

GRUPPO DI LAVORO ART. 29, *Opinion 3/2017 on processing personal data in context of cooperative intelligent transport systems (C-ITS)*, 2017.

HIGH LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (AI HLEG), *Definition of AI: Main capabilities and disciplines*, 2018.

HIGH LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (AI HLEG), *Draft of the AI Ethics Guidelines*, 2018.

HIGH LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (AI HLEG), *The Ethics Guidelines for Trustworthy Artificial Intelligence (AI)*, 2019.

HIGH LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE (AI HLEG), *The assessment list for trustworthy artificial intelligence (ALTAI) for self assessment*, 2020.

MINISTERO DELLE INFRASTRUTTURE E DELLA MOBILITÀ SOSTENIBILI, Comunicato stampa *Smart road, veicoli connessi e mobilità del futuro*, 22 giugno 2016 (*www.mit.gov.it*, ultimo accesso 5 giugno 2021).

MINISTERO DELLE INFRASTRUTTURE E DEI TRASPOSTI, *Standard funzionali per le Smart-Road*, 22 giugno 2016 (*www.mit.gov.it*, ultimo accesso 5 giugno 2021).

OECD, *Guidelines on the protection of privacy and transborder flows of personal data*, 1980 (w*ww.garanteprivacy.it/documents/10160/10704/1799578*, ultimo accesso 9 giugno 2021).

OECD, *Convergence between Communications Technologies: Case Studies from North America and Western Europe*, 1992.

OECD, *Telecommunications and Broadcasting: Convergence or Collision? No. 29*, 1992 (*https://www.oecd-ilibrary.org/science-and-technology/telecommunications-and-broadcasting_237416285388*, ultimo accesso 30 dicembre 2020).

OECD, *Glossary Of Statistical Terms*, 2007.

PARLAMENTO EUROPEO, *study Research for TRAN Committee, Self-piloted cars: the future of road transport?*, 2016 (*www.europarl.europa.eu*, ultimo accesso 5 giugno 2021).

PARLAMENTO EUROPEO, Comunicato stampa *Auto a guida autonoma in UE: dalla fantascienza alla realtà* 15 gennaio 2019 (*www.europarl.europa.eu*, ultimo accesso 5 giugno 2021).

PARLAMENTO EUROPEO, Comunicato stampa *Incidenti su strada: obbligo di tecnologie salvavita a bordo*, 16 aprile 2019 (*www.europarl.europa.eu*, ultimo accesso 5 giugno 2021).

SAE, *International Standard j3016, Levels of driving automation*, 2019.

SORO, *L'universo dei dati e la libertà della persona*, discorso del Presidente dell'Autorità Garante per la Protezione dei Dati Personali, Relazione annuale per il 2018. Roma, 7 maggio 2019 (*https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9109075*, ultimo accesso 14 settembre 2021).

TEXAS A & M TRANSPORT INSTITUTE, *Data ownership issues in a connected car environment*, 2016 (h*ttps://static.tti.tamu.edu/tti.tamu.edu/documents/165604-1.pdf*, ultimo accesso 5 giugno 2021).

UK INFORMATION COMMISSIONER'S OFFICE, *Opinion 6.4.2017. Feedback request-profiling and automated decsion-making*, 2017.

UFFICIO BREVETTI EUROPEO, *Decisione T1173/97* (*www.epo.org*, ultimo accesso 15 luglio2021).

Standard ISO/IEC TR 9126-3:2003.

Standard UNI CEI ISO/IEC 25012:2008.

Standard ISO/IEC 25010:2011.

Standard UNI CEI ISO/IEC 25024:2016.

Standard UNI EN ISO/IEC 27001:2017.

Fonti pattizie

Convenzione n. 108/1980 e successive modificazioni.

Diritto primario dell'Unione europea

Carta dei diritti fondamentali dell'Unione europea, G.U. n. C. 364 del 18.12.2000.

Convenzione europea dei Diritti dell'Uomo (CEDU), 1950.

Trattato sull'Unione europea, G.U. n. C. 191 del 29.7.1992.

Trattato sul funzionamento dell'Unione europea, G.U. n. C. 326 del 26.10.2012.

Diritto derivato dell'Unione europea

Direttiva 1995/46/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, G.U. n. L. 281 del 23.11.1995.

Direttiva 1996/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati, G.U. n. L. 077 del 27.3.1996.

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento di dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, G.U. n. L. 201 del 31.7.2002.

Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE, G.U. n. L. 94 del 28.3.2014.

Direttiva 2016/680/UE del Parlamento Europeo e del Consiglio, del 27.4.2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, G.U. n. L. 119 del 4.5.2016.

Direttiva 2016/681/UE del Parlamento Europeo e del Consiglio, del 27.4.2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati più gravi, G.U. n. L. 119 del 4.5.2016.

Direttiva 2016/943/UE del Parlamento europeo e del Consiglio, dell'8 giugno 2016, sulla protezione del Know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti, G.U. n. L. 157 del 15.6.2016.

Direttiva 2016/1148/UE 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, G.U. n. L. 194 del 19.7.2016.

Direttiva 2019/1024/UE del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, G.U. n. L. 172 del 26.6.2019.

Regolamento 2014/910/UE 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, G.U. n. L. 257 del 28.8.2014.

Regolamento 2016/679/UE 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 (regolamento generale sulla protezione dei dati), G.U. n. L. 119 del 4.5.2016.

Regolamento 2018/1807/UE 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, G.U. n. L. 303 del 28.11.2018.

Regolamento 2019/881/UE del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»), G.U. n. L. 151 del 7.6.2019.

Atti atipici dell'Unione europea

Commissione Europea, *Documento di lavoro dei servizi della commissione. Quadro dell'UE 2021-2030 per la sicurezza stradale – Prossime tappe verso l'obiettivo "zero vittime" ("Vision Zero")*, 2019.

Commissione europea, *Libro bianco sull'intelligenza artificiale – un approccio europeo all'eccellenza e alla fiducia*, 2020.

Comunicazione della Commissione, *Un'iniziativa europea in materia di commercio elettronico*, 1977.

Comunicazione della Commissione, *Sul principio di precauzione*, 2000.

Comunicazione della Commissione, *Uno spazio di libertà, sicurezza e giustizia al servizio dei cittadini*, 2009.

Comunicazione della Commissione, *Creare uno spazio di libertà, sicurezza e giustizia per i cittadini europei. Piano d'azione per l'attuazione del programma di Stoccolma*, 2010.

Comunicazione della Commissione, *Un approccio globale alla protezione dei dati personali nell'Unione Europea*, 2010.

Comunicazione della Commissione, *Verso uno spazio europeo della sicurezza stradale: orientamenti 2011-2020 per la sicurezza stradale*, 2010.

Comunicazione della Commissione, *Strategia per il mercato unico digitale in Europa*, 2015.

Comunicazione della Commissione, *Le piattaforme online e il mercato unico digitale Opportunità e sfide per l'Europa*, 2016.

Comunicazione della Commissione, *Una strategia europea per i sistemi di trasporto intelligenti cooperativi, prima tappa verso una mobilità cooperativa, connessa e automatizzata*, 2016.

Comunicazione della Commissione, *Costruire un'economia dei dati europea*, 2017.

Comunicazione della Commissione, *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche)*, 2017.

Comunicazione della Commissione, *L'Europa in movimento – Una mobilità sostenibile per l'Europa: sicura, interconnessa e pulita*, 2018.

Comunicazione della Commissione, *L'intelligenza artificiale per l'Europa*, 2018.

Comunicazione della Commissione, *Guidance on Regulation on a framework for the free flow of non-personal data in the European Union*, 2019.

Comunicazione della Commissione, *Una strategia europea per i dati*, 2020.

Comunicazione della Commissione, *Proposta di Regolamento che stabilische regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione*, 2021.

Relazione della Commissione, *Salvare vite umane: migliorare la sicurezza dei veicoli nell'UE*, 2016.

Relazione della Commissione, *sulle implicazioni dell'intelligenza artificiale, dell'internet delle cose e della robotica in materia di sicurezza e responsabilità*, 2020.

Risoluzione del Parlamento europeo 2015/2103 del 16 febbraio 2017 recante *raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica*, G.U. n. C. 252 del 18 luglio 2018.

Risoluzione del Parlamento europeo 2017/2772 del 3 ottobre 2018 *sulle tecnologie di registro distribuito e blockchain: creare fiducia attraverso la disintermediazione*, 3 ottobre 2018.

Risoluzione del Parlamento europeo 2020/2014 del 20 ottobre 2020 recante *raccomandazioni alla Commissione su un regime di responsabilità civile per l'intelligenza artificiale*, 20 ottobre 2020.

Fonti normative di diritto italiano

Legge 22 aprile 1941, n. 633 (Legge sul diritto d'autore e su altri diritti connessi al suo esercizio).

Legge 31 dicembre 1996, n. 675.

Decreto legislativo 30 giugno 2003, n. 196 (Codice della Privacy).

Legge 27 dicembre 2017, n. 205 (Legge di Bilancio per l'anno 2018).

Decreto del Ministero delle Infrastrutture e dei trasporti del 28 febbraio 2018 (Decreto Smart road).

D. lgs. 10 agosto 2018, n. 101.

Decisioni giurisprudenziali italiane

Corte cost., 12.4.1973, n. 38, in *DeJure*.

Corte cost., 26.3.1990, n. 139, in *Giur. it*., 1991, I, 376.

Corte cost., 11.3.1993, n. 81, in *Giur. it*., 1995, I, 108.

Cass., 27.5.1975, n. 2129, in *Mass. Giur. it*., 1975, 594.

Cass. 27.7.1990, n. 7571, in *Resp. civ. e prev*., 1991, 458.

Cass., 9.6.1998, n. 5658, in *Foro it.*, *1998*, I, 2387.

Cass., 28.2.2000, n. 2220, in *Foro it.*, 2000, I, 1828.

Cass., 10.2.2003, n. 1954, in *Dir. e giust.*, 2003, 98.

Cass., 7.5.2007, n. 10300, in *Mass. Giust. civ.*, 2007, 5.

Cass., sez. un., 11.11.2008, nn. 26972-26975, in *Resp. civ. e prev*., 2009, 38.

Cass., 19.5.2014, n. 10947, in *Foro it.*, 2015, I, 120.

Cass., 5.9.2014, n. 18812, in *Foro it.*, 2015, I, 119.

Cass., 15.7.2014, n. 16133, in *Foro it.*, 2015, I, 120.

Cass. 20.5.2015, n. 10280, in *Mass. Giust. civ*., 2015.

Cass., 11.1.2016, n. 222, in *Ri.da.re*, 2016.

Cass., 29.1.2016, n. 1748, in *Annali it. dir. aut*., 2016, 749.

Cass., 16.5.2016, n. 9982, in *Dir. e Guis.*, 2016.

Cass., sez. un., 27.12.2017, n. 30981, in *Foro it*., 2018, I, 2147.

Cass., 2.7.2018, n. 17278, in *Guida al dir*., 2018, 20.

Cass., 19.7.2018, n. 19180, in *Foro it.*, 2018, I, 3968.

Cass., 21.6.2018, n. 16358, in *Guida al dir.*, 2018, 32.

Cass., 11.9.2019, n. 15598, in *Guida al dir*., 2019, 60.

Cass., 20.8.2020, n. 17383, in *Mass. Giust. civ.*, 2020.

Cass., 26.4.2021, n. 11020, in *Mass. Giust. civ.*, 2021.

Cass., 10.6.2021, n. 16402 in *DeJure*.

Cass., 25.5.2021, n. 14381, in *Guida al dir*., 2021, 23.

Cons. Stato, VI sez., 8.4.2019, n. 2270, in *Foro it.*, 2019, III, 606.

Cons. Stato, VI sez., 13.12.2019, n. 8472, in *Foro it*., 2020, III, 340.

T.A.R. Lazio, 22.3.2017, n. 3769, in *Leggi d'Italia.*

TAR Lazio, 10.1.2020, nn. 260 e 261, in *Foro Amm*., I, 2020, 99.

Trib. Milano, 28.9.2016, n. 10374 in *Foro it*., 2016, I, 3594.

Trib. Bologna, 31.12.2020, in *Riv. it. dir. lav*., 2021, II, 175.

Giurisprudenza della Corte di giustizia dell'Unione europea

Corte giust. UE, 12.3.2002, causa C-186/00, consultabile all'indirizzo: *eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62000CJ0168&from=HU*.

Corte giust. UE, 6.11.2003, causa C-101/01, in *Dir. e giust*., 2004, 122.

Corte guist. CE, 9.11.2004, causa C-203/2002, in *Eur. dir. priv.*, 2006, 319.

Corte giust. CE, grande sezione, 9.11.2004, causa C-444/2002, in *Dir. aut.*, 2005, 574.

Corte giust. UE, 24.11.2011, cause riunite C-468/10 e C-469/10, in *Foro it.*, 2012, IV, 1.

Corte giust. UE, 1.3.2012, causa C-604/2010, in *Dir. com. scamb. int.*, 2012, 269.

Corte giust. UE, grande camera, 13.5.2014, causa C-131/12, in *Foro it.*, 2014, IV, 295.

Corte giust. UE, 29.10.2015, causa C-490/2014, in *Dir. inform*., 2016, 185.

Corte giust. UE, 19.10.2016, causa C-582/14, in *Dir. inform*., 2016, 748.

Corte giust. UE, 20.12.2017, causa C-434/16, in *Dir. inform*., 2017, 857.

Corte giust. UE, 15.1.2018, causa C-498/16, in Dir. inform., 2018, 136 (e considerazioni dell'Avvocato generale).

Giurisprudenza statunitense

Greenway v. St. Joseph's Hosp., No. 03-CA-011667 (Fla. Cir. Ct. 2003).

Katz v. United States, 389 U.S. 347 (1967).

Mracek v. Bryn Mawr Hosp., 610 F. Supp. 2d 401, 402 (E.D. Pa. 2009), aff'd, 363 F. App'x 925 (3d Cir. 2010).

O'Brien v. Intuitive Surgical, Inc., No. 10 C 3005, 2011 WL 304079, at *1 (N.D. Ill. Jul. 25, 2011).

Re Ashley Madison v. Customer Data Sec. Breach Litig., 148 F. Supp. 3d 1378, 1380 (JPML 2015).

State v. Loomis, 881 N. W.2d 749, 767 (Wis. 2016).

Risorse Web

ARWELL, DOU, *Huawei tested AI software that could recognize Uighur minorities and alert police, report says*, 2020 (*www.washingtonpost.com*, ultimo accesso 23 maggio 2021).

CAMPBELL, *UK urged to clarify data rules from Connected cars*, 2017 (*www.ft.com*, ultimo accesso 5 giugno 2021).

CIAMPANELLI, *Da Uber a Tesla, tutti gli incidenti della auto a guida autonoma*, 2018 (*https://corriereinnovazione.corriere.it*, ultimo accesso 5 luglio 2021).

LAGANA TOSCHI, *What's the next step in Blockchain technology?*, 2018 (*https://medium.com/hackernoon*, ultimo accesso 24 aprile 2021).

LUPIS, *Allarme etnico. Aumenta la repressione degli uiguri in Cina: con l'auto di Huawei*, 2020 (*www.huffingtonpost.it*, ultimo accesso 23 maggio 2021).

LUPIS, *Dalla* face detenction *ai droni uccello, in Cina è dittatura*, 2021 (*www.huffingtonpost.it*, ultimo accesso 23 maggio 2021).

MOZUR, *One month, 500,000 face scans: how China is using A.I. to profile a minority*, 2019 (*www.nytimes.com*, ultimo accesso 23 maggio 2021).

NATALE, *Orientamenti sul modello di qualità dell'Intelligenza Artificiale*, 2020, (*https://intelligenzartificiale.unisal.it/orientamenti-sul-modello-di-qualita-dellintelligenza-artificiale*/, ultimo accesso 28 maggio 2020).

NEGRO, *Intelligenza artificiale in Cina. Oltre il presentismo*, 2019 (*https://sinosfere.com/2019/11/28/gianluigi-negro-intelligenza-artificiale-in-cina-oltre-il-presentismo*/, ultimo accesso 14 settembre 2021).

PINI, *Tesla, guida autonoma dal 2019 e robotaxi dal 2020. Fantascienza o realtà?*, 2019 (*www.ilsole24ore.com*, ultimo accesso 5 luglio 2021).

RODRIGUEZ, *Why Decentralized AI Matters Part I: Economics and Enablers*, 2018, (*www.medium.com/datadriveninvestor/why-decentralized-ai-matters-part-i-economics-and-enablers-5576aeeb43d1*, ultimo accesso 5 settembre 2021).

SHENG, XU, CAI, *China promulgates its long-awaited civil code* (*www.pillsburylaw.com*, ultimo accesso 14 settembre 2021).

SOL, *Come la Cina usa l'intelligenza artificiale per controllare gli uiguri*, 2019 (*www.ilsole24ore.com*, ultimo accesso 23 maggio 2021).

SPERANDIO, *Ecco come il Senato Usa vuole indagare sul valore dei dati di Amazon, Facebook e Google*, 2019 (*www.startmag.it/innovazione/amazon-facebook-google-dati-valore*/, ultimo accesso 14 settembre 2021).

ZERILLI, GAVAGHAN, *Call for independent watchdog to monitor NZ government use of artificial intelligence*, 2019 (*www.theconversation.com/call-for-independent-watchdog-to-monitor-nz-government-use-of-artificial-intelligence-117589*, ultimo accesso 14 settembre 2021).

Car data: paving the way to value-creating mobility, 2016 (*www.the-digital-insurer.com*, ultimo accesso 5 luglio 2021).

The world's most valuable resource is no longer oil, but data, 2017 (*https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data*, ultimo accesso 20 dicembre 2020).

La Cina userà il riconoscimento facciale per identificare gli uiguri?, 2020 (*www.ilpost.it*, ultimo accesso 23 maggio 2021).

Renault avvia la sperimentazione pubblica del servizio di Zoe cab autonomi, 2019 (*www.ilsole24ore.com*, ultimo accesso 5 luglio 2021).

Siti internet

www.darpa.mil/program/explainable-artificial-intelligence

https://decodeproject.eu

www.garanteprivacy.it

https://ig.ft.com/how-much-is-your-personal-data-worth/#axzz2WDzN1Z8V

www.mycarmydata.com

https://playground.tensorflow.org

https://singularitynet.io/