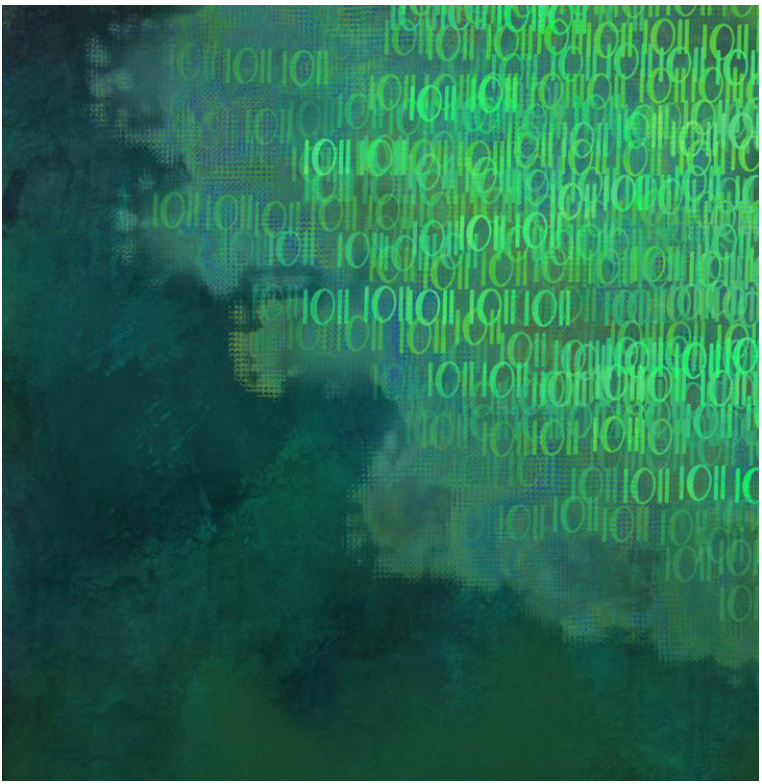
La sostenibilità dell'innovazione digitale

a cura di
Ilaria Garaci e **Roberta Montinaro**



UniorPress

UNIVERSITÀ DI NAPOLI L'ORIENTALE
DIPARTIMENTO DI SCIENZE UMANI E SOCIALI

La sostenibilità dell'innovazione digitale

a cura di
Ilaria Garaci e **Roberta Montinaro**

UniorPress
Napoli 2023

In copertina: 0110, Indigo Picciano, 2023.

La sostenibilità della innovazione digitale
a cura di Ilaria Garaci e Roberta Montinaro
UniorPress, Napoli 2023. ISBN 978-88-6719-276-2

With the support of the
Erasmus+ Programme
of the European Union

UniorPress - Via Nuova Marina 59, 80133 - Napoli
www.uniorpress.unior.it

INDICE

Consenso ed intelligenza artificiale: limiti e prospettive

Antonina Astone

Sommario: 1. Conoscibilità della decisione algoritmica ed autodeterminazione. -2. Dati misti e consenso nel GDPR.-3. I limiti del consenso nei sistemi basati sull'intelligenza artificiale.-4. Qualche soluzione prospettabile.- 5. Buona fede, trasparenza e governabilità dei meccanismi di funzionamento del trattamento algoritmico.

1. Conoscibilità della decisione algoritmica ed autodeterminazione

Per analizzare il problema complesso del rapporto tra autodeterminazione e strumenti o sistemi dotati di intelligenza artificiale appare opportuno partire da quanto la Corte Costituzionale tedesca nel 1983[1] , nella c.d. *Volkszählungsurteil* , sentenza sul censimento, ha scritto nel delineare un "diritto fondamentale all'autodeterminazione informativa" con riferimento all'utilizzo tecnologico dei dati personali. Dopo avere sottolineato come l'autodeterminazione presuppone, anche per il trattamento delle informazioni, che ai singoli individui sia data la libertà di decidere se scegliere di intraprendere o di rinunciare a determinate attività, compresa la possibilità di comportarsi di conseguenza, la Corte precisa che " Chi non è in grado di sapere quali delle sue informazioni personali sono note in determinati contesti del suo ambiente sociale, e chi non può valutarne la conoscenza da parte di possibili interlocutori, può essere considerevolmente limitato nella sua libertà di autodeterminarsi".

Ed è proprio questo il problema su cui , a distanza di anni, continua a misurarsi ancora la giurisprudenza in quanto la conoscibilità delle modalità di trattamento dei dati, che è alla base dell'Intelligenza artificiale[2], rimane una questione aperta, dal momento che i processi di apprendimento, come il *machine learning* che la caratterizzano, sembrano in grado di sfuggire persino al controllo umano.

La Suprema Corte[3] , in continuità con alcuni significativi interventi del Consiglio di Stato[4], pur sottolineando come nel "caso di utilizzo di un sistema automatizzato di calcolo, il presupposto della liceità del relativo trattamento dei dati personali è costituito dalla validità del consenso che si assume prestato al momento dell'adesione" , tuttavia, ha evidenziato come sia necessaria, preventivamente, la sussistenza della conoscibilità della decisione algoritmica in quanto "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".

Ma è evidente che esistono indubbie difficoltà connesse alla conoscibilità dei meccanismi che presidiano allo svolgimento dei compiti di cui è investito l'algoritmo, che trovano il loro *ubi consistam* nel fatto che le informazioni e le conoscenze conseguentemente acquisite, che connotano i sistemi di intelligenza artificiale, sono sorrette da una processo metodologico particolare in cui i dati costituiscono il "motore trainante" degli algoritmi che hanno il compito di individuare correlazioni difficilmente rinvenibili dalle " classiche" tecnologie[5] . Ed è questo uno dei fattori che rende i sistemi c.d. AI molto complessi anche da regolamentare per il diritto e pone in crisi quelle logiche "proprietarie", sottese al diritto all'autodeterminazione, che trovano le loro radici nel pensiero di Locke[6] e che si sono trasfuse,

nelle moderne codificazioni, con l'individuazione del consenso come base giuridica fondamentale, per compiere atti di disposizione che attengono a diritti fondamentali.

Peraltro allo stato attuale, nel mercato globale, emerge sempre più lo stretto legame fra economia, intelligenza artificiale e popolazione che, con la propria attività svolta sia nel mondo "reale" che in quello "virtuale", costituisce la principale fonte di dati che, ormai notoriamente, hanno assunto anche l'accezione di beni in senso economico[7].

È questa la ragione per cui nella geo-politica dell'attuale società postmoderna si registra un interesse molto forte sulla intelligenza artificiale, soprattutto da quando il Consiglio di Stato della Repubblica popolare cinese, nel 2017, ha elaborato il Piano di sviluppo per una nuova generazione d'intelligenza artificiale (Aidp), ponendosi il proposito di acquisire nel campo la *leadership*. Le altre superpotenze si sono attivate per evitare che la Cina abbia, anche in questo settore, un primato, a livello eurounitario[8], si è puntato l'acceleratore sull'AI come dimostra il "proluvio" di risoluzioni, libro bianco, istituzione di gruppo di esperti e da ultimo la bozza di regolamento sull'A.I.[9], da cui traspare l'esigenza e, quindi, il tentativo quanto mai arduo, di coniugare l'uso di questa tecnologia con la tutela dei diritti fondamentali della persona coinvolti.

2. Dati misti e consenso nel GDPR

Se è vero che i sistemi di IA si basano su tre architravi: accesso ad informazioni aggregate, correlazione di dati e abilità di calcolo, non sembra un caso se, nel percorso verso la regolamentazione di questa nuova frontiera tecnologica, la strategia europea si sia concentrata sui dati, dapprima con il Regolamento UE n.679/2016 (GDPR) relativo *alla protezione delle persone fisiche con riguardo al trattamento dei dati personali,* nonché alla libera circo-

lazione degli stessi che ha abrogato la direttiva 95/46/CE e, poco dopo, con quello n.1807/2018/ UE relativo a *un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea* [10]. Entrambi sono mossi da un'unica finalità: favorire la circolazione dei dati sia personali che non in quanto l'Unione europea parte dalla premessa[11] che "solo se i dati circolano liberamente l'Europa può sfruttare al meglio le opportunità offerte dalle tecnologie e dal progresso digitali". I *Big data* debbono circolare senza ostacoli "per il corretto funzionamento del mercato unico digitale, rafforzare la fiducia nel *cloud computing* e cambiare o porre fine ai contratti di *cloud computing* in modo più semplice"[12].

Base di partenza, è il riferimento alla "funzione sociale" (cons. 4 GDPR)[13], che è assegnata al trattamento anche dei dati personali, intesa come clausola riassuntiva dei valori sia economici che sociali, emergenti nell'ordinamento giuridico, idonea, di per sé, a conformarne il contenuto di tale diritto. Il diritto alla protezione dei dati personali non può, pertanto, considerarsi una "prerogativa assoluta" (cons.4 GDPR), in quanto involge una valutazione superindividuale del trattamento[14]. In particolare, è emersa, in questo contesto, la duplice veste assunta dai dati personali: da un verso espressione di un diritto della persona e dall'altro, come detto, beni in molti casi essenziali per la collettività, sia sotto il profilo non patrimoniale, basti pensare a quelli inerenti alla salute, sia sotto quello patrimoniale, in quanto, fondamentali per lo sviluppo dell'economia.

Peraltro, nel mercato dei *Big data,* esiste una commistione tra dati personali e non personali [15] , come si verifica per i dati acquisiti per l'espletamento di servizi pubblici come quelli sanitari. Se i dati personali sono facilmente individuabili e, quindi definibili, la delineazione di dato non personale è meno scontata in quanto, all'interno di questa categoria, rientrano molti tipi di dati ed, in particolare: dati che *ab origine* non sono riferiti ad

una persona, come ad esempio, quelli relativi alle condizioni meteorologiche; dati che inizialmente erano personali ma che, poi, sono stati resi anonimi[16].

Nei casi di dati "indissolubilmente legati", le tutele giuridiche previste nel Regolamento UE n.679/2016 sono applicabili anche agli insiemi di dati misti, dal momento che l'art. 2, par. 2, del Regolamento UE n.2018/1807, lascia impregiudicata l'applicazione del GDPR.

Se la normativa di riferimento è, per lo più, quella del Regolamento UE n.679/2016 bisogna quindi porsi la domanda se il consenso che, in moti casi, legittima il trattamento, possa o meno ancora rivestire un ruolo in ordine ai sistemi AI.

A tal fine, bisogna premettere che nelle varie fasi, che scandiscono il procedimento di apprendimento dei sistemi di intelligenza artificiale, generazione ed acquisizione dei dati, estrazione, correlazione, ed infine, analisi, la veste di protagonista, nelle prime due, è svolta da quelli che sono stati definiti "agenti informazionali interconnessi", le persone nell'ambito di attività svolte, sia di tipo *online* che *offline*[17]. Diversi i dispositivi che generano dati, nell'ambito dell'IoT, e tra essi un ruolo cruciale assolve lo *smartphone,* che scandisce, ormai, la vita dell'utente.

Ed è, pertanto, fondamentale, in questa seconda fase, che i dati siano legittimamente acquisiti: per quanto concerne i trattamenti automatizzati, nell'ambito dei quali potrebbero essere ricompresi tutti quelli basati sull'AI, il GDPR li sottopone a misure particolarmente restrittive. Tuttavia, anche in questo caso, la prestazione del consenso esplicito, purché, sorretto da adeguata informazione, ex art. 22, par. 2, lett. c), che integra una delle tre eccezioni al divieto di utilizzo di tale misure [18], che possono essere permesse, come è noto, anche in altre due ipotesi: la decisione automatizzata è necessaria per concludere/eseguire un contratto o se è stata autorizzata dal diritto dell'UE o da uno Stato membro.

Nei casi in cui il consenso è richiesto, quindi in presenza di dati personali e dati misti, ai sensi degli artt. 4, 7, 8 del GDPR, occorre un atto con il quale l'interessato manifesta una volontà libera, specifica, informata di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta che si dovrebbe tradurre nella compilazione di un modulo specifico corredato dal caricamento *on line* di un documento d'identità personale[19].

Inoltre, ai sensi dell'art. 7 par.2, "se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta, che riguarda anche altre questioni, la richiesta di consenso deve essere presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro". Il legislatore europeo al fine di scongiurare la frequente acquisizione ed utilizzazione surrettizia dei dati ha stabilito altresì che, nel valutare se il consenso è liberamente prestato" ai sensi dell'art. 7 par. 4, fra i parametri da considerare, vi è "l'eventualità che la prestazione di un servizio sia condizionata alla prestazione di un trattamento dei dati non necessario all'esecuzione del contratto"[20] .

Elemento conformativo del consenso è l'informazione [21]: il GDPR punta, infatti, molto l'accento sull'adempimento degli obblighi informativi, essenziale per rendere consapevole il titolare dei dati anche dell'utilizzo ultroneo che può essere connesso al trattamento. La previsione di un'informazione che non solo deve essere data "chiaramente" ma, anche, "separatamente da qualsiasi altra", recepisce quelle istanze, in merito al rafforzamento della tutela degli utenti, sollecitate dalla Commissione europea[22], che sospingono verso un adempimento degli obblighi informativi calibrato sul titolare del dato, considerato non in astratto ma in concreto. In questo senso, paradigmatico è quanto statuito

dall'art. 12, n. 1, del GDPR, e recepito nell'ordinamento italiano dall'art. 2-*quinquies*, comma 2, del d.lgs. n.101/2018, a proposito di soggetti deboli, come i minori, per i quali si precisa che l'informazione deve essere resa accessibile, attraverso un linguaggio chiaro e semplice che, come specifica il considerando n. 58, " il minore possa capire facilmente". Altra caratteristica del consenso è la sua revocabilità ai sensi dell'art.7 par.3 da parte dell'interessato, in qualsiasi momento, su cui, preventivamente deve essere edotto. A rafforzare la capacità di autodeterminazione sui dati vi è inoltre il diritto di rettifica, ex art 16 GDPR, in conformità a quanto statuito dal par.2 dell'art. 8 della Carta di Nizza cui si aggiunge l'ulteriore diritto ad opporsi al trattamento se, però, esiste un motivo legittimo, ex art. 21 GDPR. Completa il quadro anche il diritto alla c.d. "portabilità dei dati " introdotto dal GDPR [23] che semplifica le procedure connesse in favore dell'utente che stipuli un contratto di servizio con un nuovo gestore, esonerandolo dal rifornire tutti i suoi dati al nuovo. La finalità di semplificare l'utilizzo dei propri dati, da parte del legittimo titolare, si coniuga, in tal caso, con l'esigenza di stimolare la concorrenza nel mercato digitale dominato dai giganti della tecnologia[24].

3. I limiti del consenso nei sistemi basati sull'intelligenza artificiale

Il consenso, così come disegnato nel Regolamento n.679/2016/UE, applicato all'automazione che connota i sistemi di intelligenza artificiale, mostra, al momento, una certa debolezza[25] .

In essi, i dati elaborati sono estratti e sottoposti ad un processo di analisi, capace di ricavare informazioni che assolvono una funzione in grado di predire una serie di comportamenti. Si tratta di informazioni di rilevante interesse economico da vendere a soggetti, come società, che le potranno utilizzare per pubblicità mirata o per investire su beni e servizi che, attraverso, l'incrocio dei dati appaiono utili o interessanti per la popolazione.

Nell'ambito degli strumenti di analisi si rinvengono, essenzialmente, algoritmi di " interrogazione" e di "apprendimento": i primi rispondono a delle domande degli utenti, i secondi, invece, sono in grado di ricavare ulteriori informazioni, sfruttando metodologie come il *machine learning*. Queste, in particolare, recano il rischio di incontrollabilità della decisione algoritmica che si lega, sostanzialmente, al fatto che è proprio l'algoritmo che dà e gestisce gli impulsi, sulla base dei dati forniti da uno o da una comunità di programmatori.

Emerge, pertanto, un'inconciliabilità con i requisiti che costituiscono condizioni di legittimità del consenso, sulla base del GDPR, con particolare riferimento a tre aspetti: libertà di manifestazione del consenso, principio di minimizzazione dei dati e individuazione *ex ante* delle finalità del trattamento[26] .

In ordine al primo profilo, è opportuno richiamare quanto previsto nel cons. 42 del GDPR ove si afferma che il consenso non dovrebbe essere considerato liberamente prestato se l'interessato non è in grado di operare una scelta autenticamente libera; altrettanto se è nell'impossibilità di rifiutare o revocarlo senza subire pregiudizio. Queste circostanze non sembra che possano essere rispettate con l'uso delle nuove tecnologie. L'analisi delle *policies,* che accompagnano i prodotti integrati con l'AI, sono allo stato predisposte per rendere il funzionamento dei prodotti "ostaggio" del consenso nel senso che l'utilizzo degli stessi, anche nel lungo periodo, è legato al rilascio dello stesso. In tale contesto il consenso rappresenta, così, quasi un atto obbligato più che voluto per usufruire di una serie di beni e servizi erogati che, in alcuni casi attengono, anche ad infrastrutture critiche per la vita dell'uomo, nel settore dell'energia e dei trasporti, della finanza, dei servizi giudiziari, sanitari, universitari, scolastici, solo per fare qualche esempio.

In relazione al secondo aspetto, relativo al c.d. principio di minimizzazione dei dati, in quanto essenziali alle finalità che il

trattamento deve perseguire, è noto che il suo rispetto costituisce un requisito di validità dello stesso trattamento; il parametro richiesto è quello dello "stretto necessario" per usufruire del servizio richiesto. E' possibile notare, tuttavia, che i dispositivi con IA, a partire dai dati loro forniti, sono in grado di dedurre molte altre informazioni, che magari l'utente avrebbe scelto di non condividere.

Questa considerazione consente di sviluppare un analogo ragionamento per il terzo aspetto correlato al "principio di finalità": il GDPR punta l'accento sul fatto che il trattamento dei dati personali deve essere necessario ma, soprattutto, severamente calibrato sugli scopi da perseguire, che devono essere definiti specificatamente e sorretti da un'adeguata informazione, con un argine netto rispetto al passato. L'art. 6 del GDPR si esprime in termini di liceità del trattamento, in una serie di casi, tra cui vi è quello che se l'interessato abbia espresso il consenso per una o più specifiche finalità , in ottemperanza a quanto stabilito alla lett. b), par. 1 dell'art, 5 GDPR, in base al quale "i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità". Si tratta dell'applicazione di un principio espresso dal par. 2 dell'art 8 della Carta di Nizza [27], che comporta, evidentemente che le finalità, per cui i dati sono raccolti e trattati, non possono essere modificate senza chiedere nuovamente il consenso agli interessati, pena l'illegittimità del trattamento. Invece un calcolatore dotato di AI, nel processo di autoapprendimento, che comporta un adattamento all'ambiente circostante e quindi la possibile modifica dei suoi comportamenti, potrebbe cambiare tali finalità in autonomia; si configurerebbe un trattamento non supportato dal consenso essendo non preventivamente predeterminato e predeterminabile e, quindi, illecito. Ne consegue che i *dati*, in genere, possono essere trattati per scopi predeterminati solo in termini generali: le finalità non possono, in realtà, specificatamente esse-

re individuate *ex ante*, atteso che le correlazioni fra i dati emergono solo nella fase dell'estrazione successiva alla raccolta degli stessi. I dati possono, pertanto, acquisiti con il consenso ma, come visto, da essi possono essere ricavate informazioni ultronee, spesso oggetto di vendita, e di questo non vi è consapevolezza all'atto di prestazione del consenso.

Infatti un problema ulteriore è poi costituito dall'inserimento, in molte *policies* che corredano *smart object,* di una serie di clausole di esonero dalla responsabilità per l'uso che terze parti acquirenti dei dati effettueranno, sulle quali non c'è sufficiente chiarezza.

Peraltro, concentrando l'attenzione sui prodotti dotati di AI, in cui esiste un'interazione tra bene e servizio[28] , non solo esprimere un consenso realmente consapevole è complesso ma vi è, poi, l'aspetto non trascurabile della sorveglianza realizzata attraverso l'uso dei dati biometrici[29] all'interno delle abitazioni , delle autovetture ma, anche, nei luoghi pubblici che è stata accelerata dalla pandemia[30]. Il GDPR, all'art. 9, par. 1, stabilisce che, in linea generale, è vietato il trattamento di "dati biometrici intesi ad identificare in modo univoco una persona fisica". Tuttavia deroghe sono previste in una serie di casi ben precisi: infatti, al par. 2, è sancito che il trattamento dei dati biometrici è consentito quando, ancora una volta l'interessato ha prestato il proprio consenso esplicito al trattamento dei dati personali, per uno o più specifici utilizzi, come può avvenire nel caso di registrazione preliminare degli oggetti *smart*, di uso domestico. Il problema si amplifica per la sorveglianza di massa che appare profilarsi con l'uso di sistemi AI negli edifici pubblici e nelle strade.

4. Qualche soluzione prospettabile

I limiti dell'applicazione della disciplina del consenso, brevemente prima richiamata, alle nuove tecnologie basate sull'intelligen-

za artificiale sembrano imputarsi a diversi fattori . Fra questi ad incidere, sensibilmente, è quella che appare quasi una mutata conformazione giuridica dello stesso e la connessa inadeguatezza a garantire la capacità di autodeterminazione del singolo.

Se il valore in gioco non è più la *privacy* insita nel dato, ma l'informazione che da esso è ricavabile, si comprende come il consenso, attualmente, è piegato a logiche di mercato nell'ambito delle quali gli stessi titolari dei dati, solo in piccolissime percentuali, sono disposti a negarlo se sanno di non potere usufruire di un determinato bene o servizio[31]. Questo nuovo paradigma fa sì che l'atto di manifestazione del consenso all'utilizzo dei propri dati personali e dei metadati sembra assumere carattere sempre più negoziale[32] sul presupposto della configurazione del dato come corrispettivo, inquadramento che lo allontana dalla sua qualificazione classica come atto giuridico di natura autorizzatoria[33]. D'altra parte anche la giurisprudenza amministrativa[34], pur qualificando il dato personale come *res extra commercium*, ha riconosciuto "la patrimonializzazione del dato personale", da parte delle società "attraverso la messa a disposizione del dato e la profilazione dell'utente a fini commerciali". Proprio l'interpretazione, in chiave "sinallagmatica", del consenso sembrerebbe trovare sostegno sempre maggiore con riferimento al trattamento dei dati legato alla loro circolazione, in quanto il riutilizzo e/o, circolazione dei dati per fini di *marketing*, fa emergere l'aspetto del dato come bene[35]. Parte della dottrina [36] ha, opportunamente, osservato come il Regolamento n.679/2016 è fondato su una modalità di trattamento dei dati che tende ad essere superata in quanto essenzialmente basata su una dualità di soggetti: il titolare del dato e il titolare del trattamento a cui il titolare consegna i propri dati, confidando nel rispetto di quel principio di *accountability* che presuppone l'osservanza di una sere di norme e procedure imposte dal legislatore e che, in pratica, dovrebbe garantire il corretto uso dei

dati in conformità al consenso per cui il titolare lo ha rilasciato e alla normativa vigente. Ma questa dimensione duale è superata nel momento in cui i dati sono destinati a circolare ed a generare nuove informazioni come nei meccanismi di funzionamento che presidiano l'AI.

Il GDPR, sostanzialmente si concentra su una dimensione essenzialmente non patrimoniale del dato personale che appare in parte superata . Al contempo, non si può non pretermettere di riconoscere come nello stesso regolamento si manifestano i segni di una progressiva decadenza del consenso[37]: se *prima facie,* infatti, potrebbe rinvenirsi una continuità tra l'art. 23 del previgente Codice *privacy,* sostanzialmente coincidente con quello dell'art. 11 della l. n.675/1996 che sanciva, genericamente, che il trattamento era ammissibile solo "con il consenso espresso dell'interessato" , nel GDPR il consenso, pur rilevante, perde sempre più centralità. Alla base, quasi, una sfiducia verso la sua concreta efficacia e la consapevolezza della sua inadeguatezza a garantire la capacità di autodeterminazione del singolo in sistemi di trattamento automatizzati dei dati molto complessi e sofisticati.

Per superare le criticità evidenziate una soluzione, tra quelle proposte, potrebbe essere rappresentata dal ricorso al *dynamic consent*, un consenso c.d.granulare (cons. 32 GDPR) sperimentato nel settore medico riguardo le c.d. bio-banche. Si risolve nell'acquisizione, per gradi, della consapevolezza del tipo di trattamento, che dovrà essere praticato partendo, dapprima da un consenso ampio, sulla base di un'informativa generale in ordine alle finalità del trattamento e, successivamente, procedendo ad un consenso specifico riguardo a trattamenti specificatamente individuati e descritti. Inoltre il contenuto dell'informativa potrebbe essere affiancato da una simulazione, anche video o grafica, di quelli che potrebbero essere gli effetti del trattamento. Ma il limite di una simile procedura è che il soggetto interessato,

subendo troppe informazioni, sia indotto a rispondere in modo automatico, senza prestare attenzione al contenuto delle spiegazioni fornite e questo problema si amplifica per i minori i quali hanno l'età minima per esprimere il consenso nell'ambito dei servizi della società dell'informazione.

Al fine di garantire la libertà di autodeterminazione la strada da intraprendere sembra essere quella di ricercare altre soluzioni che prescindano dal consenso: ad esempio per i sistemi di automazione domestica[38], che captano indiscriminatamente anche dati dei minori o per i prodotti di consumo, dotati di IA integrata, tra cui anche giocattoli per bambini nel Regno Unito [39], l'ICO, il Garante della *privacy*, ha emanato delle linee guida che assoggettano tali prodotti, a *standards* diretti ad ampliare la garanzia di un' adeguata ed efficiente tutela dei dati raccolti. È stato elaborato un "*Codice di design"*, per i dispositivi ideati per bambini e che, secondo uno studio, potrebbe diventare un modello generale per tutte le tecnologie di automazione domestica. Secondo questa analisi, sarebbe sufficiente che ogni qualvolta i dati captati da un dispositivo *smart,* includono quelli di minori, questi non vengano venduti a terze parti e le norme relative alla *privacy* non li considerino come dati concessi volontariamente. Ma, a ben vedere, una soluzione ulteriore può essere rinvenuta nella possibilità di imporre alle società produttrici, che trattano dati altamente contestualizzati, come quelli presenti nell'ecosistema domestico, di ricorrere alle certificazioni o ai sigilli e marchi di cui all'art. 42 del GDPR, che attestino il rispetto di determinati *standards,* finalizzati ad assicurare un'adeguata protezione dei dati.

5. Buona fede, trasparenza e governabilità dei meccanismi di funzionamento del trattamento algoritmico

Se intorno al diritto sui dati sembrano, evidentemente, coagularsi più situazioni giuridiche soggettive che attengono alla sfe-

ra esistenziale e patrimoniale [40], è possibile affermare che il modello dei contratti del consumatore, innestato su quello della tutela dei dati, può utilmente essere adattato per ridurre le asimmetrie esistenti tra piattaforme ed utenti[41]. Apparentemente, allora, questo accostamento sembrerebbe riportare in auge il consenso ma, tenuto conto dei limiti evidenziati nelle pagine precedenti, per colmare lo squilibrio giuridico in cui versa l'utente nei sistemi AI, l'autodeterminazione potrebbe essere potenziata legandola più che al consenso ad altri profili quali l'informazione, il riconoscimento del diritto di accesso, il c.d. *ius poenitendi*, ma, soprattutto concentrandosi sulla conformazione normativa del contenuto delle condizioni generali predisposte dai professionisti.

Negli interventi normativi, successivi al GDPR, si assiste ad una spiccata tendenza verso "un' autonomia conformata" delle condizioni generali di contratto, che si sostanzia in una predeterminazione legale del contenuto, che schiude ad una nuova fase: ciò si evince a partire dalle proposte relative al *Digital services act* e al *Digital market act* fino ad arrivare alla bozza di Regolamento sull'intelligenza artificiale (*Regulation on European Approach for Artificial Intelligence*).

Tra i vari livelli di rischio legati all'uso di sistemi AI[42] , predeterminati dal legislatore, forse un po' rigidamente, se paragonati all'approccio più flessibile dell' a*ccountability,* che caratterizza il Regolamento n. 679/2016, si punta a specifici obblighi di trasparenza, come emerge, ad esempio, dall'art. 52 sul funzionamento del sistema, non solo nei confronti dell'interessato ma, anche, nei confronti di chi acquista e utilizza tali sistemi all'interno dei propri servizi. Nei sistemi "a rischio limitato" e in quelli a "rischio minimo", come applicazioni quali videogiochi o filtri anti *spam* basati sull'AI, sarà la documentazione tecnica a dovere dimostrare la corrispondenza, ai requisiti del regolamento al fine di renderne trasparente il funzionamento. L'uti-

lizzo di sistemi "ad alto rischio", invece, è scandita da norme imperative che impongono alto livello di robustezza, sicurezza del trattamento, documentazione dettagliata e garanzia della supervisione umana[43].

Si registra, in sostanza, una procedimentalizzazione dell'attività sottesa al funzionamento dei sistemi AI, con un'operazione simile a quella verificatasi in materia di tutela del consumatore[44] ove, però, non fossero previste tutta una serie di eccezioni al trattamento dei dati, in materia, ad esempio di giustizia e sicurezza, che appaiono indebolire la normativa proposta sull'AI. Corollario ulteriore è che lo spazio di tutela per i dati, si apre ad una dimensione più collettiva che individuale e ciò può essere importante ai fini di eventuali contenziosi, anche per superare ed affrontare le difficoltà probatorie ed i rilevanti costi economici di un giudizio[45].

In conclusione, senza cedere a tentazioni che si pongono in chiave critica sul ruolo delle tecnologie digitali, capaci di rievocare la filosofia di fondo al movimento del c.d. luddismo[46], occorre individuare altri punti cardinali di riferimento per salvaguardare la libertà di autodeterminazione[47]. Tenendo presente che "il trattamento deve porsi al servizio dell'uomo" , così come specificato nel cons. 4 del GDPR [48] e peraltro, già espresso nella direttiva n.95/46, il primo che sembra venire in rilievo è il principio di buona fede [49] , secondo quanto prescritto nel par.2 dell'art. 8 della Carta dei diritti fondamentali dell'Unione europea. La buona fede già, peraltro, delineata più generalmente in capo al prestatore di servizi *on line*, nel cons.48 della direttiva sul commercio elettronico n.31/2000, deve conformare di sé, nella prospettiva nuova introdotta dal GDPR e che arriva fino alla proposta di Regolamento sull'AI, anche le procedure di acquisizione, trattamento e circolazione dei dati, scongiurando accordi diretti a raccogliere dati per scopi vari, in maniera surrettizia, in violazione delle regole di correttezza che, nella pro-

posta del *Digital services act*[50] , sembrano assumere una valenza centrale, come risulta dal capo III , rubricato *Obblighi in materia di dovere di diligenza per un ambiente online trasparente e sicuro* .

Analogamente negli Stati Uniti la FTC ha emanato delle linee guida alle aziende per l'utilizzo dell'intelligenza artificiale ispirato a "verità ed equità". Ad essere richiamate alcune disposizioni che li operatori del settore devono obbligatoriamente rispettate: la sez. 5 del *FTC act* che vieta le pratiche commerciali scorrette, nelle quali rientrerebbe il ricorso ad algoritmi sleali, che potrebbero comportare scelte di tipo discriminatorio, il *Fair Credit Reporting Act* (FCRA), legge federale del 1970, intesa a promuovere verifiche corrette per l'utilizzo delle informazioni connesse all'erogazione del credito al consumo e *l'Equal Credit Opportunity Act* (ECOA), emanato nel 1974 come parte del più ampio *Consumer Credit Protection Act* (CCPA),[51] che vieta ai finanziatori di discriminare in base alla razza, religione, origine, sesso o fonte di reddito i consumatori. Recenti approdi giurisprudenziali, in Italia, sembrano indirizzarsi in tal senso imponendo la consegna del c.d. codice sorgente[52], che può rivelarsi utile chiave di accesso per consentire un'eventuale sindacabilità delle scelte, adottate dagli algoritmi e, conseguente individuazione dell'imputazione della responsabilità, per eventuali errori o gli illeciti ad esse connessi[53]. La conoscibilità delle scelte, anche se esteriorizzate nella forma matematica, costituisce, evidentemente, fattore chiave di trasparenza, non solo *ex ante* ma, anche *ex post*, in via rimediale, rispetto alla violazione dei diritti fondamentali, da parte di *agenti software*[54].

Un altro nodo chiave da sciogliere attiene alla complessità del "governo" della decisione algoritmica : il Consiglio di stato[55] ha individuato un ulteriore principio del diritto europeo, rilevante in materia, ossia quello di "non esclusività della decisione algoritmica". Si tratta di un principio di rilievo globale in quanto, ad esempio, utilizzato nella nota decisione *Loomis vs. Wiscon-*

sin che postula, sulla base dell'art 22 del GDPR, che ogni persona, destinataria di una decisione automatizzata, che produca effetti giuridici che la riguardano o che incidano significativamente su questa, ha diritto a che tale decisione non sia basata unicamente su tale processo automatizzato.

Proprio sul controllo di questa eventuale capacità, si svolge la partita più importante che dovrebbe vedere, in un approccio più di *accountability* che di "incasellamento" in categoria di rischio predeterminate *ex lege*, così come invece proposto , l'individuazione di meccanismi per impedire che, la decisione algoritmica divenga imprevedibile ed incontrollabile, non rispondendo più ai comandi dell'uomo.[56]

Utilizzo leale degli algoritmi e governabilità dei loro meccanismi di funzionamento eviterebbero che si prosegua nel sovvertimento, in in corso, della scala di valori in cui gli uomini contano non *uti singuli* come persona ma, nell'insieme come utenti[57], fonte principale di informazioni necessarie per il funzionamento dell'economia digitale.

Note di chiusura

[1]BVerfG, 15 dicembre 1983, in *BVerfGE,* 65, 1984, www.Bundesverfassungsgericht.de in cui la Corte delinea l'esistenza di un "Diritto che garantisce la facoltà dei singoli di autodeterminarsi" e "di stabilire se divulgare e utilizzare i propri dati personali" e, quindi, di decidere "quando e entro quali limiti rivelare questioni relative alla propria vita personale" : tale diritto è fatto discendere dal principio d'inviolabilità della dignità umana e dalla libertà di agire. In Germania, peraltro, già nel 1977, era stata emanata la prima legge federale sulla Protezione dei Dati Personali, *Bundesdatenschutzges*et e, successivamente, la Corte costituzionale tedesca, con una decisione del 27 febbraio 2008, *www.bundeverfassungsgericht.de*, in *Riv. trim. dir. pen. eco*., 3, 2009, con nota di R. Flor, p. 679 ss., ha affermato l'esistenza di un « diritto alla integrità dei sistemi informativi tecnologici, funzionale allo sviluppo della personalità», come parte del diritto alla riservatezza della persona. In tale ambito un ruolo fondamentale è stato, inoltre, svolto dalla giurisprudenza della Corte di Strasburgo, della Corte di giustizia europea e della Corte suprema americana, per un'analisi delle cui decisioni si rinvia ad O. POLLICINO, *Judicial protection of fundamental rights on the internet . A road towards digital constitutionalism ?* Oxford-New York, 2021, p.184 ss.

[2] G. Alpa (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020; S. Lanni, Dataquake: *intelligenza artificiale e discriminazione del consumatore*, in *Nuovo dir. civ.*, 2, 2020, p. 97ss.; U. Salanitro, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea*, in *Riv. dir. civ*., 6, 2020, p. 1246 ss.; G. Gitti, *Tecnologie digitali, persona e istituzioni*, ibidem, 1231ss.; A.M. Gambino - M. Manzi, *Intelligenza Artificiale e tutela della concorrenza*, in *Giur.it*., 7, 2019, p. 1744 ss.; A. Amidei, *Intelligenza Artificiale e* product liability*: sviluppi del diritto dell'Unione Europea*, *ibidem*, p. 1718; E. Gabrielli - U. Ruffolo (a cura di), *Intelligenza Artificiale e diritto*, *ibidem*, p. 1657 ss.; U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2018; F. Pizzetti (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

[3] Cass.civ., Sez.I, ord.25 maggio 2021, n. 14381, riguardo la definizione del c.d. *rating reputazionale .*

[4] Cfr. Cons.St., Sez. VI, 13 dicembre 2019, n.8472; in senso conforme Cons. St., Sez.VI, 8 aprile 2019, n. 2270 che, qualificato il *software* come un "atto amministrativo informatico", sottolinea come la regola tecnica, che governa ciascun algoritmo, "resta pur sempre una regola amministrativa generale, costruita dall'uomo e non dalla macchina, per essere poi (solo) applicata da quest'ultima". Ne consegue che la conoscibililtà di una regola, espressa in un

linguaggio differente da quello giuridico, deve essere garantita in tutti gli aspetti, " dai suoi autori al procedimento usato per la sua elaborazione, al meccanismo di decisione, comprensivo delle priorità assegnate nella procedura valutativa e decisionale e dei dati selezionati come rilevanti", v.*infra* par.5.

[5] S. CERI, *On the role of statistics in the era of big data: a computer science perspective,* in *Statistics & Probability Letters*, 136, 2018, p.68ss.

[6]Su cui v.A.AGNELLI, *J.Locke*, in *Noviss. Dig.it*., IX, Torino, 1963 , p.1060; sull'autodeterminazione, in particolare C.CASTRONOVO, *Autodeterminazione e diritto privato*, in *Europa e dir.priv*., 4, 2010, p.1037ss.; ID., *Eclissi del diritto civile*, Milano, 2015, p.100 che sottolinea come "il luogo costituzionale dell'autodeterminazione" è quello della liberà personale, ex art 13 Cost, come erede moderno dell'*habeas corpus* ed è questa l'idea di fondo al diritto alla salute ed alle scelte complesse che attengono ai trattamenti sanitari ed al fine vita su cui v. P. PERLINGIERI, *Il diritto alla salute, quale diritto della personalità,* in *Rass.dir.civ*., 4, 1982, p. 126; P.ZATTI, *Il corpo e la nebulosa dell'appartenenza, in Nuova giur.civ.comm.*, II, 2007 p.2; L.NIVARRA, *Autonomia (bio)giuridica e diritti della persona*, in *Europa e dir. priv*, 2009, p.719ss.; L. BALESTRA, *L'autodeterminazione nel «fine vita»*, in *Riv. trim.*, 2011, 4, p. 1009 ss.; G.DI ROSA, *La persona oltre il mercato.La destinazione del corpo post-mortem,* in *Europa e dir.priv*., 4, 2020, p.1179 M. FOGLIA*, Danno non patrimoniale - la lesione del diritto di determinarsi liberamente nella scelta dei propri percorsi esistenziali*, in *Giur. it.* 6, 2020, p.1.348 ss. In giurisprudenza Corte Cost., 23 dicembre 2008, n.438 su cui S.RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p.265 .

[7] Sui nuovi beni è d'obbligo il riferimento a C.REICH, *The new property*, in *The Yale Law Journal*, 1964, 73, 5, p.733 ss.; ID., *The " new property" after 25 years*, in *University San Francisco law review* 24, 1990, 232ss. ; nella dottrina italiana specificatamente sui dati, come beni, P. Perlingieri, *L'informazione come bene giuridico,* in *Rass. dir. civ.*, 1990, p. 326 ss.; V. Cuffaro, *Il consenso dell'interessato,* in, (a cura di ID. e V. Ricciuto), *La disciplina del trattamento dei dati personali* Torino, 1997, p. 216; F. Macario, *La protezione dei dati personali nel diritto privato europeo,* in *La disciplina del trattamento dei dati personali,* op.ult.cit., p. 12 ss.; S. Sica, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, in *Riv. dir. civ.,* II, 2001, p. 641 ss.; V. Zeno Zencovich, *Sull'informazione come "bene" (e sul metodo del dibattito giuridico)* in *Riv. crit. dir. priv.*, 1999, p. 485 ss.; V.RICCIUTO, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno* , in *Dir. Informazione e informatica*, 4, 2018, p. 689 ss.; G. Resta, V. Zeno Zencovich, *Volontà e consenso nella fruizione dei servizi in rete* in

Riv. trim. dir. e proc. civ., 2, 2018, p. 411 ss. ; D.POLETTI, *Comprendere il Reg.UE 2016 /679: un'introduzione,* in (a cura di) ID. e A.Mantelero, *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali.Un dialogo tra Italia e Spagna*, Pisa, 2018, p. 10; v.*infra* nt.31 e 39.

[8] Per un'analisi si rinvia a G. ALPA, *Quale modello normativo europeo per l'intelligenza artificiale?,* in *Contr. e impr*. , 4, 2021, p.1003 ss.

[9] Sul piano quinquennale, pubblicato nel 2016, in Cina v. report del CNR, *AI per lo sviluppo sostenibile,* p. 154 , www.cnr.it. Nella Risoluzione del Parlamento europeo, del 20 gennaio 2021 (2020/2013(INI)), *relativa all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale* si rinviene una definizione di "sistema di intelligenza artificiale (IA)" ossia di "un sistema basato su *software* o integrato in dispositivi *hardware* che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici". Il Parlamento europeo, nell'ottobre 2020 ha inviato alla Commissione UE alcune proposte per l'adozione di tre regolamenti, in ordine agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate. Il 21 aprile 2021 è stata depositata la bozza di **regolamento** sull'intelligenza artificiale, *Regulation on European Approach for Artificial Intelligence* che si pone sullo sfondo di un intervento di revisione della direttiva sui prodotti difettosi. Cfr., altresì, Risoluzione del 12 febbraio 2019, su una *Politica industriale europea globale in materia di robotica e intelligenza artificiale*, P8_TA–PROV(2019)0081, nonché il *White paper* del 19 Febbraio 2020, che la Commissione UE ha pubblicato per implementare la fiducia in Europa nei sistemi di *AI* ed il *Report on the safety and liability aspects of AI*; prima ancora, la Risoluzione del 16 febbraio 2017 del Parlamento europeo, che reca "Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica", in www.*europa.eu.*

[10] In generale v. (a cura di) S . SICA, V. D'ANTONIO e G.M. RICCIO, *La nuova disciplina europea della privacy,* Padova, 2016; G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, , Bologna, 2017; F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato,* in *Nuove leggi civ. comm*., 2, 2107, p. 369 ss.; A A. MANTELERO, D. POLETTI (a cura di), *Regolare la tecnologia: il Reg.UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia Spagna*, cit.; V. CUFFARO, A. D'ORAZIO, V. RICCIUTO, (a cura di), *I dati personali nel diritto europeo*, Torino, 2018; E. LUCCHINI GUASTALLA, *Il nuovo regolamento europeo sul trattamento dei dati personali:*

i principi ispiratori, in *Contr. e impr*., 1, 2018, p. 106 ss.; N.ZORZI GALGANO (a cura di) , *Persona e mercato dei dati .Riflessioni sul GDPR* a cura di Padova, 2019. Sul reg. n.1807/2018/UE, A.DEL PIZZO, *Trattamento dei dati non personali: punti di contatto tra il Regolamento (UE) 2018/1807 e il GDPR*., in *Dir. di internet*, 2020,www.dirittodiinternet.it

[11] Cons.10 reg.n.1807/2018/UE; Cons. 6 reg.n.679/2016/UE.

[12]Così la Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, Strategia per il mercato unico digitale in Europa, Bruxelles, 6.5.2015com (2015) 192 final. Sul mercato unico digitale, cfr., per tutti in dottrina G.ALPA, *Il mercato unico digitale*, in *Contr.impr.eur*., n.1, 2021, www.contrattoeimpresaeuropa.eu. Sui *Big data,* M.DELMASTRO, A.NICITA, *Big data-Come stanno cambiando il nostro mondo,* Bologna, 2019, p.10 ; A.C.DI LANDRO, *Big data. Rischi e tutele nel trattamento dei dati personali*, Napoli, 2020, p.170; cfr., altresì *Indagine conoscitiva volta ad approfondire la conoscenza degli effetti prodotti dal fenomeno dei Big Data e analizzarne le conseguenze in relazione all'attuale contesto economico- politico-sociale* , in www.agcm.it.

[13] Specificatamente A. Ricci, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in *Contr. e impr*., 2, 2017, p. 586 ss.; ma sul punto, più in generale, S. Pugliatti, *La proprietà e le proprietà,* in *La proprietà nel nuovo diritto,* Milano, 1964, p. 278; U. Natoli, *La proprietà,* Milano, 1980, p. 273ss.; V. Scalisi, *Il nuovo volto della proprietà.Da "potere" a "titolo" di godimento*, in ID. *Categorie e istituti del diritto civile nella transizione al postmoderno,* Milano, 2005, p. 482 ss; U. Mattei, *Una primavera di movimento per la " funzione sociale della proprietà",* in *Riv.crit. dir. priv*., 2013, p. 531 ss.; A. Federico, *La proprietà in Europa tra " funzione sociale" e " interesse generale"*, in G. D'AMICO (a cura di) *Proprietà e diritto europeo*, Napoli, 2013, p. 125 ss.; nella letteratura internazionale R.A. Epstein, *Takings-Private property and the power of eminent domain*, Harvard University Press, 1985, p.166 ss. che indaga il rapporto tra interessi pubblici e privati, sottesi al diritto di proprietà, al fine di dimostrarne la possibile convergenza, nell'ambito della medesima situazione giuridica.

[14]Così V. Cuffaro, *Il diritto europeo sulla protezione dei dati personali e la sua applicazione in Italia: spunti per un bilancio,* in *Regolare la tecnologia* , cit. p.30. In proposito v. L. Gatt, R. Montanari, I.A. Caggiano, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale, Spunti di riflessione sull'effettività della tutela dei dati personali,* in (a cura di) P.Passaglia e D.Poletti ,*Nodi virtuali, legai informali: Internet alla ricerca di regole,* Pisa, 2016, p. 57 ss.

[15] Cfr., in tal senso, il punto 4.1.2. della *Comunicazione della Commissione al Parlamento europeo e al Consiglio - Linee guida sul Regolamento relativo a un quadro*

applicabile alla libera circolazione dei dati non personali nell'Unione europea, del 25 settembre 2019 – COM (2019) 250 *final* che , al punto 2.2, fa più volte riferimento alla contiguità tra dati personali e non personali evidenziando come "gli insiemi di dati misti rappresentano la maggior parte degli insiemi di dati" .

[16] L'anonimizzazione ovviamente è differente dalla pseudonimizzazione, come emerge dal reg. n.679/2016/UE. Ai sensi dell'art. 4, par. 1, n. 5 del GDPR, con la pseudononimizzazione i dati trattati non vengono attribuiti a un interessato identificato ma ad uno pseudonimo e, per ricondurre i dati alla persona, sono necessarie delle informazioni aggiuntive da conservarsi separatamente. La pseudonimizzazione, a differenza dell'anonimizzazione è una misura di sicurezza che non esclude la possibilità di reidentificazione dell'interessato. Nel GDPR la pseudonimizzazione, insieme alla cifratura, è considerata tra le misure da utilizzare per proteggere i dati personali trattati.

[17] Così L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Cortina, 2017, p. 106 ss. ; ID., *Pensare l'infosfera. La filosofia come design concettuale*, Milano, 2020.

[18]L'art. 22 del GDPR riprende, in gran parte, la formulazione, già contenuta nelle diposizioni precedenti, a partire dall'art. 15 della dir. n.46/95/CE, che vietava che la persona potesse essere sottoposta a decisioni fondate, esclusivamente, su un trattamento automatizzato di dati, che produca "effetti significativi" nei suoi confronti. L'art.13, par. 2, lett. f) del GDPR chiarisce che, per garantire un trattamento corretto e trasparente, il titolare del trattamento, oltre ai contenuti essenziali dell'informativa, deve mettere a conoscenza l'interessato dell'esistenza di un processo decisionale automatizzato, compresa la profilazione, e fornire allo stesso informazioni sulla logica utilizzata nonché sull'importanza e sulle conseguenze previste.

[19] Così *Guidelines 05/2020 on consent under Regulation 2016/679/UE,* emanate dall'*European data protection board* **,** www. edpb.europa.eu, su cui v.*infra* nt. successiva.

[20] Interessante è quanto si legge nelle *Guidelines 05/2020 on consent under Regulation 2016/679/UE,* cit., sulla **pratica del c.d. *cookie walls,*** schermata che consente la visione dei contenuti del sito, solo acconsentendo ai *cookies* e alla relativa informativa. L'EDPB sottolinea come sia impossibile ritenere che il consenso sia liberamente prestato, in quanto l'utente **non si è trovato di fronte a una scelta consapevole** ed analogamente se la fornitura del servizio, da parte del *provider* , è subordinata alla prestazione del consenso nel caso di **c.d. *scrolling*,** avviso che continuare a scorrere il sito costituirà un'espressione di consenso. In proposito v. anche Cass.civ., Sez.I, 2 luglio 2018, n. 17278, in

Riv. dir. media , 3, 2018, con nota di A. VIGENTINI , www.medialaws.eu secondo cui il condizionamento sussiste quanto più la prestazione offerta dal gestore del sito Internet sia infungibile ed irrinunciabile per l'interessato, e non nei casi di offerta di un generico servizio informativo, trattandosi di informazioni agevolmente acquisibili attraverso vari siti ed anche l'editoria cartacea, con la conseguenza che ben può rinunciarsi a detto servizio senza gravoso sacrificio; Corte giust. UE, 11 Novembre 2020, caso C-61/19, Orange România SA. *c. ANSPDCP,* in *Riv. dir. media*, n.1, 2021, con nota di M. C. MENEGHETTI , www.medialaws.eu che ha sancito che "una clausola contrattuale secondo cui l'interessato è stato informato e ha acconsentito alla raccolta dei suoi dati non è idonea a dimostrare la valida manifestazione di volontà dell'interessato se : è stata preselezionata dal titolare; induce in errore l'interessato circa la necessità del consenso per la stipulazione del contratto; la libera scelta di opporsi al trattamento è pregiudicata dall'esigenza per l'interessato di negare attivamente il proprio consenso mediante la compilazione di un modulo".

[21]Nel Regolamento sui dati personali si ricorre ad una formula analoga a quella contenuta nell'art. 5 *c. cons*., in cui si prevede che il contenuto dell'informazione, che il professionista ha l'obbligo di fornire al consumatore, deve essere espresso in "modo chiaro e comprensibile" al fine di rafforzare la consapevolezza del consumatore nella scelta". Cfr. S. SICA, *Il consenso al trattamento dei dati personali: metodi e modelli di qualificazione giuridica*, cit., p. 627; sulle diverse finalità dell'informazione in questo ambito V. ZENO ZENCOVICH, *Il "consenso informato" e la "autodeterminazione informativa" nella prima decisione del garante,* in *Corr. giur*., 1997, p. 915 ss.; F. MACARIO, *La protezione dei dati personali nel diritto privato europeo*, Torino, 1997, p. 29; A. BARBA, *Le modalità del trattamento*, in *La disciplina del trattamento dei dati personali*, cit., p. 178 ss.

[22]Per la protezione dei dati, in particolare, sul consenso all'attività di *profiling,* cfr. le linee guida del 3 gennaio 2017, individuate nel piano d'azione del "Gruppo di lavoro art. 29",*www.europa.eu/dataprotection/it.*

[23] Si tratta di un diritto già riconosciuto ai consumatori, basti pensare alla portabilità del numero telefonico; ai sensi dell'art. 20 del GDPR "*l'interessato ha il diritto di ricevere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un* titolare del trattamento *e ha il diritto di trasmettere tali dati a un altro titolare del trattamento, senza impedimenti da parte del titolare del trattamento cui li ha forniti"*. In generale v. P. PACILEO, *Il diritto alla portabilità*, in *La nuova disciplina europea della privacy,* cit., p. 221 ss.

[24] A tale riguardo si rileva che la maggior parte di applicazioni e siti *web* si

avvalgono *in outsourcing* dei sistemi di tracciamento messi a punto dai c.d. *Over the top, Apple, Google e Facebook* che, evidentemente, godono di una posizione privilegiata per la disponibilità dei dati acquisiti.

[25] Così S.SICA, *La responsabilità civile per il trattamento illecito dei dati personali,* in *Regolare la tecnologia*, cit, p. 162 .Sottolinea come il modello culturale, prima ancora che giuridico, sul quale si base il Regolamento e` quello dell'autodeterminazione ma, tale logica, benchè ´ mitigata dall'*accountability,* non puo` essere applicata a grandi masse di dati.

[26] In tal senso si rinvia a T.TANI, *L'incidenza dei Big data e del machine learning sui principi alla base del Regolamento Europeo per la tutela dei dati personali (2016/679/UE) e proposte per una nuova normativa in tema di privacy,* in *Società delle tecnologie esponenziali e General Data Protection Regulation: Profili critici nella protezione dei dati,* a cura di S.Bonavita, Milano, 2018, p. 35 ss.

[27] Nell'art. 11 del D.lgs. n.196/2003 già era specificato che i dati devono essere trattati in modo lecito e corretto, per gli scopi specifici, espliciti e legittimi, non eccedenti rispetto alle finalità per le quali sono raccolti. Cfr. E. NAVARRETTA, sub art. 11, in (a cura di) M.C.Bianca e F.D.Busnelli, *La protezione dei dati personali, Commentario al D.Lgs. 30 giugno 2003, n. 196,* Padova, 2007, p. 241 ss.

[28] A.QUARTA, *La dicotomia bene-servizio alla prova del supporto digitale*, in *Contr. e impr.* , 2019, p.1013 ss.

[29] I dati genetici e dati biometrici sono stati, opportunamente, aggiunti dal GDPR al novero dei dati sensibili, anche definito "il nocciolo duro" della riservatezza da G. BUTTARELLI, *Banche dati e tutela della riservatezza,* in *La privacy nella Società dell'informazione,* Milano, 1997, p.375.

[30] Sul problema della sorveglianza v.*infra* par.5, nt.56.

[31] M.FRANZONI, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale,*in *Jus civile,* 1, 2021, p.9 ss. che sottolinea come se "l'interesse per lo scambio sembra prevalere sulla privatezza delle singole informazioni, sul piano generale, fatti salvi i limiti derivanti dalla natura stessa dei diritti della persona "allora il diritto alla riservatezza "collegato al trattamento dei dati personali non può essere sempre regolato con la logica del consenso del titolare (proprietario) per l'uso che altri fanno del dato (della cosa) e neppure con la stessa logica applicata all'esercizio del diritto alla salute, nel rapporto medico paziente fondato sul consenso informato".

[32] V. RICCIUTO, *Comunicazione e diffusione dei dati personali e trattamento di dati particolari,* in *, La disciplina del trattamento dei dati personali*, cit., p. 293 ss., che evidenzia come la circolazione dei dati, realizzata attraverso la cessione,

nel rispetto del principio di finalità, conferma l'idea di una negoziabilità dei dati; G. Oppo, *Sul consenso dell'interessato*, in (a cura di) V. Cuffaro, V. Ricciuto e V. Zeno Zencovich, *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 123, non esclude che potrebbero sussistere gli elementi per una qualificazione in chiave contrattuale del consenso.

[33]Riconduce il consenso agli atti di natura autorizzatoria D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.,* 1998, p. 350 ss.; analogamente G.M. Riccio, *Sub artt. 23-27*, in (a cura di) S.Sica e P.Stanzione, *La nuova disciplina della privacy: commento al D.lgs. 30.6.2003, n. 196,* Bologna, 2005, p.98 ss., secondo cui il consenso al trattamento dei dati personali costituirebbe un'autorizzazione privata che ha la funzione di rimuovere un limite posto dal legislatore, nell'interesse del titolare dei dati; secondo S. Patti, *sub art. 23*, in *La protezione dei dati personali. Commentario*, cit., p. 541 ss. , il consenso al trattamento dei dati personali costituisce un elemento della fattispecie legale, cui la legge attribuisce "l'effetto di far venire meno il carattere dell'antigiuridicità che altrimenti presenterebbe l'attività relativa ai dati personali".

[34]Cons. St., Sez.V , 29 marzo 2021 n. 2631, conferma così la decisone del Tar Lazio, Roma, Sez. I, 10 gennaio 2020, n. 260 afferma che "*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*". Peraltro, la configurazione del dato, come "prezzo", troverebbe riconoscimento in alcuni interventi normativi del legislatore europeo: il riferimento è alla proposta di *Regolamento su privacy e comunicazioni elettroniche*, riguardo *al trattamento dei dati personali e la tutela della vita privata, nel settore delle comunicazioni elettroniche*", nonché nella dir. n. 2019/770/UE del Parlamento europeo e del Consiglio del 20 maggio 2019, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali su cui v., in particolare, A. De Franceschi, La circolazione dei dati personali tra privacy e contratto 2017; ID., *La circolazione dei dati personali nella proposta di direttiva UE sulla fornitura di contenuti digitali,* in *Regolare la tecnologia,*cit., p. 303 ss.

[35] Considerando il dato come un bene economico da potere scambiare all'interno del mercato, sottolinea che l'approccio americano è più facilmente adattabile alle mutazioni tecnologiche, non a caso negli Stati Uniti la raccolta può essere anche indiscriminata M.BRKAN, *Do algorithms rule the world? Algo-*

rithmic decision-making and data protection in the framework of the GDPR and beyond", *International Journal of Law and Information Technology*, 27(2), 2019, p.91ss.; v.nt. 7.

[36]Così F. PIZZETTI, *GDPR e Intelligenza artificiale, Codici di condotta, certificazioni, sigilli, marchi e altri poteri di soft law previsti dalle leggi nazionali di adeguamento: strumenti essenziali per favorire l'applicazione proattiva del Regolamento europeo nell'epoca della IA*, in *Regolare la tecnologia*, cit., p. 216; A.R. POPOLI, *Codici di condotta e certificazioni,* in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* cit., p. 408ss.

[37]V.CUFFARO, *Il regolamento generale sulla protezione dei dati*, in *Trattamento dei dati personali e regolamento UE n. 2016/679,* in *Speciali digitali* del *Corriere giur.,* 2018, p. 2 ss. sottolinea il diverso ambito prospettico del codice della *privacy* dove, all'art. 1, l'accento sembra porsi sul diritto dominicale della persona sui propri dati, così da accreditare un modello di disciplina sostanzialmente prossimo a quello tradizionalmente, adottato per i diritti della personalità, appunto delineati in termini di appartenenza esclusiva del bene al soggetto, e l'art. 1, comma 1 del reg. dove "il punto di incidenza della disciplina è spostato direttamente sulla tutela della persona, nella misura in cui il trattamento dei dati possa determinare pregiudizio ai diritti ed alle libertà fondamentali"; F.DI CIOMMO, *Archivi digitali (onnivori) e diritti fondamentali (recessivi)*, in *Nuovo dir. civ*., 2, 2020, p.29ss.

[38] Sul tema v. l'ampia ricostruzione di L.VIZZONI, *Domotica e diritto, La smart home tra regole e responsabilità,* Milano, 2021, p. 35ss.

[39]È la tesi di "*Home life data and children's privacy*", *www.childdatacitizen.com*, uno studio realizzato, nel 2018, da V. BARASSI, *Digital citizens? Data traces and family life,* in *Journal of the Academy of Social Sciences,* 2017, p. 84 ss..

[40] Sulla prospettiva "dualistica", che distingue all'interno del medesimo diritto della personalità un contenuto indisponibile, strettamente personale, e uno di carattere patrimoniale, suscettibile di disposizione, C. SCOGNAMIGLIO, *Il diritto all'utilizzazione economica del nome e dell'immagine delle persone celebri*, in *Dir.inf*., 1988, p. 26 ss. Nel senso che la distinzione tra momento personale e patrimoniale, di origine francofona, sia "artificiosa" protendendo per una considerazione monistica dei diritti della persona, sulla base di una soluzione ricavabile dal diritto d'autore A. ZOPPINI, *Le nuove proprietà nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni),* in *Riv. dir. civ*., I, 2000, p. 236 ss. Dal diritto della persona si realizzerebbe, nella forma del contratto di licenza, un acquisto "derivativo costitutivo", che crea una "situazione giuridica soggettiva nuova che limita senza estinguerlo il diritto in capo

al titolare". Il risultato pratico delle due soluzioni non appare, tuttavia, così differente.

[41] In dottrina sottolineano come il mercato non sia in grado di correggere , tali asimmetrie S.BONAVITA-R. PARDOLESI, *GDPR e diritto alla cancellazione e (oblio),* in *Danno e resp.,* 3, 2018, p.274, per cui " assumere che il consenso possa essere liberamente revocato è una consolazione alquanto grama".

[42]Si distinguono **rischio inaccettabile,** che attiene a quelle applicazioni che potrebbero avere il fine di manipolare i comportamenti umani, come il c.d. *social scoring*; **rischio alto,** riguardo i sistemi di IA che potrebbero mettere a rischio la sicurezza ed i diritti fondamentali degli individui, come dispositivi medici basati su sistemi di IoT; **rischio limitato,** ad esempio, *chatbot* , che devono essere trasparenti per fare acquisire all'utente la consapevolezza di interagire con una IA ; **rischio minimo,** ad esempio, filtri spam o *videogame* basati su sistemi di IA per i quali non sono previste particolari limitazioni.

[43] All'art. 13 si prevede che i sistemi di IA ad alto rischio "devono essere progettati e sviluppati in modo da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo in modo appropriato". Ne deriva l'obbligo di svolgere una Valutazione d'Impatto sulla protezione dei dati, così come previsto dall'art. 35 GDPR. L'art. 62 impone ai fornitori dei sistemi di IA, ad alto rischio, di notificare alle Autorità competenti nazionali ogni incidente o malfunzionamento grave, analogamente a quanto previsto nel GDPR per l'obbligo di notifica del *data breach*.

[44] Per una ricostruzione storica sui contratti di massa cfr., per tutti, C.M. BIANCA, *Le condizioni generali di contratto*, Milano, 1979; G. ALPA, (a cura di), *I contratti del consumatore,* Milano, 2014.

[45] Sottolinea, d'altra parte come "non e` possibile pensare ad una gestione di tipo individuale dei dati, tanto meno se basata sul consenso. Il consenso, astrattamente il miglior modello possibile, si rivela spesso non adeguato nel fornire una tutela effettiva ed inefficace" , G. FINOCCHIARO , *Intelligenza Artificiale e protezione dei dati personali,* in *Giur.it*. 2019, p.1677; in senso analogo D. POLETTI, *GDPR tra novità e discontinuità-Le condizioni di liceità del trattamento dei dati personali*, in *Giur.it*., 2019, p.2785; in giurisprudenza v. Cons.St., Sez. VI, n.8472/2019 che ha posto l'onere probatorio a carico del soggetto che si avvale della procedura robotizzata tenuto a dimostrare "la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo", in quanto l'impossibilità di capire come sia stata presa una determinata decisione, costituisce di per sé "un vizio tale da inficiare la procedura".

[46] Ad aprire il dibattito si segnalano le opere di N.G.CARR a partire da *It doesn't matter,* in *Harvard business review,* 2003, www.hbr.org e di J LANIER *Dieci ragioni per cancellare subito i tuoi account social* , trad. F.Mastruzzo, Milano, 2018.

[47] Ritiene che "il fatto di riscontrare la insufficienza del consenso a regolare il trattamento nelle sue diverse forme, con conseguente perdita di protezione della persona " non deve essere inteso nel senso di una resa alla tecnica. Occorre muovere dalla constatazione che l'economia dei beni immateriali o dematerializzati, si muove e segue logiche differenti da quelle dell'economia reale." Sicché il mondo digitale è "un universo parallelo, che funziona con regole che necessariamente devono essere proprie e non riflesse da quelle del mondo reale che, peraltro, non può essere sostituito", M.FRANZONI, *Lesione dei diritti della persona, tutela della privacy e intelligenza artificiale,* cit., p.12.

[48]In tal senso G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr.e impr*., 2017, p. 726 ss.

[49] Principio già previsto dall'art. 12 della *Dichiarazione dei diritti di internet (Diritti e garanzie delle persone sulle piattaforme),* elaborata dalla Commissione parlamentare per i diritti e doveri in Internet, costituita presso la Camera dei deputati e presieduta da Stefano Rodotà su cui cfr. ID., *Il diritto di avere diritti,* cit., p. 386.

[50] Brussels, 15.12.2020 COM (2020) 825 final 2020/0361 (COD) *Proposal for a regulation of the european parliament and of the council on a Single Market For Digital Services, Digital Services Act (DSA) and amending* Directive 2000/31/EC. Nella stessa data è stata presentata la proposta sul *Digital Markets Act (DMA),* www.europarl.europa.eu.

[51] *Federal trade commission*, report *Aiming for truth, fairness, and equity in your company's use of AI,* su cui E. JILLSON, *Aiming for truth, fairness, and equity in your company's use of AI*, 19 aprile 2021, www.ftc.gov.

[52] In tal senso, in giurisprudenza, TAR Roma, Sez, *III-bis*, 30 giugno 2020, n. 7370, che ha ordinato la consegna del codice sorgente del *software* gestito dal consorzio Cineca, contenente gli identificativi alfanumerici per l'associazione dei compiti anonimi con i nomi e i cognomi dei candidati. In ordine alla possibile introduzione di un registro relativo al deposito del codice sorgente del *software* di intelligenza artificiale, che dovrebbe garantire maggiore trasparenza, F. BRAVO, Software *di intelligenza artificiale ed istituzione del registro per il deposito del codice sorgente*, in *Contr. e impr.*, 4, 2020, p. 1412 ss. Oltre all'istituzione di un'Autorità regolatoria indipendente tanto a livello nazionale che europeo, seguendo l'approccio già adottato dal GDPR, nel regolamento proposto sull'AI sono previste delle sanzioni amministrative in caso di violazione o mancata

osservanza delle norme in esso contenute che possono arrivare fino al 6% del fatturato globale annuo cifra ancor più elevata del 4% prevista dal GDPR.

[53] Prospettano, la necessità di una rimodulazione delle norme, che tenga conto delle peculiarità della nuova generazioni di prodotti e che, possibilmente, consenta di individuare un percorso di responsabilità unitario, allo scopo di semplificare e, quindi, agevolare il fruitore del bene nel caso in cui il " formatore" dell'algoritmo sia diverso dal produttore del bene che incorpora A. Amidei, *Intelligenza Artificiale e product liability: sviluppi del diritto dell'Unione Europea,* in *Giur. it*., 2019, p.1726; U. Ruffolo, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo,* ibidem, p. 1692 ss.; in proposito v.nt.47.

[54] E. Palmerini, *Robotica,* in *Enc. di Bioetica e scienza giuridica*, *Parte giuridica*, X, Napoli, 2016 , p. 1100; E. Palmerini, A. Bertolini, *Liability and Risk Management* in *Robotix*, in (a cura di)R. Schulre e D.Standenmayer, *Digital Revolution; Challengers for Contract Law in Practice* Baden-Baden, 2016, p. 225 ss.

[55] Cons. St., Sez.VI, n. 2270/2019, cit., v.nt.4 .

[56] Nella Risoluzione del Parlamento europeo del 20 gennaio 2021 (2020/2013(INI)), relativa *all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale*, si definisce sistema AI – "autonomo" quello "basato sull'intelligenza artificiale che opera interpretando determinati dati forniti e utilizzando una serie di istruzioni predeterminate, senza essere limitato a tali istruzioni, nonostante il comportamento del sistema sia legato e volto al conseguimento dell'obiettivo impartito e ad altre scelte operate dallo sviluppatore in sede di progettazione". Suggestive le pagine di A.Turing, i*Computing machinery and intelligence,* in *Mind*, 1950, p.456 che proponeva ai progettisti un metodo di insegnamento, rivolto alle macchine, come se si dovessero educare dei bambini, attraverso quelli che egli definiva degli "imperativi", cui la macchina è obbligata ad obbedire. In ordine ad una possibile imprevedibilità dell'azione dell'agente *software* la risposta al problema era esemplificata associando « punizioni e ricompense» nel corso del processo d'insegnamento delle macchine, come avviene per i bambini: "La macchina deve essere costruita in modo che sia impossibile che si ripetano gli avvenimenti che precedettero di poco il verificarsi di un segnale di punizione, mentre un segnale di ricompensa aumenta la probabilità di ripetizione degli avvenimenti che hanno condotto ad esso".

[57] Nelle linee guide "per un'intelligenza artificiale affidabile", pubblicate il 18 dicembre 2018, *l' Higt level expert group on AI,* al punto 5.1 del *Draft* ha, espressamente, chiarito come i diritti fondamentali rappresentino una *stepping stone*,

pietra miliare verso un approccio *human centric,* www.europa.eu. In chiave , per certi versi, distopica, S. ZUBOFF, *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power,* London 2019. Si rinvia, inoltre, all'analisi di G. ALPA , *Code is law: il bilanciamento dei valori e il ruolo del diritto,* in *Contr. impr*., n.2, 2021, p.384 che richiama il libro D.LYON, *La cultura della sorveglianza. Come la società del controllo ci ha reso tutti controllori,* Roma 2020, ove si sottolinea che dall' accettazione della logica della sorveglianza ne traiamo tutti beneficio.

Indice degli autori

Enrico Al Mureden
Professore ordinario di diritto privato presso l'Università di Bologna

Antonina Astone Professoressa associata di diritto privato presso l'Università degli Studi di Messina

Ettore Battelli
Professore associato di diritto privato presso l'Università degli Studi di Roma Tre

Giovanni Berti de Marinis
Professore associato di diritto dell'economia presso l'Università degli Studi di Perugia

Marco Carlizzi
Avvocato del Foro di Roma, dottore di ricerca in diritto commerciale – Università di Roma "Tor Vergata"

Enrico caterini
Professore ordinario di diritto privato presso l'Università della Calabria

Antonella Correnti Assegnista di diritto privato comparato presso l'Università degli Studi di Messina

Marco Fasciglione
Ricercatore di Diritto internazionale e di Tutela dei diritti umani, CNR-IRISS

Ilaria Garaci
Professoressa associata di diritto privato presso l'Università Europea di Roma

Sara Landini
Professoressa ordinaria di diritto dell'economia presso l'Università degli Studi di Firenze

Francesco Mezzanotte
Professore associato di diritto privato presso l'Università degli Studi di Roma Tre

Roberta Montinaro
Professoressa ordinaria di diritto privato presso l'Università di Napoli L'Orientale

Rosario Petruso
Professore associato di diritto privato comparato presso l'Università degli Studi di Palermo

Guido Smorto
Professore ordinario di diritto privato comparato presso l'Università degli Studi di Palermo

IL TORCOLIERE • Officine Grafico-Editoriali d'Ateneo
Università di Napoli L'Orientale
stampato nel mese di giugno 2023

UNIVERSITÀ DI NAPOLI
L'ORIENTALE
Dipartimento di Scienze Umane e Sociali

Il libro esamina le questioni giuridiche più rilevanti legate all'evoluzione delle tecnologie digitali e, in particolare, allo sviluppo di sistemi intelligenti, al loro impatto sui diritti umani e alla imputazione delle responsabilità.
Gli autori esplorano le soluzioni in grado di promuovere e garantire la sostenibilità dell'innovazione, attraverso azioni preventive e la protezione *by design*. Del resto, le tecnologie digitali contribuiscono a migliorare la valutazione dei rischi, a promuovere la trasparenza e l'efficienza dei servizi digitali, nel rispetto degli obiettivi dello sviluppo sostenibile. Specifica attenzione è rivolta ai settori assicurativo, bancario e turistico.

Ilaria Garaci - Professore associato di Diritto privato nell'Università Europea di Roma, dove insegna Diritto privato ed Elements of Italian Private Law. È membro del Collegio dei docenti nel Corso di Dottorato in "Persona, benessere e innovazione", presso l'Università Europea di Roma. Relatrice in seminari e conferenze nazionali e internazionali, è autrice di due lavori monografici e di diversi contributi in materia di beni immateriali e tutela della persona, tutela del consumatore, responsabilità civile, rimedi restitutori, diritti dei minori di età.

Roberta Montinaro - Professore ordinario di Diritto Privato, insegna Diritto privato e Diritto privato dell'economia digitale presso il Dipartimento di Scienze Umanistiche e Sociali dell'Università di Napoli L'Orientale. È coordinatore scientifico del Modulo Jean Monnet "DiCIT - Digital Citizenship in the European Union" e membro del collegio dei docenti del Dottorato Nazionale in Intelligenza Artificiale. È stata relatrice e coordinatrice scientifica di seminari e conferenze nazionali e internazionali. Autrice di monografie, ha pubblicato anche articoli e saggi in libri e riviste scientifiche, in italiano e in inglese. I suoi principali interessi di ricerca riguardano il diritto dei trust, la responsabilità civile, il diritto dei consumatori e il diritto delle tecnologie digitali.

ISBN 978-88-6719-276-2