



SUSANNA SANDULLI

Assegnista di ricerca – Università degli Studi Roma Tre

ALGORITMI, TRASPARENZA ED EFFETTIVITÀ DEL CONSENSO

SOMMARIO: 1. *La vicenda.* – 2. *La trasparenza nel GDPR e nella Proposta di Regolamento.* – 3. *Il diritto alla spiegazione nelle decisioni automatizzate.*

1. – La Corte di Cassazione con l'ordinanza n. 14381/2021 si è pronunciata su un tema attuale e complesso quale il rapporto tra la validità del consenso al trattamento dei dati personali e la trasparenza dell'algoritmo. Questa decisione costituisce l'occasione per una riflessione sulla questione muovendo da una vicenda del reale che rivela la difficoltà di applicare alcuni principi, come quelli su cui fonda il GDPR¹, a situazioni in cui il ricorso a nuove tecnologie – e in particolari agli algoritmi di profilazione – rendono il contesto in cui si muove l'interessato molto diverso dalle ipotesi immaginate dal Legislatore europeo in sede di GDPR.

Per comprendere i termini del problema occorre ripercorrere la vicenda giudiziaria, che trae origine dalla realizzazione da parte di una società di un'infrastruttura costituita da una piattaforma web e un archivio informatico preordinata all'elaborazione di profili di persone fisiche e giuridiche per calcolare in modo imparziale e veritiero il *rating* reputazionale dei soggetti censiti. Attraverso la raccolta e l'elaborazione di una mole rilevante di dati personali² e l'impiego di un algoritmo, il sistema assegna ai soggetti censiti degli indicatori alfanumerici in grado di determinare – secondo la società – l'affidabilità delle persone in campo economico e professionale.

In una prima fase è stato chiesto dalla stessa società al Garante per la protezione dei

¹ *General Data Protection Regulation*, ossia il Regolamento (UE) 2016/679.

² Forniti volontariamente dagli stessi utenti o reperiti sul web.



dati personali di valutare se questa attività fosse lecita ai sensi del Codice della privacy³.

Ad avviso dell’Autorità, che ha espresso le sue perplessità nel rimettere ad un sistema automatizzato decisioni relative ad aspetti così delicati⁴, il sistema comporta rilevanti problematiche per la *privacy* dei soggetti coinvolti, in quanto la società non può dimostrare l’*efficacia* dell’algoritmo al quale è rimessa la valutazione dei soggetti censiti.

Tali dubbi sembrano rafforzati dalla circostanza per cui il consenso espresso da chi viene valutato non pare frutto di una libera autodeterminazione⁵, poiché la mancata adesione alla piattaforma e la conseguente sottoposizione al sistema di valutazione preclude la stipula di contratti con la società o il mantenimento del vincolo negoziale. Anche il diritto all’informativa, poi, non sembrerebbe garantito, non essendo ben comprensibili le finalità del trattamento⁶.

Per tale ragione e per altre diverse considerazioni⁷, il Garante, ritenendo che il sistema di trattamento dei dati personali non fosse conforme al Codice della privacy, aveva vietato qualsiasi operazione⁸.

Sul ricorso promosso dalla società contro questa decisione si è pronunciato il Tribunale di Roma, il quale ha parzialmente riformato il provvedimento dell’Autorità, affer-

³ Nello specifico, si è chiesto se in relazione alle modalità e finalità del trattamento da porre in essere per l’attuazione dei servizi fosse necessario, prima della raccolta dei dati, ottenere l’autorizzazione di cui agli artt. 25, comma 1, e 27, comma 1, del Codice della privacy.

⁴ Ciò altresì considerando il rischio che tali valutazioni si basino su documenti falsi o viziati.

⁵ Il problema della mancata libertà del consenso si è posto anche rispetto ai terzi che non hanno aderito alla piattaforma ma i cui dati personali vengono trattati ugualmente per ottenere valutazioni autonome. Parimenti, non sembra giustificato il trattamento dei dati sensibili (oggi “particolari categorie di dati” ex art. 9 GDPR).

⁶ Sia perché i dati personali possono essere trattati da associazioni o società collegate ma che offrono servizi completamente diversi, sia perché è prevista la raccolta di un consenso (in questo caso facoltativo) per il perseguimento di finalità commerciali non identificate non menzionate fra gli scopi del titolare. A ciò si aggiunga che l’informativa prevede la possibilità – senza alcuna specificazione – che i dati siano trasferiti all’estero.

⁷ Secondo l’Autorità, sono numerosi i profili di criticità. Ad esempio, si ritengono non rispettati i principi di necessità e proporzionalità con riferimento alla rilevanza e pertinenza dei dati e documenti poiché pare impossibile dimostrare l’effettiva incidenza di determinate dinamiche etico-comportamentali sull’affidabilità dei soggetti censiti, ma anche in ragione del numero estremamente elevato di soggetti censiti, con le relative ripercussioni per i diritti individuali in caso di violazione delle norme di sicurezza. Proprio con riferimento a quest’ultimo aspetto, le misure – consistenti in sistemi di autenticazione “deboli”, vale a dire *id e password* – sono ritenute del tutto inadeguate. In conclusione, la raccolta di dati personali è suscettibile di incidere significativamente sulla vita dei soggetti censiti, tanto da poter comportare l’ammissione o l’esclusione da prestazioni, servizi o benefici.

⁸ Provvedimento n. 488 del 24 novembre 2016.



mando che i soggetti censiti sarebbero stati consapevoli della complessità del sistema di raccolta e trattamento dei dati personali e di come esso potesse incidere sulla loro rappresentazione sociale ed economica⁹.

La clausola contrattuale che subordina la stipula del contratto o il mantenimento dello stesso all'adesione alla piattaforma è stata ritenuta dal Tribunale perfettamente lecita, in quanto considerata mera condizione accessoria la cui validità è subordinata alla natura del rapporto contrattuale stesso. Pertanto, il presupposto di liceità viene rinvenuto nella "preventiva consapevolezza delle categorie utilizzate e della scala di valori codificata in relazione a diversi profili o tipi di documenti conferiti". Per l'effetto, il Tribunale ha ritenuto il consenso validamente espresso.

In questo modo, però, si è fatto riferimento solo all'*affidabilità* del sistema, non affrontando il profilo della *conoscibilità* dell'algoritmo da parte dei soggetti aderenti.

Su questo aspetto si è invece concentrata la Suprema Corte, secondo la quale la non conoscibilità dell'algoritmo comporta che il consenso venga espresso con riferimento ad un oggetto solo parzialmente determinato, mentre resta sconosciuto il meccanismo mediante il quale i dati vengono trattati. Ne consegue l'irrelevanza del consenso manifestato con riferimento alle singole operazioni "perché esso non riguarda la sostanza del trattamento, ossia il meccanismo che forma il giudizio, ma solo alcuni degli elementi immessi, la cui trasformazione in *rating* sfugge ad ogni possibile apprezzamento obiettivo".

Per la Corte, perciò, si è realizzato uno schema negoziale basato su giudizi non verificabili e lesivo del diritto all'autodeterminazione informativa, avendo reso impossibile per gli interessati valutare la necessità dei dati conferiti ai fini del trattamento.

La scarsa trasparenza dell'algoritmo impiegato non è stata, peraltro, disconosciuta dalla sentenza di primo grado, la quale ha unicamente ritenuto non decisivi i dubbi relativi al sistema automatizzato di calcolo per la definizione del *rating* reputazionale sul rilievo che la validità della formula riguarderebbe "il momento valutativo del procedimento", a fronte del quale spetterebbe invece al mercato "stabilire l'efficacia e la bontà del risultato ovvero del servizio prestato dalla piattaforma".

Diversamente ragionando, la Suprema Corte ritiene che non spetti al mercato stabilire l'efficacia e la bontà del servizio o del risultato – come avviene per il *rating* di legalità –, ma che il problema debba essere affrontato seguendo la diversa prospettiva che riguarda

⁹Per il Tribunale rientra nel concetto di autonomia privata la possibilità di realizzare sistemi di accreditamento fornendo servizi valutativi in vista di un ingresso sul mercato per la conclusione di contratti e la gestione di rapporti economici.



la validità del consenso prestato al momento dell'adesione e, soprattutto, la trasparenza del trattamento dei dati. In sintesi, ad avviso della Cassazione l'adesione ad una piattaforma non comporta di per sé anche l'accettazione di un sistema automatizzato, che si avvale di un algoritmo il cui schema esecutivo non è conoscibile, non potendosi in tal caso ritenersi soddisfatto il requisito della consapevolezza.

In altri termini, la conclusione della Suprema Corte è nel senso che il problema, per la liceità del trattamento, era (ed è)¹⁰ invece costituito dalla validità – per l'appunto – del consenso, che si assume prestato al momento dell'adesione. E non può logicamente affermarsi che l'adesione ad una piattaforma 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.

2. – Rispetto alla sentenza del Tribunale, la Corte di Cassazione sposta il fuoco dell'indagine dalla tutela della *privacy* alla trasparenza e al ruolo del consenso¹¹.

¹⁰ L'Italia, dopo un *iter* piuttosto travagliato, ha attuato la disciplina del Regolamento europeo 2016/679/UE attraverso il d.lgs. del 10 agosto 2018, n. 101 recante “*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*”. Il nuovo Codice si caratterizza per un diverso approccio alla materia, in quanto da un sistema individualistico di protezione fondato sull'istituto del consenso, si è passati ad una visione “sociale” incentrata sulla dimensione collettiva del diritto alla protezione dei dati personali. Come noto, il GDPR deve essere integralmente applicato e ciò è chiaramente espresso all'art. 1 del Codice, il quale prevede che “*il trattamento dei dati personali avviene secondo le norme del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016*”; la *ratio* di tale disposizione è stata di rimarcare che le norme codicistiche formano un “unico sistema normativo a due livelli”, composto dal GDPR, avente efficacia e vigenza nell'Unione europea, e il Codice della *privacy*, le cui norme trovano applicazione nel territorio nazionale solamente qualora risultino conformi, sia per quanto riguarda l'applicazione che l'interpretazione, al Regolamento europeo. Così, F. PIZZETTI, contributo consultabile sul sito <https://www.agendadigitale.eu/sicurezza/privacy/gdpr-pizzetti-i-consigli-per-leggere-e-applicare-bene-il-decreto-101-2018-dal-19-settembre/>. Per ulteriori approfondimenti v. ID, *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Torino, 2021.

¹¹ “Questo confidare negli algoritmi ne determina una presenza sempre più pervasiva, che non sembra conoscere confini, giustificando il parlare di una società che essi contribuiscono a definire nelle sue nuove e significative caratteristiche. L'algoritmo disegna le modalità di funzionamento di larghe aree delle nostre organizzazioni sociali, e così ridistribuisce poteri. Incarna anzi le nuove forme del potere e ne modifica la qualità. E tutto questo suscita diverse domande. Saremo sempre più intensamente alla mercé delle macchine? Quali sono gli effetti su libertà e diritti, quali le conseguenze sullo stesso funzionamento democratico di



La pronuncia della Corte offre così spunti interessanti per approfondire temi complessi, in quanto nell'era dell'algoritmo¹² è evidente il rischio di pregiudizi derivanti dal trattamento di dati personali e dalla classificazione predittiva¹³. La tutela della *privacy* va messa alla prova e verificata quanto ad effettività alla luce delle implicazioni derivanti dall'impiego dei sistemi di intelligenza artificiale¹⁴ (di seguito: IA).

I progressi tecnologici hanno contribuito ad un'accelerazione della *big data anylitic* e a sua volta questa mole sempre maggiore di dati favorisce lo sviluppo di avanzati sistemi

una società?". Così S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2012, p. 402, il quale dimostra, come sempre, di aver anticipato le problematiche della *privacy*.

¹² F. BASSAN, *Potere dell'algoritmo e resistenza dei mercati in Italia*, Soveria Mannelli, 2019.

¹³ Tali discriminazioni possono sorgere altresì da *biasas* derivanti dalla progettazione e dall'impiego di modelli di analisi, giacché gli algoritmi, in ogni caso, sono il frutto di un lavoro umano e di formulazioni del pensiero umano realizzate in forma matematica. Cfr. il Paper Joint Committee Discussion redatto da EBA-ESMA-EIOPA, consultabile sul sito https://www.esma.europa.eu/sites/default/files/library/jc-2016-86_discussion_paper_big_data.pdf; G. SCIASCIA, *Reputazione e potere: il social scoring tra distopia e realtà*, in *Giornale di diritto amministrativo*, 2021, p. 317 ss.

¹⁴ L'intelligenza artificiale (IA) è l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività. Essa permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce risolvendo problemi e agire verso un obiettivo specifico. Questa è la definizione del Parlamento europeo, ma le fonti sono vastissime; ad esempio, secondo U. RUFFOLO, *L'Intelligenza artificiale in sanità: dispositivi medici, responsabilità e "potenziamento"*, in *La responsabilità medica*, a cura di E. Gabrielli, U. Ruffolo, in *Giur. it.*, 2021, p. 502, "con la locuzione «Artificial Intelligence», ci si riferisca, in estrema sintesi semplificatrice, a software o programmi capaci di porre in essere con successo, e con un grado più o meno elevato di autonomia, operazioni simili a quelle che, negli esseri umani, sono le attività di apprendimento e di assunzione di decisioni al fine del raggiungimento di specifici obiettivi, grazie all'impiego di tecnologie fondate su processi di «machine learning», di «deep learning» (molto usato, quest'ultimo, nella diagnostica) e dell'utilizzo di reti neurali ("neural networks") programmate per funzionare sul modello del cervello umano." Per un approfondimento del tema e dei diversi profili che lo riguardano cfr., seppur non esaustivamente, U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della Commissione Europea*, in *Rivista di Diritto Civile*, 2020, p. 1246 ss.; A. FUSARO, *Quale modello di responsabilità per la robotica avanzata? Riflessioni a margine del percorso europeo*, in *La Nuova Giurisprudenza Civile Commentata*, 2020, p. 1344 ss.; C. GALLI-M. BOGNI, *Intelligenza artificiale, nuove dinamiche della ricerca e problem and solution approach*, in *Il Diritto Industriale*, 2020, p. 127 ss.; U. RUFFOLO, *Intelligenza Artificiale, machine learning e responsabilità da algoritmo*, in *Giurisprudenza Italiana*, 2019, p. 1657 ss.; A. AMIDEI, *Intelligenza Artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giurisprudenza Italiana*, 2019, p. 1657 ss.; G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, in *Contratto e Impresa*, 2020, p. 713 ss.; R. BICHI, *Intelligenza Artificiale tra "calcolabilità" del diritto e tutela dei diritti*, in *Giurisprudenza Italiana*, 2019, p. 1657 ss.; F. DI GIOVANNI, *Attività contrattuale e Intelligenza Artificiale*, in *Giurisprudenza Italiana*, 2019, p. 1657 ss.; U. RUFFOLO-A. AMIDEI, *Intelligenza Artificiale e diritti della persona: le frontiere del "transumanesimo"*, in *Giurisprudenza Italiana*, 2019, p. 1657 ss.; N.F. FRATTARI, *Robotica e responsabilità da algoritmo. Il processo di produzione dell'intelligenza artificiale*, in *Contratto e Impresa*, 2020, p. 458 ss.



di intelligenza artificiale, che si snodano in tecniche di profilazione e di *marketing* contraddistinte da una tendenziale *opacità*.

Il legame tra l'impiego dell'intelligenza artificiale e la tutela della *privacy* riguarda, in particolare, l'immagazzinamento di grandi quantità di dati personali, che vengono elaborati anche a grande distanza grazie al collegamento tra l'elaboratore principale e i terminali. In questo modo, però, l'interessato può perdere il controllo sui propri dati, non avendo cognizione dei passaggi della raccolta¹⁵.

Questo sistema, caratterizzato da reti neurali, si contraddistingue per le c.d. *black box* nelle quali vengono effettuati i calcoli algoritmici, che però non vengono ricostruiti nel loro percorso logico. L'unica certezza è che nelle *black box* le esperienze vengono combinate tra loro, con il rischio di errori e discriminazioni¹⁶ e a tal proposito si parla della *black box society*, in cui al numero crescente di attività di trattamento dei dati personali non si accompagna una trasparenza dei processi decisionali¹⁷.

I pericoli principali della *black box society* derivano dall'impiego di algoritmi predittivi che possono comportare discriminazioni¹⁸ nelle quali l'utente rimane intrappolato. Un valido esempio è rappresentato proprio dalla fattispecie analizzata dalla sentenza in esame, in quanto un punteggio negativo a cui consegue un giudizio negativo del soggetto censito comporta effetti che se, da una parte, confermano il processo decisionale dell'algoritmo, dall'altra fanno sì che l'impatto negativo del sistema appaia irrimediabile.

Per scongiurare tali rischi il principale strumento è costituito dalla *trasparenza*¹⁹,

¹⁵ E. FALLETTI, *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, in *Dir. inf.*, 2020, p. 169 ss.

¹⁶ Neppure il sistema di anonimizzazione dei dati pare efficace, in quanto l'impiego di sistemi di IA fa sì che l'utente lasci delle tracce e l'*Internet of things* non pare essere d'aiuto in un sistema che, fondamentalmente, sembra eludere la normativa di tutela dei dati personali.

¹⁷ E. PELLACCHIA, *Profilazione e decisioni automatizzate al tempo della black box society: qualità dei dati e leggibilità dell'algoritmo nella cornice della responsible research and innovation*, in *Leggi Civ. Comm.*, 2018, p. 1212. Relativamente al settore pubblico si rinvia a U. PAGALLO, *Big data, open data e black box society*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, a cura di R. Cavallo Perin, Torino, 2021, p. 49-54.

¹⁸ Sul tema si rinvia a P. GLAUNER-P. VALTCHEV-R. STATE, *Impact of Biases in Big Data*, *ESANN 2018 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning*, Bruges (Belgium), 25-27 april 2018.

¹⁹ Il concetto di trasparenza può assumere una pluralità di significati, specialmente nella società degli algoritmi, come dimostra lo studio dell'EPRS, *A governance framework for algorithmic accountability and transparency*, 2019. Particolare, ad esempio, il concetto di trasparenza dell'algoritmo inteso come comprensibilità: sul tema v. A. MASCOLO, *Gli algoritmi amministrativi: la sfida della comprensibilità*, in *Giornale*



principio che trova collocazione nel GDPR e nel Codice della privacy, ma che, calato nel contesto degli algoritmi e dell'intelligenza artificiale, fatica ad essere concretamente ed efficientemente applicato.

Il fondamento normativo di tale principio si rinviene negli artt. 13, 14 e 15 del Regolamento e sta ad indicare che il rapporto tra il titolare e l'interessato si caratterizza per un gioco di reciproche interrelazioni, contraddistinte da obblighi comportamentali, di informazioni e di aggiornamento²⁰, in quanto l'attività deve essere compatibile con il rispetto dei principi fondamentali di tutela dell'individuo.

A tal fine, il GDPR, così come il Codice della privacy²¹, contiene numerose previsioni: quelle relative all'accesso ai propri dati personali; il diritto ad un'informativa chiara e comprensibile; la portabilità dei dati; l'opposizione al trattamento; il diritto alla rettificazione e all'integrazione.

Fra queste, l'art. 15 sancisce il diritto di ottenere informazioni²² e, in particolare, la lett. h) riguarda *“l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato”*, aprendosi così nuovi scenari sul rapporto fra le decisioni automatizzate e il c.d. diritto alla spiegazione, sul quale torneremo.

In questo senso può notarsi che il principio della trasparenza rispetto all'interessato va al di là del consenso, cioè non è necessariamente correlato ad esso quale fondamento di legittimazione del trattamento, ma individua il diritto dell'interessato di intervenire, di partecipare e di comprendere il percorso logico e tecnico che conduce il trattamento delle sue informazioni personali all'esercizio del diritto di recesso²³.

In questa prospettiva si deduce che i diritti citati sono strumentali alla realizzazione di

di diritto amministrativo, 2020, p. 366 ss.

²⁰ M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo*, Torino, 2019, p. 199.

²¹ A differenza della l. n. 675/1996, che non conteneva previsioni espresse in tal senso.

²² a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine.

²³ M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, cit., p. 204.



un sistema di tutela preventiva dell'interessato²⁴, ma applicati al contesto dell'intelligenza artificiale e degli algoritmi assumono una connotazione specifica, che sembra porre un problema di tutela, giacché la Proposta di Regolamento sull'IA²⁵ – primo quanto unico esempio di regolazione normativa del fenomeno – non contiene riferimenti in tal senso.

L'applicazione concreta del principio di trasparenza appare tutto fuorché scontata, in quanto dovrebbe sostanziarsi nella possibilità per l'interessato di comprendere il funzionamento della tecnologia, ma le complessità tecniche e la tendenziale opacità che contraddistinguono l'impiego degli algoritmi rendono il tutto molto difficile, considerando che oltre all'opacità *tecnica* – per cui l'algoritmo è decifrabile esclusivamente da esperti – e a quella *intenzionale* – volta a perseguire obiettivi concorrenziali – c'è anche un'opacità che deriva dal sistema di auto-apprendimento, per cui il funzionamento dell'algoritmo rimane ignoto anche agli stessi sviluppatori²⁶.

La Proposta – incentrata su un approccio basato sul rischio²⁷, che rende necessario valutare preventivamente l'impatto del sistema di intelligenza artificiale nei confronti dell'individuo²⁸ – sancisce all'art. 13 che i sistemi ad alto rischio “*devono essere progett-*

²⁴ Sulla tutela preventiva cfr. G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI-S. SICA-V. ZENO ZENCOVICH, *Il codice dei dati personali. Temi e problemi*, Milano, 2004, p. 25 ss.

²⁵ La Proposta di Regolamento sull'IA fa parte di un Pacchetto composto da un quadro giuridico sull'intelligenza artificiale, un piano coordinato con gli Stati membri per garantire la sicurezza e i diritti fondamentali di persone e imprese e un Regolamento sulle macchine e riprende quanto già sancito nel Libro Bianco sull'intelligenza artificiale. Nel Pacchetto si sottolinea come le tecnologie si stiano sviluppando in modo sempre più rapido, divenendo strumenti di miglioramento dei vari settori, ma altresì foriere di potenziali rischi; per tale ragione è fondamentale un solido approccio che sfrutti le opportunità e affronti le sfide derivanti dall'IA, promuovendo lo sviluppo e la diffusione dell'intelligenza artificiale. La Commissione europea si impegna dunque ad incentivare i progressi scientifici, a favorire la *leadership* tecnologica dell'Unione europea e a garantire che le nuove tecnologie siano al servizio di tutti i cittadini europei, migliorando la vita e rispettando i diritti fondamentali.

²⁶ E. PELLACCHIA, *Profilazione e decisioni automatizzate al tempo della black box society*, cit., p. 1217.

²⁷ Il rischio può essere *inaccettabile* e di conseguenza vietato, essendo il sistema considerato una minaccia per la sicurezza e i diritti delle persone; *alto*, per cui i relativi sistemi sono soggetti ad obblighi rigorosi prima di poter essere immessi sul mercato, come nel caso dell'identificazione biometrica; *limitato*, con la previsione di specifici obblighi di trasparenza, come per i *chatbot* rispetto ai quali l'utente deve essere consapevole di interagire con una macchina; *minimo*, che riguarda la grande maggioranza dei sistemi di AI e nel qual caso la Proposta consente il libero utilizzo. Inoltre, la Proposta prevede il *conformity assessment* per dimostrare la sussistenza dei requisiti previsti dalla normativa, come d'altronde sancisce anche il GDPR, che prevede la costituzione di un registro delle attività di trattamento e un'attività di valutazione dei rischi che ne possono derivare.

²⁸ L'art. 9 della Proposta di Regolamento sull'IA prevede altresì un'implementazione del sistema di gestione del rischio, stabilendo che esso deve essere costantemente monitorato al fine di valutare e quindi



tati 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"; dunque, non solo occorre fornire tutta la documentazione tecnica che dimostri il rispetto dei requisiti, ma è altresì necessario che questa faccia comprendere le modalità di funzionamento del sistema²⁹.

In realtà, la Proposta stabilisce particolari obblighi di trasparenza nei termini di cui sopra solo con riferimento ai sistemi di alto rischio e sembra quindi crearsi un vuoto di tutela rispetto alle altre tipologie di sistemi di IA, in relazione ai quali la disciplina del GDPR costituirebbe l'unico fondamento normativo.

Quindi, sebbene la Proposta di Regolamento sull'intelligenza artificiale dimostri che l'obiettivo perseguito a livello europeo sia di garantire una normativa equilibrata, che incentivi l'utilizzo dell'IA assicurando il rispetto dei diritti fondamentali, essa non contiene riferimenti specifici alla *conoscibilità* dell'algoritmo.

In quest'ottica, poi, sembra che l'istituto del consenso che da sempre ha costituito la base giuridica primaria al quale ancorare la liceità del trattamento non rappresenti più la soluzione, in quanto rispetto al ruolo fondamentale occupato nel Codice della privacy e nell'abrogata Direttiva madre – in cui era presupposto legittimante e condizione di liceità del trattamento, per cui i criteri alternativi costituivano un'eccezione, – pare aver perso parte della sua rilevanza³⁰. La libera circolazione dei dati³¹ rappresenta l'obiettivo pri-

adattare il sistema di protezione a possibili mutamenti. Nello specifico, si dovrà procedere a un'identificazione, analisi e valutazione dei sistemi ad alto rischio anche qualora essi vengano utilizzati conformemente allo scopo previsto.

²⁹ Il citato art. 13 stabilisce "(...) l'obbligo di accompagnare ai sistemi commercializzati delle istruzioni per l'uso in un formato digitale appropriato o in altro modo che includano informazioni concise, complete, corrette e chiare pertinenti, accessibili e comprensibili per gli utenti.". Ossia: l'identità e i recapiti del fornitore e, nel caso, del suo rappresentante autorizzato; le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio, tra cui ad esempio il livello di accuratezza, robustezza e cybersicurezza rispetto al quale il sistema è stato testato e convalidato e che ci si può aspettare e ogni circostanza nota e prevedibile che possa apportare le modifiche al sistema e le sue prestazioni che sono state predeterminate dal fornitore al momento della valutazione iniziale della conformità, se del caso; le misure di vigilanza umana di cui all'art. 14, incluse le misure tecniche attuate al fine di semplificare l'interpretazione dei risultati dei sistemi di IA da parte degli utilizzatori; la durata prevista del sistema di IA ad alto rischio e tutte le misure di manutenzione e assistenza necessarie per assicurare il corretto funzionamento di tale sistema, anche rispetto gli aggiornamenti *software*.

³⁰ F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, a cura di G. Finocchiaro, Torino, 2017, p. 138. Secondo l'A. "l'autonomia privata non assume, nella prospettiva europea, un ruolo centrale ed esclusivo tra i criteri di selezione degli interessi relativi alla protezione dei dati quale diritto fondamentale della persona, trattandosi solo di uno dei criteri alternativi volti a dare fondamento legittimo all'attività di trattamento posta in essere dal titolare e, al contempo, operare quale meccanismo di primo livello nella se-



mario del Regolamento e, sebbene debba essere correlata al principio della protezione dell'interessato³², non ne risulta subordinata³³, cosicché il consenso diviene solo una delle condizioni di cui all'art. 6 che rendono lecito il trattamento.

Questo diverso ruolo del consenso va poi correlato all'uso degli algoritmi³⁴, che indubbiamente contribuiscono alla personalizzazione dell'offerta, permettendo di raggiungere un risultato più efficiente³⁵, ma non privo di costi³⁶.

lezione degli interessi protetti dall'ordinamento giuridico.”.

³¹ Il Regolamento 2016/679/UE, come visto, è imperniato su quest'ottica di circolazione e, pertanto, parte della dottrina ha sostenuto che il Legislatore europeo non abbia operato in modo neutrale, giacché è stato messo in risalto l'aspetto circolatorio piuttosto che quello personalistico, tanto da essere stato definito un “regolamento quale disciplina della circolazione dei dati personali piuttosto che quale disciplina di protezione della persona”. Così L. SCUDIERO, *Il consenso come condizione di libertà*, in *Il processo di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018 n. 101*, a cura di AA.VV., Milano, 2018, p. 102.

³² Ad esempio il Considerando 4 prevede che il diritto alla protezione dei dati personali vada contemporato con altri diritti fondamentali.

³³ Tanto che l'art. 1, paragrafo 3, stabilisce 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.”.

³⁴ Il tema dell'impiego degli algoritmi nei contratti di diritto civile è approfondito da A.M. BENEDETTI, *Contratto, algoritmi e diritto civile transazionale: cinque questioni e due scenari*, in *Riv. dir. civ.*, 2021, p. 413 ss., il quale, fra le altre, individua due problematiche indice della “spersonalizzazione progressiva del contratto” derivante dalla sostituzione dei contraenti-umani con programmi di macchine che gestiscono anche l'esecuzione contrattuale. La prima questione concerne l'istituto del consenso, il quale non può essere più considerato strumento di protezione del contraente in ragione delle complessità tecniche derivanti dagli algoritmi, ma esclusivamente un mezzo di argomentazione o di coordinamento; come emerge infatti dalla vicenda in esame, il consenso, pur *apparentemente libero*, viene spesso prestato in condizioni di disparità contrattuale, che inducono la parte debole del rapporto a consentire il trattamento dei propri dati personali senza un'effettiva consapevolezza o in assenza di una vera e propria scelta, in quanto il rifiuto al trattamento comporta la rinuncia al servizio. La seconda questione concerne la tecnica algoritmica, che – a prescindere dalla sua declinazione – deve essere correttamente compresa dal consumatore, ma l'applicazione della regolamentazione tradizionale dei contratti a distanza risulta complicata, apparendo così opportuno pensare ad una nuova disciplina, come d'altronde statuito nel Libro Bianco sull'intelligenza artificiale; sebbene l'A. faccia riferimento alla disciplina consumeristica, le nozioni di «consumatore» e «interessato» individuano entrambe un soggetto che si trova in una posizione di maggior debolezza rispetto alla controparte e che necessita di una tutela più pregnante, ma al contempo non eccessivamente limitativa del mercato, rendendo così possibile estendere l'ambito della questione anche a soggetti non propriamente definibili come «consumatori».

³⁵ Sul tema si rinvia a G. ZICCARDI, *Contro i big data: le modalità di controllo del cittadino digitale nella società odierna*, in *Cyberspazio e diritto*, 2020, p. 233 ss.; V. FALCE-G. GHIDINI-G. OLIVIERI (a cura di), *Informazione e Big data tra innovazione e concorrenza*, Milano, 2018, p. 303 ss.; N. NEWMAN, *Search, Antitrust and the Economics of the Control of User Data*, in *Yale Journal on Regulation*, 2014, p. 3. Sul rapporto con l'intelligenza artificiale cfr. G. OLIVI, *Big Data, metadati e Intelligenza Artificiale: i confini tra i diversi diritti*, in *Diritto Industriale*, 2020, p. 181 ss.

³⁶ In una diversa prospettiva, l'impiego degli algoritmi può dar vita a distorsioni concorrenziali, aumen-



I rischi, come detto, discendono dalla natura *predittiva* degli algoritmi³⁷, per cui gli interessati non sono pienamente consapevoli delle conseguenze derivanti dal trattamento dei loro dati personali, i cui vantaggi ottenuti sono immediati ma non duraturi.

Ne consegue che il sistema di tutela dei dati personali, imperniato sul principio della libera circolazione, non è più sufficiente a proteggere l'interessato, impossibilitato a comprendere concretamente le conseguenze delle proprie decisioni. Dunque, nonostante il principio del consenso informato e il fatto che il processo automatizzato sia chiaramente individuato, non è possibile predeterminare la complessità dei processi, poiché l'informativa potrebbe risultare eccessivamente tecnica.

Il consenso diviene così sempre meno strumento di reale autodeterminazione, costituendo una scelta obbligata per il singolo e perdendo parte della sua rilevanza, non essendo concretamente garantita una libera scelta da parte del titolare del diritto. Nel caso in esame, si è visto, infatti, che la mancata manifestazione del consenso al trattamento dei propri dati personali è un ostacolo insormontabile in termini contrattuali, rappresentando una scelta obbligata per il singolo intenzionato a costituire o a proseguire un rapporto negoziale con la società.

L'inadeguatezza del GDPR rispetto all'intelligenza artificiale e all'impiego degli algorit-

tando le barriere all'ingresso, causando pregiudizi alla trasparenza e alla concorrenza del mercato e siffatto problema si pone specialmente per quei soggetti che operano nei settori analogici e che riscontrano forti difficoltà a inserirsi nel mercato digitale; chiaramente, non tutti gli operatori economici sono in grado di disporre delle medesime tecnologie digitali e, pertanto, è altamente probabile che si creino situazioni di monopolio o di abuso di posizione dominante: il rischio è che si realizzi un *Big data divide* fra coloro che proteggono i dati personali e coloro che non lo fanno, ma soprattutto che diminuisca la concorrenza. Da ciò deriva, poi, un'ulteriore criticità, che riguarda direttamente gli utenti del mercato digitale: essendo pochi gli operatori che agiscono nell'ambito della società dell'informazione, non è raro che venga introdotta un'intermediazione ulteriore nelle piattaforme che danneggia la qualità dell'informazione, rendendo possibile per l'operatore orientare l'opinione pubblica e comportando, inevitabilmente, una compromissione nel benessere dei consumatori. Cfr. A. MINUTO RIZZO, *I profili antitrust del nuovo web e della nuova economia digitale*, in *Il Diritto Industriale*, 2019, p. 113 ss.

³⁷ L'impresa – conoscendo il grado di attitudine al consumo da parte del singolo individuo, compresa la sua disponibilità a pagare per un determinato prodotto – potrebbe praticare una differenziazione dei prezzi, che andrebbe a colpire il consumatore causandogli una spesa maggiore e portando alla pratica dei prezzi personalizzati, che riflettono non solo le preferenze dell'individuo, ma anche il *prezzo di riserva*, vale a dire la cifra massima che egli è disposto a pagare in un determinato momento con riferimento allo specifico bene o servizio. Già da anni le piattaforme *e-commerce* utilizzano algoritmi per la determinazione dei prezzi di vendita, consentendo alle imprese di segmentare il mercato mediante l'applicazione di differenti modelli di tariffe e il rischio, dunque, è che dai prezzi personalizzati si arrivi ai *prezzi discriminatori* di cui all'art. 102, lett. c), del TFUE e all'art. 3, lett. c), della l. n. 287 del 10 ottobre 1990, consistenti nella produzione di uno svantaggio competitivo per gli altri concorrenti e nel praticare prezzi ovvero condizioni differenti a prestazioni equivalenti. Su Big data e consumatori v. A. ZAMBON, *Il consumatore nella prospettiva dei big data: alcune considerazioni filosofico-giuridiche*, in *Cyberspazio e diritto*, 2019, p. 117 ss.



mi dimostra così che l'obiettivo di trasparenza non si adatta realmente al contesto digitale, contraddistinto da caratteristiche tecniche estremamente complesse e da un'opacità che difficilmente sembra limitabile³⁸, imponendo di ripensare agli strumenti di protezione della *privacy*. Ciò considerando, peraltro, che anche qualora il soggetto interessato fosse portato a conoscenza del c.d. codice sorgente, il processo decisionale rimarrebbe comunque ignoto e incomprensibile – e di conseguenza anche inutile – in virtù dei tecnicismi che contraddistinguono l'algoritmo e, dunque, più che al diritto all'informazione sarebbe opportuno riferirsi ad un diritto alla spiegazione quale ricerca di equilibrio fra l'esigenza di trasparenza del processo decisionale automatizzato e il progresso digitale.

3. – Alla luce di queste considerazioni, vale la pena approfondire questo aspetto del *diritto alla spiegazione* per vedere come si concilia con le disposizioni vigenti, tentativo ravvisabile anche nella Proposta di regolamento sull'IA.

In un contesto governato dalla logica dei Big data³⁹, il GDPR ha fornito – anche implicitamente – talune risposte, ma numerosi dubbi sorgono in merito alla compatibilità delle innovazioni digitali rispetto al contenuto del GDPR, ad esempio rispetto all'incapacità per il titolare del trattamento di prevedere i trattamenti attuabili dai sistemi di intelligenza artificiale⁴⁰.

Il legame tra l'impiego dell'intelligenza artificiale e la tutela della *privacy*, come det-

³⁸ C. STOHL-M. STOHL-P.M. LEONARDI, *Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age*, in *International Journal of Communication*, 2016, p. 123 ss.; M. AN-NANY-K. CRAWFORD, *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*, in *New Media & Society*, 2016, p. 1 ss.

³⁹ I Big data si caratterizzano per algoritmi in grado di elaborare infinite variabili in un lasso di tempo molto breve mediante strumenti statistici che permettono di effettuare previsioni comportamentali e di risultato; tali algoritmi si basano su principi deduttivi ed induttivi, associando ai dati personali un modello distributivo, ma questi modelli devono essere correlati ad una serie di coefficienti di affidabilità, che, però, rimangono in parte aleatori. Così, ITMEDIA CONSULTING, *L'economia dei dati. Tendenze di mercato e prospettive di policy*, Roma, 2018, p. 145. Per ulteriori approfondimenti si rinvia a M. DELMASTRO-A. NICITA, *Big data. Come stanno cambiando il nostro mondo*, Bologna, 2019; M. MAGGIOLINO, *I big data e il diritto antitrust*, Milano, 2018; G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Pol. dir.*, 2019, p. 199 ss.; M. OREFICE, *I big data e gli effetti su privacy, trasparenza e iniziativa economica*, Roma, 2018; R.H. WEBER, *Data portability and big data analytics. New competition policy challenges*, in *Conc. e merc.*, 2016, p. 9 ss.; V. ZENO-ZENCOVICH-G. GIANNONE CODIGLIONE, *Ten legal perspectives on "the big data revolution"*, in *Conc. e merc.*, 2016, p. 29 ss.

⁴⁰ G. OLIVI, *Big Data, metadati e Intelligenza Artificiale: i confini tra i diversi diritti*, in *Il Diritto Industriale*, 2020, p. 181 ss.



to, concerne la raccolta su grande scala di dati di varia natura in un arco spazio-temporale estremamente ridotto e se ciò consente di elaborare grandi quantità di dati comporta altresì il rischio che l'interessato ne perda il controllo, anche perché non viene sempre informato in merito alle tecniche impiegate.

Le decisioni automatizzate⁴¹ che si basano sugli algoritmi – come avviene nell'ambito dell'infrastruttura realizzata dalla società – dimostrano quindi le difficoltà di applicare il GDPR.

L'art. 22 sancisce il diritto dell'interessato a “*non essere sottoposto ad 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*”⁴². La disposizione si riferisce al c.d. ADM (*Automated Decision Making*), ossia al processo mediante il quale un sistema informatico adotta una decisione rilevante per i soggetti coinvolti senza alcun intervento umano, basandosi esclusivamente sulla valutazione algoritmica dei dati personali dei soggetti⁴³.

Dunque, la norma non vieta le decisioni automatizzate, ma di assumere decisioni *unicamente*⁴⁴ con sistemi automatizzati, non sancendo invece un divieto generale.

Fra le eccezioni al divieto particolare rilevanza assume l'ipotesi prevista dal comma 2 del citato art. 22 relativa al caso in cui il trattamento sia necessario per la conclusione/esecuzione di un contratto tra il titolare del trattamento e l'interessato o qualora l'interessato abbia prestato il proprio consenso. Questa fattispecie rispecchia l'obiettivo del GDPR di garantire una circolazione dei dati personali che si basi sulla decisione con-

⁴¹ Sull'uso di strumenti automatizzati nell'ambito delle polizze assicurative si rinvia allo studio “The Internet of Things in insurance” (disponibile su www2.deloitte.com/tr/en/pages/financial-services/articles/innovation-in-insurance-internet-of-things-iot.html) dal quale emerge che l'utilizzo di assicurazioni personalizzate che si basano sulla raccolta dati relativi alla guida non solo ridurrebbe i costi connessi al calcolo del rischio assicurativo, ma incentiverebbe l'adozione di comportamenti virtuosi, diminuendo così il numero delle controversie. Sul tema cfr. anche E. BATTELLI, *Big data e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi*, in *Corriere Giuridico*, 2019, p. 1517 ss.

⁴² Non riguardando, dunque, la conservazione o l'organizzazione dei dati.

⁴³ La disposizione in questione è frutto della ricerca di un equilibrio fra l'esigenza di trasparenza e del controllo umano, da una parte, e la necessità di un progresso tecnologico avanzato che garantisca un miglioramento dei processi decisionali, dall'altra. Così E. FALLETTI, *Decisioni automatizzate e diritto alla spiegazione: alcune riflessioni comparatistiche*, cit.

⁴⁴ Sull'avverbio “unicamente” è sorto un dibattito fra coloro che interpretano la norma come necessità di un intervento umano significativo e chi, invece, ritiene che la formulazione comporti una scarsa tutela per gli interessati, esulando dal divieto quelle decisioni che comportano un minimo intervento umano. Sul tema v. E. PELLACCHIA, *Profilazione e decisioni automatizzate al tempo della black box society*, cit., p. 1224 s.



sapevole dell'interessato, ma sembra siano state tralasciate quelle ipotesi in cui dalla mancata adesione al trattamento automatizzato derivi l'impossibilità per l'interessato di usufruire di un servizio, come nel caso *de quo*.

Nella vicenda esaminata dalla Cassazione, infatti, particolarmente dubbia è la clausola contrattuale che, come visto, impedisce ai soggetti che vogliono dare inizio o continuare un rapporto contrattuale con la società nell'ipotesi in cui non aderiscano alla piattaforma e al sistema basato sull'algoritmo. Il profilo affrontato dalla Suprema Corte è quindi parzialmente differente da quello disciplinato dal GDPR, in quanto l'adesione alla piattaforma non è necessaria per la conclusione/esecuzione di un contratto e non può parlarsi di un consenso prestato liberamente, giacché – come visto – la mancata prestazione dello stesso non rappresenta un'alternativa per l'interessato, ma una manifestazione della volontà dello stesso di non proseguire il rapporto contrattuale con la società⁴⁵.

Altrettanta rilevanza assume, poi, il comma 3, il quale prevede una peculiare declinazione del potere di controllo attribuito all'interessato che si sostanzia nel diritto di ottenere l'intervento umano, il c.d. “*a human in the loop*”⁴⁶ e nel diritto di poter contrastare la decisione prodotta dal sistema automatizzato che produce effetti nella sua sfera giuridica e/o privata. A questi diritti consegue ed è al contempo strumentale⁴⁷ quello ad ottenere informazioni sulla logica sottostante il processo decisionale automatizzato e che in questo contesto va inteso in una prospettiva più ampia, ossia non come semplice *informazione*, ma come *conoscenza*⁴⁸ e che si sostanzia nel diritto alla spiegazione.

⁴⁵ Inoltre, pare trattarsi un'eccezione piuttosto rischiosa, considerando che anche un semplice *banner* pare rientrare nell'ambito di applicazione della fattispecie.

⁴⁶ Il dovere del titolare del trattamento di adottare misure appropriate per garantire l'intervento umano viene definito dalla dottrina americana come un “*right to a human decision*”. Così A.Z. HUQ, *A Right to a Human Decision*, in *Virginia Law Review*, 2019; T. WU, *Will Artificial Intelligence Eat the Law? The Rise of Hybrid Social-ordering Systems*, in *Columbia Law Review*, 2019, p. 2023. Il medesimo diritto viene riconosciuto anche dalla Proposta di Regolamento sull'IA. In ambito sanitario ci si riferisce al c.d. *human in command approach*, per cui è necessario che la programmazione iniziale e la scelta finale spettino sempre al chirurgo umano; questo principio si rinviene anche nelle *Raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica* del 16 febbraio 2017, per un approfondimento delle quali cfr. A. AMIDEI, *Robotica intelligente e responsabilità: profili e prospettive nel quadro normativo europeo*, in U. Ruffolo (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2017, p. 63 ss.

⁴⁷ Se la decisione non è compresa non può essere contestata e la possibilità di un intervento umano risulterebbe completamente frustrata. In questi termini R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale. Potere decisionale dell'apparato tecnologico e diritto alla spiegazione automatizzata*, in *Contratto e impresa*, 2019, p. 861 ss.

⁴⁸ *Ibidem*.



Sorgono, dunque, dubbi sull'efficacia di tale diritto, in quanto non sempre si ha la consapevolezza di interagire con gli algoritmi e l'art. 22 non pare statuire un vero e proprio obbligo a carico del titolare del trattamento.

Nella decisione della Corte di Cassazione che qui si commenta emerge questo concetto, in quanto la Suprema Corte afferma esplicitamente che il requisito della consapevolezza non può ritenersi soddisfatto qualora lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restano ignoti o non conoscibili per gli interessati. Perciò, il diritto alla spiegazione racchiude in sé un significato esplicativo delle particolarità che contraddistinguono la tutela dell'interessato rispetto all'impiego degli algoritmi.

Tale diritto, che emerge da una lettura combinata degli artt. 13, 14, 15 e 22 e del considerando 71 del GDPR – l'unico che lo enuncia espressamente – dimostra che la logica sottesa non è di *full disclosure*, ma di comprensione ai fini di tutela. La *ratio* può essere così rinvenuta nella necessità di garantire che l'intelligenza artificiale rimanga strumentale a quella umana⁴⁹, ma la strategia del Legislatore europeo per tutelare l'individuo rispetto ai trattamenti automatizzati non garantisce un concreto ed efficiente potere di controllo sui processi decisionali basati sugli algoritmi⁵⁰.

Il diritto alla spiegazione nel contesto del GDPR si sostanzierebbe, in realtà, non nel diritto di ottenere concretamente una spiegazione sulla decisione automatizzata, in ragione dei tecnicismi sottesi all'algoritmo, incomprensibili per la maggior parte degli interessati, ponendosi come limite cognitivo che rende impossibile un *right to an explanation* assoluto. Riguarderebbe, invece, la possibilità per l'interessato di essere informato in merito alla logica funzionale sottesa al sistema automatizzato, che deve essergli rappre-

⁴⁹ Parte della dottrina si riferisce al diritto di comprendere la macchina come uno strumento per aprire la "scatola nera" degli algoritmi e salvare l'uomo dal rischio di una schiavitù dell'intelligenza artificiale. In questi termini F. PASQUALE, *The Black Box Society: The Secret Algorithms that Control Money and Information*, in *Harvard University Press*, 2015; M. HILDEBRANDT, *The Dawn of a Critical Transparency Right for the Profiling Era*, in *Digital Enlightenment Yearbook*, 2012, a cura di Hildebrandt et al., Amsterdam, 2012.

⁵⁰ Alcuni dottrina ritiene che l'art. 15 del GDPR non sancisca un pieno diritto alla spiegazione, configurandolo propriamente come un *diritto all'informazione*. Così G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, cit., p. 1657 ss. secondo la quale "Non si tratta, infatti, di un diritto alla spiegazione ma di un diritto ad avere informazioni ai sensi dell'art. 15, 1° comma, lett. h), che limita il diritto dell'interessato ad accedere all'informazione concernente «l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, par. 1 e 4, e, almeno in tali casi, (ad ottenere) informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato». Qui si legge una mancata sintonia fra il considerando n. 71 e la norma appena citata, disponendo il primo «il diritto di ottenere l'intervento umano, di esprimere la propria opinione, di ottenere una spiegazione della decisione conseguita dopo tale valutazione e di contestare la decisione»."



sentata prima dell'esecuzione del trattamento⁵¹. Nel caso in esame, quindi, la società non doveva fornire tutte i dettagli tecniche concernenti il funzionamento dell'algoritmo, ma neppure limitarsi ad informare i consociati dell'impiego dello stesso.

Questa prospettiva pare rafforzata dalla lettura dell'art. 13 del GDPR, il quale sancisce un diritto ad ottenere “*informazioni significative sulla logica utilizzata nel trattamento, sull'importanza e le conseguenze previste per la persona*”.

La logica non è imporre un diritto alla spiegazione nella sua interezza, il concetto stesso di consapevolezza muta ineludibilmente e la prospettiva è di una partecipazione dell'interessato, che pone problemi per certi aspetti simili a quelli riscontrati già da tempo rispetto al diritto all'educazione e all'informazione.

Il considerando 71 del GDPR, d'altro canto, nello statuire l'opportunità di non procedere a trattamenti di dati personali mediante decisioni interamente automatizzate, stabilisce che “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.”.

Il diritto alla spiegazione viene così espressamente sancito dalla disposizione e sebbene i considerando, come noto, non abbiano un'efficacia precettiva e non possano essere qualificati come vere e proprie norme giuridiche, ciò non toglie la possibilità che siano impiegati quali regole interpretative. Ne consegue che l'art. 22 e il considerando 71 possono essere ritenuti un valido punto di partenza per rafforzare la prospettiva del *right to an explanation*.

Se, dunque, un diritto alla spiegazione sembra ricavabile dal GDPR, alcuni dubbi sorgono relativamente al profilo temporale.

Come noto, gli artt. 13, 14 e 15 citati sanciscono il diritto dell'interessato all'informazione, che alla luce del *right to an explanation* comporterebbero il diritto di avere informazioni in merito alla logica funzionale sottesa alla decisione automatizzata che precede il trattamento dei dati personali e dunque prima dell'elaborazione degli *outputs* del processo decisionale: in altri termini, il diritto alla spiegazione – così come emerge dall'in-

⁵¹ In questi termini S. WATCHER-B. MITTELSTADT-L. FLORIDI, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, in *International Data Privacy Law*, 2017, p. 19. Gli Autori criticano, tuttavia, la prospettiva del GDPR, in quanto il diritto sancito dalla normativa europea sarebbe differente e più debole rispetto al diritto alla spiegazione: esso non riguarderebbe la decisione concretamente raggiunta quale *output* del processo, non fornendo indicazioni conclusive sulle ragioni della decisione e non consentendo di inferire la razionalità che spiega il risultato concreto della decisione.



interpretazione del GDPR – concerne esclusivamente la fase antecedente alla decisione, per cui una volta che tale decisione è stata adottata dalla macchina l'interessato non avrebbe più un diritto alla spiegazione, ma sarebbe sottoposto ad essa.

Un'effettiva tutela sembra così preclusa in virtù della conoscenza della sola logica funzionale generale del sistema automatizzato e, pertanto, ai fini di tutela dell'interessato, le norme richiamate dovrebbero essere interpretate estensivamente avendo riguardo anche alla fase successiva all'adozione della decisione rispetto ai c.d. dati derivati⁵². Così interpretando, la logica del Legislatore europeo rispetto al trattamento automatizzato dei dati pare essere la medesima che governa l'*accountability*⁵³, ossia di agire in termini di prevenzione del rischio attraverso un'allocatione dello stesso e in termini di riparazione solo in una fase successiva e subordinata⁵⁴. In questo modo il principio di trasparenza e l'esercizio del diritto all'informazione accompagnerebbero ogni fase del processo automatizzato⁵⁵, garantendo una tutela diversificata e maggiormente completa.

Ne consegue che l'interessato ha diritto di conoscere la logica utilizzata nel processo decisionale automatizzato e tale diritto concerne sia una spiegazione *sulla fase antecedente alla decisione, concernente* le modalità di funzionamento del sistema, sia alla fase *successiva*, relativa al *come* e al *perché* del processo decisionale.

In questa logica, la società avrebbe dovuto rendere edotti i soggetti i cui dati personali vengono trattati non solo dell'impiego dell'algoritmo, ma altresì delle modalità con cui esso ha operato.

Anche il Comitato europeo per la protezione dei dati personali si è mosso in questa direzione, ritenendo sussistente un diritto alla spiegazione e sottolineando che il titolare del trattamento deve fornire all'interessato informazioni sufficientemente complete che facciano comprendere gli elementi presi in considerazione nell'ambito del processo decisionale affinché siano chiare le ragioni della decisione, ma senza che ciò implichi una spiegazione complessa degli algoritmi impiegati⁵⁶.

⁵² Il WP29 ha rilevato la peculiare natura dei dati personali, non potendo essere ricondotti né alla categoria dei dati personali osservati sull'interessato, né a quella dei dati raccolti presso l'interessato, né a quelli comunicati da altri e diversi titolari del trattamento. Così ARTICLE 29 DATA PROTECTION WORKING PARTY, *Guidelines on Automated decision-making and Profiling for the purposes of regulation 2016/679*, p. 8.

⁵³ Cfr. A. CERILLO I MARTINEZ, *Accountability delle decisioni algoritmiche*, in *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, a cura di R. Cavallo Perin, cit., p. 61 ss.

⁵⁴ M. GAMBINI, *Algoritmi e sicurezza*, in *Giurisprudenza Italiana*, 1° luglio 2019, p. 1657 ss.

⁵⁵ R. MESSINETTI, *La tutela della persona umana versus l'intelligenza artificiale*, cit.

⁵⁶ *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, p. 28, nelle quali si legge: "La complessità non è una scusa per non fornire informazioni all'in



Escludendo, dunque, le ipotesi in cui il processo decisionale automatizzato non possa essere conosciuto a causa dei c.d. algoritmi non lineari⁵⁷, diversa valutazione richiederà l'ipotesi in cui l'interessato non sia portato a conoscenza del processo decisionale da parte del titolare del trattamento nonostante fosse possibile ricostruire la logica della decisione automatizzata. In questa ipotesi il trattamento dei dati personali deve considerarsi illecito e la decisione automatizzata non può produrre effetti nella sfera giuridica dell'interessato⁵⁸.

A ciò si aggiunga che la *ratio* e la natura dei processi automatizzati rendono difficile tradurre in un linguaggio comprensibile per un "interessato medio" determinate strutture tecniche e, quindi, al fine di garantire la consapevolezza del soggetto interessato, si dovrebbe attuare quanto affermato dal Comitato europeo⁵⁹ e utilizzare un approccio preventivo in cui il titolare del trattamento impieghi metodi chiari ed esaustivi che non comprendano anche la spiegazione matematica sul funzionamento degli algoritmi⁶⁰, ma che contribuiscano a favorire il principio della trasparenza nel trattamento dei dati.

Si tratterebbe, in altre parole, dell'obbligo per il titolare del trattamento di fornire informazioni *significantive*.

In conclusione, la sussistenza di limiti cognitivi e tecnici non può costituire un espe-

teressato. Il considerando 58 afferma che il principio di trasparenza è «particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità sono raccolti dati personali che lo riguardano, quali la pubblicità online».

⁵⁷ Sul tema si rinvia a T.H. CORMEN-C.E. LEISERSON-R.L. RIVEST-C. STEIN, *Introduction to Algorithms*, 3rd ed., Cambridge, MA, 2009.

⁵⁸ Così F. BRAVO, *Trasparenza del codice sorgente e decisioni automatizzate*, *Dir. inf.*, 2020, p. 693 ss., secondo il quale "La soluzione, si noti, è in sintonia con l'assetto delineato dalla Carta dei diritti fondamentali dell'UE, che all'art. 17, par. 2, include tra i diritti fondamentali oggetto di protezione il diritto alla proprietà intellettuale e all'art 52, par. 1, delineando la «Portata dei diritti garantiti», statuisce espressamente che «Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui».

⁵⁹ *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, cit., p. 35.

⁶⁰ Per il Comitato queste informazioni riguarderebbero, ad esempio, le categorie di dati che sono state o saranno utilizzate nella profilazione o nel processo decisionale; i motivi per i quali tali categorie sono considerate pertinenti; le modalità di creazione del profilo utilizzato nel processo decisionale automatizzato, ivi comprese le statistiche utilizzate nell'analisi; i motivi per i quali tale profilo è pertinente per il processo decisionale automatizzato; le modalità di utilizzo del profilo ai fini di una decisione riguardante l'interessato.



diente per ridimensionare l'apparato di tutela, ma anzi deve essere lo stimolo verso l'adozione di misure che rispecchino la logica sottesa al sistema, garantendo la realizzazione di uno sviluppo digitale affidabile che assicuri una partecipazione attiva dell'interessato, il quale deve capire rischi e opportunità delle decisioni automatizzate.

Per tali ragioni si comprende il giudizio della Suprema Corte in ordine all'illegittimità del trattamento dei dati personali effettuato da parte della società, in quanto la non conoscibilità dell'algoritmo ha impedito agli interessati di avere cognizione in merito alle modalità e ai criteri in base ai quali esso operava, tenendo conto del diritto alla spiegazione nei termini suindicati. Se, indubbiamente, la società non era gravata da un obbligo di *disclosure* completa in virtù degli inevitabili tecnicismi, era tuttavia necessario porre gli interessati nella condizione di comprendere e di conoscere il funzionamento dell'algoritmo; ciò altresì considerando che la libertà del consenso risultava pregiudicata dalla clausola relativa al rapporto contrattuale tra consociati e società.

La violazione del principio della trasparenza ha fatto sì che l'interessato non potesse realmente effettuare considerazioni in merito al proprio *rating* reputazionale, demandato esclusivamente ad una decisione automatizzata di cui non è stato spiegato il funzionamento, né dimostrata l'efficacia, venendo così lesi i principi che rendono lecito il trattamento dei dati, non assumendo alcuna rilevanza la valutazione circa l'affidabilità dell'algoritmo.

Ne consegue che un trattamento che condizioni l'autonomia anche negoziale del soggetto⁶¹ e non garantisca il diritto alla spiegazione non può considerarsi lecito. La Suprema Corte ha così portato alla luce una questione fondamentale, ossia che la profilazione tramite algoritmi, potendo limitare i diritti dell'interessato, impone di riconsiderare il ruolo del consenso, il quale può dirsi liberamente prestato soltanto qualora il funzionamento del predetto algoritmo sia conoscibile e, pertanto, solo rispettando il principio della trasparenza e attraverso una concreta attuazione del diritto alla spiegazione è possibile limitare gli effetti negativi di un inevitabile processo di "algoritmizzazione".

⁶¹ Tra l'altro, la revoca del consenso al trattamento era subordinata all'assolvimento di un onere economico rappresentato dal pagamento di una penale e dal risarcimento del maggior danno.