

Consenso, intelligenza artificiale e privacy

Federica Paolucci

Corte di Cassazione, sez. I civile, 25 maggio 2021, n. 14381

In tema di trattamento di dati personali, il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato; ne segue che nel caso di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali di singole persone fisiche o giuridiche, incentrata su un sistema di calcolo con alla base un algoritmo finalizzato a stabilire i punteggi di affidabilità, il requisito di consapevolezza non può considerarsi soddisfatto ove lo schema esecutivo dell'algoritmo e gli elementi di cui si compone restino ignoti o non conoscibili da parte degli interessati.

Sommario

1. Introduzione. – 2. La vicenda. – 3. Il requisito del consenso validamente prestato: tra tradizione e innovazione giuridica. – 4. Riflessioni conclusive

Keywords

consenso - intelligenza artificiale - protezione dei dati personali – privacy – Cassazione

1. Introduzione

Il provvedimento in commento vede la I sezione civile della Corte di Cassazione pronunciarsi con l'ordinanza n.14381/2021 sulla validità del consenso reso dall'utente che non è venuto preventivamente a conoscenza dello schema esecutivo di un algoritmo. Nei fatti di causa del ricorso *de qua* proposto dal Garante per la Protezione dei Dati Personali è altresì rilevante che tale sistema automatizzato veniva impiegato da parte resistente per l'elaborazione di profili reputazionali degli utenti.

Nell'annullare, dunque, la sentenza del Tribunale di Roma, la Corte elabora un importante principio di diritto che non si sofferma solamente sulle criticità legate all'impiego di strumenti algoritmici per la definizione di un rating di persone fisiche e giuridiche. La Corte si focalizza, in particolare, sul requisito della consapevolezza nella concessione del consenso: gli ermellini hanno esaminato l'opacità di cui il presupposto di liceità del trattamento è ammantato nel momento in cui ci si avvale di un algoritmo per la valutazione di dati personali. Molteplici sono le problematiche etiche e di diritto che vengono in rilievo in questa vicenda. Un primo insieme di osservazioni afferisce al tema del consenso, alla sua validità quando raccolto per sottoporre i dati personali dell'interessato a un *ranking* reputazionale tramite un sistema automatizzato e ai neces-

sari *quid pluris* per la formazione di un consenso reso consapevolmente.

In secondo luogo, occorre invece guardare alla conoscibilità dello schema esecutivo dell'algoritmo e la sua comunicabilità agli interessati: un tema che è persino oggetto della Direttiva (UE) 2019/2161 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori¹.

Prima di passare, dunque, all'esame dei fatti di causa occorre sottolineare che se da un lato queste problematiche si inseriscono nel solco di una serie di novelle normative dell'Unione Europea, dall'altro la pronuncia della Cassazione ha offerto uno sguardo al passato. La causa ha, difatti, avuto inizio nel 2016, periodo in cui il Regolamento (UE) 2016/679, noto come General Data Protection Regulation², ancora non era entrato in vigore. Come osservano alcuni commentatori³, la Cassazione ha ivi messo nero su bianco un principio centrale delle nuove norme europee in materia di protezione dei dati personali e di *governance* dell'intelligenza artificiale pur applicando la disciplina previgente.

2. La vicenda

Con provvedimento n. 488 del 24 novembre 2016⁴, l'Autorità garante per la protezione di dati personali aveva considerato la piattaforma illecita a causa della forte incidenza del servizio sulla dignità dei soggetti interessati. Dalle documentazioni al tempo offerte in comunicazione all'Autorità da parte dell'Associazione Mevaluate Onlus, titolare del trattamento⁵, si evince che il peculiare modello di business in oggetto è costituito da una piattaforma web (e correlato *database*) e viene descritto come "Infrastruttura Immateriale Mevaluate per la Qualificazione Reputazionale" gestita da Mevaluate Holding Ltd., Mevaluate Italia s.r.l. e Associazione Mevaluate Onlus⁶. Tale piattaforma consta di un sistema di raccolta, verifica, ed elaborazione di dati personali e una successiva fase di assegnazione di «indicatori alfanumerici asseritamente in grado di misurare l'affidabilità reputazionale dei soggetti censiti (persone fisiche e giuridiche)»⁷.

Per ovvie ragioni, l'Autorità si è soffermata sugli aspetti che riguardano esclusivamente gli individui e ha riscontrato delle criticità con riferimento all'erogazione di un siffatto servizio che ha delle ripercussioni sulla rappresentazione economica di una pletera di soggetti, siano essi clienti, dipendenti, o candidati a vario titolo per una qualche posi-

¹ Di qui in avanti, Direttiva Omnibus.

² Di qui in avanti, GDPR.

³ G. Scorza, *L'algoritmo deve essere trasparente, la Cassazione rilancia il GDPR*, in *Agenda Digitale*, 26 maggio 2021.

⁴ [Registro dei provvedimenti n. 488 del 24 novembre 2016](#), Autorità garante per la protezione dei dati personali.

⁵ Si veda punto 1.8 del provvedimento n. 488/2016 dell'Autorità.

⁶ Si veda punto 2.1 del citato provvedimento.

⁷ Cfr nota n. 6.

zione. Come osserva il Garante, dal momento in cui tali effetti si ripercuotono pesantemente non solo nella vita professionale, bensì (e soprattutto) nella vita privata degli interessati, «occorre, pertanto, estrema cautela nell'affrontare tematiche così delicate, anche in considerazione del fatto che la “reputazione” che si vorrebbe qui misurare, in quanto strettamente correlata alla considerazione delle persone e alla loro stessa “proiezione” sociale, risulta intimamente connessa con la loro dignità, elemento cardine della disciplina di protezione dei dati personali»⁸.

L'Autorità, alla luce di queste considerazioni, aveva disposto, *ex art.* 154, c. 1, lett. *d*) del d.lgs. 196/2003⁹, il divieto di qualunque operazione di trattamento dei dati personali (presente e futura) effettuata dall'Associazione nell'ambito, precedentemente individuato, della “Infrastruttura Immateriale Mevalute per la Qualificazione Professionale”.

L'Associazione adiva il Tribunale di Roma chiedendo l'annullamento del provvedimento. Con parziale accoglimento del ricorso, il giudice di merito accoglieva l'istanza di parte ricorrente facendo salva la portata del provvedimento solamente per un particolare ambito del servizio: il c.d. “Profilo Contro”, ovvero sia soggetti terzi non associati a Mevalute Onlus. A prescindere dalle osservazioni in punto di diritto, ciò che, secondo la valutazione della Corte di Cassazione sconcerta è la motivazione addotta dal giudice di merito. Quest'ultima è stata basata sull'autonomia privata di organizzare sistemi di accreditamento di soggetti, mancando di valutare la *condicio sine qua non* del servizio stesso: la validità del consenso e la conseguente liceità del trattamento. Il Tribunale di merito soffermandosi sulla valutazione del modello di business di questa “Pizia contemporanea”, ha mancato di centrare il punto provocando un cortocircuito logico-giuridico che la Cassazione ha risolto con l'ordinanza in commento. Il problema, difatti, è da rinvenirsi nella scarsa trasparenza dell'algorithm impiegato. Tale aspetto non riguarda semplicemente «il momento valutativo del procedimento»¹⁰ e, dunque, la bontà del servizio offerto, ma la liceità stessa di un servizio che sfrutta una base giuridica viziata. Ricorrendo, *mutatis mutandis*, a una metafora cara ai giudici d'oltreoceano, il punto in discussione non è da ricondursi al *free marketplace of ideas*¹¹ e il fatto che il mercato stesso farebbe prevalere i migliori servizi a scapito di quelli deficitari. La sostanza del discorso è costituita «dalla validità - per l'appunto - del consenso che si assume prestato al momento dell'adesione»¹². Nel dettare, dunque il principio di diritto precedentemente richiamato, la Supreme Corte cassa la sentenza del Tribunale di Roma ed osserva che non può desumersi il consenso dalla semplice adesione dell'utente ad una piattaforma: tale modalità non costituisce accettazione di un sistema automatizzato per la valutazione di dati personali laddove l'utente non sia venuto a conoscenza dello

⁸ Punto 2.2 del provvedimento in esame.

⁹ Decreto legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, pubblicato nella *Gazzetta Ufficiale* n. 174 del 29 luglio 2003.

¹⁰ Sentenza del Tribunale di Roma, così come citata Corte di Cassazione, sez. I civile, ordinanza n. 14381/21, depositata il 25 maggio). Cit. al punto VII, 7.

¹¹ Teoria che anche quando applicata nel suo campo di indagine tradizionale, la libertà di parola, necessita di ripensamenti e aggiustamenti, come osserva O. Pollicino, *La prospettiva costituzionale sulla libertà di espressione nell'era di Internet*, in *questa Rivista*, 1, 2018, 31 ss.

¹² *Ivi*, nt. 8.

schema esecutivo dell'algoritmo.

3. Il requisito del consenso validamente prestato: tra tradizione e innovazione giuridica

Quando si parla di consenso per gli addetti ai lavori è automatico pensare, da tre anni a questa parte, al GDPR. Dovendo, tuttavia, guardare alla normativa previgente, ovvero, sul piano comunitario, la direttiva 95/46/CE¹³, possiamo notare come il Regolamento non abbia stravolto la concezione di consenso. Difatti, l'art. 6 inserisce, come è logico, il consenso tra i presupposti di liceità del trattamento¹⁴ e nel far ciò ricalca quanto era già previsto, sul piano nazionale, dal d.lgs. 196/2003¹⁵: il Codice Privacy. Sebbene, dunque, non sia l'unica base giuridica, il consenso è tradizionalmente¹⁶ considerato il principale perno dell'intera disciplina della protezione dei dati personali¹⁷. Ai fini della liceità del trattamento, esso deve essere comunicato ma, secondo le previsioni del d.lgs. 196/2003, soprattutto, deve essere validamente prestato¹⁸. Nel definire tale criterio, l'art. 23 dispone che il trattamento di dati personali è ammesso solo nei seguenti casi:

- il consenso dell'interessato deve essere espresso;
- questo può riguardare l'intero trattamento o operazioni singole;
- è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'art. 13¹⁹;
- il consenso deve rispettare la forma scritta *ad substantiam* quando trattasi di dati sensibili.

La Corte nell'ordinanza in commento osserva, inoltre, che il consenso può dirsi validamente prestato solo quando il trattamento viene "chiaramente individuato": «ben

¹³ Il riferimento è alla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

¹⁴ Come osserva R. Panetta, *Consenso o non consenso? Ecco cosa cambia con il GDPR*, in *Corriere Comunicazioni*, 16 aprile 2018, il GDPR ricalca taluni aspetti già presenti nel Codice, quali la necessità che il consenso sia libero, specifico, informato e manifesto. È opportuno sottolineare, anche alla luce della vicenda in esame, che il consenso non è né l'unica né la principale base giuridica del trattamento, dovendo di contro considerare l'ossequio ad obblighi di legge o in adempimento ad un contratto quali i sistemi maggiormente in applicazione tra soggetti pubblici o privati.

¹⁵ Si veda nota n.9.

¹⁶ Si veda M. C. Meneghetti, *Consenso bis: la Corte di giustizia torna sui requisiti di un valido consenso privacy*, in *questa Rivista*, 1, 2021, 266 ss

¹⁷ Si richiamano in tal senso gli studi di Stefano Rodotà, il quale considerava il consenso la massima espressione del controllo da parte dell'individuo sulle proprie informazioni. Un principio che, del resto, ha tradizionalmente ispirato gli stessi padri della privacy, Warren e Brandeis. Si veda, pertanto con riferimento ai concetti richiamati S. Rodotà, *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Bari, 2004; S. D. Warren-L. Brandeis, *The Right to Privacy*, in *Harvard Law Review* 4(5), 1890, 193 ss.

¹⁸ Requisito da desumere anche dalla giurisprudenza della Corte richiamata anche nell'ordinanza in esame. *Ex multis*, Cass. civ., sez. I, 11 maggio 2018, n. 17278; Cass. civ., sez. I civ., 22 marzo 2018, n. 16358.

¹⁹ Articolo che si riferisce all'informativa.

definito nei suoi elementi essenziali»²⁰. Nel caso in esame il titolare del trattamento poneva alla base della raccolta del consenso una semplice adesione volontaria ai «valori della community»²¹: dunque, l'adesione dell'utente alla piattaforma. In che modalità il titolare del trattamento può sincerarsi del fatto che la scelta è stata effettuata in maniera ponderata, informata, libera, consapevole? Il Gruppo di lavoro Articolo 29 risponde a questa domanda dicendo che il consenso è libero quando «l'interessato [ha effettuato] una scelta effettiva e il controllo sui propri dati»²². E il controllo sui propri dati passa (soprattutto) attraverso la consapevolezza delle finalità per le quali sia stato validamente prestato. Il problema che viene ivi in rilievo è che dall'adesione dell'utente ad una piattaforma non può desumersi l'accettazione di ulteriori finalità del trattamento quali la determinazione automatizzata del suo profilo reputazionale²³. Posto che secondo la disciplina del GDPR tale attività sarebbe critica tanto per i dati oggetto del trattamento, quali, ad esempio, *ex art. 10*²⁴ afferenti a condanne penali (in quanto l'Associazione sottoporrebbe ad analisi algoritmica anche i casellari giudiziari), quanto per i rimedi, *ex art. 22.1* del GDPR, la Corte, sebbene non applichi le richiamate norme, si allinea sostanzialmente ad esse. Difatti, gli ermellini, stabilendo il nuovo principio di diritto, hanno posto la conoscibilità dello «schema esecutivo dell'algoritmo»²⁵ da parte dell'utente come elemento per rendere il consenso validamente prestato. Pertanto, consenso, trasparenza e *accountability* si riconfermano i nodi focali dell'intera disciplina della protezione dei dati personali.

4. Riflessioni conclusive

Nell'ordinanza in commento la Corte si è, da un lato, pronunciata sulla validità del consenso e, dall'altro, sulla liceità del trattamento. Un terzo ordine di domande riguarda, invece, un problema che è rimasto a latere della vicenda giurisprudenziale. Sebbene i giudici tanto di merito quanto di Cassazione, nel rispetto del principio della domanda, non si siano soffermati sul punto, la vicenda in esame fa sorgere diversi quesiti circa la necessità di operare un design chirurgico di tali sistemi algoritmico-reputazionali che siano affidabili, etici e rispettosi dei diritti degli interessati. In secondo luogo, occorre chiedersi: la generalità dei consociati è in grado di comprendere, anche se menzionati

²⁰ Si veda punto VI, 6, dell'ordinanza.

²¹ Si veda punto 1.5 del provvedimento del Garante.

²² Gruppo di lavoro Articolo 29, Linee guida sul consenso ai sensi del regolamento (UE) 2016/679.

²³ «Le informazioni e i documenti caricati dagli aderenti, infatti, verrebbero raccolti, verificati e resi disponibili agli altri utenti della piattaforma, unitamente ai relativi profili reputazionali, solo a seguito della preventiva raccolta del consenso da parte degli interessati, che “coprirebbe” anche le successive operazioni di trattamento effettuate da terzi (visualizzazione, estrazione e riutilizzo dei dati e dei documenti); il medesimo consenso, inoltre, verrebbe acquisito per giustificare eventuali operazioni di trattamento collegate a presunte “irregolarità” documentali segnalate da altri, nonché per pubblicare atti e documenti attinenti a controversie giudiziarie pendenti o future», citazione dal provvedimento del Garante, punto 1.5.

²⁴ Cfr punto 1.3 del provvedimento del Garante.

²⁵ Punto VI, 6, dell'ordinanza.

nell'informativa, gli elementi essenziali che caratterizzano lo schema esecutivo dell'algoritmo?

Con riferimento al primo aspetto e senza l'intenzione di sviscerare le questioni etiche prima che giuridiche dell'impiego di tali strumenti, come ribadisce la bozza di Regolamento dell'intelligenza artificiale recentemente pubblicata, devono essere definiti dei limiti nell'implementazione di strumenti automatici che si sostituiscono al giudizio umano e che hanno delle conseguenze legali e sociali nella vita degli individui. Tuttavia, come osserva il noto saggista Frank Pasquale²⁶, esistono sempre più meccanismi in grado di contraffare l'esperienza umana e non è logico attendere la consacrazione creazione di un limite al momento della formazione del consenso. Ciò non solo per mancanza di competenze da parte degli stessi utenti, come si vedrà in seguito, ma anche perché è da ripensare il legame tra limiti giuridico-etici e tecnologia, affidando a quest'ultima, e sin dalla sua programmazione, la interiorizzazione dei primi. Tale necessità si manifesta dal momento in cui la trasparenza dell'algoritmo non può essere considerata una panacea, come sostengono anche taluni commentatori²⁷. Una criticità questa che appare impellente sia con riferimento alla vicenda in esame sia alla luce della disciplina dell'art. 22 del GDPR ove la vaghezza della norma non protegge adeguatamente gli interessi degli individui. Difatti, come osservano Simoncini e Suweis²⁸, il punto cruciale è che, pur ammettendo di essere di fronte ad un algoritmo conoscibile e comprensibile e sempre che questo non rappresenti la motivazione esclusiva della decisione, l'algoritmo può essere di per sé discriminatorio e, quindi, incostituzionale.

Per quanto concerne il secondo aspetto, come si accennava all'inizio, l'Unione Europea si sta già muovendo nella direzione di rendere gli utenti-consumatori consapevoli del funzionamento dell'algoritmo. Una scelta normativa che si può rintracciare tanto nella Direttiva Omnibus, lato persone fisiche, quanto nel c.d. Regolamento P2B, lato persone giuridiche²⁹. Tali previsioni normative si scontrano però con una triste realtà dei fatti: secondo i risultati del Rapporto Annuale 2020 dell'Istituto Nazionale di Statistica (ISTAT), in termini di *digital divide* l'Italia è ancora in una posizione di svantaggio rispetto agli altri paesi avanzati³⁰. In una società, dunque, scarsamente provvista di competenze tecnologiche e caratterizzata dal fenomeno "accetta e continua"³¹, il consenso non risulta essere più una base giuridica affidabile. Le prossime sfide per il diritto (e non solo) dovranno essere, dunque, trainate dalla attualizzazione delle norme alle novità tecnologiche, tenendo necessariamente conto della realizzazione di nuovi rimedi e sistemi per rendere effettivo il requisito (imprescindibile) della trasparenza: il rischio è, altrimenti, di imporre rigidi meccanismi di *compliance* alle persone giuridiche

²⁶ F. Pasquale, *New Laws of Robotics*, Cambridge MA, 2020.

²⁷ L. Edwards-M. Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, in *Duke Law & Technology Review*, 16, 2017, 18 ss.

²⁸ A. Simoncini-S. Suweis, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1, 2019, 87 ss.

²⁹ Regolamento (UE) 2019/1150 ("Regolamento P2B").

³⁰ Si veda il *Rapporto annuale 2020. La situazione del Paese*, Istat, 3 luglio 2020.

³¹ G. Scorza, *Sulle regole AI l'Europa pone la prima pietra, ma sarà sfida enorme: ecco perché*, in *Agenda Digitale*, 23 aprile 2021.

Note a sentenza

e dimenticarsi di educare al contempo le persone fisiche per renderle fattivamente in controllo dei propri dati personali.