

Digito ergo sum: la tutela giuridica della persona dagli algoritmi*

di Pasquale Serrao D'Aquino
magistrato addetto all'Ufficio Studi del Csm

L'accesso al *Web* è un diritto fondamentale. Il suo rovescio è la scia informatica che ogni persona lascia inconsapevolmente nella rete. L'identità digitale di ciascuno viene analizzata sistematicamente dagli algoritmi dei motori di ricerca.

Pseudonomizzazione, diritto all'oblio, deindicizzazione e altri strumenti di tutela europea dei dati personali (reg. n. 679/2016/UE) non eliminano i rischi di una nuova Sorveglianza partecipativa; anzi è in gestazione una inquietante *Giustizia predittiva*.

SOMMARIO: 1. *Digito ergo sum* – 2. Accedo e mi accedono – 3. Identità personale e identità digitale 3.1. Identità digitale come plurale 3.2. Disambiguare, misurare, identificare – 4. Essere profilato – 5. Analizzare, predire, sorvegliare – 6. Oblio e deindicizzazione – 7. Altre tutele – 8. *Account* commemorativi – 9. La sentenza dell'Automa e il diritto ad una decisione Umana – 10. Scenari

1. *Digito ergo sum*

Appena sveglio, mi cattura una sequenza di nuove abitudini, rapidamente stratificatesi. Accendo lo *smartphone*; scorro la rassegna stampa dei giornali; controllo il mio profilo *Facebook*; ascolto la musica con *Spotify*. Clicco sulla pubblicità personalizzata. Corro e vado al lavoro.

Non ho ancora parlato né scritto. I vicini mi ignorano. La mia identità personale è inalterata; la mia *privacy* appare inattaccata.

Eppure in questo breve inizio della mia giornata, io già sono, non solo per me stesso, ma *per* il mondo intero. La scia telematica dei miei dati personali è intorno a me, si muove con me e oltre me: *digito ergo sum*.

Il mio profilo sui *social network*, le mie preferenze di lettura o musicali, di acquisto, la geolocalizzazione permanente, i miei contatti personali e la trama delle loro interconnessioni disegnano la mia *identità digitale*. Il mio *Io digitale* agisce ed è agito: si arricchisce e si trasforma man mano che la giornata scorre grazie ai miei *microchip* costantemente attivi.

2. Accedo e mi accedono

Ho il mondo intero a distanza di un *click*: aggiungo lettera dopo lettera nel campo di ricerca del mio *search engine*, limitando in frazioni di secondo le mie direttrici di interesse sociale e politico: una libertà di ricerca infinita.

Dimentico con superficiale leggerezza che per accedere ho consentito accesso pieno ai miei dati personali. Il motore di ricerca ne è il padrone: li acquisisce, li condivide, li vende. I miei dati

sensibili finiscono in mani ignote, per finalità incomprensibili. Persone, *robot*, algoritmi, luoghi sconosciuti.

Anche se sono fermo e in silenzio, qualcuno o qualcosa continua a scegliere per me cosa mi interessa e chi desidero conoscere. Sono condizionato, delimitato, modellato.

Impotente non cancello la mia scia digitale. La pubblicità comportamentale (*behavioural advertising*) la segue costantemente, suggerendomi e anticipandomi cosa e da chi comprare, dove e cosa leggere, vedere o sentire. L'unico campanello di allarme che si accende nella mia testa sono gli annunci mirati che mi arrivano coerenti con la direzione della mia navigazione.

2.1. Accedo come diritto fondamentale

«Tutti hanno *eguale diritto* di accedere alla rete Internet, in condizione di parità, con modalità tecnologicamente adeguate e che rimuovano ogni ostacolo di ordine economico e sociale. La legge stabilisce provvedimenti adeguati a prevenire le violazioni dei diritti di cui al Titolo I della parte I» avrebbe recitato l'art. 21-*bis* della Costituzione proposto da Stefano Rodotà[1].

Questa riforma costituzionale, mai messa in cantiere è necessaria?

Il diritto di accesso alla Rete è costituzionalmente garantito come proiezione diretta delle libertà costituzionali già riconosciute: manifestazione del pensiero, garantita «con ogni altro mezzo di comunicazione», istruzione, cultura, religione; necessità tutte per il pieno sviluppo della personalità.

Prestiamo però attenzione, nella norma proposta, non al diritto ma, come si usa dire tra giuristi, al *quomodo* dell'accesso: la riforma proposta invoca *uguaglianza* ed *adeguatezza* dell'accesso.

Il Regolamento europeo del 25 novembre 2015[2], che stabilisce il diritto all'accesso ad Internet[3], ha come scopo quello di garantire la *neutralità* della Rete nel territorio dell'Unione, ma il primo considerando del regolamento opportunamente annuncia: «Il presente regolamento mira a definire norme comuni per garantire un *trattamento equo e non discriminatorio* del traffico nella fornitura di servizi di accesso a Internet e tutelare i relativi diritti degli utenti finali».

La Dichiarazione dei diritti di Internet, elaborata dalla Commissione della Camera per i diritti e i doveri in Internet, prevede che:

«1. L'accesso ad Internet è diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale.

2. Ogni persona ha eguale diritto di accedere a Internet in condizioni di parità, con modalità tecnologicamente adeguate e aggiornate che rimuovano ogni ostacolo di ordine economico e sociale»[4].

Si tratta, a mio avviso, di norme non costitutive del diritto di accesso, non solo perché i diritti fondamentali riconosciuti già offrono completa copertura costituzionale alla libertà di accesso, ma anche perché l'accesso alla Rete può agevolmente fondarsi sul principio del pieno sviluppo della persona umana e sul catalogo aperto dei diritti fondamentali garantito dagli articoli 2 e 3 della Costituzione[5]. La funzione di tali innovazioni, quindi, è rafforzativa di un diritto già esistente, favorendone la sua garanzia giuridica sia con la sua esplicitazione sia combinando declinando l'accesso alla rete secondo il principio di uguaglianza sostanziale di libertà dei mezzi.

3. Identità personale e identità digitale

L'ordinamento tutela da un quarantennio il mio «patrimonio intellettuale, politico o sociale»; il suo *travisamento* è violazione del mio diritto all'identità personale, protetto dall'art. 2 Cost., anche in assenza di una lesione del diritto all'onore o alla dignità.

Internet è campo aperto di espressione della mia identità personale, distinta tanto dal nome quanto dalla reputazione, perché «formula sintetica per contraddistinguere il soggetto da un punto di vista globale nella molteplicità delle sue caratteristiche e manifestazioni»[6].

Ma l'identità digitale non è la semplice traslazione nel mondo dei *byte* di quella reale; non si riduce solo ad una nuova dimensione per diritti già riconosciuti. «La persona digitale è un modello di personalità individuale pubblica basato su dati e mantenuto da transazioni, destinato ad essere utilizzato su delega dell'individuo»[7].

3.1. Identità digitale come plurale

L'identità digitale è qualcosa di più ristretto rispetto all'identità personale, perché non prevede tutte le espressioni di vita reale, ma solo quelle tracciate e modellate dalla rete, ma è anche qualcosa di più ampio, perché riguarda, oltre che la proiezione nel *Web* del patrimonio di idee e azioni della persona, anche ulteriori aspetti specifici della dimensione informatica: l'identificazione della persona mediante lo SPID (Sistema pubblico di identità digitale), dati biometrici, abitudini di spostamento, di acquisto, di lettura, reputazione.

L'identità digitale è un insieme di dati personali che delinea una persona, non solo per quello che dice e quello che fa fuori e dentro la rete, anche e soprattutto per la traccia informatica che lascia tanto scientemente con la navigazione informatica quanto inconsapevolmente mantenendo i propri *chip* attivi.

3.2. Disambiguare, misurare, identificare

Il mio nome nella Rete è disambiguato, preferito, postergato, collegato.

L'associazione mi collega a fatti, persone e notizie; la disambiguazione delinea la mia unicità; l'ordine di ricerca e il numero di risultati determinano la mia conoscenza digitale e da questa quella personale.

Posso misurare quantitativamente la rilevanza della mia personalità digitale e ambire ad incrementarla: *like* sulle mie dichiarazioni, articoli, scelte letterarie, sportive, sulle foto, *retweet* dei miei cinguettii la modellano e la misurano.

La persona reale emerge nel mondo digitale.

Posso, al contrario, svincolare il mio *Io digitale* dal mio agire reale. Agisco con uno o più *nickname*; coltivo il mio *avatar*. La mia identità digitale prende una strada diversa dalla mia identità personale. Uso lo pseudonimo come una barriera tra la mia persona e il mio agire telematico.

Sono ormai l'uno e l'altro. Scelgo il mio nome digitale per celarmi o, all'opposto, per disgelarmi senza la zavorra della mia identità reale.

Lo pseudonimo non è più appannaggio elitario dell'artista, ma diviene uno strumento di massa per occultarsi, maldestramente o efficacemente, al controllo della Rete o, al contrario, per affermarsi nel mondo virtuale, rendendolo autonomo dal proprio vissuto reale.

La legge tutela, oltre che il nome, anche il mio pseudonimo (art. 9). La persona può chiedere tutela al giudice quando le sia contestato «il diritto all'uso del proprio nome» oppure «possa risentire pregiudizio dall'uso che altri indebitamente domandando la cessazione del fatto lesivo e il risarcimento dei danni» (art. 7 cc)[8]. Ne beneficia necessariamente anche il *nickname*[9].

Più articolate sono i possibili strumenti di tutela dello SPID. Tale strumento mi permette di accedere a tutti i servizi online della Pubblica amministrazione con un'unica Identità Digitale (*username e password*) utilizzabile da computer, *tablet* e *smartphone*. Si tratta del mio nome digitale.

4. Essere profilato [10]

Ricorre nell'ordinamento come participio passato, e non come sostantivo maschile.

Il Regolamento europeo 679/2016 descrive di cosa si tratta: «profilazione» è «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica»[11].

Già nel 1981 il legislatore europeo[12] aveva realizzato i pericoli della circolazione dei dati sulla persona e la necessità di un equilibrio con la libertà di informazione, facendone materia di convenzione antesignana, fornendo la nozione di “elaborazione automatizzata” che «comprende le seguenti operazioni effettuate nel loro insieme o in parte grazie a procedimenti automatizzati: registrazione di dati, applicazione ad essi di operazioni logiche e/o aritmetiche, loro modifica, cancellazione, estrazione o diffusione». L'elaborazione dei diritti di *privacy* è quindi remota: qualità dei dati[13], tutela rafforzata dei *dati sensibili*[14], sicurezza[15], conoscenza, rettifica, cancellazione[16]. L'Europa mi protegge: «La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale», recita l'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea[17].

L'elaborazione di nuove tutele è in corso, ma richiede tempo: «Ogni persona ha diritto alla rappresentazione integrale e aggiornata della propria identità in Rete. La sua definizione riguarda la libera costruzione della personalità e non può essere sottratta all'intervento e alla conoscenza dell'interessato. L'uso di algoritmi e di tecniche probabilistiche deve essere portato a conoscenza delle persone interessate, che in ogni caso possono opporsi alla costruzione e alla diffusione di profili che le riguardano»[18].

Il motore di ricerca, indiscusso *profilatore seriale*, sostiene di essere un inconsapevole trasportatore di dati, immessi nella rete dai padroni dei domini e offerti al pubblico dai suoi algoritmi, senza alcuna possibile selezione mediante intervento umano.

Il *Gigante* si nasconde grottescamente dallo sguardo del giudice dietro lo stelo di un fiammifero.

Ma i *search engines* non sono solo inconsapevoli trasportatori di dati (*mere conduit*). La Corte di giustizia[19] è chiara: Google è *responsabile del trattamento dei dati*, come il titolare del sito

Internet che li custodisce «estrae», «registra» e «organizza» dati personali secondo la Direttiva 95/46/CE e consente a qualsiasi utente di Internet, allorché effettua una ricerca a partire dal nome di una persona fisica, «di ottenere, mediante l'elenco di risultati, una visione complessiva strutturata delle informazioni relative a questa persona su Internet».

5. Analizzare, predire e sorvegliare

Sono diventato *homo digitalis*. Intuisco appena quale sia il prezzo del mio accesso gratuito: soggettivarmi come acquirente di beni e idee, oggettivarmi perché si alieni il mio profilo, secondo le necessità commerciali o politiche dell'impresa digitale.

Con il motore abbiamo un contratto commutativo a titolo gratuito. Conosco la prestazione che ricevo, intuisco quella che eseguo. Mi illudo che si tratti di un comodo *non facio ut des*.

“Profilare la persona” è un obbligo secondo le direttive europee Mifid a tutela dell'investitore per valutare l'adeguatezza delle operazioni che gli sono proposte. La profilatura dell'identità digitale della persona, invece, nasconde pericoli più gravi ed insidiosi di acquisti di prodotti finanziari inadeguati rispetto alla sua esperienza finanziaria. Il legislatore europeo lancia un chiaro avvertimento. Torniamo alla descrizione dell'art. 22: la profilatura non è trattamento automatizzato di dati personali fine a sé stesso, ma ha lo scopo di *analizzare o prevedere* aspetti della persona «riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

L'analisi del trattamento automatizzato è, in pratica, prognosi sul mio futuro: capirmi e anticipare le mie abitudini e preferenze personali sembra quasi innocuo; rendimento professionale, affidabilità, comportamenti, salute, spostamenti, appare, invece, subito inquietante.

Comprendo ora il prezzo dello scambio gratuito tra il mio accesso alla rete e l'accesso della rete alla mia persona: nell'immediato vi partecipo, ma la consegna dei miei dati può condannarmi alla futura esclusione da notizie, lavori, relazioni, da opportunità necessarie di vita.

Qualcuno ora mi *include*, ma solo selettivamente e a mia insaputa; sceglie cosa può essermi proposto (notizie, merci, arte, conoscenze, opportunità, e a cosa e a chi non potrò accedere). Qualcun altro decide, invece, l'altro lato della medaglia: a cosa non posso accedere, nella rete e nella vita reale; mi *esclude*, analizzando il mio profilo e prevedendo i miei comportamenti: incidenti di *social networking*; ancor di più le mie abitudini di acquisto, di pensiero, di frequentazione, ma mia identità digitale, poco conosciuta dalle persone a me vicine, compiutamente analizzata da quelle lontane.

Analizzare, predire, condizionare, includere ed escludere: tratti fondamentali di ogni tipo di controllo politico e sociale. Narcisismo e consumismo nel *Web* sono motori fondamentali della nuova *sorveglianza partecipativa*[20], basata sul piacere dell'accesso agli sterminati contenuti della rete.

Masse quasi infinite di dati sono accumulate per scopi attuali e futuri, ancora da elaborare. Ciascuno si costruisce una storia digitale che riguarda l'intera persona e che, ad un certo punto, diventa strumento per discriminarla o, in momenti di crisi democratica, per privarla di parte dei suoi diritti inviolabili.

Furti massivi di dati personali, come quello avvenuto recentemente da parte di Uber, pressioni sui loro grandi accumulatori (ancora una volta i motori e i *social network*) da parte di governi autoritari sono spie dei futuri pericoli.

6. Oblio e deindicizzazione

Qualcuno scrive di me. Traccia la mia identità digitale. I *web spiders* del motore di ricerca lo analizzano e mi associano a fatti, notizie, persone.

Il mio patrimonio sociale si compone di una moltitudine di momenti di vita che diventano presto inattuali, almeno per me; vorrei ripudiarli, ma sono scolpiti nel *cyberspazio*.

I *search engines* propongono sistematicamente porzioni della mia vita personale che non rivestono più rilevanza. Reputazione e identità personale sono coinvolte. Gli algoritmi dei motori di ricerca tessono la rete e collegano e associano abilmente nomi ed eventi-notizie. Il trascorrere del tempo gli è ignoto.

Porzioni di identità personale a cui è stato dato legittimo risalto non sono più custodite in innocui luoghi polverosi e inaccessibili, ma sono accessibili all'istante.

Non lo voglio. Non sono una persona pubblica. Rivendico il mio diritto *to be let alone*: essere dimenticato nel *Web* e dal *Web*. Meglio ancora, voglio far dimenticare non tutto me stesso, ma parti della mia vita che ritengo superate; trasformare ed evolvere la mia identità sociale e digitale. Si tratta di una legittima aspirazione, pregiudicata non tanto dall'esistenza in indistinti punti cardinali del *Web* (siti, *chat*, *social network*) delle notizie che mi riguardano, ma dalla quantità e qualità e *immediatezza* dell'accedervi universale.

Il trattamento svolto dai gestori dei motori di ricerca si sostanzia in una attività di organizzazione e aggregazione delle informazioni già pubblicate dagli editori di siti *web*, che rende accessibili agli utenti Internet una quantità maggiore di dati, e in forma strutturata. Tale trattamento riveste pertanto, *carattere distinto e ulteriore rispetto all'attività svolta da tali editori* e, laddove incida «in modo significativo e in aggiunta all'attività degli editori di siti *web*, sui diritti fondamentali alla vita privata e alla protezione dei dati personali», il gestore del motore di ricerca è tenuto a rispettare le prescrizioni della direttiva (par. 38) come responsabile del trattamento dei dati[21].

Per la Corte di giustizia anche Google tratta i dati ed è, quindi, “responsabile dei dati” secondo la direttiva 1995/46. «Occorre constatare che, esplorando Internet in modo automatizzato, costante e sistematico alla ricerca delle informazioni ivi pubblicate, il gestore di un motore di ricerca “raccolge” dati siffatti, che egli “estrae”, “registra” e “organizza” successivamente nell'ambito dei suoi programmi di indicizzazione, «conserva» nei suoi *server* e, eventualmente, “comunica” e “mette a disposizione” dei propri utenti sotto forma di elenchi dei risultati delle loro ricerche. Poiché tali operazioni sono contemplate in maniera esplicita e incondizionata all'articolo 2, lettera b), della direttiva 95/46, esse devono essere qualificate come “trattamento” ai sensi di tale disposizione, senza che rilevi il fatto che il gestore del motore di ricerca applichi le medesime operazioni anche ad altri tipi di informazioni e non distingua tra queste e i dati personali».

Il mio diritto è giustiziabile con l'ordine amministrativo o giudiziale di sopprimere dall'elenco dei risultati della ricerca i link verso le pagine *web* pubblicate da terzi e che contengono informazioni sulla mia persona[22]. Intervenire solo sulla testata giornalistica, per la facilità di riproduzione delle informazioni contenute nell'articolo in altri siti *web* non può bastare[23] e potrebbe non essere corretto[24].

Non è necessario che sia danneggiato: il diritto alla cancellazione non sussiste soltanto quando l'inclusione dell'informazione arreca un pregiudizio all'interessato, ma anche quando, al momento

in cui viene chiesta la cancellazione, non vi è più una giustificazione idonea a legittimare la continua accessibilità dei dati personali[25].

Il gestore è tenuto alla cancellazione dei *link* anche nel caso in cui le informazioni a cui questi conducono non vengano previamente o simultaneamente cancellati dalle pagine *web*, e ciò eventualmente anche quando la loro pubblicazione su tali pagine *web* sia di per sé lecita: la testata potrebbe beneficiare di una delle deroghe previste dalla direttiva, quale ad esempio quella di cui all'art. 9, relativa alla pubblicazione effettuata «esclusivamente a scopi giornalistici» (par. 85). Inoltre, la direttiva potrebbe non trovare applicazione all'autore della pubblicazione per ragioni territoriali (par. 84). Facilitando l'accesso degli utenti di Internet a molti dati relativi ad una persona, l'attività del gestore del motore di ricerca «è idonea a costituire un'ingerenza più rilevante nel diritto fondamentale al rispetto della vita privata della persona interessata che non la pubblicazione da parte dell'editore della suddetta pagina *web*» (par. 87)[26].

Come cancellare? Spontaneamente, su richiesta dell'interessato, per decisione del Garante, con ordine dell'autorità giudiziaria. Si tratta di ipotesi non alternative, ma anche cumulative. Anche un sistema automatizzato di richieste di rimozione (cd. *robo-takedown*) potrebbe costituire una scelta inadeguata[27].

I miei dati. Il mio profilo digitale. Accedervi, rettificarli, opporsi al loro trattamento, cancellarli (cons. 63-70 reg. 2016/679): diritti incompressibili, salva la necessità di curarmi e di tutelare diritti fondamentali altrui.

Parti della mia identità hanno una tutela rafforzata: «È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona». Anche in questo caso le eccezioni non mancano (art. 9, par. 2)[28]: «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

La soluzione del conflitto tra riservatezza dei dati e interesse pubblico a conoscere la reputazione economica della persona richiede un discorso a parte, che trascende tale occasione[29].

7. Altre tutele

La mia identità digitale è parte inalienabile di me stesso. Sostituirsi indebitamente creando un *account* a mio nome è reato. Al giudice, per tutelarli, basta la trama delle fattispecie già positivizzate: «Integra il reato di sostituzione di persona (art. 494 cod. pen.), la condotta di colui che crei ed utilizzi un “account” di posta elettronica, attribuendosi falsamente le generalità di un diverso soggetto, inducendo in errore gli utenti della rete “Internet” nei confronti dei quali le false generalità siano declinate e con il fine di arrecare danno al soggetto le cui generalità siano state abusivamente spese, subdolamente incluso in una corrispondenza idonea a lederne l'immagine e la dignità»[30].

L'ordinamento punisce chi me la ruba per accedere abusivamente in mio nome. Il codice Rocco nato nel Ventennio ora conosce l'identità digitale: *Frode informatica commessa con sostituzione d'identità digitale* (art. 640-ter cod. pen.)[31].

Il minore ha una tutela speciale. La legge 29 maggio 2017, n. 71, punisce il cyberbullismo, inteso come «qualunque forma di pressione, aggressione, molestia, ricatto, ingiuria, denigrazione, diffamazione, *furto d'identità*, alterazione, acquisizione illecita, manipolazione, trattamento illecito di dati personali in danno di minorenni, realizzata per via telematica, nonché la diffusione di contenuti on-line aventi ad oggetto anche uno o più componenti della famiglia del minore il cui scopo intenzionale e predominante sia quello di *isolare* un minore o un gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo».(art. 1, comma 2)[32].

L'art. 2 della legge, come il *Regolamento europeo sulla protezione dei dati*, formalizza il tipo di procedimento per l'oscuramento, la rimozione, il blocco dei contenuti specifici rientranti in condotte di cyberbullismo, prevedendo che l'istanza possa essere inoltrata dal minore ultraquattordicenne, vittima di un atto di questa natura, oppure dal genitore, al titolare del trattamento, al gestore del sito Internet o del *social media*, e, in caso di inerzia, al Garante per la protezione dei dati personali.

8. Account commemorativi

Amici e familiari condividono foto, *post*, diari di una persona deceduta. Sono dati modificabili dal "contatto erede", la persona scelta dal deceduto per gestire il suo *account*. Nascono conflitti tra amici e familiari sulla conservazione, gestione o cancellazione dell'*account* commemorativo[33].

Il diritto successorio si apre a nuove sfide. Lo *ius sepulchri* e ormai rade questioni sulle marmoree cappelle gentilizie cedono il passo a nuovi riti commemorativi digitali, ma ricordano, nel perenne adattamento del diritto alle nuove realtà, che la preservazione dell'identità della persona *post mortem* non è questione puramente patrimoniale e richiede soluzioni giuridiche diverse da quelle della mera devoluzione dell'eredità[34].

9. La sentenza dell'Automa e il diritto ad una decisione Umana

Nell'agosto 2016 la Corte Suprema del Wisconsin nega l'appello a Eric Loomis, accusato di essere sfuggito al controllo della polizia, ritenendo legittimo il ricorso da parte del magistrato all'algoritmo segreto *Compas* per stabilire l'entità della pena del condannato e valutare la potenziale recidività e la propensione a ripetere lo stesso reato.

Più o meno contemporaneamente migliaia di professori italiani, sono assegnati con l'algoritmo della *Buona Scuola* alle loro sedi di lavoro. Alcuni, scontenti, adiscono il giudice del lavoro, che ritiene la decisione automatizzata non infallibile.

Altre persone possono decidere di me, da sempre: mi condannano, mi risarciscono, mi divorziano, mi assumono o licenziano.

Ora può decidere di me anche un robot: *trattamento automatizzato* del mio profilo.

Chief Justice John G. Roberts negli Stati Uniti afferma, a proposito del caso Loomis, che è già arrivato il tempo «*when smart machines, driven with artificial intelligences, will assist with courtroom fact-finding or, more controversially even, judicial decision-making*»[35].

L'Europa sembra opporsi. Umana – dice ora il legislatore europeo – non è solo una qualità del giudizio, conforme alla tutela dei diritti Cedu, o semplicemente conforme a sentimenti di giustizia, ma anche dell'*entità decidente*.

Ho il diritto di non essere sottoposto «a una decisione giuridica» che mi riguarda o che incida *significativamente* sulla mia persona «basata unicamente sul trattamento automatizzato, compresa la profilazione» (art. 22, par. 1 reg. 479/2016). La regola europea ha la sua premessa: «L'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona, quali il rifiuto automatico di una domanda di credito online o pratiche di assunzione elettronica senza interventi umani» (considerando 71).

Anche il Codice della *privacy*, richiamando l'art. 15 della precedente direttiva 46/1995/CE, afferma che: «Nessun atto o provvedimento giudiziario o amministrativo che implichi una valutazione del comportamento umano può essere fondato unicamente su un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato» (art. 14).

Diffidiamo dell'*Automa togato*. L'algoritmo che decide delle nostre vite spaventa. Rifiuto verso il destino della scienza giuridica o lampi di lungimiranza? L'applicazione della norma al caso concreto non è semplice sillogismo? E il sillogismo non è forse un algoritmo semplificato?[36].

Le sue premesse, maggiore o minore possono essere errate. La macchina può sbagliare, perché la *data entry* o la sequenza di operazioni sono errate, incomplete, non malleabili. Ma anche il giudice sbaglia.

Cosa impedisce veramente di sostituirlo con l'Automa? Ignoto è il suo algoritmo decisionale. Ma ancora più ignoto è il foro interno del giudice.

La decisione del giudice italiano è obbligatoriamente motivata: trasparenza, sindacato esterno. Ogni decisione deve poter essere impugnata davanti al giudice della legittimità (art. 111. Cost.)[37].

Motivazione espressa a impugnazione rendono il giudice che ha deciso nudo dopo la decisione. Questo però non basta ad escludere la decisione automatizzata: la motivazione non è incompatibile con la Macchina; il suo prodotto può contenere argomentazioni[38].

Diritto a una umana decisione, non come qualità del prodotto-sentenza, ma come natura del decidente, in carne e ossa, e non un'intelligenza artificiale.

L'umanità del decisore, però, per il legislatore europeo è una garanzia solo parziaria. Gli avverbi delimitano il mio diritto, lo privano di absolutezza: la decisione automatizzata è consentita se la macchina non decide da sola il mio destino (non basata *unicamente*), se esiste, quindi, anche solo una frazione del processo che vede l'intervento dell'uomo.

Ma lo stesso divieto di decisione esclusivamente automatizzata soffre di eccezioni. La decisione del robot è legittima qualora «sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato» [art. 22, par. 2, lett. b)]. Il Considerando 71 del regolamento afferma che è opportuno che sia consentito adottare decisioni sulla base di tale trattamento, compresa la profilazione, *se ciò è espressamente previsto dal diritto* dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento[39]: il divieto del legislatore europeo non è affatto perentorio.

Il titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del titolare del

trattamento, di esprimere la propria opinione e di contestare la decisione (art. 22, par. 3 del reg. europeo).

Se la statistica degli errori giudiziari fosse dalla parte della Macchina, cosa sceglieremmo?

Reclamiamo istintivamente l'umanità non solo della decisione, ma anche del decisore. Alla razionalità preferiamo, in definitiva, l'umanità. Da imputati vogliamo condividere la stessa natura del giudice, anche se la scelta questa scelta potrebbe essere la nostra rovina.

Una decisione che scaturisce da una Persona e per una Persona. L'umana decisione è etica e responsabilità giuridica della decisione. L'Intelligenza Artificiale non ne è condizionata e non risponde del suo prodotto.

Per ora l'art. 220, comma 2, del codice di procedura penale, ci tranquillizza: non è ammessa perizia per stabilire l'abitudine o la professionalità nel reato, la tendenza a delinquere, il carattere e la personalità dell'imputato e in genere le qualità psichiche dell'imputato indipendenti da cause patologiche. Vietata è anche la perizia su questioni di diritto. Il giudice che la dispone passa, per l'atto abnorme, sotto la lente della giustizia disciplinare.

Non è forse abbastanza.

10. Scenari

Identità personale, riservatezza, oblio: diritti fondamentali anche nella rete; non dovrebbero essere alienabili, ma lo sono. Il mercato planetario del mio *Io digitale* è frutto avvelenato della mia volontà. Nessuno mi obbliga. Il piacere, rapidamente diventa necessità, e mi comanda.

Lo strumentario della *privacy* (accesso ai dati, appropriatezza, adeguatezza, uso non eccedentario, rettifica, opposizione, *Data Protection Officer*) è efficace per le amministrazioni pubbliche, ma impotente, se non grottesco, rispetto ai grandi attori privati. Diritti limitati rispetto a *Governi pubblici e privati della Sorveglianza predittiva*. Armi a salve contro *Big Data*.

Abbandonare la mia identità digitale è ormai impraticabile; è impossibile tornare indietro senza essere esclusi da una fetta determinante della nostra dimensione sociale.

Accesso ad Internet, identità digitale, deindicizzazione, pseudonomizzazione, lealtà di trattamento dei dati personali, cittadinanza elettronica emergono come diritti della persona distinti, che richiedono urgentemente ricognizione, sistemazione e garanzia.

Accumulazione massiva di dati, profilazione generalizzata, decisioni automatizzate aprono scenari in parte imprevedibili.

Si tratta di un compito non facile: forgiare nuovi diritti o inquadrare le novità in quelli già riconosciuti? Affidarsi agli Stati nazionali, all'Europa o a una dimensione globale? L'ordinamento, secondo l'utopia illuministica, non conosce lacune. Il giudice italiano a cui si rivolge il cittadino cerca la fattispecie nell'ordinamento multilivello, la modifica, ne estende lo spettro applicativo, la applica a casi analoghi, ricostruisce principi, richiama, come si è detto, fonti aperte come l'art. 2 Cost., *inventa* il diritto nel suo incessante divenire^[40]: accesso alla rete e identità digitale sono agevolmente riconoscibili come parte nucleo dei diritti inviolabili, come in passato lo sono stati – autonomamente o quali proiezioni di altri diritti esplicitamente riconosciuti dalla Costituzione – il diritto all'identità personale, alla *privacy*, alla libertà sessuale, alla libertà di autodeterminazione.

Molto più difficile apprestare le contromisure giuridiche contro il controllo capillare delle persone attraverso i loro metadati.

Gli attrezzi offerti al giurista dagli ordinamenti attuali non bastano. Sfruttare il *Web* per elaborare una nuova democrazia digitale è un passaggio assolutamente ineludibile se si vuole garantire efficacemente, dopo l'*Habeas Corpus*, anche l'*Habeas Data*[41].

*** Relazione tenuta in occasione della Giornata europea della Giustizia civile della Corte di appello di Napoli del 30 novembre 2017.**

[L'immagine di copertina è tratta da www.arte.tv](http://www.arte.tv)

[1] Proposto il 29 novembre 2010, nell'ambito dell'*Internet Governance Forum Italia* a Roma. Il Regolamento UE del Parlamento Europeo e del Consiglio, del 25 novembre 2015, recante «misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al *roaming* sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione» è entrato in vigore il 30 aprile 2016.

[2] Il Regolamento UE del Parlamento Europeo e del Consiglio, del 25 novembre 2015, recante «misure riguardanti l'accesso a un'Internet aperta e che modifica la direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica e il regolamento (UE) n. 531/2012 relativo al *roaming* sulle reti pubbliche di comunicazioni mobili all'interno dell'Unione».

[3] Art. 3: «Gli utenti finali hanno il diritto di accedere a informazioni (...) tramite il servizio di accesso a Internet».

[4] Testo elaborato dalla Commissione per i diritti e i doveri in Internet costituita presso la Camera dei deputati.

[5] Vds. recentemente, G. De Minico, *Antiche libertà e nuova frontiera digitale*, Giappichelli, Torino, 2016.

[6] Cass., 22 giugno 1985, n. 3769.

[7] [R. Clarke, *The Digital Persona and its Application to Data Surveillance*, 1994](#). «Una persona digitale è la rappresentazione digitale di un individuo reale, che può essere connessa a questo individuo reale e comprende una quantità sufficiente di dati (rilevanti) per essere usata, in uno specifico ambito e ai fini del suo utilizzo, come delega dell'individuo». ([A. Roosendaal, *Digital personae and profiles as representations of individuals*, 2013](#)).

[8] Cass. n. 15/1947 riconosce la validità del testamento olografo sottoscritto con lo pseudonimo e ciò anche per quel che riguarda la tutela del diritto d'autore, ([art. 8, comma 2, legge n. 633/1941](#)).

[9] Lo pseudonimo ha una riconoscimento normativo anche negli atti digitali, perché, riguardo alla firma digitale, in luogo del nome del titolare il certificatore può riportare sul certificato elettronico uno pseudonimo, qualificandolo come tale ([art. 33, d.lgs n. 82/2005](#)). La *pseudonomizzazione* ha un ripetuto riconoscimento nel regolamento europeo 679/2016.

[10] Art. 4, comma 4 del Regolamento UE 2016/679 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).

Evidenzia il considerando 30 che le persone fisiche possono essere associate a identificativi *on-line* prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, a marcatori temporanei (*cookies*) o a identificativi di altro tipo, come i *tag* di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai *server*, possono essere utilizzate per creare profili delle persone fisiche e identificarle (considerando 30).

[11] Esso «consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona» (considerando 71).

[12] Convenzione n. 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, adottata a Strasburgo il 28 gennaio 1981, ratificata in Italia nel 1989. Preambolo: «Considerando che è auspicabile estendere la protezione dei diritti e delle libertà fondamentali di ciascuno, in particolare il diritto al rispetto della vita privata, tenuto conto dell'intensificazione della circolazione attraverso le frontiere di dati a carattere personale oggetto di elaborazioni automatizzate; Riaffermando nello stesso tempo il loro impegno in favore delle libertà di informazione senza tener conto delle frontiere; Riconoscendo la necessità di conciliare i valori fondamentali del rispetto della vita privata e della libera circolazione dell'informazione tra i popoli».

[13] Art. 5. *Qualità dei dati*. I dati a carattere personale oggetto di un'elaborazione automatizzata sono: *a)* ottenuti e elaborati in modo lecito e corretto; *b)* registrati per scopi determinati e legittimi ed impiegati in una maniera non incompatibile con detti fini; *c)* adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati; *d)* esatti e, se necessario, aggiornati; *e)* conservati in una forma che consenta l'identificazione delle persone interessate per una durata non superiore a quella necessaria ai fini per i quali sono registrati.

[14] Art. 6. *Categorie speciali di dati*. I dati di carattere personale indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno non preveda garanzia adatte. Lo stesso dicasi dei dati di carattere personale relativi alle condanne penali.

[15] Art. 7. *Sicurezza dei dati*. Adeguate misure di sicurezza vengono adottate per la protezione di dati di carattere personale registrati nei casellari automatizzati contro la distruzione accidentale o non autorizzata, ovvero la perdita accidentale così come contro l'accesso ai dati, la modifica o la diffusione non autorizzate.

[16] Art. 8. *Ulteriori garanzie per la persona interessata*. Ogni persona deve poter: *a)* conoscere l'esistenza di un casellario automatizzato di dati a carattere personale, i suoi fini principali, nonché l'identità e la residenza abituale, ovvero la sede amministrativa, del responsabile del casellario; *b)* ottenere ad intervalli di tempo ragionevoli e senza ritardo o spese eccessive la conferma dell'esistenza o meno nel casellario automatizzato dei dati di carattere personale ad essa relativi, come pure la trasmissione di tali dati in una forma intellegibile; *c)* ottenere, se del caso, la rettifica di tali dati o la loro cancellazione qualora questi siano stati elaborati in violazione delle disposizioni di diritto interno di esecuzione dei principi fondamentali di cui agli artt. 5 o 6 della presente Convenzione; *d)* disporre di una possibilità di ricorso qualora non venga dato seguito ad una richiesta di conferma o, a seconda del caso, di comunicazione, rettifica, o cancellazione di cui ai paragrafi *b)* e *c)* del presente articolo.

[17] Vds. art.16, par. 1, del trattato sul funzionamento dell'Unione europea.

[18] Dichiarazione dei diritti di Internet, elaborata dalla Commissione della Camera per i diritti e i doveri in Internet, citata in precedenza.

[19] Nel caso *Google Spain*, la Corte di giustizia ha affermato che la direttiva 95/46 (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) trova applicazione anche ai gestori di motori di ricerca Internet. La Corte ha fornito, inoltre, delle precisazioni sull'ambito di applicazione territoriale della direttiva, nonché dei diritti che la stessa prevede in favore delle persone cui i dati personali oggetto del trattamento si riferiscono (tra cui il cd. diritto all'oblio), e dei correlativi obblighi a carico dei gestori di motori di ricerca.

[20] Imbrigliati tra identità sociale ed io digitale siamo prigionieri necessari e felici del “*panopticon partecipativo*” (Whitaker, 1999).

[21] Par. 83, Corte giustizia Unione europea, 13 maggio 2014, n. 131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD)*, Mario Costeja Gonzalez. La Corte si è pronunciata sull'interpretazione di una serie di disposizioni della 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 (d'ora in poi la “direttiva 95/46/CE” oppure “direttiva”), oltreché degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. La domanda di pronuncia pregiudiziale deriva da una controversia in cui il sig. *Mario Costeja González* conveniva in giudizio le società *Google Spain SL* (“*Google Spain*”) e *Google Inc.* (congiuntamente con *Google Spain* “*Google*”), da un lato, e *La Vanguardia Ediciones SL*, editore di un quotidiano spagnolo largamente diffuso nella Catalogna, dall'altro, a seguito di un reclamo presentato dal primo avverso i secondi presso l'Agencia spagnola di protezione dei dati personali (in prosieguo l'“*Agencia*”). Il denunciante reclamava che, introducendo il suo nome sul motore di ricerca di *Google* (a volte “*Google Search*”), venivano visualizzati dei *link* che rinviavano a due pagine del quotidiano sulle quali figurava un annuncio per la vendita all'asta di mobili connessa ad un pignoramento effettuato nei confronti del denunciante per la riscossione coattiva di crediti previdenziali. Considerato che il pignoramento era stato interamente definito da svariati anni e che la menzione dello stesso era ormai privo di qualsiasi rilevanza, il denunciante chiedeva all'Agencia di ordinare al quotidiano la soppressione o la modifica delle pagine suddette di modo che i suoi dati personali non vi comparissero più, oppure di ricorrere agli strumenti forniti dai motori di ricerca per proteggere tali dati. In aggiunta il denunciante domandava all'Agencia di intimare a *Google* l'eliminazione o l'occultamento dei suoi dati personali, cosicché cessassero di comparire tra i risultati di ricerca e non figurassero più nei *link* del quotidiano.

Il motore di ricerca non può nascondersi dietro i trattamenti automatizzati che opera: «Il trattamento dei dati effettuato nel contesto dell'attività di un motore di ricerca si distingue da e si aggiunge a quello effettuato dagli editori di siti *web* e incide ulteriormente sui diritti fondamentali della persona interessata, il gestore di tale motore di ricerca quale responsabile del trattamento in questione deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che tale trattamento soddisfi le prescrizioni della direttiva 95/46, affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti».

[22] Par. 82 sent. “*Google Spain*”.

[23] La CGUE obbliga il motore a sopprimere – dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona – dei *link* verso pagine *web* pubblicate da terzi e contenenti informazioni relative a questa persona quando il bilanciamento tra i diritti di quest'ultima e l'interesse degli utenti di Internet depone nel senso della prevalenza dei primi. Nell'effettuare questa valutazione si dovrà tenere conto «[della] natura dell'informazione di cui trattasi e [del] suo carattere sensibile per la vita privata della persona suddetta, nonché [dell]’interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica» (par. 81). Il principio, riconosciuto dai giudici italiani, riguarda anche altri motori di ricerca come Yahoo. Par. 29: «La constatazione di cui sopra non viene invalidata neppure dal fatto che tali dati abbiano già costituito l'oggetto di una pubblicazione su Internet e non vengano modificati dal suddetto motore di ricerca 84 In proposito occorre rilevare che, tenuto conto della facilità con cui informazioni pubblicate su un sito *web* possono essere

riprodotte su altri siti, nonché del fatto che i responsabili della loro pubblicazione non sempre sono assoggettati alla normativa dell'Unione, non sarebbe possibile realizzare una tutela efficace e completa delle persone interessate nel caso in cui queste dovessero preventivamente o in parallelo ottenere dagli editori di siti *web* la cancellazione delle informazioni che le riguardano».

[24] Par. 85: «Inoltre, il trattamento da parte dell'editore di una pagina *web*, consistente nella pubblicazione di informazioni relative a una persona fisica, può, eventualmente, essere effettuato “esclusivamente a scopi giornalistici” e beneficiare così, a norma dell'articolo 9 della direttiva 95/46, di deroghe alle prescrizioni dettate da quest'ultima, mentre non sembra integrare tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca. Non si può dunque escludere che la persona interessata possa, in determinate circostanze, esercitare i diritti contemplati dagli articoli 12, lettera b), e 14, primo comma, lettera a), della direttiva 95/46 contro il suddetto gestore del motore di ricerca, ma non contro l'editore della pagina *web*».

[25] Sentenza “Google Spain”: diritto all'oblio, cfr. par. 96.

[26] La giurisprudenza italiana ha ritenuto assimilabile a Google anche il motore Yahoo: «Deve essere riconosciuto il diritto dell'interessato di rivolgersi al gestore del motore di ricerca al fine di ottenere la rimozione dei risultati ottenuti inserendo come criterio di indagine il nome del soggetto cui si riferiscono le informazioni, in particolare quando le stesse, tenuto conto dell'insieme delle circostanze caratterizzanti il caso oggetto della richiesta, risultino inadeguate, non pertinenti o non più pertinenti ovvero eccessive in rapporto alle finalità per le quali sono state trattate e al tempo trascorso» (Trib.Milano, sez. I, 4 gennaio 2017, n. 12623).

[27] R. Petruso, *Responsabilità degli intermediari di Internet e nuovi obblighi di conformazione: robot-takedown, policy of termination, notice and take steps*, in *Europa e Diritto Privato*, fasc.2, 1 giugno 2017, pag. 451.

[28] Articolo 9. Trattamento di categorie particolari di dati personali: «1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il paragrafo 1 non si applica in diversi casi. 4.Gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute».

[29] Prevale l'interesse pubblico all'accesso alle informazioni pubblicate sul registro da parte delle imprese rispetto alla protezione dei dati personali dell'amministratore di una società a responsabilità limitata che, dopo il fallimento (1992) e la liquidazione con cancellazione dal registro delle imprese (2005), erano stati oggetto di trattamento da parte di una società specializzata nella raccolta e nell'elaborazione di informazioni di mercato e nella valutazione del rischio (*rating*). (Corte giustizia UE, sez. II, 09 marzo 2017, n. 398) Allo stato attuale del diritto dell'Unione spetta agli Stati membri determinare se le persone fisiche di cui all'art. 2, par. 1, lett. d) e j), della direttiva 95/46/Ce possano chiedere all'autorità incaricata della tenuta, rispettivamente, del registro centrale, del registro di commercio o del registro delle imprese di verificare, in base ad una valutazione da compiersi caso per caso, se sia eccezionalmente giustificato, per ragioni preminenti e legittime connesse alla loro situazione particolare, decorso un periodo di tempo sufficientemente lungo dopo lo scioglimento della società interessata, limitare l'accesso ai dati personali che le riguardano, iscritti in detto registro, ai terzi che dimostrino un interesse specifico alla loro consultazione.

[30] Nella specie a seguito dell'iniziativa dell'imputato, la persona offesa si ritrovò a ricevere telefonate da uomini che le chiedevano incontri a scopo sessuale ([Cass. Pen. 46674/2007](#); [conf. Sez. 3, sent. n. 12479 del 2012](#)). Un sistema informatico è quel «complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'uso, anche parziale, di tecnologie informatiche», ovvero sia attraverso l'uso di una tecnologia che sia «caratterizzata – per mezzo di una attività di “codificazione” e “decodificazione” – dalla “registrazione” o “memorizzazione” di impulsi elettronici, su supporti adeguati di “dati”, e cioè da rappresentazioni elementari di un fatto, effettuate attraverso simboli (*bit*), in combinazioni

diverse, e dalla elaborazione automatica di tali dati», la quale «genera “informazioni”, costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consente loro di esprimere un particolare significato per l’utente» (così, Cass. pen., sez. II, 15.4.2011, n. 17748, in *DeJure*). [Cass. 24 febbraio 2017 n. 9191](#): «*La frode informatica si caratterizza rispetto alla truffa per la specificazione delle condotte fraudolente da tenere che investono non un determinato soggetto passivo, bensì il sistema informatico, attraverso la manipolazione. Si tratta di un reato a forma libera finalizzato sempre all’ottenimento di un ingiusto profitto con altrui danno, ma che si concretizza in una condotta illecita intrusiva ma non alterativa del sistema informatico o telematico*».

Vds. R. Bartoli, *La frode informatica tra “modellistica”, diritto vigente, diritto vivente e prospettive di riforma*, in *Dir. inf.*, 2011, 3, pp. 383 ss.; F. Cajani, *Profili penali del phishing*, in *Cass. pen.*, 2007, 2294; L.D. Cerqua, *Accesso abusivo e frode informatica: l’orientamento della Cassazione*, in *Dir. prat. soc.*, 2000, 51; C. Pecorella, *Commento Art. 640 ter c.p.*, in *Codice penale commentato, Artt. 575-734 bis*, a cura di E. Dolcini e G. Marinucci, III ed., Milano, 2011, pp. 6417 ss.; G. Pica, *Internet*, in *Dig. pen.*, Torino, 2004, pp. 425 ss.; F. Resta, *Banche di dati on-line. I limiti della tutela penale*, in *Giur. mer.*, 2007, 2052.

[31] L’art. 9, comma I, lett. a), della legge, 15 ottobre 2013, n. 119 (in Gazz. Uff., 15 ottobre 2013, n. 242) che ha convertito in legge, con modificazioni, del decreto-legge 14 agosto 2013, n. 93, («*recante disposizioni urgenti in materia di sicurezza e per il contrasto della violenza di genere, nonché in tema di protezione civile e di commissariamento delle province*») ha previsto, all’interno dell’art. 640-ter cp («*frode informatica*»), una nuova statuizione normativa rubricata: *Frode informatica commessa con sostituzione d’identità digitale*. Detta disposizione legislativa dispone che la «*pena è della reclusione da due a sei anni e della multa da euro 600 a euro 3.000 se il fatto è commesso con furto o indebito utilizzo dell’identità digitale in danno di uno o più soggetti*».

[32] Il comma 1 dell’art. 1 fissa l’obiettivo di contrastare il fenomeno del cyberbullismo in tutte le sue manifestazioni, con azioni a carattere preventivo e con una strategia di attenzione, tutela ed educazione nei confronti dei minori coinvolti, sia nella posizione di vittime, sia in quella di responsabili di illeciti, assicurando l’attuazione degli interventi nell’ambito delle istituzioni scolastiche senza distinzione di età.

[33] Facebook ha individuato convenzionalmente una regola che dà preferenza alle ragioni della famiglia.

[34] In Italia la personalità trova tutela anche *post mortem* nel codice penale l’art. 597 cp prevede una sanzione penale per la lesione della memoria del defunto. Gli artt. 8, 10 cc disciplinano l’esercizio delle norme sulla tutela del nome e dell’immagine dopo la morte del titolare riconoscendo azioni esercitabili dai familiari.

[35] <https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html>

[36] La definizione semplificata di algoritmo è quella di una sequenza ordinata e finita di passi (operazioni o istruzioni) elementari che conduce a un ben determinato risultato in un tempo finito, con alcune proprietà necessarie, senza le quali un algoritmo non può essere definito tale: i passi costituenti devono essere “elementari”, ovvero non ulteriormente scomponibili (atomicità); i passi costituenti devono essere interpretabili in modo diretto e univoco dall’*esecutore*, sia esso umano o artificiale (*non ambiguità*); l’algoritmo deve essere composto da un numero finito di passi e richiedere una quantità finita di dati in ingresso (*finitezza*) l’esecuzione deve avere termine dopo un tempo finito (*terminazione*); l’esecuzione deve portare a un risultato univoco (*effettività*).

Una definizione più accurata è quella ricavabile dalla Macchina di Turing. Essa rappresenta una sorta di *computer* ideale corredato di un programma da eseguire, ma, rispetto a un computer ideale, la macchina di Turing ha un funzionamento estremamente più semplice cosicché il suo funzionamento possa essere facilmente descritto in termini matematici, facendo uso di concetti come insieme, relazione e funzione (fonte Wikipedia).

[37] Il *National Bureau of Economic Research*, ha commissionato a ricercatori delle università di Stanford, Harvard, Cornell e dell'ateneo di Chicago lo sviluppo di un algoritmo in grado di ottimizzare la decisione relativa alla libertà di una persona. Il *software* analizza dati personali per identificare dei modelli di comportamento. I dati presi in esame sono stati in prima istanza quelli di tutti gli imputati detenuti nelle carceri della città di New York tra il 2009 e il 2013. I risultati dello studio sarebbero interessanti. Il *software*, apprendendo dall'esperienza pregressa, ha prodotto una propria classificazione del rischio di rilasciare un imputato e in base a questa ha formulato delle proprie decisioni in merito alla custodia cautelare. Questa l'alternativa: *a*) mantenendo invariato il numero di detenuti, e quindi invariata la spesa a carico della pubblica amministrazione, ma modificandone la qualità, il numero di reati diminuirebbe di circa il 25%. Oppure, *b*) si può mantenere lo stesso numero di reati liberando però più del 40% di imputati in attesa di giudizio, e riducendo in tal modo, sensibilmente, la spesa pubblica. Inoltre, è emerso anche che seguendo i suggerimenti dell'algoritmo, i giudici avrebbero dovuto rilasciare molti più afroamericani e ispanici di quanto non sia realmente accaduto, ciò perché tra i dati degli imputati inseriti nel *software*, infatti, non c'erano quelli relativi alla razza. Si è commentato che "Un giudice che ci vede meglio, anche se non ha occhi umani" (<http://www.pagina99.it/2017/03/15/algoritmo-intelligenza-artificiale-razzismo/>).

[38] In ogni caso, tale trattamento, che non dovrebbe riguardare la persona minorenne, 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.

[39] Anche a fini di monitoraggio e prevenzione delle frodi e dell'evasione fiscale secondo i regolamenti, le norme e le raccomandazioni delle istituzioni dell'Unione o degli organismi nazionali di vigilanza e a garanzia della sicurezza e dell'affidabilità di un servizio fornito dal titolare del trattamento, o se è necessario per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento, o se l'interessato ha espresso il proprio consenso esplicito.

[40] P. Grossi, *L'invenzione del diritto*, Laterza, 2017.

[41] L'espressione, fatta propria dalla Costituzione del Brasile del 1988, è ripresa da numerosi autori, tra i quali Stefano Rodotà.

21 dicembre 2017

[diritti fondamentali internet identità digitale](#)