Diritto all'oblio, verità, design tecnologico: una prospettiva di ricerca

Right to Be Forgotten, Truth and Technological Design

Stefano Leucci
Fellow del Nexa Center for Internet & Society

Abstract

Come cambia il concetto di memoria nell'ambiente digitale? Quali forme e contorni presenta il nuovo diritto all'oblio dopo il caso *Google Spain* e il nuovo Regolamento europeo sulla protezione dei dati personali? Quanto pesa la veridicità o la falsità di una fonte informativa sul bilanciamento necessario al *de-listing* dagli indici di un motore di ricerca? Gli stessi algoritmi che contribuiscono ad invadere sempre più la nostra sfera privata possono essere utilizzati anche quale rimedio alla loro stessa invasività?

Questi sono i principali quesiti di un possibile percorso di ricerca che il contributo mira a disegnare. Domande non semplici, che necessitano dell'unione trans-disciplinare di intelligenze diverse e complesse. Il punto di partenza è l'analisi del caso *Google Spain*, in cui la Corte di giustizia dell'Unione europea ha definito una nuova forma di diritto all'oblio, sviscerandone i meccanismi, i contenuti e i pesi da sistemare sulla complessa bilancia della giustizia. La precisazione degli aspetti legali ed etici precede la traduzione degli stessi in ambiente digitale sotto forma di requisiti e scelte operate direttamente dall'utente. Successivamente, la tensione tra i concetti di veridicità dell'informazione ("esattezza" del dato personale) e i principi di *Privacy by Design* e by *Default* - previsti al nuovo Regolamento Europeo sulla protezione dei dati personali - permettono di disegnare un possibile cammino di studio ed approfondimento da cui potrebbero emergere risposte ai quesiti sopra rappresentati, utili a rendere maggiormente efficaci i sofisticati meccanismi giuridici introdotti dall'Unione Europea. Rimane fisso un solo elemento: la nuova legge del memorizzare e del dimenticare è l'algoritmo. Spetta a noi conoscerlo e governarlo, prevedendo sempre uno spazio di decisione umana nei giudizi di bilanciamento necessari a fronte della pluralità di interessi che insistono nell'ambiente digitale.

How does the concept of memory change in the digital environment? What shapes and contours presents the new right to be forgotten after the case of *Google Spain* and the new European Regulation on the protection of personal data? How important are truth and falsehood of an information source on the balancing act required for de-listing a link from indexes of a search engine? May the same algorithms that contribute to invade our private sphere also be used as a remedy to their own invasiveness?

These are the main questions of a possible research path that this paper aims to draw. Questions are not simple, and they require a trans-disciplinary approach. The starting point of this paper is the analysis of the *Google Spain* case, where the European Court of Justice has reshaped the right to be forgotten, setting up new mechanisms, contents and weights that need to be carefully balanced. The clarification of the legal and ethical aspects precedes the translation of them in the form of requirements and user-made choices. Subsequently, the tension between the concepts of truthfulness of information ("accuracy" of personal data) and the principles of Privacy by Design and by Default - as stated by the new European Regulation on the protection of personal data - allow to draw a possible path of investigation. The final aim is to find answers to the questions asked above, increasing the effectiveness of the sophisticated legal mechanisms introduced by the upcoming General Data Protection Regulation. Only one element remain fixed: algorithm is the new law of our digital memory. Our responsibility is to govern its intelligence, safeguarding spaces for human decisions for balancing different interests that insist in the digital environment.

Sommario

diritto all'oblio
design
esattezza
intelligenza artificiale
trasparenza algoritmica

1 Memoria e motori di ricerca

Dimenticare è «perdere la memoria di qualcosa», ricorda il Sabatini-Colletti. Il noto dizionario è solo uno dei tanti strumenti che l'umanità ha prodotto nel corso dei secoli per supplire a quel misterioso atto mentale volto a rimuovere inconsciamente fatti, pensieri e valutazioni che, in uno spazio temporale variabile, non consideriamo più utili. Biblioteche e archivi da sempre sopperiscono alla volatilità della nostra memoria, costruendo quella conoscenza collettiva poi custodita e catalogata dai "sacerdoti dell'informazione" che erano e sono archivisti e bibliotecari.
Ma quando le informazioni che raccogliamo ed accumuliamo nella quotidianità riguardano persone fisiche, l'impatto sulla reputazione di queste è immediato e persistente nel tempo, e può generare pesante pregiudizio. Dimenticare permette, dunque, di "ripulire" la reputazione delle persone da fatti - veri, verificati o anche totalmente falsi - che potrebbero comportare detrimento. In altre parole, dimenticare corrisponde a riabilitare la persona alla piena dignità[1]. Ma se dimenticare è fatto mentale, e dunque difficilmente controllabile in quanto umano, inconscio ed inconsapevole, cosa succede a sostituire le sinapsi o gli strumenti cartacei un con bit e hardware?
"*Internet never forgets*", recita un adagio ad oggi molto in voga. Effettivamente, la Rete è stata progettata in modo entropico[2]. Ciò significa che l'informazione molecolare collegata in conoscenza collettiva può solo aumentare, e le operazioni per cancellare (de-collegare) un'evidenza sono molto costose e faticose, a volte del tutto inutili. La differenza tra biblioteche e internet risiede nell'automazione: la faticosa attività degli archivisti è stata lentamente riprodotta[3] e poi interamente sostituita dai *crawler* dei motori di ricerca che scandagliano il web senza sosta, organizzando e catalogando quelle molecole informative di cui è composto. Dunque, i motori di ricerca diventano meta-strumenti della conoscenza digitale, misteriosi intermediari dell'informazione, con la capacità di mostrare le evidenze più appropriate ogni qual volta una parola è inserita nel campo di ricerca. E quando quella parola corrisponde al nome proprio di una persona, tutti i siti web e i documenti in cui quel nome è contenuto appaiono sullo schermo in ordine metodico.
Come ricorda elegantemente il prof. Solove[4], il vero problema non è ciò che riveliamo di noi in rete, più o meno consapevolmente. I rischi più grandi per la nostra *privacy* «derivano da quello che rivelano pubblicamente di noi i nostri amici e i nostri nemici, coniugi e amanti, impiegati e datori di lavoro, professori e studenti». Piccoli dettagli insignificanti della nostra vita *online* si uniscono costruendo profili onnicomprensivi del nostro essere ed avere. La peculiarità dei nostri tempi è poter sopperire alla frammentarietà dell'informazione tramite l'immenso potere di aggregazione degli algoritmi di ricerca, sempre più performanti e sempre più raffinati.
Ma quanto possiamo fidarci di questi "aggregati informativi" composti in maniera automatica da un – pur raffinatissimo – motore di ricerca? Come possiamo controllarne il funzionamento e governarne le funzionalità a nostro favore - e non a scapito - dei nostri diritti più intimi?

2 Caso *Google Spain*: il nuovo diritto all'oblio

Può capitare che fatti lesivi della dignità "tornino a galla" molto tempo dopo, in seguito ad una semplice ricerca *online*. Ed è proprio questo che è successo al signor Costeja González, che per proteggere la sua *privacy* ha adito prima l'*Agencia Española de Protecciòn de Datos* e poi la Corte di

[1] L. Floridi, *On Human Dignity as a Foundation for the Right to Privacy. Philosophy and Technology*, Berlino, 2016.
[2] Come il padre del web semantico ricordava in uno dei suoi articoli più importanti, un'area particolarmente problematica dell'aggregazione di dati provenienti da diverse sorgenti riguarda proprio la tutela della privacy. Il mondo accademico lavora ancora oggi alla ricerca di proposte sostenibili alla soluzione di questo problema, oramai assimilato ad un paradosso. Si veda C. Bizer - T. Heath - T. Berners-Lee, *Linked data: the story so far*, in *Special issue on linked data. International Journal on Semantic Web and Information Systems*, 2009.
[3] La ricerca riassunta in questo articolo ha reso possibile il cambiamento di paradigma nella catalogazione automatica delle informazioni. Le tecnologie derivate hanno permesso la nascita del più importante motore di ricerca ad oggi esistente (Google): S. Brin - L. Page, The anatomy of a large-scale hypertextual Web search engine, in Computer Networks and ISDN Systems archive, 30/1998.
[4] D. Solove, *The future of reputation*, New Haven, 2007.

giustizia dell'Unione Europea[5], ri-aprendo un enorme dibattito[6] destinato ad avere nuove e continue ripercussioni sul modo e sulle precauzioni con cui gestiamo (e vediamo gestite) le informazioni che ci riguardano, diffuse nell'ambiente digitale.

Infatti, introducendo il proprio nome in *Google*, venivano mostrate notizie pubblicate due anni prima sul quotidiano *La Vanguardia*, che narravano di una vendita all'asta di immobili connessa ad un pignoramento effettuato per la riscossione coattiva di crediti previdenziali. Il sig. Costeja González affermava che «il pignoramento, che era stato effettuato nei suoi confronti, era stato interamente definito da svariati anni e che la menzione dello stesso era ormai priva di qualsiasi rilevanza»[7].

Evidente è il rischio di reperire queste informazioni. Si pensi a un istituto bancario che, nella millimetrica cautela tipica delle decisioni in tema di benefici finanziari, decida di non concedere un prestito proprio a causa dell'evidente insolvenza, semplicemente immettendo il nome del possibile futuro debitore. Immaginiamo, ancora, la lesività di queste informazioni se unite a dettagli lavorativi, orientamenti sessuali o politici del soggetto. Come rilevato anche dalla sentenza in commento, da una semplice ricerca del nome di una persona, è possibile ricostruire «una visione complessiva strutturata delle informazioni relative a questa persona reperibili su internet, che consente di stabilire un profilo più o meno dettagliato di quest'ultima».[8]

Non si dubita, in questo caso, dell'applicabilità della direttiva 95/46[9], nonostante si tratti esclusivamente di operazioni atte a non modificare, bensì ad organizzare e aggregare dati pubblicati precedentemente. Come afferma graniticamente l'estensore, non considerare trattamento di dati personali tutti quei trattamenti ulteriori e successivi di dati personali già diffusi in rete «priverebbe in larga parte del suo significato tale direttiva»[10]. Il trattamento in questione «si distingue da e si aggiunge a»[11] quello effettuato dagli editori nel web, e proprio per questo è il gestore del motore di ricerca - in qualità di responsabile del trattamento - a dover assicurare il rispetto dei dogmi della normativa in materia di protezione dei dati personali affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti. Considerando la ricerca di una tutela efficace e completa come faro-guida di tutta l'applicazione della normativa in materia, non sarebbe possibile raggiungere pienamente questi risultati se si dovessero preventivamente rimuovere le informazioni che riguardano la persona interessata dai siti web degli editori.

Oltretutto, nemmeno si dubiterebbe dell'applicabilità agli editori web delle maggiori deroghe previste a tutela della libertà d'espressione. L'art. 9 della direttiva[12] sposta infatti il peso verso l'interesse pubblico alla conoscenza, richiedendo attenti bilanciamenti tra il diritto alla vita privata e le norme sulla libertà d'espressione[13]. Nel caso di specie, è necessario tenere in considerazione la maggior ingerenza nel diritto fondamentale al rispetto della vita privata della persona interessata nel caso dell'inclusione all'interno dell'elenco dei risultati a fronte della semplice pubblicazione di una pagina web. Come spiega la sentenza, «l'inclusione nell'elenco dei risultati facilita notevolmente l'accessibilità di tali informazione a qualsiasi utente di internet che effettui una ricerca sulla persona di cui trattasi»[14].

Con questi presupposti è chiaro l'arduo compito del gestore del motore di ricerca, a cui spetta garantire che i dati personali siano trattati lecitamente, per finalità determinate esplicite e legittime, che siano adeguati pertinenti e non eccedenti rispetto alle suddette finalità, che siano esatti ed

[5] Il presente contributo mira ad analizzare il solo piano giuridico e giurisdizionale europeo. Non verranno, perciò, commentate normative e pronunce nazionali, se non marginalmente.

[6] Il tema è, infatti, da molto tempo dibattuto nelle corti nazionali di tutta Europa, ma anche in ambiti istituzionali e accademici. In Italia, oltre ad alcuni precedenti provvedimenti dell'Autorità Garante per la Protezione dei Dati Personali, l'orientamento che ha preceduto la Corte europea è stato espresso in Cass. civ., sez. III,, sent. 5525/2012. Il caso di specie presenta solo alcuni tratti di similitudine con il giudicato della Corte europea, trattandosi della richiesta di blocco del trattamento dei dati personali rivolto all'archivio storico digitale di una nota testata giornalistica. A commento di questa sentenza, si veda: A. Mantelero, *Right to be forgotten ed archivi storici dei giornali: la Cassazione travisa il diritto all'oblio*, in *La nuova giurisprudenza civile commentata*, 28/2012, 543 ss. Per una vista comparativa si veda O. Pollicino – M. Bassini, *Diritto all'oblio: i più recenti spunti ricostruttivi nella dimensione comparata ed europea*, in F. Pizzetti (a cura di), *Il caso del diritto all'oblio*, Torino, 2013, 185 ss. Per un approfondimento storico si veda invece G. Zanfir, *Tracing the Right to be Forgotten in the Short History of Data Protection Law: the "New Clothes" of an Old Right*, in *Computers, Privacy and Data Protection Conference*, 2014.

[7] Paragrafo 15, Corte di giustizia dell'Unione Europea, Grande Camera, Causa C-131/12, da subito ribattezzata "Sentenza *Google Spain*".

[8] Paragrafo 37, sentenza *Google Spain*.

[9] 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. Le nuove tensioni a fronte del rinnovato contesto giuridico che segue l'emanazione del Regolamento Europeo sulla Protezione dei Dati (Regolamento (UE) 2016/679) verranno esaminate nei paragrafi successivi.

[10] Paragrafo 30, sentenza *Google Spain*.

[11] Paragrafo 35, sentenza *Google Spain*.

[12] Art. 9, direttiva 95/46/CE, rubricato "Trattamento di dati personali e libertà d'espressione", che recita quanto segue: «Gli Stati membri prevedono, per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria, le esenzioni o le deroghe alle disposizioni del presente capo e dei capi IV e VI solo qualora si rivelino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione».

[13] Si veda, sul tema, l'Allegato A1 (Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica) al decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

[14] Paragrafo 87, sentenza *Google Spain*.

aggiornati e che siano conservati per un arco di tempo non superiore a quello necessario al conseguimento delle suddette finalità. Proprio le informazioni riguardanti il sig. Costeja González, indicizzate e diffuse dal motore di ricerca, sono state considerate non più pertinenti, ovvero eccessive in rapporto alle finalità del trattamento in questione. Vari sono i pesi che devono essere sistemati sulla complessa bilancia della giustizia. Di primaria importanza sono gli articoli 7[15] e 8[16] della Carta dei diritti fondamentali dell'Unione europea, che «prevalgono non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse del pubblico a trovare l'informazione suddetta[17] in occasione di una ricerca concernente il nome di questa persona»[18]. È necessario però precisare il parametro fondamentale di questa decisione: il «ruolo ricoperto da tale persona nella vita pubblica»[19], che potrebbe anche giustificare l'ingerenza dell'interesse preponderante del pubblico nei suoi diritti fondamentali, nel pieno rispetto del principio di proporzionalità[20]. Il signor Costeja González - comune cittadino senza alcuna particolare rilevanza pubblica né sociale - ha così potuto attivare le tutele previste dalla Direttiva: la possibilità di operare rettifica, cancellazione o congelamento dei dati che lo riguardano[21], e il diritto di opporsi al trattamento di tali dati[22].

3 Il "peso" della verità

Ad oggi, dopo l'assorbimento dei nuovi meccanismi operativi del diritto all'oblio da parte delle Corti nazionali e nel nuovo Regolamento Generale sulla Protezione dei Dati[23], non tanto è poi cambiato. Importanti precisazioni sono state recentemente stilate da un secondo intervento della Corte di Giustizia dell'Unione Europea[24] (ribattezzato "caso *Manni*") che ha permesso di svelare i rapporti tra i tempi di conservazione e di cancellazione dei dati. Nonostante il caso di specie sia lontano dalle tipicità dei trattamenti operati dai motori di ricerca, quest'ultima pronuncia ha arricchito ancor di più la tesi per cui la decisione relativa alla cancellazione dei dati personali debba esser guidata da un'attenta «valutazione da compiersi caso per caso»[25] che tenga conto degli elementi contestuali e degli specifici interessi di terzi potenzialmente coinvolti.
Ma la domanda che appare rilevante in questa sede è la seguente: quanto incide la veridicità del fatto sul giudizio di bilanciamento utile all'applicazione del diritto all'oblio? Veridicità che - collocata nelle categorie concettuali del diritto alla *privacy* - si avvicina al concetto di "esattezza" del dato personale quale principio fondativo di tutta la disciplina[26].

[15] L'art. 7 della Carta dei Diritti Fondamentali dell'Unione Europea, rubricato "Rispetto della vita privata e della vita familiare", recita quanto segue: «Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni».

[16] L'art. 8 della medesima Carta, rubricato "Protezione dei dati di carattere personale", recita quanto segue: «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[17] I Garanti europei erano già giunti a conclusioni simili nel seguente documento Article 29 Data Protection Woking Party, *Opinion on data protection issues related to search engines*, 00737/EN, WP148, Bruxelles, adottato il 4 aprile 2008.

[18] Paragrafo 97, sentenza *Google Spain*.

[19] *Ibidem*.

[20] Sul piano giuridico italiano, alcuni autorevoli autori hanno commentato l'importanza di questo orientamento, confrontandolo con gli orientamenti maggioritari nazionali. Tra gli altri, si veda: G. Finocchiaro, *Il diritto all'oblio nel quadro dei diritti alla personalità*, in *Il Diritto dell'Informazione e dell'Informatica*, 4-5/2014, 591 ss.; T.E. Frosini, *Diritto all'oblio e internet*, in *Federalismi.it*, 11 giugno 2014.

[21] L'art. 12, comma 1, lett. b), della direttiva 95/46/CE, rubricato "diritto di accesso", stabilisce che «Gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento: la notificazione ai terzi, ai quali sono stati comunicati i dati, di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato».

[22] L'art. 14, comma 1, lett. a), della direttiva 95/46/CE, rubricato "diritto di opposizione della persona interessata", stabilisce che «Gli Stati membri riconoscono alla persona interessata il diritto [...] di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano [...]».

[23] 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). L'art. 17 affianca al più lineare diritto alla cancellazione gli interessi da bilanciare per decidere in merito all'oblio di un soggetto interessato.

[24] CGUE, C-398/15, *Manni* (2016). La Corte è intervenuta a decidere sul caso di cancellazione dei dati personali contenuti in un pubblico registro delle imprese, legando l'esaurimento della necessità del trattamento del dato personale non allo scioglimento della società, bensì ad un momento successivo. Anche dopo l'avvenuto scioglimento, infatti, questi dati «possono risultare necessari, in particolare, per verificare la legittimità di un atto compiuto a nome di detta società nel periodo in cui essa era attiva o affinché i terzi possano avviare un'azione contro membri degli organi della società o contro i suoi liquidatori. Inoltre, in funzione dei termini di prescrizione applicabili nei diversi Stati membri, anche molti anni dopo che la società ha cessato di esistere possono ancora sorgere questioni per cui è necessario disporre di tali dati«. La conclusione della Corte del Lussemburgo è la necessità di una valutazione caso per caso al fine di poter stabilire con precisione il momento in cui è possibile concludere il trattamento dei dati personali in oggetto o limitarne l'accesso ai soli terzi che dimostrino un «interesse specifico alla loro consultazione».

[25] Paragrafo 64, sentenza *Manni*.

[26] L'art. 6, comma 1, lett. d), della direttiva 95/46/CE, rubricato "diritto di accesso", stabilisce che i dati personali devono essere «esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati». Pressoché ugualmente, l'art. 5, comma 1, lett. d), del Regolamento Generale sulla Protezione dei Dati stabilisce che «esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati».

Le evidenze utili per indagare e approfondire questo aspetto sono, ad oggi, molto poche. Il fatto che le decisioni sopra richiamate siano intervenute a giudizio di notizie fattuali e – almeno apparentemente - veritiere ha permesso agli estensori delle sentenze in commento di evitare approfondimenti specifici sulla rilevanza del criterio. I pochissimi elementi che emergono tra le righe della sentenza *Google Spain* e del caso *Manni* portano a desumere come l'intero giudizio di bilanciamento propenda già verso l'oscuramento del dato quando si parli di notizie non veritiere. Elemento coerente con il principio di esattezza del dato personale sopra richiamato e su cui il Gruppo di Lavoro Articolo 29[27] ha contribuito a far chiarezza. Infatti, l'accuratezza è da considerarsi concetto più ampio della mera veridicità del fatto rappresentato e va ricollegata ad effetti e cause anche solo potenzialmente provocabili, tra cui l'inadeguatezza e la generazione di impressioni fuorvianti che potrebbero scaturire dall'acquisizione o dall'interpretazione di tali informazioni[28]. Diversamente, il *Google Advisory Council*[29] - nominato appositamente per definire gli aspetti operativi dell'esercizio del diritto all'oblio - ha concordato che falsità e inaccuratezza della notizia contribuiscono a spostar l'ago della bilancia verso un rafforzamento della *privacy* del soggetto piuttosto che verso l'interesse pubblico diffuso alla conoscenza.

Non è quindi assolutamente chiaro chi abbia la responsabilità di indagare accuratezza e veridicità della notizia o del dato personale di cui si richiede la rimozione. E' però interessante apprendere come i Garanti rimettano in capo al richiedente[30] l'onere di fornire tutte le fonti utili a dimostrazione dell'inaccuratezza delle informazioni di cui si richiede il *de-listing* dai risultati di ricerca, ma solo in caso di richiesta specificamente indirizzata all'Autorità Garante competente[31]. Dunque, al di fuori dai casi patologici portati all'attenzione delle autorità competenti, la responsabilità di indagare la veridicità dell'informazione di cui si chiede la rimozione pare essere riposta in gran parte nelle mani del motore di ricerca[32], il quale non potrà far altro che decidere in base all'informazione parziale e a volte fuorviante che i suoi operatori riusciranno a reperire.

Ma se già valutare veridicità o falsità nonché accuratezza della notizia e del dato personale è un aspetto da sempre particolarmente convulso, come potranno i principali motori di ricerca gestire correttamente il carico immenso di richieste ricevute?

La soluzione è sostenibile solo ragionando in scenari di totale verità o totale falsità dell'informazione di cui si richiede l'eliminazione. Ma la situazione si complica appena – e come quasi sempre succede – il giudizio deve essere operato su fatti particolarmente complessi e mutevoli nel tempo, con sorgenti informative veritiere ed altre mendaci[33]. Si aggiunga poi che l'ingente numero di richieste a cui è necessario dar seguito con rapidità aumenta le probabilità di errori umani ed espone i soggetti interessati e i terzi portatori di interesse a situazioni pregiudizievoli.

Così, la domanda che val la pena porsi in questa sede è la seguente: può la tecnologia intervenire a supporto di questo processo per renderlo più sostenibile e controllabile? Quali rischi potrebbero celarsi dietro ad una soluzione "tecnicista", e quali possibili rimedi potrebbero essere attivati per prevenire queste situazioni rischiose?

4 Diritto all'oblio, verità e design tecnologico

La strada per trovare risposte a quesiti di tale ampiezza non può che essere impervia, e la complessità è dovuta alla numerosità degli strumenti che potrebbero supportare soluzioni realmente scalabili ed efficaci[34]. Sul piano generale, la tensione accresce quando il diritto all'oblio è affiancato

[27] Article 29 Data Protection Woking Party, *Guidelines on the implementation of the Court of Justice of the european union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12*, 14/EN, WP225, Bruxelles, adottato il 26 novembre 2014.

[28] In tal senso, la suprema corte italiana ha affermato che «la notizia originariamente complete e vera diviene non aggiornata, risultando quindi parziale e non esatta, e pertanto sostanzialmente non vera». Corte di Cassazione, sent. 5525/2012, cit.

[29] The Advisory Council to Google on the Right to be Forgotten, Final Report, 6 febbraio 2015..

[30] L'iniziativa del soggetto interessato scaturisce dalla richiesta di esercizio del diritto di rettifica previsto dalla Direttiva. Così, L. Bianchi – G. D'Acquisto, *La sentenza Google e la questione delle esternalità dei trattamenti di dati personali*, in F. Pizzetti (a cura di), *Internet e la tutela della persona. Il caso del motore di ricerca*, Firenze, 2015, 67 ss.

[31] Article 29 Data Protection Woking Party, *Guidelines on the implementation of the Court of Justice*, cit., 11.

[32] Sulle complesse e minuziose questioni da cui potrebbero scaturire responsabilità per il motore di ricerca, si veda in particolare: S. Karapapa – M. Borghi, *Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm*, in *International Journal of Law and Information Technology*, 23/2015.

[33] Molte situazioni simili sono emerse negli ordinamenti giuridici nazionali. Si pensi, ad esempio, il recente caso relativo al motore di ricerca Yahoo! deciso dal Garante per la Protezione dei Dati Personali italiano. La situazione vedeva una notizia vera e verificabile solo in un preciso momento storico, poi confutata dai fatti emersi in momenti successivi nel tempo. In merito, si veda l'ultimo provvedimento in materia: Garante Privacy, *Rimozione di un URL riconducibile ad una pagina web*, 26 febbraio 2017 (doc. web 6026501).

[34] Da un punto di vista metodologico, l'approccio transdisciplinare pare essere il più adatto al piano di ricerca in esposizione. Sul metodo si veda, in particolare: S.L.T. McGregor, *The nature of transdisciplinary research and practice*, Kappa Omicron Nu Human Sciences Working Paper Series, Boston, 2004.

ai concetti di *Privacy by Design* e *Privacy by Default*[35] quali strumenti di *enforcement* architetturale del fascio dei diritti a tutela dell'identità personale. Certo, tenere in considerazione i requisiti di protezione dei dati personali e dell'identità - nonché gli impatti per i diritti e le libertà delle persone fisiche[36] - fin dalle fasi di progettazione degli ambienti digitali non potrà far altro che portare ad una diminuzione dei costi di gestione dei diritti sia per i titolari che per i soggetti interessati ai trattamenti, riducendone le patologie connesse. Proprio nel contesto degli strumenti a supporto del diritto all'oblio è interessante notare come gli stessi strumenti che scalfiscono la nostra *privacy online* potrebbero essere utili proprio al suo medesimo rafforzamento, permettendo ad ogni utente di personalizzare la protezione della propria identità[37]. In altre parole, la medesima sofisticatezza degli algoritmi di ricerca e aggregazione delle informazioni[38] alla base dei motori di ricerca potrebbe essere utilizzata per prevenire lesioni del diritto alla riservatezza e allo stesso tempo aiutare titolari e responsabili a mantenere aggiornati ed esatti i dati personali dei soggetti interessati[39].

Non finisce qui. Gli strumenti più avanzati di *identity management* già permettono agli utenti di visualizzare e modificare ("accedere", "rettificare" o "cancellare" secondo la nuova tassonomia dei diritti previsti dal Regolamento) i dati personali che il titolare tratta ed alimenta continuamente.

Il passaggio successivo consisterebbe nell'applicazione di questi strumenti alle funzioni di ricerca in rete. Potrà così essere l'utente a selezionare le sorgenti informative che compongono il suo «profilo informazionale»[40]: alcune di queste sono da lui aggiunte, altre sono fornite da testate giornalistiche *online*, siti web o *social network* ed aggregate alternativamente. E se addirittura nascessero nuovi motori di ricerca utente-centrici[41] con modelli remunerativi basati sulla personalizzazione delle *SERP*[42]?

I problemi sono variegati, e muovono dalla soluzione dei casi di omonimia (e dunque ad evitare che notizie attinenti una persona non vengano automaticamente riferite ad un'altra persona solamente per omonimia) alla gestione delle richieste di rimozioni dei link da parte degli utenti nel momento in cui insistano interessi contrapposti di terzi, fino ai criteri di determinazione automatica del grado di esposizione pubblica del soggetto quale criterio basilare del bilanciamento necessario all'esercizio del diritto all'oblio. Varrebbe forse la pena di indagare i parametri dell'ontologia informativa di un soggetto e dei suoi valori etici al fine di "automatizzare" alcune richieste di cancellazione certamente legittime o illegittime, controllandone *ex post* la correttezza, magari anche con meccanismi di *feedback* diffusi, ma agendo immediatamente per rimediare a situazioni che potrebbero avere impatti devastanti sulla reputazione dei singoli soggetti. Governare l'informazione è dunque il primo elemento necessario da cui ri-partire.

Ma è proprio tornando al parametro oggetto dell'indagine del presente contributo – la veridicità della fonte informativa di cui si richiede il *delisting* – che emergono i maggiori profili problematici. Già svariati operatori si sono dotati di algoritmi per automatizzare l'esercizio del diritto all'oblio a fronte delle richieste degli utenti integrando tra loro le tecnologie disponibili[43], ma di fatto richiedendo sempre l'intervento di un operatore a fronte di *alert* inviati dal sistema proprio per verificare l'autenticità della notizia. In altre parole, questi algoritmi permettono di smistare le richieste tra i vari operatori disponibili e di gestire il flusso decisionale a fronte dell'apparente complessità della richiesta rilevata solamente a fronte di parametri quantitativi segnalati dall'utente (come, ad esempio, il numero di fonti a supporto della veridicità o della falsità dell'informazione).

---

[35] Art. 25, Regolamento Generale sulla Protezione dei Dati. Sul tema si veda anche il manifesto fondativo pubblicato da A. Cavoukian (Information and Privacy Commissioner - Ontario - Canada) titolato *Privacy by design - the 7 foundation principles*, 2009 (rev. 2011).

[36] L'analisi degli impatti sui diritti e sulle libertà delle persone fisiche è richiesto dagli articoli 32 (Sicurezza del trattamento) e 35 (Valutazione d'impatto sulla protezione dei dati) del Regolamento Generale sulla Protezione dei Dati al fine di rendere più efficaci le misure tecniche ed organizzative di protezione dei dati personali attivate nelle singole organizzazioni.

[37] Si è anche proposto di prevedere spazi a commento delle notizie in cui l'utente stesso possa "completare" l'informazione parziale, rendendola veritiera. In merito si veda L. Bianchi – G. D'Acquisto, *La sentenza Google e la questione delle esternalità dei trattamenti di dati personali*, cit.

[38] Nel gergo informatico, ci si riferisce agli strumenti di *data mapping*, *data classification* e *data aggregation*. Questi tre termini sono utilizzati per descrivere fasi diverse del processo di *knowledge management* necessario al governo dei sistemi informativi. In particolare, le tecniche di *data mapping* permettono di individuare i dati sparsi nei vari sistemi dell'organizzazione; successivamente, questi dati vengono classificati in base a categorie utili all'ente (*data classification*); infine, dati riferibili alla medesima entità vengono aggregati (*data aggregation*) per poter estrarre ulteriore conoscenza utile al business tramite inferenze logiche. Sul tema, si veda: C. Collison – G. Parcell, *Learning to fly: practical knowledge management from leading and learning organizations*, Canberra, 2005.

[39] A questo fine, Google ha recentemente predisposto una nuova funzionalità che mira a notificare all'utente ogni qual volta il motore indicizzi una notizia sul suo conto, collegandola al suo profilo. Questo potrà certamente permettere un intervento più immediato a rettifica o aggiornamento della notizia appena pubblicata tramite il sistema Alert. Per maggiori informazioni, si veda: https://www.google.com/alerts.

[40] L. Floridi, *The philosophy of information*, Oxford, 2011.

[41] Alcuni "*real-time people search engines*" già esistono, ma ancora non esistono studi approfonditi sulla materia. Tra questi: Waatp (waatp.com), Spokeo (spokeo.com) e QWant (qwant.com).

[42] La *Search Engine Result Page* (*SERP*) si intende la pagina contenente l'elenco ordinato dei risultati restituiti dall'interrogazione di un motore di ricerca.

[43] Tra tutti, si veda: M. Simeonovski - F. Bendun – M.R. Asghar - M. Backes - N. Marnau - P. Druschel, *Oblivion: Mitigating privacy leaks by controlling the discoverability of online information*, International Conference on Applied Cryptography and Network Security, 2015.

La vera rivoluzione consisterà nell'applicazione di strumenti di *deep learning*[44] a decisioni inerenti verità e oblio. Questa tecnica, infatti, riproduce le strutture neurali più complesse della mente umana permettendo all'algoritmo di apprendere dall'analisi di una base esperienziale e di continuare a migliorare le prestazioni in base ad una costante osservazione dell'operato dell'utente, replicando così decisioni complesse in maniera autonoma. Considerando la potenza computazionale oggi disponibile e la vastità informativa con cui potrebbe essere "nutrito" l'algoritmo, è facile immaginare che quel famoso parametro qui in analisi – la veridicità dell'informazione – sia analizzato e "calcolato" automaticamente. A fronte degli immensi benefici in termini di efficienza e tempestività, i rischi sociali da gestire e mitigare sono legati alla possibile perdita di controllo dell'algoritmo. Infatti, anche dopo poco tempo di attività, nemmeno chi ha programmato il sistema sarebbe in grado di ricostruire a ritroso le decisioni prese.
La domanda da porsi, quindi, è la seguente: se decideremo di delegare ad un algoritmo la decisione in merito alla veridicità delle notizie in fase di rimozione, come potremo esser sicuri che le decisioni da esso prese siano ottimali? In altre parole, come sarà possibile aumentare la fiducia che riponiamo in algoritmi a cui è rimessa in maniera pressoché automatica la ricostruzione, l'alimentazione e la gestione della nostra personalità in ambiente digitale, quando di fatto non conosciamo i meccanismi più intimi del loro funzionamento?

5 Trasparenza algoritmica: un possibile punto di partenza

Da dove partire, dunque, per sciogliere questa complessa matassa?
Tra le righe dell'analisi fin qui condotta emerge immediatamente l'importanza del concetto di "fiducia" *online* tra utenti e *service provider*, quale catalizzatore principale dell'economia digitale in costante crescita[45].
E' proprio il nuovo Regolamento Europeo in materia di protezione dei dati personali a ergere la fiducia degli utenti in rete a pilastro portante di tutta l'economia digitale[46]. Questo nuovo e innovativo strumentario giuridico contribuisce a ri-bilanciare i poteri del mercato tecnologico, riponendo nelle mani degli utenti svariati diritti[47] utili a controllare l'operato di chi gestisce le informazioni personali che li riguardano. Tra le maglie di queste nuove previsioni, centrale per questa analisi è il diritto dell'utente di conoscere l'esistenza di un processo decisionale automatico e di «ricevere informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato»[48]. A questo diritto corrisponde un nuovo dovere del titolare del trattamento: governare l'algoritmo e le strutture logiche del suo funzionamento per far fronte tempestivamente alle richieste avanzate dagli utenti[49].
Il concetto di trasparenza algoritmica è dunque un fondamentale punto di partenza, ma non già anche la soluzione. Molti degli strumenti descritti nel precedente paragrafo, oggi alla base dei principali servizi che utilizziamo quotidianamente, già contribuiscono a rendere i provider maggiormente "*accountable*"[50] e trasparenti. Nonostante ciò, il dibattito scientifico è attualmente uno dei più accesi, e dovrà essere analizzato attentamente per capirne gli effetti sulla fiducia dei consumatori e

[44] Il *deep learning* è uno degli strumenti più avanzati di intelligenza artificiale che permette ad un algoritmo di imparare e migliorare le sue reazioni dalla rappresentazione fornita da grandi quantità di dati. Queste tecniche derivano dagli strumenti di riconoscimento facciale e vocale e attualmente sono in corso ricerche per esportarne i benefici in domini quali il riconoscimento di medicinali, droghe e genomi. Sul tema si veda, in particolare: Y. LeCun - Y. Bengio - G. Hinton, *Deep learning*, in *Nature*, 521/2015.
[45] Gran parte dei piani dell'Unione Europea per il Digital Single Market sono proprio rivolti ad aumentare la fiducia degli utenti in rete migliorando i livelli di protezione dei dati personali e la sicurezza. Sul tema si veda, in particolare: Commissione europea, *Digital Single Market, Digital Economy and Society, Digital Privacy*.
[46] Fin dal 2010, Viviane Reding (all'epoca Vice-presidente della Commissione Europea responsabile per il Direttorato Giustizia, Diritti Fondamentali e Cittadinanza) esponeva come «*we need to modernise our data protection rules, which date from 1995. We need to build up a trusted environment for the use of personal data. The internet's full potential will only be realised if it is seen as a trusted and open platform. This is where the European Union can make a difference*». Si veda, in particolare: V. Reding, *Building trust in Europe's Online Single Market*, 2010.
[47] Il Regolamento Generale sulla Protezione dei Dati, oltre ad aver rafforzato il generico diritto ad avere informazioni esaustive ed effettive sulle modalità di raccolta e di trattamento dei dati personali (artt. 13 e 14), ridisegna l'armamentario dei diritti, comprendendo il diritto d'accesso dell'interessato (art. 15), il diritto di rettifica (art. 16), il diritto alla cancellazione (art. 17), il diritto alla limitazione del trattamento (art. 18), il diritto alla portabilità dei dati (art. 20), nonché l'importantissimo diritto di opposizione al processo decisionale automatizzato relativo alle persone fisiche (art. 21).
[48] Questo particolare diritto emerge in varie regioni del Regolamento. *In primis*, il titolare del trattamento è obbligato ad informare il soggetto interessato dell'esistenza di un processo decisionale automatizzato, anche compreso l'eventuale trattamento di profilazione, e fornire informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato, sia nel caso in cui i dati siano raccolti presso l'interessato (art. 13), sia in caso in cui i dati non siano raccolti in sua presenza (art. 14).
[49] Alcuni attenti autori sottolineano le debolezze del Regolamento in questo ambito. Pare, infatti, che questo diritto non sia che un labile tentativo di rendere edotto *ex-ante* il soggetto interessato al fine della decisione in merito al consenso e che non possa invero agire in fase successiva all'avvenuto trattamento. Sulla questione, si veda 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.
[50] Sul concetto di *accountability* si veda, in particolare, European Data Protection Supervisor, *Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability*, Opinion, 19 novembre 2015.

sugli impatti che potrebbe avere nel mercato dei diversi motori di ricerca attivi in rete. Nonostante importanti gruppi di lavoro ne sottolineino i benefici[51], le critiche al concetto sono svariate e autorevoli[52], e muovono dalla necessità di mantenere nascoste certe metriche di calcolo per evitare raggiri all'algoritmo[53], alla necessità di rispettare il segreto industriale[54], fino ad indicarne la totale inutilità in varie occasioni[55] e addirittura all'incomprensibilità per gli utenti non dotati di conoscenze tecniche avanzate sulla materia[56]. Anche soluzioni simili quali procedure di *audit*[57] degli algoritmi sarebbero pressoché inefficaci.
L'unica soluzione ad oggi condivisa ritorna sul governo dell'algoritmo e delle sue componenti, in primis sulla correttezza delle basi esperienziali con cui il sistema è "allenato" in fase di avvio. Permettere al software di osservare una serie di decisioni in cui i bilanciamenti di interessi in gioco e la valutazione dell'accuratezza e della veridicità delle notizie sia svolta correttamente potrebbe aiutare ad ottenere decisioni automatizzate ottimali.
Quel che però serve sempre tenere a mente è che l'algoritmo è opera dell'ingegno di un essere umano, con le sue credenze e i suoi pregiudizi. Sempre un uomo lo governa e lo gestisce. Forse, la componente da valorizzare è proprio questa: ogni organizzazione che automatizza importanti decisioni fortemente impattanti sul nostro vivere quotidiano dovrebbe essere obbligata per legge a prevedere momenti di intervento umano in casi di difficile soluzione o non sicuramente prevedibili. Una figura - "*Artificial Intelligence Officer*"[58] - potrebbe essere pensata a supporto di questi controlli, oppure le medesime funzioni potrebbero essere gestite tramite richieste di *feedback* diffusi ad una comunità esperta e formata sulla specifica materia d'interesse[59] al fine di evitare soluzioni improvvisate, non ottimali o addirittura discriminatorie[60]. Ancora: e se questo ruolo fosse ricoperto da un agente software certificato che agisse come controllore dei principi giuridici ed etici durante il funzionamento dell'algoritmo?

6 Conclusioni

In conclusione, ciò che abbiamo di fronte a noi è chiaro: è necessario definire un percorso di ricerca per un'attenta gestione della conoscenza collettiva operata tramite la cura degli indici nei motori di ricerca[61], focalizzando l'attenzione sul governo degli algoritmi intelligenti che ne supportano l'attuazione. Siamo di fronte ad una nuova specie di oblio, che nasce dal bisogno intimo e personale di tutelare la proiezione sociale anche - ma non solo - in ambiente digitale, dove le regole del memorizzare e del cancellare (del conoscere e del dimenticare) sono sempre più imposte dagli algoritmi. Ogni soluzione che si raggiungerà non potrà prescindere dalla crescente importanza sociale del motore di ricerca che, collaborando proattivamente con gli utenti e governando adeguatamente gli algoritmi, avrà l'ardua responsabilità di limitare l'aggregazione delle fonti utili alla costruzione e

[51] Sul tema si veda, in particolare: F. Pasquale, *The Black Box Society - The Secret Algorithms That Control Money and Information*, Cambridge, 2015; R. Pollack-Ichou, *Opening the black box: in search of algorithmic transparency*, in Av.Vv. *GigaNet: Global Internet Governance Academic Network*, Annual Symposium, Chicago, 2016. Più recentemente, la US Association for Computing Machinery dell'US Public Policy Council ha pubblicato un documento che sintetizza i principi cardine della trasparenza algoritmica e di *accountability*. I princìpi sono: *awareness, access and redress, accountability, explanation, data provenance, auditability, validation and testing*. ACM US Public Policy Council, *Statement on algorithmic transparency and accountability*, 12 gennaio 2017.

[52] J. A. Kroll - J. Huey - S. Barocas - E.W. Felten - J.R. Reidenberg - D.G. Robinson - H. Yu, *Accountable algorithms*, in 165(3) *University of Pennsylvania Law Review* (2017), 633 ss.

[53] È stato dimostrato come, conoscendo l'algoritmo sottostante, sia possibile aggirare il sistema di controllo relativo al versamento delle tasse. In merito, si veda J. Reeves, *IRS Red Flags: How to Avoid a Tax Audit*, in www.usatoday.com. 3 maggio 2015.

[54] Basti pensare che gli algoritmi su cui si basano i risultati delle ricerche presentati da Google sono tra i più importanti segreti industriali dell'azienda, e mai potrebbero essere rivelati al grande pubblico contro la perdita di gran parte del potere di mercato.

[55] L'esempio classico riguarda gli algoritmi che presentano componenti di generazione di numeri randomici (si pensi alle lotterie ad estrazione automatica).

[56] Così, proprio J. A. Kroll - J. Huey - S. Barocas - E.W. Felten - J.R. Reidenberg - D.G. Robinson - H. Yu, *op cit.*, 24.

[57] In informatica, per audit si intende la revisione basata su evidenze di ciò che un algoritmo produce in output considerando uno specifico input. Sul tema, si veda D.W. Jones, *Auditing Elections*, ACM Computing Reviews, 2004.

[58] La figura dovrebbe presentare le seguenti caratteristiche: capacita tecniche in materia di intelligenza artificiale e conoscenza delle infrastrutture di gestione dei dati; abilità di lavorare tra le funzioni aziendali; abilita imprenditoriali; attitudine ad attrarre e mantenere altre capacità in materia di intelligenza artificiale. Si veda A. Ng, *Hiring your first chief AI Officer*, in *Harvard Business Review*, 2016. Svariate posizioni contro questa figura muovono dalla necessità di diffondere tra le figure aziendali già presenti le sensibilità necessarie a evidenziare possibilità e problemi in materia di intelligenza artificiale. Si veda, in particolare K.J. Hammond, *Please don't hire a Chief Artificial Intelligence Officer*, in *Harvard Business Review*, 2017. Ad ogni modo, le problematiche intorno questa figura potrebbero essere moltissime: chi è responsabile di controllarne l'operato? In base a quali principi giuridici o etici?

[59] Un ottimo esempio di collaborazione tra giornalisti e grande pubblico, basato su meccanismi di feedback diffusi per il *fact-checking* è la neonata piattaforma *WikiTribune*.

[60] Sulle conseguenze del *training* dell'algoritmo con fonti di origine razziali, si veda: B. Resnick, *How artificial intelligence learns to be racist*, in www.vox.com, 17 aprile 2017.

[61] Di fondamentale importanza per l'implementazione di questo diritto nell'organizzazione dei processi interni dei motori di ricerca è l'opinione dei Garanti europei che ha immediatamente seguito l'emanazione della sentenza Google Spain. Article 29 Data Protection Woking Party, *Guidelines on the implementation of the Court of Justice of the european union judgment on "Google Spain and inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" c-131/12*, 14/EN, WP225, adottato il 26 novembre 2014.

ricostruzione continua nel tempo del profilo dei soggetti interessati, riducendo le sfaccettature e i dettagli della persona che espone nella pubblica piazza digitale.
Certo è che, per continuare a far sì che i trattamenti dei dati personali siano al servizio dell'uomo[62], per continuare a rinforzare la tutela del diritto all'oblio in ambiente digitale nel rispetto di tutti gli altri diritti ed interessi coinvolti, rimarrà comunque necessaria una forte componente umana nel giudizio di bilanciamento, non trasponibile in algoritmo, da operare per imporre ad un sistema informatico di dimenticare. I molti ingranaggi di questo sofisticato meccanismo necessitano di essere quotidianamente oliati - raffinati dall'esperienza - evitando la deriva verso facili censure e abusi[63] che siano operati da umani o da algoritmi. Chissà poi se un cambiamento dirompente causato da strumenti decentralizzati e trasparenti come l'utilizzo della *blockchain*[64] per le liste del motore di ricerca riuscirà a supportare una tutela più efficace ed immediata dei diritti degli utenti, attivando quell'ancora oscuro principio di "responsabilizzazione"[65] del titolare del trattamento previsto dal Regolamento europeo.
Concludiamo ritornando al Sabatini-Colletti, per cui dimenticare è «perdere la memoria di qualcosa». Potremmo tentare un aggiornamento alla voce del noto dizionario. In ambiente digitale, dimenticare corrisponde a de-collegare molecole informative, tornando a frammentare l'informazione in nome della tutela dei nobili diritti fondamentali della persona, perdendo traccia di queste molecole nel profondo mare della conoscenza che è il web.

[62] Il Considerando 4 del Regolamento Generale sulla Protezione dei Dati enuncia che «il trattamento dei dati personali dovrebbe essere al servizio dell'uomo».
[63] Tra le tante critiche, la principale addita l'espansione del diritto alla cancellazione dei dati personali come un rischio alla libertà d'espressione in rete. Si veda, in particolare, D. Keller, *The new, worse 'right to be forgotten'*, in *Politico*, 27 gennaio 2016.
[64] Per le implicazioni della *blockchain* sulle policy europee si veda, in particolare: P. Boucher, *How blockchain technologies could change our lives*, in *European Parliament Research Service*, 2017.
[65] Il concetto di responsabilizzazione del titolare è riassunto dall'art. 5, comma 2, del Regolamento Generale sulla Protezione dei Dati, che attribuisce al titolare il dovere di comprovare il rispetto dei principi applicabili al trattamento dei dati personali elencati nel medesimo articolo, al comma 1.