Diritto all'oblio dei dati
Corso di computer ethics
2022

Francesco Guzzetta
Politecnico di Milano
francescoguzzetta97@gmail.com

Abstract

In questo lavoro si analizza un aspetto specifico legato alla privacy e alla teoria dell'informazione, ovvero la permanenza dei dati online. L'analisi riguarda le ripercussioni che "l'endurance" illimitata dei dati sulla Rete ha sull'individuo, sulla società e sull'ambiente. Viene proposta come soluzione quella di sancire un nuovo diritto: il diritto all'oblio. Questo per limitare la permanenza dell'informazione e i suoi conseguenti effetti negativi.

1. Introduzione

«La risorsa di maggior valore non è più il carburante, ma i dati»[1]. Con questo titolo si apre l'articolo del 2017 di *The Economist* che, insieme a tanti altri interventi nel dibattito pubblico, permette di capire il valore intrinseco dei dati e l'importanza della loro tutela. Fondamentale diventa, innanzitutto, la conoscenza di concetti quali *informazione* e *privacy* al fine di difendere al meglio i dati, ma allo stesso tempo consentire loro di fluire, perché «Intimamente connessi all'autonomia e alla dignità umana» [2].

Per quanto riguarda il concetto di *informazione*, se ne richiama la definizione: «Notizia, dato o elemento che consente di avere conoscenza più o meno esatta di fatti, situazioni, modi di essere.» [3].

Il concetto di *informazione* [4], invece, può attingere ai seguenti elementi:

- *scale* (condizioni di creazione, utilizzo e manipolazione del dato)
- *type* (tipologia del dato)
- *distribution* (modalità del flusso di informazioni)
- *endurance* (tempo e modalità di permanenza del dato)
- *magnifing effect* (l'effetto di amplificazione della propagazione del dato)

Il concetto di privacy è connesso all'informazione in quanto «La privacy è il grado [degree] fino al quale l'informazione riguardante l'essere umano non può essere né conosciuta né usata» [3].

In questo lavoro verrà analizzato un aspetto specifico legato all'informazione e alla privacy, ovvero la permanenza dei dati online. Se ne valuteranno i rischi diretti e indiretti che ne conseguono. Si è giunti alla soluzione di sancire il diritto all'oblio in relazione ai dati in quanto potrebbe fornire una efficace soluzione ai problemi che si pongono. Si noti che il diritto all'oblio non è presente né nella Dichiarazione Universale dei Diritti Umani [6] né nella legge italiana o europea [7] e talvolta viene ricompreso nel diritto all'identità personale, con conseguente minore efficacia. Infatti, si vuole sostenere la necessità di limitare la permanenza dei dati online al di là del fatto che essi violino direttamente l'identità personale.

2. Tutela delle persone fisiche

L'espressione "diritto all'oblio", estendendo il concetto illustrato ne *Il diritto all'oblio nel quadro dei diritti della personalità* di Giusella Finocchiaro [8], viene utilizzata in diverse accezioni di seguito riportate.

[1] «The World's Most Valuable Resource Is No Longer Oil, but Data.» [1]

[2] «intimately linked to autonomy and human dignity» [2]

[3] «Privacy is the degree to which human information is neither known nor used.»[5]

1. Accezione tradizionale

   Questa prima accezione vede i suoi albori nell'ordinamento giuridico italiano nel 1983 con il testo *Diritto alla riservatezza e "droit à l'oubli"* [9]. Più specificatamente, in questa pubblicazione si è cercato di comprendere «se la persona o le vicende legittimamente pubblicizzate possano sempre costituire oggetto di nuova pubblicizzazione o se, invece, il trascorrere del tempo e il mutamento delle situazioni non la rendano illecita»[4]. La giurisprudenza è giunta nel 1990 alla conclusione che il diritto all'oblio appartiene «alle ragioni e 'alle regioni' del diritto alla riservatezza»[5].

   In questa prospettiva, nei casi in cui sia pubblicizzata una vicenda, seppur vera e autentica, e sia trascorso un notevole tempo senza ulteriori eventi che giustifichino la riproposizione della notizia, la ri-pubblicizzazione costituirà una violazione del diritto all'identità personale. Infatti, le fonti della pubblicazione e della ripubblicazione sono ben distinte nel caso della stampa e sarà sufficiente evitare la seconda perché il trascorrere del tempo non venga azzerato.

   Quindi, l'informazione, per non ledere il diritto all'identità personale, non basta che sia veritiera e autentica, ma ha bisogno che sia di valore nel momento stesso della ri-pubblicizzazione. Come si vedrà nella prossima sezione, invece, nel caso della pubblicazione in rete vietare la riproposizione della notizia non è sufficiente a contestualizzarla temporalmente, dal momento che le informazioni pubblicate in rete tendono a perdere la dimensione temporale e appiattirsi sul presente.

2. Diritto all'oblio su internet

   Con l'avvento della rete internet, il tema oggetto di esame ha richiesto una più profonda trattazione che ha condotto a una seconda accezione di diritto all'oblio. La maggiore complessità è dovuta a due fattori principali:
   il primo, associato alle possibilità che la tecnologia legata a internet offre;
   il secondo, correlato alla natura dell'essere umano e, più precisamente, alla sua percezione.
   Approfondendo il primo punto si può facilmente notare che tra le proprietà specifiche della rete si possono annoverare la perenne disponibilità delle informazioni e l'enorme quantità di esse. La perenne disponibilità fa sì che la ripubblicazione di una vicenda non sia più necessaria poiché tutte le informazioni al riguardo sono sempre accessibili; la moltitudine di informazioni fa sì che spesso non siano tutte presenti in un unico luogo raggiungibile con una singola ricerca, ma siano sparse e non facilmente accessibili nel loro insieme.

   Un notevole impatto lo ha anche il secondo fattore analizzato, ovvero la percezione del lettore il quale, seppur di fronte a informazioni veritiere e distinte nel tempo, inconsciamente le "appiattisce"[6] nel presente. «Siamo di fronte a un continuum temporale e non più a [...] eventi puntuali» [11].

   La commistione di questi due fattori produce molto facilmente l'effetto di un' eterna ed erronea "attualizzazione" dell'informazione che ne distorce conseguentemente il valore.

   Parte del problema perciò riguarda lo sradicamento dell'avvenimento dal tempo, dallo spazio e dal contesto di origine[7] con un conseguente travisamento dell'identità del soggetto e, dunque, una violazione del diritto all'identità personale.

   In questa seconda prospettiva l'obbiettivo di tutelare l'identità personale non si risolve vietando la ripubblicazione (perché non vi è nemmeno una ripubblicazione), ma contestualizzandola, evitando al lettore di ricevere la singola informazione estrapolata dal motore di ricerca e consentendogli di essere messo nelle condizioni di acquisire la giusta prospettiva al riguardo. Per raggiungere lo scopo si dovrebbe corredare l'informazione originale con l'aggiunta degli elementi mancanti, innanzitutto quelli temporali.

   Poiché però, come si è detto, un rilievo notevole è legato alla percezione del lettore, non è detto che contestualizzare l'evento nel tempo eviti il rischio menzionato. Infatti, il lettore di fronte alla pagina web, malgrado in essa sia indicato un tempo passato, non riesce a percepirne la distanza. Una *endurance* illimitata mantiene sempre vivida la percezione dell'avvenimento falsandola e ciò a prescindere dagli ulteriori elementi di contesto ad essa aggiunti.

[4] T. Auletta, Diritto alla riservatezza ecc. op. cit., p. 129. [9]
[5] G.B. Ferri, Diritto all'informazione ecc. op. cit., p. 808. [10]

[6] Questa problematica è affrontata da V. Mayer-Schönberger, Delete: the virtue of forgetting in the digital age, Princeton University Press, 2011

[7] «la decontestualizzazione consiste nella enucleazione dell'immagine di un individuo dal contesto nel quale essa si trovava originariamente e collocazione in uno stato diverso, con l'effetto di creare un contrasto negativo esteriormente percepibile.» (V. Z. Zencovich. Onore e reputazione nel sistema del diritto civile. Jovene, 1985.) [12]

Quindi, l'informazione, per non ledere il diritto all'identità personale, non basta che sia veritiera e legittima, ma necessita quantomeno una completa contestualizzazione.

3. Il diritto all'oblio nel diritto europeo [8]

   La Direttiva europea 95/46 supera le accezioni sopra menzionate consentendo, da un lato, di agire sulla modifica e contestualizzazione dei dati e dall'altro aggiungendo la possibilità di eliminazione, blocco e congelamento dell'informazione. Inoltre si prevede la creazione di un' autorità di controllo che prende in carico le richieste riguardo la tutela delle persone e il trattamento dei dati. La suddetta autorità, come stabilito nell'art. 28 di tale Direttiva, ha il potere di «di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento». In questa nuova accezione di diritto all'oblio viene quindi considerata anche la possibilità di eliminazione e blocco dell'informazione se veridicità e contestualizzazioni non sono possibili o se non sufficienti alla tutela della persona.

   Questo è in qualche modo un punto di svolta, in quanto con detta terza accezione si conferisce all'individuo, seppur in maniera indiretta, la possibilità di esigere un' eliminazione dei dati allorché la propria identità personale sia stata lesa con un vero e proprio oblio dei dati. Rispetto ai casi precedenti si ha quindi un modo per agire attivamente ed efficacemente visto che ci si può avvalere di tale norma anche rispetto ai motori di ricerca[9], i quali possono effettivamente rendere "irraggiungibile" l'informazione (anche qualora l'ente o persona che ha pubblicizzato l'informazione ne sia il possessore, come nel caso di editori di giornali).

In tutte queste valutazioni non è stato preso in considerazione il diritto alla libertà di espressione, che potrebbe sembrare, a una prima lettura, in contraddizione con il diritto di oblio per come sancito nella Dichiarazione Universale dei Diritti Umani[10], sopratutto nel caso in cui i dati possano essere del tutto eliminati. Tuttavia, in realtà, si tiene conto di questa argomentazione nel documento Europeo *General Data Protection Regulation*, nel quale viene esplicitamente scritto che l'eliminazione e il blocco dei dati sono consentiti solo nel caso in cui non siano in netto contrasto con «il Diritto alla libertà di espressione» o ci siano «interessi pubblici» da difendere [11]. Tali limitazioni, peraltro, sono consentite generalmente anche dalle Costituzioni nazionali che riconoscono il diritto di manifestazione del pensiero.

3. Ulteriori aspetti problematici

Dopo aver discusso il tema del diritto all'oblio nell'ambito della difesa dell'identità personale ora il discorso si amplierà ad ulteriori aspetti problematici legati all'*endurance* dei dati online. Tra le informazioni che vengono condivise ogni giorno sulla rete ci sono dati di tutti i tipi: da quelli "sensibili" a quelli che non hanno apparentemente importanza e rilevanza per il singolo (cosa viene comprato al supermercato, cosa piace su instagram o che ricerche vengono fatte sul web).

Queste informazioni permettono alla persona di avere interazioni sociali o miglioramenti nei servizi che vengono utilizzati tutti i giorni, quali per esempio, Google maps, pubblicità di maggiore interesse, feed sui social network. A questi si aggiungono anche le informazioni che permettono di avere una vita più comoda come aprire la serratura dell'autovettura o della casa senza un chiave fisica, o accendere e spegnere la luce senza bisogno di alzarsi da dove ci si trova.

Non si discute però a sufficienza dei rischi che possono derivare dalla cattiva gestione di queste informazioni. A partire dai casi citati, i possibili rischi potrebbero essere, ad esempio, l'assunzione illecita delle credenziali per entrare nelle abitazioni e commettere furti o la sottrazione dei dati bancari o sanitari di un individuo con lo scopo di estorsione o ricatto. Esistono, inoltre, rischi legati a pregiudizi quali quelli connessi all'orientamento sessuale, al genere, all'appartenenza religiosa, ecc. che potrebbero incidere in ambito lavorativo, nel

[8] Si veda la Direttiva europea 95/46 del 1995 agli Art. 12 e Art. 28 [13]

[9] La Corte di Giustizia dell'Unione Europea si pronuncia con la sentenza del 13 maggio 2014 (causa c131/12) del caso Google Spain così: «Per quanto concerne la portata del diritto di cancellazione e/o opposizione al trattamento di dati in relazione al diritto all'oblio, si chiede: se si debba ritenere che i diritti di cancellazione e congelamento dei dati, disciplinati dall'articolo 12, lettera b), e il diritto di opposizione al loro trattamento, regolato dall'articolo 14, [primo comma,] lettera a), della direttiva [95/46], implichino che l'interessato può rivolgersi ai motori di ricerca per impedire l'indicizzazione delle informazioni riguardanti la sua persona pubblicate su pagine web di terzi».[14]

[10] «Ogni individuo ha diritto alla libertà di opinione e di espressione incluso il diritto di non essere molestato per la propria opinione e quello di cercare, ricevere e diffondere informazioni e idee attraverso ogni mezzo e senza riguardo a frontiere.» [6]

[11] «However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.» [7]

caso alcune informazioni private vengano alla luce, anche quando innocue e perfettamente lecite, tanto da portare al demansionamento o al licenziamento. La non corretta gestione dei dati potrebbe anche portare semplicemente alla fuoriuscita di informazioni che non si vuole condividere con il mondo, ma solo con una ristretta cerchia di familiari, amici, o partner e che se sottratti possono portare a conseguenze pregiudizievoli, o in casi estremi potrebbero favorire l'instaurazione e il mantenimento dei così detti *governi di sorveglianza*. Inoltre l'indiscriminata e illimitata permanenza dei dati online tende a esaltare tutti questi rischi[12], che si ha la tendenza a sottovalutare. Questo è parzialmente dovuto all'assuefazione[13] e alla sottovalutazione del fenomeno. Infatti, il più delle volte ci si ritiene al riparo da tutte queste possibili eventualità perché difesi dalle normative sulla privacy, dalla possibilità di anonimato online e dall'aver prestato il consenso al trattamento dei propri dati. Questo fa sì che ci sia quindi un' illusione di potere di gestione dei propri dati e conseguentemente un' apparente protezione riguardo agli stessi.

Per spiegare però come da questi dati si possa giungere ai rischi sopra descritti è necessario introdurre il concetto di *inferenza* [14]. Questa è un processo di elaborazione attraverso il quale una serie di informazioni note consentono di conoscere, o quantomeno ipotizzare, in maniera molto accurata, una serie di altri fatti riguardanti l'individuo.

Per comprendere meglio in cosa consiste in pratica l'inferenza e come essa sia possibile si può suddividere il problema in due parti. La prima riguarda l'accumulo dei dati per creare un modello e identificare pattern di comportamento. La seconda è lo sfruttamento dei comportamenti identificati per prevedere future scelte o acquisire informazioni aggiuntive riguardo l'individuo.

Per quanto riguarda l'identificazione dei pattern essa è possibile grazie alla moltitudine di dati raccolti su ciascuno, come per esempio sugli spostamenti o su cosa viene comprato nei negozi. Se questi pattern vengono poi riconosciuti nel comportamento di un individuo si possono inferire e dedurre informazioni aggiuntive sul suo conto. La nota azienda di merchandising Target è un esempio efficacie del potere dell'inferenza, in quanto è riuscita a creare un modello che, in base agli acquisti al supermercato dell'individuo, permette di sapere se si tratti di una donna incinta o meno. E ciò che rende il modello ancor più eccezionale è che è in grado di farlo nelle prime 20 settimane di gravidanza. Questo tipo di processi di inferenza vengono svolti dalle aziende in modo da poter mandare pubblicità specifiche per il singolo consumatore che, nel caso analizzato, sono pubblicità su prodotti per l'infanzia[15].

Da questo esempio si può dedurre che le problematiche più strettamente legate alla privacy riguardano l'acquisizione di una moltitudine di dati e la possibilità di associarli a un individuo specifico. Ma il vero potere dell'inferenza non è tanto quella di raccogliere i dati, in quanto vengono forniti dell'utente stesso, ma piuttosto la possibilità di predire e ottenere informazioni aggiuntive sull'individuo.

Si potrebbe obiettare che però queste ultime sono associate non tanto al proprio nome e cognome, quanto a un identificativo anonimo che l'azienda fornisce, spesso composto da numeri e lettere in ordine casuale e quindi in pratica scorrelate dal nome. Non per questo non è violata la nostra privacy, da intendersi come controllo su chi possa accedere alle proprie informazioni.

Come viene messo il luce in *Big Data's End Run around Anonymity and Consent* , questo «unico e persistente identificativo deve essere inteso come uno pseudonimo più che "un identificativo anonimo"» [16]. Perciò in pratica «anche quando gli individui non sono "identificabili", potrebbero comunque essere "raggiungibili"»[17] con pubblicità, mail e chiamate facendo sì che il controllo sulle informazioni non sia più nelle mani di ciascuno, ma piuttosto nelle mani di chi le gestisce.

Si potrebbe allora proporre la soluzione di criptare i dati, così da non permettere al gestore o eventuali intermediari il "raggiungimento" della persona, di fatto risolvendo il problema del *Data-Reachability*[18].

[12] Se si volessero analizzare in maniera più specifica tutti i rischi elencati lo si può fare con il libro *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage* [15]

[13] Quello che prima sconvolgeva e in qualche modo inquietava riguardo la messa a disposizione delle informazioni online (il caso per esempio del primo Facebook), per chiunque in qualsiasi momento, è oggi considerata normale e talvolta è considerato non normale il fatto di non pubblicare tutta la nostra vita online.

[14] Nel linguaggio filos., ogni forma di ragionamento con cui si dimostri il logico conseguire di una verità da un'altra; sinon. quindi di illazione. Regole d'i., in un sistema deduttivo, l'insieme delle regole secondo le quali le proposizioni possono essere dedotte dai postulati. [3]

[15] Se si volesse approfondire il tema interessante è l'articolo di Forbes sull'esempio appena descritto [16]

[16] «a unique persistent identifier should be understood as a pseudonym rather than an 'anonymous identifier'» [17]

[17] La frase completa approfondisce ancora il problema sostenendo: «Even when individuals are not 'identifiable', they may still be 'reachable', may still be comprehensibly represented in records that detail their attributes and activities, and may be subject to consequential inferences and predictions taken on that basis.» [17]

[18] Questione ulteriormente approfondita in *A Data-Reachability Model for Elucidating Privacy and Security Risks Related to the Use of Online Social Networks*

Anche la criptazione dei dati non ha un effetto risolutivo. Infatti, un recente studio su *Privacy-Protected Databases*[18] ha illustrato come la criptazione di un database non è affatto sufficiente a evitare l'inferenza che porta, comunque, a risultati con una predizione accurata nel 97% dei casi.

Come è stato mostrato, poichè non è sufficiente proteggere le informazioni, un più efficacie strumento di tutela potrebbe essere costituito dalla limitazione dell' *endurance* dei dati. Un limite temporale legato alla permanenza dei dati online diminuisce, se non addirittura elimina, gran parte dei rischi associati e causati dall'inferenza. Questo perché con pochi dati non è possibile costruire modelli sufficientemente accurati e di conseguenza non si può inferire nulla sulle informazioni dell'individuo. Ovviamente questo processo di eliminazione può e deve avere delle direttive che ne gestiscano le tempistiche di permanenza in relazione alla loro importanza e a tutti i concetti che sono stati precedentemente espressi.

Viene però immediato chiedersi cosa possa fare il gestore dei dati nel caso non volesse adottare la strategia di conferire a questi ultimi una data di scadenza. Una soluzione potrebbe trovarsi nel chiedere il consenso all'utente riguardo alla gestione dei propri dei dati. In questo modo la responsabilità dei rischi non ricadrebbe sul gestore. Questo naturalmente è vero se gli utenti fossero anche perfettamente informati e quindi coscienti riguardo a cosa stanno prestando il consenso. Per quanto possa essere «assurdo credere che il consenso possa specificare tutti i termini di interazione tra il richiedente i dati e il soggetto» [19] si proverà a ipotizzarlo e a procedere di conseguenza. Quindi, ammettendo che il gestore riesca a fornire tutte le spiegazioni all'utente attraverso l'informativa sulla privacy, necessariamente lunga e complessa, come si può pretendere che ogni utente possa leggerla? L'impossibilità però di stare al passo con queste norme è emersa in un noto studio del 2009 il quale mostra che ad oggi , se si leggessero anche solo rapidamente, tutte le normative sulla privacy di ogni sito visitato annualmente, l'ammontare di tempo impegnato sarebbe di 76 giorni[19]. Questo numero aumenterebbe nel caso ipotetico analizzato, in cui le normative sulla privacy fossero più complete di quanto già non siano.

La situazione potrebbe ulteriormente peggiorare se l'utente dovesse rileggere l'informativa sulla privacy ogni qualvolta questa venga aggiornata. Il tema della rilettura, infatti, è posto anche dalla politica sulla privacy di Amazon che non la valuta come una difficoltà. Il colosso dell'e-commerce (e non solo) infatti scrive sulla sua pagina: [siccome] «Il nostro business cambia costantemente, e anche le nostre politiche sulla privacy lo faranno. Voi dovreste controllarle spesso sul nostro sito per vedere i cambiamenti più recenti.»[20]. Questo fa sì che siano poche, per non dire nessuna, le persone che effettivamente leggono le normative alle quali si fornisce il consenso.

La soluzione sarebbe quella di semplificare e sintetizzare tali normative in modo da renderle fruibili e quindi permettere all'utente di prestare un consenso informato. Ma così facendo si ricadrebbe facilmente nel paradosso esposto da Helen Nissembaum ovvero il *trasparency paradox* [21], secondo cui la semplicità che si vorrebbe ottenere nelle *privacy policies* condurrebbe a una netta perdita di fedeltà del documento. In questo modo, l'ipotesi iniziale che il gestore riesca ad ottenere un consenso dei termini sulla privacy, in maniera informata all'utente, crolla definitivamente.

Nonostante si sia giunti a un nodo Gordiano, che rende impossibile la soluzione, si può considerare il caso ideale di avere risolto il problema descritto nel seguente modo: il gestore dei dati ha stilato una normativa sulla privacy pienamente accurata che dopo essere stata letta è stata acconsentita solo dagli utenti che si assumono tutti i rischi del caso e tutti gli utenti che invece non siano favorevoli non utilizzino l'applicazione, non visitino il sito o non comprino il dispositivo sotto analisi[21].

In detta ipotesi astratta tutti coloro che hanno negato il consenso non dovrebbero essere sottoposti ai rischi che l'inferenza porta con sé. La tesi crolla di fronte allo studio di Mislove, che sostiene che «si può risalire a molteplici attributi globali attraverso tecniche di inferenza quando anche solo il 20% degli utenti rivelano le informazioni riguardo i loro attributi»[22]. Questo concetto è definito come *The Tiranny of the Minority* e fa sì che anche assumendo valide le molteplici ipotesi (molto stringenti e irrealistiche) non si possa bloccare il processo di inferenza e che anche non conferire il consenso sia una difesa insufficiente.

Qualora tutte queste difficoltà, con improbabile completa soluzione, possano effettivamente essere superate, permane comunque il problema relativo al rischio di furto delle informazioni che è maggiore se maggiore è il tempo di permanenza. Naturalmente questa è una

[19] «In the case of consent, too, commonly perceived operational challenges have distracted from the ultimate inefficacy of consent as a matter of individual choice and the absurdity of believing that notice and consent can fully specify the terms of interaction between data collector and data sub- ject.»[17]

[20] "Our business changes constantly, and our Privacy Notice will change also. You should check our websites frequently to see recent changes."[20]

[21] ipotesi molto poco realistica ma che non verrà analizzata più a fondo per semplicità di trattazione.

[22] «multiple attributes can be inferred globally when as few as 20% of the users reveal their attribute information.»[22]

problematica molto meno complessa da risolvere, ma necessita comunque di essere citata in quanto molto spesso i dati non sono criptati o difesi a sufficienza dai gestori [23].

4. Rischi per l'ambiente

La questione legata alla permanenza dei dati non si limita alla singola persona ma estende il prorpio impatto sulla società e sull'ambiente. Ciò è dovuto al fatto che l'elaborazione, trasporto, gestione e mantenimento di tutte queste informazioni ha un costo in termini di energia utilizzata e risorse, come per esempio l'acqua [24], oltre che tutte le materie prime necessarie per la costruzione di tali strutture. Gli impianti ai quali si sta facendo riferimento sono i *Data Center* che sono «strutture centralizzate dove i componenti per la computazione e collegamenti alla rete sono concentrati per il raccolta, archivio, accesso, distribuzione e elaborazione di enormi quantità di dati» [25]. Per cercare di comprendere la dimensione, la complessità e grandezza dei *Data Center* si può partire dall'attuale dimensione di *Internet* stimata intorno a 23 Zettabytes [27], ovvero 23.000.000.000.000.000.000.000.000 Bytes (ventitré ottilioni di byte). Si può visualizzare questa memoria immaginando che venga contenuta in 489.361.7021.276.595 DVD che, se impilati l'uno sull'altro, porterebbero ad avere una lunghezza di circa 55300 volte quella del sistema solare[26].
Questa mole immensa di dati è gestita ad un altissimo livello di efficienza energetica [29], ma nonostante ciò i *Data Centers* hanno un consumo pari all'1-1.5% [30] dell'energia elettrica prodotta a livello globale, che si traduce perciò in un impatto a livello di gas a effetto serra (prevalentemente CO_2) pari al 2% delle emissioni globali. Per comprenderne l'entità basti pensare che tale consumo equivale alla percentuale complessiva relativa all'intero settore dei trasporti aerei[31]. Per quanto riguarda il consumo di acqua, per la gestione degli impianti di raffreddamento e di energia, anche se basso in termini relativi il valore assoluto è comunque pari a 1.7 miliardi di litri al giorno solo negli USA [32]. Il futuro al riguardo non migliora affatto se si considera l'ancora neonata *Industria 4.0* e l'*Internet of Things* che ad oggi contano 35 miliardi di dispositivi e che si stimano aumentare a 120 miliardi entro il 2025 con un afflusso di dati corrispondenti a 180 trillioni di gigabyte [33]. Globalmente quindi si stima che si possa arrivare fino a 40 volte il consumo energetico attuale entro il 2030 [34]. Per semplicità si è analizzato tutto ciò che riguarda i *Data Center* in maniera diretta ma un impatto importante lo hanno anche tutti i consumi indiretti, come viene analizzato nel *United States Data Center Energy Usage Report* [25]. Il vero problema però non è tanto il flusso di informazioni, quanto il mantenimento indeterminato di questi dati e il riutilizzo degli stessi. Quest'ultimo è necessario, nell'ordine attuale delle cose, in quanto uno degli elementi caratteristici dell'industria dei *Big Data* che gestisce questa infinita mole di dati è la "*voracità*" [35]. La maggiore quantità di dati, infatti, fornisce alle grandi compagnie i mezzi per fare previsioni e conseguentemente incrementare il fatturato.

Il tema dell'*endurance* dei dati perciò è molto delicato e limitare la permanenza dell'informazione significherebbe anche limitare i profitti di grandi compagnie, ma come si è sostenuto l'impatto che questo ha, ma sopratutto avrà, sull'ambiente non permette più di soprassedere sull'argomento. Limitare l'*endurance* è infatti un possibile metodo risolutivo efficace e pressocchè istantaneo di fronteggiare il problema. Attualmente tale ipotesi non è neanche presa in considerazione tra le sfide che pone l'industria dei *Big Data* come mostra anche lo studio *Addressing big data challenges for scientific data infrastructure* [36].

5. Conclusione

In conclusione, si può sostenere che molte sono le sfide giuridiche, etiche e ambientali che la gestione dei dati, sopratutto dovuta a *Internet*, porta con sé rispetto al singolo, alla società e al pianeta. Ma se *Internet* e l'*endurance* dei dati sono il problema, potrebbero rivelarsi la loro soluzione[27]. Perciò diventa un imperativo etico usare queste risorse per la prosperità della collettività e del pianeta ed è importante elaborare strategie che possano migliorare l'utilizzo della rete e la gestione delle informazioni in essa contenute.

[23] Se si volesse analizzare più a fondo il compromesso che viene fatto tra sicurezza e complessità di gestione dei database per avere un idea del problema e della sua diffusione si rimanda allo studio dell'NYU *Understanding Password Database Compromises*[23] o se si vuole una più accurata visione del problema nel suo complesso si rimanda a *Top Ten Big Data Security and Privacy Challenges* [24]

[24] Tematica approfondibile nell' "*United states data center energy usage report*" [25]

[25] «Data centers are centralized locations where computing and networking equipment is concentrated for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of data.» [26]

[26] Questo potrebbe far sorgere il dubbio di come riescano a essere contenuti sulla terra tutti questi dati. La risposta risiede nelle innovative tecniche di memorizzazione elettroniche e ottiche che permettono di diminuire la dimensione fisica delle memorie di vari ordini di grandezza. Breve storia delle memorie è visualizzabile online sul sito: "https://www.computerhistory.org/timeline/memory-storage/" [28]

[27] Estremamente interessante al riguardo è lo studio della Global e-Sustenability initiative [37]

In questo lavoro si è ritenuto che una delle possibili soluzioni sia la limitazione dell'*endurance* dell'informazione che richiede un intervento legislativo per la creazione di un nuovo diritto: *il diritto all'oblio* nella sua declinazione del *diritto all'oblio dei dati*.

Riferimenti bibliografici

[1] Sam Jossen. The world's most valuable resource is no longer oil, but data. *The Economist*, pages 1–8, 2017. 1

[2] MACILER CHARITY MBULA. A review on europe's general data protection regulation. 2019. 1

[3] Enciclopedia treccani online con ultimo accesso 0l /01/2023. 1, 4

[4] Viola Schiaffonati. Computer ethics information flow, privacy, and surveillance. 2022. 1

[5] Neil Richards. *Why Privacy Matters*. Oxford University Press, 2021. 1

[6] Assemblea Generale delle Nazioni Unite. Dichiarazione universale dei diritti umani. *Retrieved June*, 28:2016, 1948. 1, 3

[7] Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation) (text with eea relevance), [2016] oj l 119/1. 1, 3

[8] Giusella Finocchiaro. ll diritto all'oblio nel quadro dei diritti della personalità. *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, 2016. 1

[9] Tommaso Amedeo AULETTA. Diritto alla riservatezza e« droit à l'oubli». *L'informazione ei diritti della persona. Jovene, Napoli*, 127, 1983. 2

[10] GB Ferri. Diritto all'informazione e diritto all'oblio, in. *Rivista di diritto civile*, (1), 1990. 2

[11] Giusella Finocchiaro. La memoria della rete e il diritto all'oblio. *Diritto dell'Informazione e dell'Informatica, Il*, 26(3):391, 2010. 2

[12] Vincenzo Zeno Zencovich. *Onore e reputazione nel sistema del diritto civile*. Jovene, 1985. 2

[13] 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 gazzetta ufficiale n. l 281 del 23/11/1995 pag. 0031 - 0050. 3

[14] Corte di giustizia ue, sentenza del 13 maggio 2014, causa c131/12; google spain sl,google inc. contro agencia española de protección de datos (aepd). la corte (grandesezione), composta da v. skouris, presidente, k. lenaerts, vicepresidente, m. ilešič (relatore), l.baylarsen,t.vondanwitz,m. safjan,presidentidisezione,j.malenovský,e.levits, a.Ó caoimh,a.arabadjiev,m.berger,a.prechalee.jarašičnas,giudici, avvocato generale: N. jääskinen. 3

[15] Oscar H Gandy. *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*. Routledge, 2016. 4

[16] Kashmir Hill. How target figured out a teen girl was pregnant before her father did. *Forbes, Inc*, 2012. 4

[17] Solon Barocas and Helen Nissenbaum. Big data's end run around anonymity and consent. *Privacy, big data, and the public good: Frameworks for engagement*, 1:44–75, 2014. 4, 5

[18] Vincent Bindschaedler, Paul Grubbs, David Cash, Thomas Ristenpart, and Vitaly Shmatikov. The tao of inference in privacy-protected databases. *Cryptology ePrint Archive*, 2017. 5

[19] Alexis C Madrigal. Reading the privacy policies you encounter in a year would take 76 work days. *The Atlantic*, 1, 2012. 5

[20] Amazon privacy notice su https://www.amazon.com/gp/help/customer/display.html?nodeid=468496 (ultima visita 6/12/2022). 5

[21] Helen Nissenbaum. A contextual approach to privacy online. *Daedalus*, 140(4):32–48, 2011. 5

[22] Alan Mislove, Bimal Viswanath, Krishna P Gummadi, and Peter Druschel. You are who you know: inferring user profiles in online social networks. In *Proceedings of the third ACM international conference on Web search and data mining*, pages 251–260, 2010. 5

[23] Dennis Mirante and Justin Cappos. Understanding password database compromises. *Dept. of Computer Science and Engineering Polytechnic Inst. of NYU, Tech. Rep. TR-CSE-2013-02*, 2013. 6

[24] A cloud security alliance collaborative research, expanded top ten big data security and privacy challenges. 2013. 6

[25] Arman Shehabi, Sarah Smith, Dale Sartor, Richard Brown, Magnus Herrlin, Jonathan Koomey, Eric Masanet, Nathaniel Horner, Inês Azevedo, and William Lintner. United states data center energy usage report. 2016. 6

[26] Pagina: "https://densenetworks.com/data-center" con accesso tra il: 8/12/2022. 6

[27] Pagina: "https://densenetworks.com/data-center" con accesso tra il: 15/12/2022. 6

[28] "timeline of computer history" reperibile su: "https://www.computerhistory.org/timeline/memory-storage/" con accesso tra il: 10/12/2022. 6

[29] Jumie Yuventi and Roshan Mehdizadeh. A critical analysis of power usage effectiveness and its use in communicating data center energy consumption. *Energy and Buildings*, 64:90–94, 2013. 6

[30] Eric Masanet, Arman Shehabi, Nuoa Lei, Sarah Smith, and Jonathan Koomey. Recalibrating global data center energy-use estimates. *Science*, 367(6481):984–986, 2020. 6

[31] Yingbo Zhang, Kui Shan, Xiuming Li, Hangxin Li, and Shengwei Wang. Research and technologies for next-generation high-temperature data centers–state-of-the-arts and future perspectives. *Renewable and Sustainable Energy Reviews*, 171:112991, 2023. 6

[32] David Mytton. Data centre water consumption. *npj Clean Water*, 4(1):1–6, 2021. 6

[33] Sivadi Balakrishna, M Thirumaran, and Vijender Kumar Solanki. A framework for iot sensor data acquisition and analysis. *EAI Endorsed Transactions on Internet of Things*, 4(16):e4–e4, 2018. 6

[34] Ralph Hintemann and Simon Hinterholzer. Energy consumption of data centers worldwide. *Business, Computer Science (ICT4S)*, 2019. 6

[35] Yuri Demchenko, Canh Ngo, Cees de Laat, Peter Membrey, and Daniil Gordijenko. Big security for big data: Addressing security challenges for the big data infrastructure. In *Workshop on secure data management*, pages 76–94. Springer, 2013. 6

[36] Yuri Demchenko, Zhiming Zhao, Paola Grosso, Adianto Wibisono, and Cees De Laat. Addressing big data challenges for scientific data infrastructure. In *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, pages 614–617. IEEE, 2012. 6

[37] Accenture Strategy. Smarter2030: Ict solutions for 21st century challenges. *The Global eSustainability Initiative (GeSI), Brussels, Brussels-Capital Region, Belgium, Tech. Rep*, 3, 2015. 6