

EUROPEAN DATA PROTECTION SUPERVISOR

Parere 4/2015

# Verso una nuova etica digitale

*Dati, dignità e tecnologia*



EDPS

11 settembre 2015

*Il Garante europeo della protezione dei dati (GEPD) è un'istituzione indipendente dell'UE che, ai sensi dell'articolo 41, paragrafo 2, del regolamento 45/2001, ha il compito di «garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, riguardo al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari», e «(...) di fornire alle istituzioni e agli organismi comunitari nonché agli interessati pareri su tutte le questioni relative al trattamento dei dati personali». Il Garante è stato nominato nel dicembre 2014 congiuntamente al Garante aggiunto, con il mandato specifico di essere più costruttivo e proattivo. Nel marzo 2015 il GEPD ha pubblicato una strategia quinquennale, nella quale ha delineato il modo in cui intende attuare tale mandato e assumerne la responsabilità.*

*Il presente parere fa seguito al precedente parere del GEPD concernente il regolamento generale sulla protezione dei dati, inteso ad aiutare le principali istituzioni dell'UE nella ricerca di un consenso su un insieme di norme attuabili e orientate al futuro, che valorizzino i diritti e le libertà della persona. Come il parere sulla sanità mobile all'inizio del 2015, anche questo affronta la sfida della protezione dei dati nella transizione al sistema digitale – il terzo obiettivo della strategia del GEPD – con l'obiettivo di «adattare i principi esistenti di protezione dei dati alla realtà digitale globale», tenendo conto anche dei piani dell'UE per il mercato unico digitale. Il presente parere è coerente con l'approccio del Gruppo dell'articolo 29 sugli aspetti, inerenti alla protezione dei dati, dell'uso delle nuove tecnologie, come l'«Internet degli oggetti» a cui il GEPD ha contribuito come membro a pieno titolo del gruppo.*



Dignity	Dignità
Future-oriented rules and enforcement	Norme orientate al futuro e loro applicazione
Accountable controllers	Responsabilità degli addetti al controllo dei dati
Empowered individuals	Conferimento di maggiore autonomia alle persone
Innovative privacy engineering	Ingegneria della privacy innovativa
Ethics	Etica

**«La dignità umana è inviolabile. Essa deve essere rispettata e tutelata».**

**Articolo 1,** Carta dei diritti fondamentali dell'UE

**I diritti fondamentali alla vita privata e alla protezione dei dati personali sono diventati più importanti che mai per la tutela della dignità umana.** Essi sono sanciti dai trattati dell'UE e dalla Carta dei diritti fondamentali dell'UE. Permettono agli individui di sviluppare la propria personalità, condurre una vita indipendente, innovare ed esercitare altri diritti e libertà. I principi di protezione dei dati definiti nella Carta dell'UE – necessità, proporzionalità, equità, minimizzazione dei dati, limitazione delle finalità, consenso e trasparenza – si applicano al trattamento dei dati nella sua interezza, alla raccolta come all'utilizzo.

**La tecnologia non dovrebbe dettare valori e diritti; il rapporto tra questi, tuttavia, non dovrebbe nemmeno essere ridotto a una falsa dicotomia.** La rivoluzione digitale promette benefici per la salute, l'ambiente, lo sviluppo internazionale e l'efficienza economica. Nel quadro dei piani dell'UE per un mercato unico digitale, il cloud computing, l'«Internet degli oggetti», i megadati e altre tecnologie sono considerati fondamentali per la competitività e la crescita. I modelli aziendali stanno sfruttando nuove funzionalità per la raccolta massiccia, la trasmissione istantanea, la combinazione e il riutilizzo di dati personali per finalità non previste, giustificate da lunghe e impenetrabili informative sulla protezione dei dati. Questo ha esposto i principi della protezione dei dati a nuove pressioni, che richiedono un rinnovamento di pensiero quanto al modo in cui vengono applicati.

**Nell'attuale ambiente digitale, il rispetto della legge non è sufficiente: dobbiamo considerare la dimensione etica del trattamento dei dati.** Il quadro normativo dell'UE lascia già spazio a decisioni e misure di salvaguardia flessibili e puntuali nella gestione delle informazioni personali. La riforma del quadro normativo costituirà un passo avanti positivo. Si pongono tuttavia interrogativi più profondi per quanto riguarda l'impatto che le tendenze in una società basata sui dati hanno sulla dignità, la libertà individuale e il funzionamento della democrazia.

**Tali questioni presentano implicazioni di tipo ingegneristico, filosofico, giuridico e morale.** Il presente parere mette in luce alcune importanti tendenze tecnologiche che possono comportare un trattamento delle informazioni personali inaccettabile o interferire con il diritto alla vita privata. Esso delinea un «ecosistema di protezione dei megadati» articolato su quattro livelli, per rispondere alla sfida del digitale: uno sforzo collettivo fondato su considerazioni etiche.

- (1) Regolamentazione del trattamento dei dati orientata al futuro e rispetto del diritto alla vita privata e del diritto alla protezione dei dati.
- (2) Presenza di responsabili che definiscono il trattamento dei dati personali.
- (3) Progettazione e creazione di prodotti e servizi di trattamento dei dati rispettose della vita privata.
- (4) Conferimento di maggiore autonomia alle persone.

**Il Garante europeo della protezione dei dati intende incentivare un dibattito aperto e informato fuori e dentro l'UE,** che coinvolga società civile, autori e progettisti, aziende, accademici, autorità e organismi di regolamentazione pubblici. Il nuovo comitato etico per la

protezione dei dati dell'UE, che sarà istituito dal GEPD, contribuirà a definire una nuova etica digitale, permettendo di ottimizzare i benefici della tecnologia per la società e l'economia, in modalità tali da rafforzare i diritti e le libertà dei singoli.

## INDICE

<b>1. L'onnipresenza dei dati: tendenze, opportunità e sfide .....</b>	<b>7</b>
1.1 MEGADATI.....	7
1.2 L'«INTERNET DEGLI OGGETTI» .....	8
1.3 AMBIENT COMPUTING (INFORMATICA AMBIENTALE).....	8
1.4 CLOUD COMPUTING .....	9
1.5 MODELLI AZIENDALI DIPENDENTI DAI DATI PERSONALI.....	9
1.6 DRONI E VEICOLI AUTONOMI .....	10
1.7 TENDENZE CON UN'INCIDENZA POTENZIALMENTE MAGGIORE E A LUNGO TERMINE	10
<b>2. Un ecosistema di protezione dei megadati .....</b>	<b>11</b>
2.1 UNA NORMATIVA ORIENTATA AL FUTURO .....	11
2.2 ADDETTI AL CONTROLLO DEI DATI RESPONSABILI .....	12
2.3. INGEGNERIA RISPETTOSA DELLA VITA PRIVATA .....	12
2.4 CONFERIMENTO DI MAGGIORE AUTONOMIA ALLE PERSONE.....	13
<i>Un ambiente di «prosumatori» .....</i>	<i>13</i>
<i>Consenso.....</i>	<i>13</i>
<i>Controllo e «proprietà» dei dati.....</i>	<i>13</i>
<b>3. La dignità al centro di una nuova etica digitale .....</b>	<b>14</b>
3.1 DIGNITÀ E DATI .....	14
3.2 UN COMITATO CONSULTIVO ETICO EUROPEO.....	16
<b>4. Conclusione: è tempo di approfondire il dibattito .....</b>	<b>16</b>
<b>Note .....</b>	<b>18</b>

## 1. L'onnipresenza dei dati: tendenze, opportunità e sfide

Quantità crescenti di dati personali vengono raccolte e trattate con modalità sempre più opache e complesse. Negli anni '80, con la progressiva diffusione dei computer nelle imprese e nelle amministrazioni pubbliche, è emersa la percezione diffusa che le pratiche in materia di trattamento dei dati personali dei soggetti dotati di potere, come governi e grandi imprese, stessero riducendo gli individui allo stato di semplici persone interessate, minacciando i diritti e le libertà fondamentali. Ciò che distingue l'attuale ondata di tecnologie dell'informazione e della comunicazione integrata sono la sua onnipresenza e potenza.

Lo scorso anno è stato riferito che il pianeta conta più dispositivi connessi che esseri umani<sup>1</sup>. I progressi in termini di capacità dei processori<sup>2</sup>, archiviazione e banda di trasmissione si traducono in una quantità sempre più ridotta di restrizioni di carattere tecnico nel trattamento dei dati personali. Si prevede che l'«Internet degli oggetti» e le analisi dei megadati convergeranno con l'intelligenza artificiale, il trattamento del linguaggio naturale e i sistemi biometrici, per dotare le applicazioni di capacità di apprendimento automatico al servizio di un avanzato livello di intelligence. Governi e aziende possono andare oltre «l'estrazione dei dati» per arrivare all'«estrazione della realtà», che penetra l'esperienza quotidiana, la comunicazione e perfino il pensiero<sup>3</sup>. Mentre la società si sta adeguando alle esigenze del mercato digitale, si rinnovano attualmente gli sforzi per insegnare la programmazione ai bambini in giovane età<sup>4</sup>. L'inquadramento di queste tendenze in un settore in cui l'UE, pur essendo tra i principali consumatori, è in ritardo quanto alla fornitura di servizi, è un tema ricorrente della strategia della Commissione per il mercato unico digitale<sup>5</sup>.

Malgrado la loro attualità, queste tendenze e molte altre nozioni utilizzate oggi sono vaghe e si sovrappongono. Per contribuire a stimolare un dibattito, desideriamo evidenziare alcune tendenze specifiche che, pur non essendo ovviamente esaustive, sollevano a nostro avviso le questioni etiche e pratiche più importanti per l'applicazione dei principi di protezione dei dati.

### 1.1 Megadati

La nozione di «megadati»<sup>6</sup> si riferisce alla pratica di combinare enormi volumi di informazioni di provenienza diversa e di analizzarli, spesso con l'ausilio di algoritmi di autoapprendimento per prendere decisioni informate. Tali informazioni non hanno sempre carattere personale: i dati generati da sensori per il monitoraggio di fenomeni naturali o atmosferici, come il tempo o l'inquinamento, o per il monitoraggio di aspetti tecnici di processi di produzione, non si riferiscono a «una persona fisica identificata o identificabile»<sup>7</sup>. Ma uno dei principali vantaggi dei megadati per imprese e governi deriva dalla sorveglianza del comportamento *umano*, a livello collettivo e individuale, e risiede nel loro potenziale predittivo<sup>8</sup>.

Una delle conseguenze è l'emergere di un modello di reddito per le imprese che lavorano con Internet, fondato sul monitoraggio dell'attività on-line allo scopo di ottimizzare il valore economico delle operazioni per i fornitori di servizi, non solo nella pubblicità mirata, ma anche in termini di condizioni e tassi di polizze assicurative, mutui e altri rapporti contrattuali. Nel competitivo mercato dell'attenzione degli utilizzatori, la maggior parte delle persone non è consapevole dell'ampiezza della portata di questo monitoraggio<sup>9</sup>. Tali megadati dovrebbero essere considerati informazioni a carattere personale anche nel caso in cui siano state applicate tecniche di anonimizzazione: diventa sempre più facile dedurre l'identità di una persona attraverso la combinazione di dati asseritamente «anonimi» con altre serie di dati, comprese le informazioni disponibili al pubblico, ad esempio, sui social media<sup>10</sup>.

Quando tali dati vengono commercializzati, in particolare nel quadro degli scambi transfrontalieri e tra giurisdizioni, la responsabilità del trattamento delle informazioni diventa nebulosa e di difficile accertamento ai sensi della normativa sulla protezione dei dati, in particolare in assenza di norme internazionali.

## 1.2 L'«Internet degli oggetti»

Molti dispositivi connessi a Internet sono già diventati di uso comune, come gli smartphone, i tablet, i distributori automatici di banconote e i dispositivi per effettuare il check-in dei voli. Entro il 2020 si prevede che la connettività diventi una caratteristica standard, con 25 miliardi di oggetti collegati (rispetto a 4,8 miliardi nel 2015) in domini che vanno dalla telemedicina ai veicoli, dai contatori intelligenti a tutta una serie di nuovi dispositivi fissi e mobili, destinati a creare città intelligenti<sup>11</sup>.

Tali sensori forniranno informazioni immediate e dettagliate, che gli istituti di statistica e i sondaggi non sono in grado di acquisire oggi, ma che non sono necessariamente più precise e che potrebbero addirittura essere potenzialmente fuorvianti<sup>12</sup>. Le connessioni da macchina a macchina nel settore automobilistico, che dovrebbero raggiungere 1,8 miliardi nel 2022, potrebbero ridurre gli incidenti e l'inquinamento, aumentare la produttività e migliorare l'autonomia di anziani e disabili<sup>13</sup>. Gli oggetti indossabili, come abiti e orologi, tratteranno le informazioni personali allo stesso modo di altri dispositivi collegati. Per esempio, saranno in grado di rilevare coaguli di sangue e monitorare la condizione fisica e la cicatrizzazione delle ferite, mentre i tessuti collegati potrebbero offrire protezione in ambienti estremi, come nella lotta agli incendi. Questi dispositivi caricheranno i dati personali direttamente in spazi di archiviazione nel cloud collegati alle reti sociali e suscettibili di essere pubblicati, consentendo l'identificazione degli utilizzatori e il monitoraggio del comportamento e dei movimenti di individui e flussi di persone<sup>14</sup>.

Il modo in cui tali informazioni vengono gestite potrebbe avere ripercussioni sulla vita privata non solo degli utilizzatori dei dispositivi, tra cui i dispositivi utilizzati sul luogo di lavoro, ma anche sui diritti di terzi, che vengono osservati e registrati dal dispositivo. Sebbene pochi elementi dimostrino l'esistenza di un'effettiva discriminazione, è chiaro che l'enorme volume di informazioni personali raccolte dall'«Internet degli oggetti» è di grande interesse in quanto strumento di ottimizzazione degli introiti attraverso una tariffazione più personalizzata, basata sul comportamento monitorato, segnatamente nel settore dell'assicurazione sanitaria<sup>15</sup>. Saranno messe in discussione anche altre regole specifiche a taluni domini, ad esempio nel caso in cui dispositivi che comportano il trattamento di dati sanitari non siano tecnicamente considerati dispositivi medici e non rientrino nel campo di applicazione del regolamento<sup>16</sup>.

## 1.3 Ambient computing (informatica ambientale)

L'**informatica ambientale o invisibile** è una tecnologia chiave che sta alla base dell'«Internet degli oggetti». Una delle sue applicazioni più evidenti è quella delle «case intelligenti» e degli «uffici intelligenti», costituiti da dispositivi che integrano sofisticate capacità di trattamento delle informazioni, con la promessa di una maggiore efficienza energetica e una migliore informazione delle persone, che sono in grado di agire a distanza sui propri consumi (anche se questo dipende dal grado di autonomia del residente rispetto al proprietario o gestore dell'edificio). Dovrà essere chiarito chi è responsabile della finalità e degli strumenti di trattamento dei dati personali coinvolti nelle applicazioni di informatica ambientale, non solo per tutelare i diritti fondamentali delle persone fisiche, ma anche per ripartire in maniera

adeguata le responsabilità, al fine di rispettare le esigenze generali in materia di sicurezza del sistema.

#### 1.4 Cloud computing

Per cloud computing si intende una tecnologia centrale abilitante, che permette lo sfruttamento di capacità analitiche e di estrazione avanzate nonché la raccolta e l'analisi di megadati e del flusso di dati dall'«Internet degli oggetti», attualmente utilizzato da circa un quinto delle persone fisiche e delle imprese nell'UE<sup>17</sup>. Il cloud computing permette di concentrare dati provenienti dalla miriade di dispositivi dell'«Internet degli oggetti» e si basa sulla disponibilità e la connettività di volumi enormi di dati in spazi di archiviazione e trattamento su larga scala situati in tutto il mondo<sup>18</sup>. Si stima che un uso più esteso del cloud computing<sup>19</sup> da parte dei settori pubblico e privato potrebbe potenzialmente tradursi in un aumento di 449 miliardi di EUR del PIL dell'UE a 28 (0,71 % del PIL totale dell'UE).

Il controllo delle informazioni personali è spesso ripartito tra il cliente e il fornitore di servizi di cloud computing, e la responsabilità relativamente al rispetto degli obblighi di protezione dei dati non è sempre chiara. Ciò potrebbe significare che, in pratica, la protezione fornita è insufficiente. Questi obblighi prescindono dall'**ubicazione fisica dell'archivio dati**. **Inoltre**, anche se si tratta solo di una tecnologia di base che funge da supporto per applicazioni destinate alle imprese, quella del cloud computing potrebbe diventare un'infrastruttura critica e accrescere gli squilibri del mercato in termini di potere. Di fatto, il 30 % delle imprese ha recentemente incontrato difficoltà nell'annullare un abbonamento o cambiare fornitore<sup>20</sup>.

#### 1.5 Modelli aziendali dipendenti dai dati personali

Queste tecnologie hanno consentito l'emergere di nuovi modelli aziendali, che si basano su informazioni generate non solo dalla prestazione di servizi, ma anche da altre fonti, come la presenza sui social media, per valutare i rischi e la solvibilità e ottimizzare i benefici. Attualmente, un modello aziendale rilevante è rappresentato dalle piattaforme che collegano venditori e acquirenti, consentendo la condivisione e la redistribuzione di prodotti, servizi, competenze e risorse. Spesso definite con espressioni come «economia di condivisione», «consumo collaborativo» o «peer-to-peer» on-line e mobili,<sup>21</sup> queste piattaforme possono consentire incrementi di efficienza economica tradizionali, promuovere la competitività sui mercati e ridurre gli sprechi. Si stima che nei prossimi anni il loro valore globale sia destinato a quadruplicarsi, passando da 26 a 110 miliardi di USD<sup>22</sup>. Questi modelli aziendali basati sui dati stanno già generando entrate enormi per quanto riguarda i servizi di car sharing (auto in condivisione), gli affitti di immobili, la tecnologia finanziaria e i prestiti sociali. I sondaggi indicano che i consumatori apprezzano la loro apparente maggiore abbordabilità e convenienza<sup>23</sup>.

Il metro di misura di tali piattaforme è generalmente la reputazione degli utilizzatori, la valutazione degli esperti e la verifica dell'identità. Tali elementi possono potenzialmente essere visti come un miglioramento in termini di trasparenza e responsabilità, ma non necessariamente in relazione al fornitore stesso della piattaforma. I grandi operatori protagonisti in questi mercati sono stati criticati per avere presumibilmente nascosto dati relativi alla reputazione proprio ai singoli utilizzatori ai quali le informazioni si riferiscono. Sussiste un rischio enorme che degli individui possano essere esclusi dai servizi sulla base di una reputazione fondata su dati inesatti, che essi non possono mettere in causa e di cui non possono chiedere l'eliminazione. Basarsi su dati provenienti da molteplici fonti rimette altresì in causa il principio di minimizzazione dei dati sancito dal diritto dell'UE. La portata delle

ripercussioni che i modelli aziendali basati sulle attuali e future tecnologie avranno sulle persone fisiche e sulla società merita attenta riflessione<sup>24</sup>.

## 1.6 Droni e veicoli autonomi

I droni, o aeromobili semiautonomi, sono attualmente usati a fini prevalentemente militari, ma anche e sempre più spesso per scopi di sorveglianza, mappatura, trasporto, logistica e sicurezza pubblica, come la lotta agli incendi<sup>25</sup>. Fotografie, video e altri dati personali raccolti dai droni possono essere scambiati attraverso le reti di telecomunicazione. Il loro utilizzo rischia di condurre a gravi interferenze con la vita privata e di avere un effetto dissuasivo sulla libertà d'espressione. Si pone la questione di come regolamentare in maniera efficace la loro progettazione e il loro utilizzo, in modo che gli interessati possano esercitare i propri diritti di accesso ai dati rilevati da queste macchine.

A terra, veicoli autonomi o auto senza conducente cambieranno il modo in cui gli spostamenti individuali avvengono e sono organizzati, rendendo potenzialmente meno netti i confini fra trasporto pubblico e privato. Entro il 2035 si stima che saranno in circolazione 12 milioni di veicoli totalmente autonomi e 18 milioni di veicoli parzialmente autonomi, di cui l'Europa sarà tra i primi utilizzatori<sup>26</sup>. Gli algoritmi di guida degli autoveicoli, come ad esempio quelli utilizzati per l'opzione programmata in caso di collisione inevitabile, detteranno decisioni che potranno riguardare direttamente l'integrità fisica, e perfino la vita o la morte, delle persone. Oltre all'evidente esigenza di chiarezza per individuare chi si assume la responsabilità e chi deve rendere conto in termini di controllo e sicurezza dei dati, tali applicazioni sollevano una serie di questioni etiche.

## 1.7 Tendenze con un'incidenza potenzialmente maggiore e a lungo termine

La **biostampa 3D** di elementi organici, che utilizza copie delle cellule di pazienti e «biobende» di collagene (vale a dire dati sensibili, in base al diritto dell'Unione) per generare strati successivi di cellule vive, dovrebbe essere facilmente accessibile a breve<sup>27</sup>. Tale tecnica faciliterebbe la fornitura di parti anatomiche umane su misura e risulterebbe particolarmente preziosa nelle regioni più povere nel mondo in cui vi siano stati conflitti. La biostampa solleva ovvie questioni di deontologia medica, di salvaguardia della proprietà intellettuale e di tutela dei consumatori, ma anche, dal momento che si basa sul trattamento di dati sensibili e di natura intima, in quanto concernenti la salute delle persone, di applicazione delle norme in materia di protezione dei dati.

L'**intelligenza artificiale**, come la robotica, si riferisce a un'esigenza tecnologica applicata a macchine autonome fisse e mobili. L'ulteriore sviluppo di tali macchine possiede un potenziale immenso, che va oltre la loro applicazione attuale. I computer dotati di capacità di apprendimento approfondito imparano da soli a eseguire delle operazioni, trattando grandi insiemi di dati tramite l'utilizzo (tra l'altro) di reti neurali che sembrano emulare il cervello. Ricercatori e aziende mirano a ottimizzare l'apprendimento senza supervisione. Gli algoritmi sono già in grado di comprendere e tradurre lingue diverse, riconoscere immagini, scrivere articoli di stampa e analizzare dati medici<sup>28</sup>. I social media forniscono grandi quantità di informazioni personali, già efficacemente indicizzate in precedenza dalle persone stesse. Potrebbe trattarsi dell'ultimo di una serie di miglioramenti cognitivi volti a potenziare le capacità del cervello umano, come la carta o l'abaco, o integrati in macchine autonome (robot), ma è ora il momento di considerare le ripercussioni più estese per gli individui e la società<sup>29</sup>.

## 2. Un ecosistema di protezione dei megadati

Oggi l'UE ha l'occasione di svolgere un ruolo di guida nel dimostrare in che modo governi, organismi di regolamentazione, responsabili del trattamento dei dati, autori e progettisti, sviluppatori e singoli soggetti possono agire congiuntamente per rafforzare i diritti e per guidare, e non bloccare, l'innovazione tecnologica. Secondo un commentatore, le tendenze descritte in questa seconda parte hanno «ampliato il divario tra ciò che è possibile e ciò che è legalmente consentito»<sup>30</sup>. Contrariamente ad alcune affermazioni, la vita privata e la protezione dei dati costituiscono uno dei fondamenti alla base di un ambiente digitale sostenibile e dinamico, e non un ostacolo. Le autorità indipendenti preposte alla protezione dei dati, come il GEPD, svolgono un ruolo chiave per dissipare tali miti e rispondere alle giustificate preoccupazioni delle persone relativamente alla perdita del controllo sulle proprie informazioni personali<sup>31</sup>.

La prossima generazione di dati personali rischia di essere ancora meno accessibile alle persone alle quali tali dati si riferiscono. La responsabilità di plasmare un mercato unico digitale sostenibile è necessariamente ripartita tra più organismi; esiste tuttavia anche un'interdipendenza, come nel caso di un ecosistema, che richiede un'interazione efficace tra sviluppatori, imprese e autorità di regolamentazione, nell'interesse degli individui. In questa sezione delinea il contributo che questi quattro attori fondamentali possono apportare.

### 2.1 Una normativa orientata al futuro

Recentemente abbiamo esortato l'UE a cogliere questa occasione storica per mettere in atto norme più semplici per il trattamento delle informazioni a carattere personale, che conserveranno pertinenza per una generazione<sup>32</sup>. I negoziati sul regolamento generale sulla protezione dei dati e sulla direttiva per la protezione dei dati nei settori giudiziario e di polizia sono alle fasi finali e, a breve, l'attenzione sarà rivolta al futuro della direttiva sulla vita privata in materia di comunicazioni elettroniche e al nuovo regolamento che disciplina il trattamento dei dati personali da parte delle istituzioni e degli organismi europei stessi. Ora che il costo economico della raccolta e dell'archiviazione dei dati è divenuto ormai pressoché trascurabile, spetterà alle autorità preposte alla protezione dei dati garantire l'applicazione coerente di tali norme, per evitare il «rischio morale» di un trattamento dei dati eccessivo<sup>33</sup>.

Nella strategia per il mercato unico digitale, la Commissione riconosce il legame tra il controllo di grandi volumi di dati e il potere di mercato. Essa condivide la convinzione, da noi espressa nel parere preliminare del 2014 «Vita privata e competitività nell'era dei megadati», circa la necessità di una maggiore coerenza tra le autorità di regolamentazione. L'UE dispone già degli strumenti necessari per correggere gli squilibri di potere nel mercato digitale: ad esempio, i procedimenti antitrust della Commissione europea attualmente in corso costituiscono un riconoscimento della predominanza dei dispositivi mobili per accedere a Internet. Un'applicazione più olistica è possibile nell'ambito del quadro giuridico esistente, ad esempio attraverso un organismo di compensazione dell'UE che consenta alle autorità di vigilanza di valutare se casi singoli possono sollevare questioni di conformità con le norme in materia di concorrenza, consumatori e protezione dei dati. Ad esempio:

- esigendo una maggiore trasparenza del prezzo (in contanti o in altre forme) di un servizio, permettendo così di sostanziare e facilitare l'analisi di casi nei procedimenti in materia di concorrenza<sup>34</sup>;

- individuando i casi di ingiusta discriminazione nei prezzi in base a dati di qualità mediocre e definizioni di profili e correlazioni sleali<sup>35</sup>.

Un rafforzamento del dialogo tra le autorità di regolamentazione di settori diversi potrebbe permettere di rispondere alla crescente domanda di partenariati globali, che possono creare «beni comuni» di dati aperti dove informazioni e idee, come statistiche e mappe, potrebbero circolare, essere messe a disposizione e fare oggetto di scambi nell'interesse generale, con minori rischi di sorveglianza, allo scopo di dare alle persone maggiore influenza sulle decisioni che le riguardano<sup>36</sup>.

## 2.2 Addetti al controllo dei dati responsabili

La responsabilità richiede l'attuazione di politiche e sistemi di controllo interni, che garantiscano la conformità e forniscano elementi di prova pertinenti, in particolare alle autorità di controllo indipendenti.

Ci siamo pronunciati a favore dell'eliminazione della burocrazia dalla normativa sulla protezione dei dati, attraverso la minimizzazione delle esigenze di documentazione superflua, per lasciare quanto più spazio possibile a un'iniziativa maggiormente responsabile da parte delle imprese, con l'ausilio degli orientamenti delle autorità preposte alla protezione dei dati. Il principio secondo cui i dati personali devono essere trattati solo in modi compatibili con le finalità (specifiche) per le quali sono stati raccolti è fondamentale per rispettare le legittime aspettative degli individui. Ad esempio, codici di condotta, controlli, certificazioni, audit e una nuova generazione di clausole contrattuali e regole aziendali vincolanti possono contribuire a costruire una solida fiducia nel mercato digitale. I responsabili della gestione delle informazioni personali dovrebbero mostrarsi molto più dinamici e propositivi, prendendo le distanze dalla tendenza, cosiddetta della «scatola nera», consistente nel mettere in atto pratiche commerciali caratterizzate da segretezza e opacità e nell'esigere, al contempo, massima trasparenza da parte dei clienti<sup>37</sup>.

## 2.3. Ingegneria rispettosa della vita privata

L'innovazione umana è sempre stata il prodotto di attività di gruppi sociali e contesti specifici, che di solito riflettono le norme sociali del tempo<sup>38</sup>. Tuttavia, le scelte progettuali in ambito tecnologico non dovrebbero imporre le nostre interazioni sociali e la struttura delle nostre comunità, ma piuttosto sostenere i nostri valori e diritti fondamentali.

L'UE dovrebbe sviluppare e promuovere tecniche di ingegneria e metodologie che permettano la messa in opera di tecnologie di trattamento dei dati nel pieno rispetto della dignità e dei diritti della persona. I creatori di sistemi informatici e di software devono comprendere i principi di rispetto della vita privata fin dalla progettazione e applicarli in modo più soddisfacente ai nuovi prodotti e servizi, durante tutte le fasi di progettazione, e a tutte le tecnologie. La responsabilità deve fondarsi su attività di ricerca e sviluppo più approfondite in termini di metodi e strumenti, per garantire controlli accurati e accertare la conformità alle regole da parte dei responsabili e degli incaricati del trattamento dei dati, per esempio tramite «tagging» (identificazione tramite l'attribuzione di «etichette») di ciascuna unità di dati personali, con «megadati» che descrivono i requisiti di protezione dei dati.

Le soluzioni progettuali dovrebbero conferire, alle persone che lo desiderano, la possibilità di salvaguardare la propria privacy e libertà attraverso l'anonimato. L'UE dovrebbe promuovere la progettazione e lo sviluppo di algoritmi che mascherano l'identità e aggregano i dati al fine di proteggere le persone, sfruttando al contempo il potere predittivo degli stessi dati<sup>39</sup>.

Dobbiamo gettare oggi le basi per affrontare questi compiti, riunendo sviluppatori ed esperti di protezione dei dati di settori diversi nell'ambito delle grandi reti, come l'Internet Privacy Engineering Network (IPEN), che contribuiscono a un proficuo scambio interdisciplinare di idee e approcci.

## 2.4 Conferimento di maggiore autonomia alle persone

### Un ambiente di «prosumatori»

Gli individui non sono semplici oggetti passivi che la legge deve proteggere contro lo sfruttamento. Le tendenze digitali sopra descritte offrono innegabili opportunità per rafforzare il ruolo dell'individuo. Ad esempio, gli individui sono oggi al contempo produttori e consumatori di contenuti e servizi, e sempre più spesso potrebbero essere considerati congiuntamente responsabili con i fornitori di servizi per il trattamento dei dati personali, a meno che tale trattamento abbia fini esclusivamente «domestici»<sup>40</sup> (la nozione di «prosumatore» è emersa per descrivere tale sviluppo<sup>41</sup>). Nel frattempo, valute virtuali offrono agli utilizzatori l'anonimato e la possibilità di eludere la verifica delle transazioni da parte di terzi, abbassando così i costi delle operazioni che si applicano al pagamento di prodotti e servizi transfrontalieri. D'altra parte, l'anonimato e la natura intergiurisdizionale (o, si potrebbe sostenere, *agiurisdizionale*) di tali valute virtuali rendono gli individui vulnerabili rispetto a frodi e attività connesse a mercati criminali, difficili da individuare e sulle quali è più difficile indagare. Oltre agli obblighi che incombono a organismi di regolamentazione, aziende e ingegneri, anche i cittadini sono tenuti a effettuare scelte consapevoli, vigili, critiche e informate, che siano on-line o off-line<sup>42</sup>.

### Consenso

Contrariamente al pensiero tradizionale, inoltre, non ogni comportamento umano può essere spiegato attraverso principi economici basati sul presupposto che gli esseri umani siano perfettamente razionali e sensibili agli incentivi economici<sup>43</sup>. Questo ha rilevanza nel ruolo futuro del consenso dell'individuo al trattamento delle informazioni personali che lo riguardano. In base al diritto dell'UE, nella maggior parte dei casi di trattamento dei dati personali, il consenso non costituisce il solo fondamento legittimo. Anche quando riveste un ruolo importante, il consenso non assolve i responsabili del trattamento dei dati dalla responsabilità per l'utilizzo che fanno di questi ultimi, in particolare ove sia stato ottenuto sotto forma di assenso generale al trattamento dei dati in vista di una vasta gamma di scopi.

### Controllo e «proprietà» dei dati

Gli individui devono essere in grado di contestare errori e distorsioni indebiti risultanti dalla logica utilizzata dagli algoritmi per determinare presunzioni e previsioni. A titolo di esempio, negli Stati Uniti, uno studio condotto su quasi 3 000 rapporti sui crediti facenti capo a 1 000 consumatori, ha rivelato che il 26 % di essi conteneva errori «importanti», sufficientemente gravi da incidere sui punteggi creditizi dei consumatori e, di conseguenza sul costo di accesso a detto credito<sup>44</sup>.

I dati sono spesso considerati una risorsa, come il petrolio, destinata a essere commercializzata, idealmente tra parti ugualmente informate sulla transazione<sup>45</sup>. I clienti non ricevono un compenso adeguato in cambio delle loro informazioni personali, per cui alcuni hanno auspicato un modello di proprietà dei dati. Un controllo assoluto sui dati personali è tuttavia difficile da garantire: ne risulterebbero altre preoccupazioni, come l'interesse pubblico e i diritti e le libertà di altri. Il controllo è necessario ma non sufficiente<sup>46</sup>. La dignità

umana resta tuttavia sempre una costante e, conformemente al diritto comunitario, l'analogia della proprietà non può essere applicata in quanto tale alle informazioni personali, che presentano un legame intrinseco con la personalità degli individui. Nella legislazione dell'UE non vi è alcuna disposizione in materia di protezione dei dati, che permetta a un individuo di rinunciare a questo diritto fondamentale.

Un metodo alternativo affinché gli individui abbiano un maggiore controllo sui propri dati, chi può accedervi e a quale scopo, potrebbe consistere nell'utilizzare spazi di archiviazione dei dati personali o «casseforti di dati»<sup>47</sup>. Tale concerto di «spazio di archiviazione personale» presuppone l'esistenza di meccanismi di sicurezza in grado di garantire che i dati siano accessibili solo dalle entità alle quali le persone interessate hanno accordato l'autorizzazione, e solo per le parti cui tale autorizzazione si riferisce. Gli spazi di archiviazione dei dati personali sarebbero particolarmente efficaci nel caso delle informazioni attuali e costantemente aggiornate, come i dati geospaziali o i segni di vita. Oltre alle garanzie tecniche, gli utilizzatori dei dati sarebbero tenuti a rispettare le regole di condivisione e utilizzo dei dati. La concorrenza e la possibilità di utilizzare un servizio diverso costituiscono il mezzo più efficace di cui un consumatore dispone per incidere sul mercato dei servizi a sua disposizione. La garanzia di portabilità delle connessioni, compresi gli identificatori e i recapiti, si è dimostrata un potente catalizzatore per la concorrenza e ha effettivamente ridotto i prezzi al consumo quando il mercato delle telecomunicazioni è stato liberalizzato. La portabilità dei dati, che costituisce la possibilità effettiva e pratica di trasferire la maggior parte dei propri dati da un fornitore di servizi a un altro, è un efficace punto di partenza per creare le condizioni perché sia possibile una vera scelta da parte del consumatore.

### **3. La dignità al centro di una nuova etica digitale**

Gli elementi costitutivi di questo ecosistema digitale devono essere sostenuti da un quadro etico. Il GEPD ritiene che un maggiore rispetto e la tutela della dignità umana potrebbero fungere da contrappeso alla sorveglianza pervasiva e all'asimmetria di potere con la quale gli individui si devono attualmente confrontare. Essa dovrebbe essere al centro di una nuova etica digitale.

#### **3.1 Dignità e dati**

Sulla scia della rivoluzione industriale del XVII e XIX secolo, il movimento per i diritti umani ha cercato di assicurare il benessere sociale generale, riducendo gli ostacoli al rispetto dell'individuo. Con la Carta dei diritti fondamentali e in seguito alla Dichiarazione universale dei diritti umani e alla Convenzione europea dei diritti dell'uomo, l'UE ha ormai assunto come punto di partenza l'inviolabilità della dignità umana. La dignità della persona umana non è soltanto un diritto fondamentale in sé, ma è anche un fondamento per altri diritti e libertà, compresi i diritti alla vita privata e alla protezione dei dati personali<sup>48</sup>. Le violazioni della dignità possono includere l'oggettivazione, ossia il fatto di trattare una persona come uno strumento al servizio di scopi perseguiti da altri<sup>49</sup>. La vita privata è parte integrante della dignità umana e il diritto alla protezione dei dati è stato concepito originariamente negli anni '70 e '80 come mezzo per compensare il potenziale di erosione della vita privata e della dignità attraverso il trattamento dei dati personali su larga scala. In Germania il diritto all'«autodeterminazione informativa» era basato sui diritti alla dignità della persona e al libero sviluppo della personalità, sanciti dagli articoli 1 e 2 della Costituzione tedesca<sup>50</sup>.

Tuttavia, alle soglie del XXI secolo, le persone sono sempre più spesso obbligate a divulgare una quantità molto maggiore di informazioni personali in Internet, per poter partecipare ad attività di natura sociale, amministrativa e commerciale, e la possibilità di rifiutare tale divulgazione è ancora più limitata. Poiché tutte le attività sono potenzialmente sempre online, la nozione di consenso libero e informato è posta sotto enorme pressione. Ogni minuto che passa «briciole digitali» vengono raccolte e combinate per classificare le persone in tempo reale e creare profili multipli e talvolta contraddittori, che possono essere diffusi in microsecondi all'insaputa delle persone e utilizzati come base per decisioni importanti che le riguardano.

Nei profili utilizzati per predire il comportamento delle persone è insito un rischio di stigmatizzazione, di rafforzamento di stereotipi esistenti, di segregazione sociale e culturale e di esclusione<sup>51</sup>: una tale «intelligenza collettiva» sovverte la scelta individuale e le pari opportunità. Tali «bolle di filtri» o «spazi di eco personali» potrebbero finire per soffocare quella stessa creatività, innovazione e libertà d'espressione e di associazione che hanno consentito alle tecnologie digitali di prosperare.

Nel frattempo, per giustificare la stratificazione multipla di tecniche intrusive impiegate per monitorare le attività degli individui viene invocato un continuo stato di eccezione per motivi di «sicurezza»<sup>52</sup>. Per capire questo «aumento progressivo della sorveglianza» occorre considerare gli effetti globali a più lungo termine sulla società e sui comportamenti.

Insieme ai paesi terzi, l'UE deve impegnarsi a fondo per trovare il modo di garantire che tali valori, pur rispettati sulla carta, non siano di fatto neutralizzati nel ciberspazio. L'Unione in particolare, prima che tali tecnologie vengano adottate in massa, ha oggi davanti a sé una «finestra critica» attraverso la quale integrare i valori nelle strutture digitali che definiranno la nostra società<sup>53</sup>. Ciò richiede una nuova valutazione volta a stabilire se i potenziali benefici delle nuove tecnologie dipendano veramente dalla raccolta e dall'analisi di informazioni personali identificabili di miliardi di persone. Tale valutazione permetterebbe di porre gli sviluppatori davanti alla sfida di progettare prodotti che «depersonalizzino» in tempo reale enormi volumi di informazioni non organizzate, rendendo così più difficile, se non impossibile, distinguere una singola persona dalla massa.

Riconosciamo già che alcuni trattamenti, ad esempio quelli concernenti i dati genetici, non solo devono essere regolamentati, ma devono anche essere valutati con riferimento a preoccupazioni sociali più ampie, ad esempio da comitati etici. Per loro stessa natura, i dati genetici non riguardano un solo individuo, ma anche i suoi ascendenti e discendenti. Tali dati genetici non servono solo a identificare le relazioni familiari: gli elementi che si trovano nei geni di un individuo possono fornire informazioni anche sui loro genitori e figli, e indurre i responsabili del loro trattamento a prendere decisioni che incidono sulle opportunità che tali persone avranno nel corso della loro vita, ancor prima della nascita. La potenziale concentrazione di dati genetici personali nelle mani di pochi grandi operatori del mercato produce effetti sulle economie di mercato e sulle persone interessate. La crescente dipendenza da un sistema globale di raccolta e analisi di un flusso costante di dati potrebbe rendere la società e l'economia più vulnerabili a falle di sicurezza e attacchi dolosi senza precedenti.

L'attuale sistema potrebbe naufragare se non affrontiamo il futuro con una mentalità innovativa. Esistono una crescente domanda – e la necessità – di considerare gli interessati come individui, non semplicemente come consumatori o utilizzatori. Autorità preposte alla protezione dei dati che siano realmente indipendenti svolgono un ruolo fondamentale

nell'impedire che si materializzi un futuro in cui le persone sono definite da algoritmi e dalle loro continue variazioni. Tali autorità devono disporre degli strumenti necessari per assolvere a un «dovere di diligenza» nei confronti degli individui e della loro dignità on-line. Le nozioni e i principi tradizionali di rispetto della vita privata e di protezione dei dati contenevano già elementi di etica volti alla protezione della dignità, ad esempio in materia di occupazione e salute. Le tendenze odierne, tuttavia, hanno aperto un capitolo del tutto nuovo e nasce l'esigenza di approfondire se tali principi siano sufficientemente solidi per l'era digitale<sup>54</sup>. La stessa nozione di dati personali è destinata a cambiare radicalmente poiché la tecnologia permette sempre più di ridefinire gli individui a partire da dati presumibilmente anonimi. Inoltre, l'apprendimento automatico e la fusione tra intelligenza umana e artificiale mineranno i concetti di diritti e responsabilità dell'individuo.

### **3.2 Un comitato consultivo etico europeo**

Non si tratta di dipingere un quadro allarmista in cui si ritrae una realtà distopica. Dibattiti sono già in corso nelle sfere giuridica, politica, economica, sociale, scientifica e perfino religiosa<sup>55</sup>. Approcci semplicistici, che conferiscono un vantaggio unilaterale al beneficio economico o alla sorveglianza a fini di sicurezza non sono, probabilmente, più utili di un'applicazione troppo restrittiva della legislazione esistente, che soffocherebbe l'innovazione e il progresso. Il GEPD propone, pertanto, un'analisi approfondita, ampia e multidisciplinare per fornire raccomandazioni e informare un dibattito sociale sul modo in cui una società libera e democratica dovrebbe affrontare la sfida tecnologica.

Nella sua strategia, il GEPD<sup>56</sup> si è impegnato a sviluppare un approccio etico alla protezione dei dati, nel quale afferma che «fattibile, utile o vantaggioso non sono sinonimi di sostenibile» e riconosce la «supremazia della responsabilizzazione sul rispetto meccanico della lettera della legge». Intendiamo andare oltre la comunità dei funzionari UE, degli avvocati e degli specialisti di tecnologie informatiche, per rivolgerci a personalità di rilievo in grado di giudicare le implicazioni a medio e lungo termine del cambiamento tecnologico e le risposte a livello di normativa. Nei prossimi mesi intendiamo creare, all'interno della nostra istituzione indipendente, un gruppo di consulenti esterni sulla dimensione etica della protezione dei dati, per studiare le relazioni tra diritti umani, tecnologia, mercati e modelli aziendali nel XXI secolo.

Il nostro comitato consultivo etico sarà composto da un gruppo selezionato di personalità eminenti nei settori dell'etica e della filosofia, della sociologia, della psicologia, della tecnologia e dell'economia, e se del caso, beneficeranno del sostegno di altri esperti dotati di conoscenze ed esperienza in materia di sanità, trasporti ed energia, integrazione sociale e media, economia e finanza, governance e democrazia, sicurezza e polizia. Questi soggetti saranno invitati a considerare le ampie implicazioni etiche del modo in cui i dati personali sono concepiti e utilizzati, e le loro deliberazioni saranno caratterizzate da massima trasparenza.

## **4. Conclusione: è tempo di approfondire il dibattito**

La protezione della vita privata e dei dati costituisce parte della soluzione e non del problema. Per il momento, la tecnologia è controllata da esseri umani. Non è facile classificare questi potenziali sviluppi in modo esatto, come buoni o cattivi, opportuni o deleteri, vantaggiosi o pregiudizievoli, tanto meno quando un certo numero di tendenze potenziali deve essere considerato nel contesto. Responsabili politici, sviluppatori di nuove tecnologie, potenziali imprenditori e noi tutti dobbiamo prendere seriamente in considerazione se e come vogliamo

influenzare lo sviluppo della tecnologia e la sua applicazione. Ma altrettanto importante è che l'UE valuti con urgenza l'etica e il posto occupato dalla dignità umana nelle tecnologie del futuro.

I principi di protezione dei dati si sono dimostrati in grado di salvaguardare le persone e la loro vita privata dai rischi di trattamenti irresponsabili. Tuttavia, le attuali tendenze possono richiedere un approccio del tutto innovativo. Stiamo dunque aprendo un nuovo dibattito sulla misura in cui l'applicazione di principi come l'equità e la legittimità sia sufficiente. La comunità che si occupa della protezione dei dati può svolgere un nuovo ruolo utilizzando strumenti già esistenti, come controlli e autorizzazioni preventive, perché nessun altro organismo è dotato dei mezzi per controllare un tale trattamento dei dati. Attraverso lo sviluppo vertiginoso della tecnologia, dell'innovazione globale e dell'interconnessione umana, abbiamo l'opportunità di attirare l'attenzione, suscitare interesse e raggiungere un consenso.

Con questo parere ci auguriamo di fornire un quadro di riferimento per un dibattito più ampio e approfondito su come l'UE possa garantire l'integrità dei propri valori, sfruttando al contempo i vantaggi delle nuove tecnologie.

Fatto a Bruxelles, l'11 settembre 2015

**(firmato)**

Giovanni BUTTARELLI  
Garante europeo della protezione dei dati

## Note

---

<sup>1</sup> Fonte: GSMA Intelligence.

<sup>2</sup> La «legge di Moore», secondo la quale la densità di transistor su un microchip raddoppia ogni 18 mesi circa, si è generalmente dimostrata esatta (Moore, Gordon E., 1965/04/19, «Cramming more components onto integrated circuits», *Electronics*, 22/08/2011).

<sup>3</sup> Nathan Eagle, Alex (Sandy) Pentland, «Reality mining: sensing complex social systems», *Journal Personal and Ubiquitous Computing* Volume 10, numero 4, marzo 2006, pagg. 255–268. Shoshana Zuboff in «Big Other: surveillance capitalism and the prospects of an information civilization», *Journal of Information Technology* (2015) 30, pagg. 75-89, scrive: «In seguito alla mediazione informatica generalizzata, quasi ogni aspetto del mondo viene rappresentato in una nuova dimensione simbolica, mentre eventi, oggetti, processi e persone diventano visibili, conoscibili e condivisibili in modo nuovo». La Zuboff prospetta «la nascita di una nuova architettura universale» che designa con il nome di «Big Other», «un regime onnipresente di istituzioni in rete, che registra, modifica e mercifica l'esperienza del quotidiano, dai tostapane agli organismi, dalla comunicazione al pensiero, il tutto con lo scopo di stabilire nuovi percorsi di monetizzazione e profitto» (pagg. 77 e 81).

<sup>4</sup> «BBC Micro Bit computer's final design revealed» 7.7.2015, <http://www.bbc.com/news/technology-33409311>(accessed 10.09.2015); «No assembler required: How to teach computer science in nursery school», *The Economist*, 1.8.2015.

<sup>5</sup> Secondo la classifica mondiale delle dieci prime aziende per capitalizzazione di borsa, redatta dalla PWC e aggiornata al 31 marzo 2015, nessuna di tali dieci aziende nel settore della tecnologia per capitalizzazione di borsa ha sede nell'UE (otto sono società statunitensi, una ha sede in Cina e una a Taiwan).

<sup>6</sup> «Il termine megadati (big data) si riferisce alla crescita esponenziale sia della disponibilità sia dell'utilizzo automatizzato di informazioni, indicando enormi serie di dati digitali detenuti da società, governi e altre organizzazioni di grandi dimensioni, successivamente analizzati in modo estensivo (da cui il nome "analisi") attraverso algoritmi informatici» (parere 3/2013 del gruppo dell'articolo 29 sulla limitazione delle finalità). Nel 2014 una relazione della Casa Bianca descriveva i megadati come «la crescente capacità tecnologica di raccogliere, aggregare e trattare volumi, velocità e varietà di dati ancora maggiori», cfr. *Big Data: Seizing Opportunities, Preserving Values*, Ufficio esecutivo del presidente (rapporto «Podesta»), maggio 2014.

<sup>7</sup> Ai sensi del diritto dell'UE, per «dati personali» si intende «qualsiasi informazione relativa a una persona fisica identificata o identificabile ("persona interessata"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale» (articolo 2, lettera a), direttiva 95/46/CE). Questa definizione è sostanzialmente analoga a quelle adottate dal Consiglio d'Europa nella Convenzione per la protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale (nota come Convenzione 108) e dall'OCSE nei suoi orientamenti sulla protezione della vita privata e dei flussi transfrontalieri di dati personali. Per un'analisi approfondita, cfr. il «Parere 4/2007 del gruppo dell' articolo 29 sul concetto di dati personali», WP136.

<sup>8</sup> Cfr., ad esempio, il discorso della presidente della Commissione federale per il commercio negli Stati Uniti nel 2014: «La proliferazione di dispositivi connessi, il crollo dei costi associati alla raccolta, all'archiviazione e al trattamento delle informazioni e la capacità degli intermediari di dati e di altri soggetti di combinare i dati on-line e off line, significano che le imprese possono accumulare quantità praticamente illimitate di informazioni concernenti i consumatori, e archiviarle a tempo indeterminato. L'analisi predittiva permette loro di acquisire una sorprendente quantità di informazioni su ciascuno di noi, basandosi su tali informazioni»; intervento di apertura della presidente della FTC Edith Ramirez, «Big Data: A Tool for Inclusion or Exclusion?», Washington,

---

DC, 15 settembre 2014. Secondo Sandy Pentland, «la fisica sociale è una scienza sociale quantitativa, che descrive connessioni affidabili e matematiche tra il flusso di informazioni e di idee da un lato e, dall'altro, il comportamento delle persone (...) e ci permette di prevedere la produttività di piccoli gruppi, di reparti all'interno delle imprese e perfino di intere città». Ciò è «necessario per creare sistemi sociali migliori» (pagg. 4 e 7) e «permettere (a funzionari governativi, dirigenti del settore industriale e cittadini) di utilizzare gli strumenti di incentivazione della rete sociale per *stabilire nuove norme comportamentali*» (pag. 189, corsivo nostro, Pentland, *Social Physics: How Good Ideas Spread: The Lessons from a New Science*).

<sup>9</sup> Eurobarometro speciale 431 sulla protezione dei dati, giugno 2015, e rapporto dell'inchiesta del Pew Research Panel, gennaio 2014: «Public Perceptions of Privacy and Security in the Post-Snowden Era». Secondo i risultati di uno studio, in media, la consultazione di un singolo sito Internet dà luogo a 56 istanze di raccolta di dati (Julia Angwin, *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*, 2012). Dalla relazione 2014 della Casa Bianca sui megadati risulta che «una potenza di calcolo e una sofisticazione senza precedenti (...) creano un'asimmetria di potere tra chi detiene i dati e chi intenzionalmente o inavvertitamente li comunica»; «alcune tra le sfide più importanti rilevate nel corso di tale analisi riguardano il modo in cui l'analisi dei megadati può (...) creare un ambiente decisionale talmente opaco, che l'autonomia individuale si perde in un insieme impenetrabile di algoritmi».

<sup>10</sup> Utilizzando dati anonimi pubblici risultanti da un censimento del 1990, l'87 % della popolazione statunitense potrebbe con ogni probabilità essere identificato associando il codice postale a cinque cifre al sesso e alla data di nascita di tali persone; cfr. Paul Ohm «Broken promises of privacy: responding to the surprising failure of anonymisation», *UCLA Law Review* 2010, e «Record linkage and privacy: issues in creating new federal research and statistical info», aprile 2011. Il DNA è unico (tranne che per i gemelli omozigoti) e rimane stabile per tutta la vita. Contenendo informazioni sull'appartenenza etnica e la predisposizione alle malattie, permette di identificare altri membri della famiglia. Nel gennaio 2013 alcuni ricercatori hanno potuto identificare persone e famiglie a partire da dati anonimi relativi al DNA figuranti in banche dati genealogiche accessibili al pubblico (Gymrek, M., McGuire, AL, Golan, D., Halperin, E. & Erlich, Y. *Science* 339, 321-324, 2013). Cfr., inoltre, «Poorly anonymized logs reveal NYC cab drivers' detailed whereabouts», 23.06.2014, <http://arstechnica.com/tech-policy/2014/06/poorly-anonymized-logs-reveal-nyc-cab-drivers-detailed-whereabouts/> (consultato il 10.09.2015). Cfr., inoltre, il parere 04/2007 del gruppo dell' articolo 29 sul concetto di dati personali; il parere 03/2013 del gruppo dell' articolo 29 sulla limitazione delle finalità; il parere 06/2013 del gruppo dell' articolo 29 sui dati aperti e sul riutilizzo delle informazioni del settore pubblico («ISP»); e il parere 05/2014 del gruppo dell' articolo 29 sulle tecniche di anonimizzazione.

<sup>11</sup> Fonte: Gartner.

<sup>12</sup> Cfr., ad esempio, il dibattito «What is the future of official statistics in the Big Data era?», the Royal Statistical Society, Londra, 19 gennaio 2015 (<http://www.odi.org/events/4068-future-Official-Statistics-Big-Data-era> , consultato il 10.09.2015).

<sup>13</sup> Dieci tecnologie che potrebbero cambiare la nostra vita: potenziali ripercussioni e implicazioni politiche, Unità prospettica scientifica, Servizio europeo di ricerca parlamentare, gennaio 2015.

<sup>14</sup> Il programma di lavoro 2016-2017 Orizzonte 2020 dell'UE sostiene tali sviluppi, prevedendo, tra l'altro, progetti pilota su vasta scala dedicati alle questioni concernenti la vita privata e di ordine etico.

<sup>15</sup> Il settore delle assicurazioni è stato descritto come il «modello aziendale nativo per l'Internet degli oggetti» («From fitness trackers to drones, how the "Internet of Things" is transforming the insurance industry», *Business Insider* 11.6.2015). La nozione di discriminazione tramite i prezzi nel diritto della concorrenza, derivata dall'articolo 102 del TFUE, che vieta a un'impresa dominante in un mercato di «imporre direttamente o indirettamente prezzi d'acquisto, di vendita ovvero altre condizioni di transazione non eque» è molto controversa; cfr., ad esempio, Damien Gerardin e Nicolas Petit, «Price Discrimination Under EC Competition Law: Another Antitrust Theory in Search of Limiting

---

Principles» (luglio 2005), Global Competition Law Centre, collana di documenti di lavoro n. 07/05. Con riferimento ai megadati e al loro (secondo gli autori, non ancora realizzato) potenziale relativo all'accelerazione della messa in atto della tariffazione personalizzata, cfr. la relazione dell'ufficio esecutivo del presidente degli Stati Uniti, «Big Data and Differential Pricing», febbraio 2015, e una recente analisi in cui si conclude che la tariffazione personalizzata comporta, in genere, il trattamento dei dati personali e, pertanto, deve rispettare il principio di trasparenza previsto dalla normativa sulla protezione dei dati, la quale impone alle aziende di informare le persone circa la finalità del trattamento dei loro dati personali: se le imprese personalizzano i prezzi, devono indicarlo. Inoltre, se un'impresa utilizza «cookie» per riconoscere le persone, la direttiva relativa alla vita privata e alle comunicazioni elettroniche impone all'impresa di informare tali persone della finalità di detti cookie (bozza di lavoro di Frederik Borgesius «Online Price Discrimination and Data Protection Law», disponibile all'indirizzo [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2652665](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2652665), consultato il 10.09.2015).

<sup>16</sup> I dispositivi medici sono definiti nel diritto dell'UE dalla direttiva 93/42/CEE concernente i dispositivi medici, modificata dalla direttiva 2007/47/CE del Parlamento europeo e del Consiglio, del 5 settembre 2007. Per quanto concerne le implicazioni della «sanità mobile», cfr. il parere del GEPD 1/2015.

<sup>17</sup> Secondo l'Eurostat, il 21 % delle persone fisiche e il 19 % delle imprese nell'UE si avvale di servizi di archiviazione sul cloud.

<sup>18</sup> «Se l'Internet mondiale fosse un paese, sarebbe il dodicesimo consumatore di elettricità per importanza su scala mondiale, attestandosi tra Spagna e Italia. Questo rappresenta circa l'1,1-1,5 % del consumo globale di elettricità (nel 2010) e corrisponde alle emissioni di gas a effetto serra prodotte da 70-90 grandi centrali elettriche a carbone (500 megawatt)» (Natural Resources Defense Council, «Data Centre Efficiency Assessment: Scaling Up Energy Efficiency Across the Data Centre Industry: Evaluating Key Drivers and Barriers», 2014).

<sup>19</sup> Relazione sullo studio «SMART 2013/0043 - Uptake of Cloud in Europe».

<sup>20</sup> Fonte: Eurostat

<sup>21</sup> Il termine «economia di condivisione» è stato criticato in quanto fuorviante («The Sharing Economy Isn't About Sharing at All», Giana M. Eckhardt e Fleura Bardhi, Harvard Business Review, 28.01.2015).

<sup>22</sup> Rachel Botsman e Roo Rogers, *What's Mine Is Yours: How Collaborative Consumption is Changing the Way We Live*, 2011.

<sup>23</sup> Forum «Future of Privacy», «User Reputation: Building Trust and Addressing Privacy Issues in the Sharing Economy», giugno 2015.

<sup>24</sup> Cfr. il laboratorio del 9 giugno 2015 organizzato dalla Commissione federale del commercio degli Stati Uniti, dal titolo «Competition, Consumer Protection, and Economic Issues Raised by the Sharing Economy», <https://www.ftc.gov/news-events/events-calendar/2015/06/sharing-economy-issues-facing-platforms-participants-regulators/> (consultato il 10.09.2015).

<sup>25</sup> Per quanto concerne le implicazioni di droni o sistemi aerei a pilotaggio remoto in termini di protezione dei dati, cfr. il parere del GEPD in merito alla comunicazione della Commissione al Parlamento europeo e al Consiglio «Una nuova era per il trasporto aereo – Aprire il mercato del trasporto aereo all'uso civile dei sistemi aerei a pilotaggio remoto in modo sicuro e sostenibile», novembre 2014.

<sup>26</sup> Fonte: Boston Consulting Group.

<sup>27</sup> Gartner.

<sup>28</sup> Si è riferito che l'algoritmo di riconoscimento facciale DeepFace di Facebook ha registrato una percentuale di successo del 97 %, superando in risultato gli esseri umani («DeepFace: Closing the

---

Gap to Human-Level Performance in Face Verification», contributo pubblicato nella relazione della conferenza «Computer Vision and Pattern recognition» dell'IEEE del giugno 2014).

<sup>29</sup> Robo è stato definito come una «macchina situata nel mondo, che sente, pensa e agisce» (Bekey, G, Current trends in robotics: technology and ethics, in *Robot Ethics - The ethical and social implications of robotics*, The MIT Press<sup>2</sup>, 2012, pag. 18). Si stima che il numero di robot di servizio venduti tra il 2013 e il 2016 raggiungerà i 22 milioni (IRF World Robotics Report, 2013). Per quanto concerne l'intelligenza artificiale, cfr. «Rise of the Machines», Economist, 09.5.15 e il progetto Internet del Pew Research Centre del 2014. Di fronte a un'offerta da parte di una società leader nel settore tecnologico, un'azienda operante nel settore dell'intelligenza artificiale ha subordinato la sua acquisizione nel 2014 all'istituzione di un comitato etico e di sicurezza e al divieto di qualsiasi utilizzo del lavoro sull'intelligenza artificiale a fini militari o di intelligence (Forbes, Inside Google's Mysterious Ethics Board, 03.02.2014).

<sup>30</sup> Pentland, *Social physics*, pag. 147.

<sup>31</sup> Cfr. nota 9 supra. Pentland, *Social Physics*, pag. 153: «È possibile compiere grandi passi avanti nei settori della sanità, dei trasporti, dell'energia e della sicurezza (...) i principali ostacoli al raggiungimento di questi obiettivi sono le preoccupazioni in materia di privacy e il fatto che non esiste ancora un consenso quanto alle soluzioni di compromesso tra i valori personali e i valori sociali.» Il dibattito del 2014 sulla pandemia di Ebola in Africa occidentale è esemplificativo di questa falsa dicotomia tra la vita privata dell'individuo e le esigenze della società. Le malattie vengono tendenzialmente monitorate e la loro durata è misurata per mezzo di sondaggi e censimenti, che diventano facilmente obsoleti e sono difficili da estrapolare per prevedere dove faranno la loro apparizione in futuro. Esiste qualche esempio di utilizzo dei «megadati» per monitorare le epidemie di malaria in Namibia e Kenya e, nel 2009, per monitorare l'efficacia delle avvertenze sanitarie del governo durante la crisi dell'influenza suina messicana. Una delle fonti di dati è quella relativa alle chiamate dai telefoni cellulari, che indica la stazione base che ha gestito la chiamata e può fornire in tempo reale la localizzazione e gli spostamenti approssimativi delle persone. La raccolta di tutte queste registrazioni non è mirata: non è possibile distinguere tra gli interlocutori portatori del virus Ebola e gli altri. Un'organizzazione svedese senza scopo di lucro ha mappato la mobilità della popolazione in Africa occidentale, ma i dati non sono stati utilizzati perché gli operatori di telefonia mobile hanno rifiutato di comunicarli ai ricercatori esterni autorizzati, sostenendo di necessitare di istruzioni provenienti dai governi. Questi ultimi, a loro volta, hanno espresso preoccupazioni in ordine alla privacy, che non poteva essere salvaguardata ai sensi della legislazione dell'UE (<http://www.pri.org/stories/2014-10-24/how-big-data-could-help-stop-spread-ebola>, consultato il 10.09.2015).

<sup>32</sup> Parere del GEPD 3/2015.

<sup>33</sup> L'ipotesi secondo la quale, in materia di megadati, «N = tutto», si riferisce alla necessità di considerare tutti gli elementi dei dati, e non solo un campione (Viktor Mayer-Schönberger, e Kenneth Cukier, *The Rise of Big Data: How it's changing the way we think about the world*, 2013). Il Consiglio di Lisbona e il Progressive Policy Institute sostengono che l'ottimizzazione della «densità numerica» – «i volumi di dati utilizzati per abitante in un'economia» – condurrà a un aumento della prosperità (cfr. <http://www.lisboncouncil.net/component/downloads/?id=1178>, consultato il 10.09.2015). Il Gruppo di lavoro internazionale sulla tutela dei dati nelle telecomunicazioni (conosciuto come «gruppo di Berlino») ha proposto deroghe ai principi di protezione dei dati per i megadati ([http://www.datenschutz-berlin.de/attachments/1052/WP\\_Big\\_Data\\_final\\_clean\\_675.48.12.pdf](http://www.datenschutz-berlin.de/attachments/1052/WP_Big_Data_final_clean_675.48.12.pdf), consultato il 10.09.2015). Il Forum economico mondiale ha fatto appello alla necessità di concentrarsi sull'utilizzo e non sulla raccolta e a rinunciare all'esigenza del consenso per la raccolta dei dati personali (Unlocking the Value of Personal Data: From Collection to Usage, 2013).

<sup>34</sup> Cfr. il parere preliminare del GEPD «Vita privata e competitività nell'era dei megadati».

---

<sup>35</sup> L'articolo 21 della Carta dei diritti fondamentali vieta «qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle, l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza a una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale». Molte di queste categorie di dati («che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale») godono di una maggiore tutela ai sensi dell'articolo 8 della direttiva 95/46/CE.

<sup>36</sup> Sul concetto di beni comuni digitali cfr. *Ambition numérique: Pour une politique française et européenne de la transition numérique*, French Digital Council, giugno 2015 pag. 276; Bruce Schneier invita alla creazione di «spazi pubblici senza proprietario» in Internet, comparabili ai parchi pubblici (*Data and Goliath*, pagg. 188 e 189); Sandy Pentland si pronuncia a favore di «beni comuni pubblici» (*Social Physics*, pag. 179). Sulla valutazione della sicurezza rispetto alla pubblicazione di serie di dati aggregati sotto forma di dati aperti, cfr. il parere 06/2013 del gruppo dell' articolo 29 sui dati aperti e sul riutilizzo delle informazioni del settore pubblico.

<sup>37</sup> «Während die Einzelnen immer transparenter werden, agieren viele Unternehmen hochgradig intransparent» (<http://crackedlabs.org/studie-kommerzielle-ueberwachung/info>). Sulla trasparenza qualificata cfr., ad esempio, Frank Pasquale: *The Black Box Society: The Secret Algorithms that Control Money and Information*.

<sup>38</sup> «Dietro le tecnologie che incidono sulle relazioni sociali, ritroviamo quelle stesse relazioni sociali» (David Noble, «Social Choice in Machine Design: The Case of Automatically Controlled Machine Tools», in *Case Studies in the Labor Process*, ed. Andrew Zimbalist, 1979). Si veda anche Judy Wajzman, *Pressed for Time: The Acceleration of Life in Digital Capitalism*, 2014 pagg. 89 e 90; e Zuboff, «Big Other» (citato alla nota 3 supra).

<sup>39</sup> Parere 05/2014 sulle tecniche di anonimizzazione, adottato il 10 aprile 2014 (WP 216).

<sup>40</sup> Per quanto concerne l'interpretazione restrittiva della deroga alle norme sulla protezione dei dati per fini esclusivamente personali o domestici, cfr. la sentenza della CGUE nella causa C-212/13, *František Ryneš v Úřad pro ochranu osobních údajů*.

<sup>41</sup> Il termine prosumatore è stato coniato da Alvin Toffler in *The Third Wave*, 1980. Per un dibattito sull'ambiente dei «prosumatori» e il modo in cui dovrebbe essere regolamentato, cfr. Ian Brown e Chris Marsden, *Regulating Code*, 2013.

<sup>42</sup> Parere del Gruppo europeo di etica delle scienze e delle nuove tecnologie indirizzato alla Commissione europea: *Etica delle tecnologie di sicurezza e sorveglianza*, parere n. 28, 2015/05/20, pag. 74.

<sup>43</sup> Cfr., ad esempio, *Homer Economicus: The Simpsons and Economics*, ed. Joshua Hall, 2014.

<sup>44</sup> Secondo la definizione più conservatrice del termine errore, ciò significa che 23 milioni di americani sono stati oggetto di uno studio sui consumatori contenente errori importanti. I risultati del 5 % dei partecipanti allo studio contenevano errori la cui correzione migliorava il loro punteggio creditizi in maniera sufficiente da consentire loro di accedere a un credito con costi minori (Commissione federale del commercio, relazione al Congresso in conformità all'articolo 319 del Fair And Accurate Credit Transactions Act del 2003, dicembre 2012; Chris Jay Hoofnagle, *How the Fair Credit Reporting Act Regulates Big Data*, 10 settembre 2013. Forum «Future of Privacy», laboratorio «Big Data and Privacy: Making Ends Meet, 2013. Disponibile sul sito Internet SSRN: <http://ssrn.com/abstract=2432955>).

<sup>45</sup> Il Foro economico mondiale considera i dati come una preziosa risorsa dell'individuo, i cui diritti di possesso, utilizzo e rinuncia possono essere ceduti a imprese e governi in cambio di servizi. Cfr. anche i recenti discorsi del vicepresidente della Commissione, Ansip, ad esempio il discorso del 7.9.2015 in occasione della riunione annuale di Bruegel dal titolo «Productivity, innovation and

---

digitalisation - which global policy challenges?», in cui affermava: «Proprietà e gestione dei flussi di dati, utilizzo e riutilizzo dei dati, gestione e archiviazione dei dati: questi elementi sono alla base di importanti settori emergenti, come il cloud computing, l'Internet degli oggetti e i megadati».

<sup>46</sup> «Chi possiede, dunque, il diritto di utilizzare informazioni e dati che non gli appartengono veramente? Si tratta di una questione che trascende i confini del commercio, dell'etica e della morale, e che comporta questioni connesse alla privacy e alla protezione della vita privata»; Al-Khoury, novembre 2012, [http://www.academia.edu/6726887/Data\\_Owner\\_ship\\_Who\\_Owns\\_My\\_Data\\_036](http://www.academia.edu/6726887/Data_Owner_ship_Who_Owns_My_Data_036). Cfr., inoltre, Incomplete Commodification in the Computerized World, in *The Commodification of Information* 3, 17, Niva Elkin-Koren e Neil Weinstock Netanel, ed. 2002. «Fa una grande differenza se la privacy viene considerata un diritto umano, associato alle persone in virtù della loro individualità, oppure un diritto di proprietà, qualcosa che può essere posseduto o controllato dalle persone. Presumibilmente, i diritti umani dovrebbero essere inalienabili sul mercato, mentre i diritti di proprietà dovrebbero essere alienabili sul mercato».

<sup>47</sup> Il progetto del MIT «Computer Science and Artificial Intelligence Lab's Crosscloud», che beneficia del sostegno di diverse imprese con sede nell'UE, mira a «1) facilitare lo sviluppo di software multiutente ("sociale") utilizzando solo progettazione front-end (che gestisce l'interazione con l'utente) e rispettando i diritti e la vita privata degli utilizzatori; 2) lasciare agli utilizzatori la libertà di spostarsi liberamente tra applicazioni, piattaforme hardware e reti sociali, conservando i propri dati e le proprie connessioni sociali» (<http://openpds.media.mit.edu/#architecture>, consultato il 10.09.2015).

<sup>48</sup> Cfr. la spiegazione dell'articolo 8 della Carta europea dei diritti fondamentali.

<sup>49</sup> Martha Nussbaum, *Objectification*, in *Philosophy and Public Affairs*, 24/4/1995.

<sup>50</sup> Sentenza del 15 dicembre 1983, BVerfGE 65, 1-71, Volkszählung.

<sup>51</sup> Cfr. il parere del Gruppo europeo di etica delle scienze e delle nuove tecnologie sull'etica e la sorveglianza, pag. 75. Uno studio ha suggerito che un algoritmo di scelta degli annunci pubblicitari era discriminatorio: la ricerca restituiva, in media, risultati che rinviavano gli uomini verso lavori meglio pagati rispetto ai visitatori di sesso femminile degli stessi siti (Carnegie Mellon University e International Computer Science Institute). Sulla tendenza a utilizzare per impostazione predefinita una voce femminile per gli assistenti digitali cfr., ad esempio, Judy Wajcman, *Feminist theories of technology*. *Cambridge Journal of Economics*, 34 (1), pagg. 143-152, 2010.

<sup>52</sup> Giorgio Agamben, *State of Exception*, 2005.

<sup>53</sup> Neil Richards, Neil e Jonathan King, *Big Data Ethics* (19 maggio 2014), *Wake Forest Law Review*, 2014.

<sup>54</sup> BBC, *Information watchdog investigates «charity data sales»*, 1.9.2015.

<sup>55</sup> Cfr. lettera del Future of Life Institute, Enciclica papale *Laudato Si*: «quando [i media e il mondo digitale] diventano onnipresenti, non favoriscono lo sviluppo di una capacità di vivere con sapienza, di pensare in profondità, di amare con generosità. I grandi sapienti del passato, in questo contesto, correrebbero il rischio di vedere soffocata la loro sapienza in mezzo al rumore dispersivo dell'informazione. Questo ci richiede uno sforzo affinché tali mezzi si traducano in un nuovo sviluppo culturale dell'umanità e non in un deterioramento della sua ricchezza più profonda. La vera sapienza, frutto della riflessione, del dialogo e dell'incontro generoso fra le persone, non si acquisisce con una mera accumulazione di dati che finisce per saturare e confondere, in una specie di inquinamento mentale. (...) Le relazioni reali con gli altri, con tutte le sfide che implicano, tendono ad essere sostituite da un tipo di comunicazione mediata da internet. Ciò permette di selezionare o eliminare le relazioni secondo il nostro arbitrio, e così si genera spesso un nuovo tipo di emozioni artificiali, che hanno a che vedere più con dispositivi e schermi che con le persone e la natura. I mezzi attuali ci permettono di comunicare tra noi e di condividere conoscenze e affetti. Tuttavia, a volte ci impediscono anche di prendere contatto diretto con l'angoscia, con il tremore, con la gioia dell'altro e con la complessità della sua esperienza personale. Per questo non dovrebbe stupire il fatto che,

---

insieme all'opprimente offerta di questi prodotti, vada crescendo una profonda e malinconica insoddisfazione nelle relazioni interpersonali, o un dannoso isolamento».

<sup>56</sup> Cfr. azione 4 della strategia del GEPD 2015-2020, «Developing an ethical dimension to data protection» (dare vita a una dimensione etica per la protezione dei dati).