Camera Civile di Firenze

Le Corti Fiorentine

Rivista di diritto e procedura civile

Quadrimestrale di giurisprudenza e dottrina

Anno V n. 1/2018

Edizioni Scientifiche Italiane

Registrazione presso il Tribunale di Firenze n. 5966 del 9 settembre 2014

INDICE

FOCUS
Atti dalla Giornata di Studi del 13 ottobre 2017
«Le Corti Fiorentine:
Dialogo tra Giurisprudenza e Dottrina – Anno III»

OSSERVATORIO

GIURISPRUDENZA

Rassegna di massime

 ISSN 2385-1279

ISSN 2385-1279

Anna Carla Nazzaro

PRIVACY E *BIG DATA*[1]

Sommario: 1. *Big data*: una prima definizione. – 2. Art. 23, Codice Privacy e consenso. – 3 Le soluzioni del legislatore comunitario. – 4. Doppia valenza del dato: valore economico e personale. – 5. Finalità del trattamento e profilazione. – 6. Pericoli della profilazione e responsabilità del titolare del trattamento.

1. *Big data: una prima definizione*

Privacy e *big data*[2] è un titolo che chiede forse di conciliare l'inconciliabile e cioè la tendenza del c.d. mondo tecnologico alla connessione continua e al libero e, a volte incontrollato, scambio di dati, e le scelte del legislatore del Codice in materia di protezione dei dati personali imperniate sul controllo della circolazione da parte del titolare tramite il consenso[3].

[1] Lo scritto riproduce, con l'aggiunta di alcune note, la relazione del titolo "Privacy e big data", tenuta il 13 ottobre 2017, al convegno "Le Corti fiorentine: dialogo tra giurisprudenza e dottrina. Anno III", organizzato dalla Camera civile di Firenze.

[2] Si specifica, fin da subito che la *privacy* deve essere correttamente intesa laddove la tutela d i dati personali deve sempre essere finalizzata alla tutela della persona nel continuo bilanciamento con altri interessi costituzionalmente rilevanti, anche di altre persone. I pericoli di una strumentalizzazione del concetto di *privacy* sono ben riassunti nel noto caso che ha visto contrapposti la *Apple inc.* e *il Federal Bureau of Investigation* (FBI), relativamente alla richiesta di quest'ultimo nei confronti di *Apple*, di creare un software n grado di superare il meccanismo di sicurezza dell'*iphone* che cancella i dati oltre il decimo tentativo infruttuoso di inserire una *password* di sblocco. Il telefono in questione era quello di uno degli attentatori della strage di San Bernardino, e lo scopo era quello di recuperare dati utili all'indagine. La *Apple* si rifiuta di collaborare, anche a seguito di un *order* girisprudenziale, adducendo il pericolo che un simile software avrebbe creato alla tutela della *privacy* dei suoi clienti. Di conseguenza, l'FBI, nell'urgenza della questione ha trovato altre "vie" non meglio precisate per recuperare i dati. Il caso (sul quale v. e osservazioni di M. Bonini, *Sicurezza e tecnologia, fra libertà negative e principi liberali.* apple, schrems *e* microsoft*: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista AIC*, 3/2016) è testimonianza di come la tecnologia possa indebolire la corretta esplicazione del pubblico potere nelle sue consuete procedure, richiedendo strumenti non convenzionali per il raggiungimento dei risultato sperati. La questione, peraltro, non è nuova e numerosi altri sono i casi che hanno visto contrapposti la *Apple* è il governo Federale per problematiche del tutto simili.

[3] La disciplina interna del trattamento dei dati personali deriva dalla normativa dell'Unione Europea che fa del loro trattamento uno dei dati distintivi del sistema giuridico europeo. Per questo inquadramento cfr., V. Zeno-Zencovich, Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di telecomunicazione, in G. Resta, V.

 ISSN 2385-1279

Il Codice ha mostrato i suoi difetti proprio con lo sviluppo delle potenzialità del fenomeno dei big data.

Quest'ultimo, in genere definito puntando l'attenzione sulla enorme mole di dati che è possibile reperire in rete, nasconde in realtà un complesso sistema organizzativo e di gestione dei dati, che va ben al di là di un mero, anche se vasto, strumento di raccolta[4].

La verità è che puntare l'attenzione soltanto sulla vastità dei dati raccolti lascia l'indagine ad un livello descrittivo mentre invece i problemi giuridici maggiori derivano dalla modalità di raccolta di dati, dalla loro elaborazione e dalle finalità per cui vengono trattati[5].

Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Private Shield"*, Roma, 2016, p. 7 ss.

[4] I rischi e le potenzialità dello sviluppo della *Big data analytics* sono efficacemente evidenziate da A. Soro, *Apertura dei Lavori*, in *Big Data e Privacy. La nuova geografia dei poteri*, Atti del Convegno organizzato dal Garante per la protezione dei dati personali in occasione della "Giornata europea della protezione dei dati personali" 2017, in *www.garanteprivacy.it*. Cfr., altresì le interessanti osservazioni di G. D'Acquisto, M. Naldo, Big data *e* privacy by design, Torino, 2017, p. 12 ss., i quali nel tentativo di definire cosa ci sia di Big nei Big data, specificano che ciò che qualifica il fenomeno è non soltanto la numerosità del dato ma soprattutto la qualità dei collegamenti. In questa prospettiva propongono una differenziazione tra sistema di *search engine*, dove è l'utente che cerca la soluzione necessaria tra le varie opzioni disponibili e un sistema di *find engine*, nel quale il sistema elettronico fornisce già la risposta cercata. Nello stesso senso anche la definizione fornita dal Committee of the convention for the protection of individuals with regard to automatic processing of personal data nelle *guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*: "Big Data: there are many definitions of Big Data, which differ depending on the specific discipline. Most of them focus on the growing technological ability to collect process and extract new and predictive knowledge from great volume, velocity, and variety of data. In terms of data protection, the main issues do not only concern the volume, velocity, and variety of processed data, but also the analysis of the data using software to extract new and predictive knowledge for decision-making purposes regarding individuals and groups. For the purposes of these Guidelines, the definition of Big Data therefore encompasses both Big Data and Big Data analytics". Consiglio d'Europa, Strasbourg, 23 January 2017 T-PD(2017)01.

[5] Il problema della utilizzazione dei *Big data* si è rivelato dirompentemente all'indomani degli attacchi terroristici dell'11 settembre con le dichiarazioni del 2013 di Edward Snowden, un ex agente dell'intelligence americana, che ha rivelato il piano di protezione americano basato su un controllo massiccio di dati aggregati e trattati in modalità completamente differenti rispetto agli *small data*. Quindi, non tramite una acquisizione mirata, ma con un approccio basato su "acquisizione su larga scala e in maniera automatica dei dati, conservazione per un lungo periodo di tempo, integrazione con altre banche dati e analisi attraverso potenti elaboratori elettronici dell'intero compendio informativo, con l'obiettivo di ricavarne inferenze statisticamente rilevanti per fini di «foreign intelligence»". Il trattamento dei *Big data* risulta caratterizzato da un accesso sistematico si dati di traffico degli utenti e dal carattere indiscriminato della raccolta. La questione è illustrata efficacemente da G. Resta, *La sorveglianza elet-*

La raccolta dei dati avviene principalmente in modo automatizzato. Le tecnologie di raccolta coinvolgono molteplici aspetti della vita quotidiana, infatti coinvolgono il fenomeno del c.d. Internet delle cose (Internet of Things, IoT) che utilizza oggetti, come ad esempio telecomandi, sensori, domotica, *wearable devices*, cellulari, collegati a dispositivi smart che li rendono tramite la connessione costante al web una fonte attiva di raccolta, scambio e gestione di dati in tempo reale. In altri termini, non vengono in rilievo soltanto le informazioni fornite dall'utente (in modo più o meno consapevole) durante la navigazione[6] ma si tratta di una raccolta di informazioni fornite in modo per lo più inconsapevole. Dunque, neanche è più possibile discorrere di mondo virtuale separato da quello reale, quasi che per difendersi ci si possa semplicemente astenere dal fornire informazioni su internet. Infatti, l'IoT rappresenta la materializzazione del c.d. mondo virtuale poiché gli oggetti e i luoghi luoghi fisici, attraverso il web acquistano un'identità elettronica e un ruolo attivo con il collegamento alla rete.

È bene poi avvertire che la locuzione "big data" non rappresenta esclusivamente la somma di dati, ma anche e soprattutto la loro organizzazione. È necessario cioè evidenziare la dimensione sovra-individuale propria della big data analytics, la quale non si concentra sul singolo individuo, ma ha di mira i comportamenti di interi gruppi di persone aggregati, grazie a complessi algoritmi, sulla base dei fini specifici del trattamento. In questo modo il dato perde la propria connotazione individuale e, a volte, anche sociale per risultare, in una certa misura, spersonalizzato. In questo senso allora sarebbe più corretto, se proprio si vuole assecondare il filone anglofono, discorrere di "data mining", ovvero quel «processo di ottenimento di conoscenze utili da insiemi di dati di grandi dimensioni, mediante l'impiego,

tronica di massa e il conflitto regolatorio USA/UE, in G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali*, cit., p. 23 ss.; S. Rodotà, *La vita e le regole – Tra diritto e non diritto*, Milano, 2006, p. 82 ss.

[6] In questo senso, sicuramente la fanno da padrone le strutture contrattuali dei contratti di accesso ai *social network* che spesso tra le *privacy policies* comprendono lo studio ed elaborazione dei contenuti prodotti e/o visualizzati, delle preferenze, delle azioni e delle interazioni dell'utente. Su questo specifico argomento cfr., G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali*, cit., p. 271 ss.; G. Colangelo, Big data, *piattaforme digitali e antitrust*, in *Merc. conc. reg.*, 2016, p. 426 s. Il quale riporta la distinzione tra *volunteered data* e *observed data* per indicare le differenze tra i informazioni fornite dall'utente (aggiungiamo noi) anche se non sempre volontariamente e dati automatizzati desumibili dal *tracking*, cioè dalle operazioni compiute in rete dall'utente. A questi si aggiungono i c.d. *inferred data* e cioè i metadati derivati dall'analisi dei dati disponibili.

 ISSN 2385-1279

in maniera automatica o semiautomatica, di tecniche informatiche e statistiche»[7]. Sembra quasi banale aggiungere che il complesso processo cui si è poc'anzi fatto cenno richiede l'utilizzo di tecniche di armonizzazione, poiché spesso i dati derivano da fonti eterogenee e non strutturate. Il fine ultimo è l'utilizzo scientifico, industriale o operativo di questo sapere.

2. *Art. 23, Codice Privacy e consenso*

Di fronte a questa complessa realtà che intreccia mondo reale e mondo virtuale, l'art. 23 del nostro Codice della Privacy lascia perplessi[8]:

«1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili».

E le perplessità assumono contorni variegati[9].

Innanzitutto il problema del requisito del consenso espresso (che tra l'altro dovrebbe essere libero e incondizionato).

Nel sistema dell'IoT è impensabile che ogni utilizzo del bene sia accompagnato ad una richiesta di consenso, eppure ogni utilizzo è fonte di raccolta di dati[10]. Ogni volta che navighiamo su internet i cerca di infor-

[7] Per questa definizione v., S. Zani e A. Cerioli, *Analisi dei dati e* data mining *per le decisioni aziendali*, Milano, 2007, p. 3.

[8] Perplessità che si alimenta in modo esponenziale ove si considerino le possibilità che la tecnologia offrirebbe per permettere un controllo dei dati, o anche un consenso, con strumenti nuovi. Sul punto v., G. D'Acquisto, M. Naldi, Big data *e* privacy by design, Torino, 2017, p. 34, i quali semplicemente ma efficacemente rilevano come «non ci potrà essere una tecnologia di "nuova generazione" applicata ai *Big Data* e una di "vecchia generazione" per la privacy».

[9] Le medesime perplessità sono state espresse con riguardo agli art, 7 e 8 della Carta europea dei diritti dell'uomo, e sulla interpretazione che ne è stata data dalla giurisprudenza comunitaria. Sull'argomento v., O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di Google Spain*, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su* Internet *dopo la sentenza Google Spain*, Roma, 2015, 7 ss.

[10] In questa prospettiva cfr., G. D'Acquisto, M. Naldi, Big data *e* privacy by design,

mazioni, ogni volta che utilizziamo una applicazione del cellulare per cercare un percorso o per valutare le nostre performances sportive, ogni volta che accendiamo a distanza i condizionatori o i riscaldamenti, ogni volta che utilizziamo il *car* o il *bike sharing*, stiamo fornendo dati sulle nostre abitudini di vita, sui nostri consumi, sulle nostre preferenze, sulle nostre ideologie.

È vero che al primo atto di utilizzazione esprimiamo il nostro consenso, ma è pur vero che quel consenso non è spesso né libero né informato[11].

Non è libero perché è necessitato per l'utilizzo stesso del servizio che vogliamo utilizzare, non è informato perché i dati sulle nostre abitudini vengono raccolti e scambiati tra gli operatori per finalità completamente differenti per quelle iniziali di utilizzazione[12].

Quanto al primo punto, cioè alla necessità di raccolta, è necessario distinguere la necessità creata contrattualmente da quella tecnica legata al funzionamento dello strumento. La prima, come è facilmente comprensibile, è spesso reputata illegittima dal giudicante. Così, solo per portare un esempio, di recente il Garante ha definito illecito il trattamento dei dati da parte di una società che gestiva una piattaforma per la prenotazione di biglietti aerei, che imponeva all'atto della creazione dell'account anche il consenso al trattamento dei dati per finalità promozionali o di *marketing*[13].

La seconda richiede invece una valutazione più specifica è non sempre porta ad un risultato di illiceità del trattamento[14].

cit., p. 33 i quali propongono di valutare con accuratezza i tempi del trattamento e l'impatto sulle persone interessate «per comprendere se per ogni nuova finalità siamo in presenza di scopi realmente distinti e incompatibili o, per esempio, di due diverse fasi temporali dello stesso trattamento dei dati, ovvero di una nuova finalità non incompatibile con la precedente».

[11] Sulla possibilità che le norme sia pure precise e puntuali in tema di tutela della privacy siano facilmente disattese nel mondo di internet cfr., S. Rodotà, *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, p. 36 s.

[12] «Lo stesso dato anonimo o 'pseudonimizzato', ovvero sottoposto ad un processo di cancellazione di tutti gli elementi astrattamente identificativi, generalmente non protetto dalle norme sulla privacy, fornisce valore aggiunto e, combinato con altri dati anonimi può anche condurre all'identificazione di un soggetto. In altre parole, un *data-set* anonimo, qualora venga sottoposto ad un determinato trattamento, può dar vita a dati nuovi (anche di carattere personale), a loro volta riutilizzabili in maniera impredicibile finché non si riterranno più utili, ovvero una volta esaurite le tecniche (e le idee) per una loro combinazione», così, G. Giannone Codiglione, *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, cit., p. 284 ss.

[13] Autorità Garante per la protezione dei dati personali, ordinanza 22 giugno 2017, Doc. Web, n. 6697009.

[14] Sull'ampiezza della nozione di trattamento come interpretata dagli organi giudiziari europei, v., G. Finocchiaro, *La giurisprudenza della Corte di Giustizia in materia di dati per-*

 ISSN 2385-1279

Così, la Corte di cassazione[15] ha respinto il ricorso del Garante per la protezione dei dati personali contro una società che gestiva un impianto sciistico. Il garante lamentava la raccolta di dati personali tramite il tesserino di accesso ai tornelli senza preventivo consenso. In particolare l'utilizzo del tesserino permetteva la geolocalizzazione e la verifica del credito residuo. La Corte di cassazione «esclude una preventiva informazione che è in se stessa perché lo sciatore si avvicina per ottenere l'apertura del tornello ed è consapevole che il meccanismo consente l'accesso e verifica il non superamento del credito prepagato», concludendo che «la mancata formale informativa in materia di dati personali non è sanzionabile quando l'utente fruisce di un meccanismo, azionabile a sua iniziativa, che consente determinate prestazioni programmate, dovendosi escludere, a motivo di tale automatismo e del consenso dell'interessato, una preventiva informazione che è in se stessa».

Quanto al secondo punto è copiosa la giurisprudenza relativa alla utilizzazione di dati acquisiti legittimamente tramite consenso per fini che sono invece differenti. La giurisprudenza inquadra queste ipotesi in violazione del Codice della Privacy perché la diversa utilizzazione integra un nuovo trattamento.

3. *Le soluzioni del legislatore comunitario*

Il problema è che i pur numerosi interventi del Garante giungono necessariamente quando il danno si è già prodotto è cioè quando i dati hanno già circolato[16]. Più coerenti con le finalità di tutela dell'interessato sembrano allora le soluzioni individuate dal legislatore comunitario[17] che, differenziandosi dall'impostazione adottata nel nostro Codice della Privacy nell'art. 23, non assegna al consenso un ruolo trainante; non è la regola generale di liceità dei trattamenti; costituisce, invece, una tra le diverse condizioni di liceità previste.

sonali da Google Spain a Schrems, in G. Resta e V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su* Internet *dopo la sentenza Google Spain*, cit., p. 113 ss. Evidenziano che nel funzionamento della *Big data analytics* spesso è lo stesso soggetto che raccoglie i dati a non conoscere con precisione l'uso che ne farà, G. Sartor, M. Viola de Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU*, *ivi*, p. 104.

[15] Cass., 26 gennaio 2016, n. 1422, in *dejure online*.

[16] Anche gli studiosi di discipline non giuridiche riconoscono la necessità di una tutela preventiva della privacy e di una situazione di asimmetria tra gestore dei dati ed interessato. Cfr., G. D'Acquisto, M. Naldi, Big data *e* privacy by design, cit., p. 25 ss.

[17] Reg. (UE), 27 aprile 2016 n. 679.

ISSN 2385-1279

L'attenzione si sposta cioè sulle modalità di gestione dei dati imponendo l'adozione di meccanismi volti ad anonimizzare il dato: è il caso della c.d. privacy by design la quale, in un'ottica non reattiva ma proattiva, esprime il principio secondo cui le tecnologie adoperate per il trattamento dei dati personali devono essere, in primo luogo, progettate e, poi, impiegate in maniera tale da ridurre al minimo le possibilità di individuare il soggetto al quale tali informazioni si riferiscono, ricorrendo a tecniche di criptazione, anonimizzazione e non tracciabilità (art. 25, par. 1, reg. 2016/679) [18].

Ad essa si associa la regola della *privacy by default* che impone al titolare di adottare misure tecniche e organizzative in grado di garantire, per impostazione predefinita, il trattamento dei soli dati strettamente necessari alla specifica finalità perseguita, sotto il profilo sia della quantità, sia dell'ampiezza del loro trattamento, sia ancora del periodo di conservazione e del grado di accessibilità (art. 25, par. 2, reg. 2016/679).

Il legislatore europeo, cioè, pare accogliere un'accezione sempre più spersonalizzata di dati personali dando prevalenza al momento circolatorio e riconoscendo che la Big data analytics consente di ricostruire informazioni anche da frammenti di dati privi di specifici elementi identificativi[19]. Ciò non vuol dire rinnegare il potenziale rappresentativo del dato, ma definire una tutela specifica per il soggetto soltanto qualora esso sia identificato o identificabile. E in definitiva coglie l'essenza del fenomeno poiché ciò che rileva non è il dato in sé nella sua caratterizzazione personale, ma la sua organizzazione sinergica con altri dati, personalizzati o meno, che permet-

[18] Cfr. Sul punto le osservazioni di G. D'Acquisto, M. Naldi, Big data *e* privacy by design, cit., p. 2, i quali individuano nell'introduzione del principio di cui all'art. 25 del Regolamento, un ruolo di tutela, aggiuntivo alle tutele tradizionali, attribuito alla componente tecnologica. Il principio della *privacy by design* è poi specificato, con riferimento alla gestione dei Big data, dal Committee of the convention for the protection of individuals with regard to automatic processing of personal data nelle guidelines on the protection of individuals with regard to the processing of personal data in a world of big data, il quale richiede specificamente «Preventive policies and risk-assessment» e, in particolare, «to develop and provide appropriate measures, such as "by-design" and "by-default" solutions, mitigate these risks». Il documento chiarisce anche il contenuto di un approccio *by design*: «Controllers and, where applicable, processors should carefully consider the design of their data processing, in order to minimise the presence of redundant or marginal data, avoid potential hidden data biases and the risk of discrimination or negative impact on the rights and fundamental freedoms of data subjects, in both the collection and analysis stages».

[19] Ciò è da valutare tuttavia in un'ottica non personalista ma patrimoniale laddove i dati spersonalizzati posso essere liberamente venduti non incorrendo nei limiti della normativa sulla privacy. Per queste riflessioni v., M. Bogni, A. Defant, Big data*: diritti ip e problemi della* privacy, in *Dir. industr*., 2015, p. 117 ss.

 ISSN 2385-1279

tono di raggiungere il risultato sperato. Soltanto in quest'ottica il dato acquista valore per il suo utilizzatore, in ragione della sua potenzialità a prevedere l'agire degli individui.

4. *Doppia valenza del dato: valore economico e personale*

Il valore del dato, tuttavia, deve essere attentamente valutato poiché, il dato potrebbe rappresentare anche il corrispettivo di un servizio che invece appare gratuito al consumatore[20]. La questione è stata da tempo segnalata dalla dottrina più accorta, ed è stata valutata anche nelle decisioni del Garante della Concorrenza e del mercato[21] che definisce "una fattispecie di pubblicità ingannevole un messaggio, rappresentato da un banner presente sulla home page di un sito, collegato logicamente attraverso un link ipertestuale ad altre pagine web, recante l'invito a inserire gratuitamente il proprio annuncio economico, in ragione del fatto che non vengono portati a conoscenza dell'utente contestualmente al link ipertestuale, gli oneri economici cui la fruizione gratuita del servizio di inserzione degli annunci economici viene assoggettata, attraverso la prestazione del consenso al trattamento dei propri dati personali, quali la ricezione di e-mail pubblicitarie e la "profilazione".

Eppure così il dato viene ancora riguardato sotto l'aspetto del suo valore economico e giuridico utilizzando, anche se non sempre palesemente, la qualificazione di bene giuridico[22]. Che esso lo sia non vi sono dubbi[23],

[20] Altre volte invece l'autorizzazione ad utilizzare dati personali è contrattualmente configurata come un corrispettivo palese. Si v. l'esempio riportato da G. Colangelo, Big data, *piattaforme digitali e antitrust*, in cit., p. 425 ss., il quale riporta il caso rappresentato dall'offerta di At&T per il servizio Gigapower: con l'opzione «Premiere» gli utenti hanno la possibilità di connettersi risparmiando circa il 30% rispetto alla tariffa mensile concedendo in cambio al provider di utilizzare per finalità di *behavioural targeting* le informazioni connesse alla navigazione ed all'utilizzo dei motori di ricerca.

[21] Autorità Garante per la concorrenza, 20 dicembre 2001, n. 10279, in *Giust. civ.*, 2002, I, p. 1747.

[22] Il tema della qualificazione del dato informativo come bene economico, e dunque giuridico, è stato variamente affrontato dalla dottrina. Cfr., P. Perlingieri, *L'informazione come bene giuridico*, in *Rass. dir. civ.*, 1987, p. 33 ss.; S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p. 52 ss.; V. Zeno-Zencovich, *Informazione (profili civilistici)*, in *Dig. disc. priv., sez. civ.*, IX, Torino, 1993, p. 420 ss.; R. Pardolesi e C. Motti, *L'informazione come bene*, in G. De Nova (a cura di), *Dalle* res *alla* new properties, Milano, 1991, p. 37 ss.; G. Resta, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 209 ss. Specificamente, sul valore economico dei dati e sulle possibilità che siano oggetto di compravendita v., A. Mantelero, *Attività di impresa in Internet e tutela della persona*, Padova, 2004, p. 152 ss.

ciò che deve essere ripensata, e non solo in questo campo, è la disciplina, poiché non è più possibile ragionare in un'ottica proprietaria.

Ovviamente ciò significa modificare l'angolo visuale e spostare l'attenzione dal consenso quale atto di disposizione del bene ad un potere di controllo sulla effettiva modalità di gestione dei dati raccolti e sulle finalità del trattamento.

5. *Finalità del trattamento e profilazione*

Siamo giunti dunque alle finalità del trattamento. È qui che si gioca la partita più importante!

È noto che attraverso la *big data analytics* possono essere creati profili degli utenti del web che riuniscono numerosi dati eterogenei e slegati tra loro ma combinati in una sintesi dotata di contenuto informativo ulteriore, potenzialmente espressivo delle caratteristiche personali o professionali degli individui. Il risvolto, ove i dati siano relativi ad una determinata persona, è la possibilità di ottenere elementi di conoscenza in merito alle abitudini commerciali, alla credibilità e affidabilità nelle transazioni economiche, ma può rispondere anche a ragioni differenti che possono rivelarsi lesive dei diritti della personalità, (stato di salute, preferenze ideologiche e politiche)[24].

Lo scorso 24 novembre (2016) l'autorità Garante per la protezione dei dati personali[25] ha valutato la richiesta di una società che aveva tra i propri

[23] Si sta sviluppando, infatti, uno specifico mercato, denominato *market for data*, nel quale il dato rappresenta il bene oggetto di scambio. Cfr., sul punto, G. Colangelo, *Big data, piattaforme digitali e* antitrust, cit., p. 426.

[24] Tale possibilità è il problema principale della diffusione della *big data analytics* che gli Stati europei valutano nella definizione della regolamentazione del fenomeno. Ciò si riflette in un differente sottostrato della normativa in tema di Privacy tra Europa e Stati Uniti, poiché nel vecchio continente il concetto di privacy è fortemente legato alla dignità personale, mentre oltre oceano si discorre maggiormente di tutela dello "spazio vitale" della persona (Per questa differenza v., G. Sartor, M. Viola de Azevedo Cunha, *Il caso Google e i rapporti regolatori USA/EU*, in *Dir. inform. informatica*, 2014, p. 658 ss.). La differenza è palese anche nella diversa modalità in cui le Autorità hanno affrontato il caso *Facebook/Whatsapp*, laddove le autorità statunitensi hanno valutato la violazione delle norme antitrust e in Italia è intervenuto in Garante della privacy. Uno sviluppo dei *Big data* disancorato dalle tutele dettate dalla normativa sulla privacy creerebbe problemi di equilibrio allo stesso sistema di *information technology*. Sul punto v., G. D'Acquisto, M. Naldi, Big data *e* privacy by design, cit., p. 25 ss., i quali evidenziano problemi di discriminazione, *lock in*, vincoli sociali condizionamenti e scelte indotte dal medium utilizzato.

[25] Garante per la protezione dei dati personali, 24 novembre 2016, doc. web n. 5796783.

 ISSN 2385-1279

obiettivi la "qualificazione reputazionale". In particolare la società aveva "manifestato l'intenzione di voler procedere alla realizzazione di una piattaforma web (con annesso archivio informatico) preordinata all'elaborazione di profili reputazionali concernenti persone fisiche e giuridiche. Il sistema, volto anzitutto a contrastare fenomeni basati sulla creazione di profili «artefatti» o «inveritieri», (si prefiggeva l'obiettivo) di calcolare in maniera imparziale, affidabile e oggettivamente misurabile il «rating reputazionale» dei soggetti censiti, sì da consentire a eventuali terzi di poter verificare la loro reale credibilità".

Il sistema, nelle intenzioni dei suoi ideatori, era fondato su una base volontaria e cioè prendeva le mosse da un atto di iscrizione del soggetto recensito il quale avrebbe dovuto provvedere al caricamento sulla piattaforma di documenti contenenti informazioni ritenute significative sul piano della propria reputazione. Questi ultimi venivano poi valutati da appositi «consulenti reputazionali» al fine di garantirne la genuinità e l'integrità. Infine, all'esito delle operazioni di verifica, il sistema avrebbe provveduto a calcolare, mediante un sofisticato algoritmo matematico, un «punteggio» complessivo da assegnare agli interessati (c.d. «*rating* reputazionale») atto a determinarne il grado di affidabilità. Rating suddiviso in cinque sub-rating: «penale», «fiscale» e «civile», oltre, eventualmente, a «lavoro e impegno civile» e, limitatamente alle persone fisiche, «studi e formazione».

Il servizio, dunque, con la previsione della preliminare iscrizione alla «community», avrebbe operato principalmente su base volontaristica, perché possibile solo a seguito della preventiva raccolta del consenso da parte degli interessati; tuttavia tale consenso iniziale avrebbe dovuto coprire anche le successive operazioni di trattamento effettuate da terzi (visualizzazione, estrazione e riutilizzo dei dati e dei documenti); il medesimo consenso, inoltre, sarebbe stato acquisito per giustificare eventuali operazioni di trattamento collegate a presunte «irregolarità» documentali segnalate da altri, nonché per pubblicare atti e documenti attinenti a controversie giudiziarie pendenti o future.

Di là dalla valutazione di illiceità del Garante, fondata sul pericolo di lesione della dignità personale, appare significativa la perplessità espressa in merito alla «opportunità stessa di rimettere a un sistema automatizzato ogni determinazione in merito ad aspetti particolarmente delicati e complessi quali quelli connessi alla reputazione dei soggetti coinvolti. A prescindere, infatti, dall'oggettiva difficoltà di misurare situazioni, parametri e variabili non sempre agevolmente «classificabili» o «quantificabili», il Garante evidenzia che la suddetta (acritica[26]) valutazione potrebbe fondarsi su atti, do-

[26] Anche nel documento del Committee of the convention for the protection of

cumenti o certificati viziati *ex ante* da falsità ideologica, ovvero caratterizzati da alterazioni materiali non facilmente riscontrabili da parte di pur esperti "consulenti" reputazionali (peraltro non esenti, contrariamente a quanto sostenuto, da pericoli di errore o tentativi di corruzione); con il rischio, neanche tanto remoto, di creare profili reputazionali inesatti e non rispondenti alla reale rappresentazione – e, quindi, all'identità personale, intesa anche quale immagine sociale (art. 2 del Codice; Provv. 9 marzo 2006 [doc. web n. 1269316]; Trib. Roma 7 dicembre 2015) – dei soggetti censiti».

Del resto i pericoli relativi alla profilazione sono da tempo affrontati, anche se non con riferimento ai big data in materia bancaria, ed è ormai accertato che pur vigendo un obbligo di profilazione del cliente da parte della Banca, è dovere dell'intermediario fornire le informazioni sull'investimento e valutare l'adeguatezza dell'operazione. Di recente ad esempio, la Cassazione[27] ha affrontato il caso di inadempimento agli obblighi informativi di un istituto bancario nei confronti di un cliente, definitosi esperto finanziario, che aveva omesso di fornire indicazioni sul suo profilo di rischio concludendo che ciò «non esonerava l'intermediario della valutazione dell'adeguatezza dell'operazione, (e) rilevando che, in applicazione del principio di diligenza, la banca avrebbe dovuto anzi agire in base alla massima cautela». La Corte «ha evidenziato, inoltre, come non potesse ritenersi rilevante il fatto che l'investitore si considerasse esperto in strumenti finanziari, non esimendo tale circostanza dall'adempimento, da parte dell'intermediario, degli obblighi informativi». In definitiva, «l'intermediario finanziario non è esonerato dall'obbligo di valutare l'adeguatezza dell'investimento nemmeno ove l'investitore si sia rifiutato di fornire le informazioni sui propri obiettivi di investimento e sulla propria propensione al rischio: in tal caso, infatti, l'intermediario stesso deve comunque compiere quella valutazione, in base ai principi generali di correttezza e trasparenza, tenendo conto di tutte le notizie di cui egli sia in possesso (Cass. 16 marzo 2016, n. 5250; Cass. 19 ottobre 2012, n. 18039)».

INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA NELLE GUIDELINES1 ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA IN A WORLD OF BIG DATA, viene rimarcata la necessità che il giudizio o una decisione riguardanti una persona non può dipendere esclusivamente da meccanismi automatizzati ma è sempre necessario assegnare centralità al *Role of the human intervention in Big Data-supported decisions.*

[27] Cass., 31 agosto 2017, n. 20617, in *ilcaso.it*

 ISSN 2385-1279

6. *Pericoli della profilazione e responsabilità del titolare del trattamento*

Riportando l'esperienza maturata nell'ambito della questione telematica vengono in rilievo due aspetti.

Un primo aspetto, relativo ai pericoli della profilazione[28].

Il legislatore comunitario sceglie di non vietare *tout court* l'operazione ma di vietare che essa possa divenire un parametro di valutazione della persona; infatti all'art. 22 del Regolamento Privacy si specifica che «L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona». È ovvio che far rispettare un tale divieto è cosa ardua poiché significherebbe riuscire ad indirizzare la formazione della coscienza sociale, è pur vero però che anche vietare le operazioni di profilazione *tour court* sarebbe, anche tecnicamente, molto difficile. Del resto la profilazione anonima, cioè non legata a persone identificate ma orientata a creare profili tipo, è intimamente connessa alla *Big data analytics* e possiede anche elementi di utilità sociale[29].

Un secondo aspetto, spinge ad addossare una maggiore responsabilità al titolare del trattamento, quale soggetto professionista e maggiormente ca-

[28] L'art. 4 del Reg. N. 679/2016 definisce il fenomeno come «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

[29] Infatti, non si tratta soltanto di profilazione commerciale come quella di cui si discute spesso in ambito di Social network laddove la raccolta di *user data* da parte dei *providers* può ben rappresentare il corrispettivo di un servizio che, invece, viene percepito come gratuito; o di quella operata da Amazon che ha depositato negli Stati Uniti una domanda di brevetto per un servizio di "*anticipatory shipping*", un servizio cioè in grado di prevedere le richieste dell'utente, sulla base dell'analisi delle precedenti esperienze di acquisto e di navigazione sul sito da questi effettuate, collocando dunque, in via preventiva, tali prodotti nel magazzino più vicino a colui che sarà verosimilmente l'acquirente di un certo bene. Si tratta anche del sistema elaborato da un altro sito (*Farecast*) che, sulla base dell'analisi di un enorme database relativo alle transazioni di acquisto di biglietti aerei, è in grado di prevedere con un'attendibilità dichiarata dell'85%, se il prezzo indicato nel momento dell'interrogazione al sito calerà o crescerà nel periodo successivo e fino alla partenza, con un risparmio considerevole per gli utenti.

O, infine in ambito assolutamente non commerciale, la dimostrazione di forza data da Google che è riuscito a mappare in tempo reale la diffusione dell'influenza, senza il ritardo medio di 1 o 2 settimane accusato dalle istituzioni governative, (utilizzando i 50 milioni di parole chiave più digitate dagli americani e confrontando l'elenco con i dati sulla diffusione dell'influenza nel quinquennio il 2003-2008, sì da individuare ben 45 parole chiave che ricorrono nelle aree in cui il virus è diffuso).

ISSN 2385-1279

pace di valutare i pericoli del trattamento. In ciò la posizione del titolare è sempre più vicina a quella poc'anzi richiamata dell'intermediario finanziario che deve valutare *ex ante* la pericolosità dell'operazione: l'art. 35 del Regolamento 679/2016 ha introdotto l'obbligo preventivo per i titolari di effettuare una valutazione di impatto che si sostanzia in un processo volto, da un lato, a valutare la necessità e proporzionalità del trattamento e dall'altro a gestire i rischi per i diritti e le libertà delle persone fisiche che siano coinvolte in operazioni di trattamento di dati personali.

Il sistema europeo, dunque, si mostra maggiormente coerente con la realtà tecnologica che intende disciplinare impostando criteri più realistici, quali il controllo, piuttosto che il consenso, dal lato dell'interessato e un rafforzamento del binomio libertà/responsabilità, dal lato del titolare del trattamento. Ovviamente ciò significa compiere una piccola rivoluzione culturale e scardinare idee radicate, ma in fondo è questa la base di ogni rivoluzione:

«Un'epoca è caratterizzata non tanto dalle idee che vi sono discusse ma da quelle che sono date per scontate […] Il potere funziona grazie a idee che solo un folle metterebbe in dubbio […] Questo significa che una società a volte si inceppa… Il compito più difficile per gli attivisti sociali e politici di questi tempi è trovare il modo di indurre le persone a ripensare ciò che tutti noi diamo per vero. La sfida sta nel seminare il dubbio»[30].

[30] Lawrence Lessig, *Il futuro delle idee*, 2001.

 ISSN 2385-1279

Edizioni Scientifiche Italiane s.p.a.
80121 Napoli, Via Chiatamone, 7
Tel. 081/7645443 PBX - Telefax 081/7646477

Condizioni di abbonamento per il 2018:

Privati:	Abbonamento € 60,00	Fascicolo € 30,00
Enti:	Abbonamento € 80,00	Fascicolo € 40,00
Estero:	Abbonamento € 150,00	Fascicolo € 75,00
Sostenitori:	Abbonamento € 250,00	

I prezzi si intendono comprensivi di IVA.
La sottoscrizione a due o piú riviste, se effettuata in un unico ordine e direttamente presso la casa editrice, dà diritto ad uno sconto del 10% sulla quota di abbonamento. Gli sconti non sono cumulabili.

L'abbonamento decorre dal 1° gennaio di ogni anno e dà diritto a tutti i numeri dell'annata, compresi quelli già pubblicati. Il pagamento può essere eseguito con queste modalità:

- con versamento tramite bollettino postale sul n.c.c. 00325803, intestato a Edizioni Scientifiche Italiane S.p.a, via Chiatamone, 7 - 80121 Napoli.
- Sul modulo devono essere indicati, in modo leggibile i dati dell'abbonato (nome, cognome ed indirizzo) e gli estremi dell'abbonamento.
- mediante bonifico bancario sul c/c 70, intestato a Edizioni Scientifiche Italiane S.p.a., via Chiatamone, 7 - 80121 Napoli; - Banca popolare dell'Emilia Romagna - IBAN IT48U0538703411000000000070.
- a ricevimento fattura (formula riservata ad enti e società)

Per garantire al lettore la continuità nell'invio dei fascicoli l'abbonamento che non sarà disdetto entro il 30 giugno di ciascun anno si intenderà tacitamente rinnovato e fatturato a gennaio dell'anno successivo.
I fascicoli non pervenuti all'abbonato devono essere reclamati entro 15 giorni dal ricevimento del fascicolo successivo. Decorso tale termine si spediscono contro rimessa dell'importo. Per ogni effetto l'abbonato elegge domicilio presso le Edizioni Scientifiche Italiane S.p.a.

Le richieste di abbonamento, le segnalazioni di mutamenti di indirizzo e i reclami per mancato ricevimento di fascicoli vanno indirizzati all'Amministrazione presso la casa editrice:
Edizioni Scientifiche Italiane S.p.a., via Chiatamone 7 - 80121 Napoli
Tel. 081/7645443 - Fax 081/7646477
Internet: www.edizioniesi.it
e-mail: periodici@edizioniesi.it

Codice civile
annotato con la dottrina e la giurisprudenza

a cura di GIOVANNI PERLINGIERI

Formato cartonato 17x24; volumi I-IX+CdRom; € 820,00

Enciclopedia di Bioetica e Scienza giuridica

diretta da ELIO SGRECCIA E ANTONIO TARANTINO

Formato cartonato 17x24; volumi I-XII; € 1400,00
