CIRSFID
CENTRO INTERDIPARTIMENTALE DI RICERCA IN
STORIA DEL DIRITTO, FILOSOFIA E SOCIOLOGIA DEL DIRITTO E INFORMATICA GIURIDICA

STEFANO NERI

LA DISCIPLINA DEL *DATA MINING* ALLA LUCE DELLA PROPOSTA DI REGOLAMENTO COMUNITARIO IN MATERIA DI TRATTAMENTO DI DATI PERSONALI: CRITICITÀ, LIMITI E PROSPETTIVE *DE JURE CONDENDO*.

FiLO diritto
dal 2001
la legge, il diritto, le risposte

Osservatorio CIRSFID di informatica giuridica e diritto delle nuove tecnologie

Il CIRSFID (Centro Interdipartimentale di Ricerca in Storia del Diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica dell'Università degli Studi di Bologna "Guido Fassò - Augusto Gaudenzi") venne istituito con decreto rettorale n. 1751 del 1° ottobre 1986.
Il CIRSFID è un Centro di Ricerca in cui confluiscono competenze di docenti e ricercatori delle Facoltà di Giurisprudenza (Dipartimento Giuridico "A. Cicu"), Ingegneria (Dipartimento di Elettronica, Informatica e Sistemistica), Lettere e Filosofia (Dipartimento di Filosofia), Scienze Matematiche, Fisiche e Naturali (Dipartimenti di Matematica e di Scienze dell'Informazione), Scienze Statistiche (Dipartimento di Scienze Statistiche "P. Fortunati") dell'Ateneo bolognese.
Le linee di ricerca del CIRSFID interessano l'informatica giuridica, il diritto dell'informatica e delle nuove tecnologie, la storia del diritto, la filosofia, teoria e sociologia del diritto, la bioetica, aree nelle quali il CIRSFID esplica un'intensa attività di pubblicazioni, iniziative editoriali e scientifiche, didattica universitaria e post-universitaria, consulenze e servizi, in collaborazione con organismi di ricerca nazionali e internazionali.

L'Autore

Stefano Neri è avvocato del Foro di Livorno, laureatosi in Scienze Giuridiche ed in Giurisprudenza presso l'Università di Pisa, pratica prevalentemente diritto del lavoro e diritto penale, coltivando un interesse professionale e personale per l'informatica, in particolare per quanto riguarda la *privacy* e la protezione dei dati personali.
Nell'a.a. 2012/2013 ha acquisito il titolo di Master in Diritto delle Nuove Tecnologie e Informatica Giuridica presso l'Università di Bologna, entrando in contatto con il Cirsfid per la preparazione del *project work*, nonché per la ricerca e l'approfondimento di tematiche di ambito giuridico-informatico.

La disciplina del *data mining* alla luce della proposta di regolamento comunitario in materia di trattamento di dati personali: criticità, limiti e prospettive *de jure condendo*

STEFANO NERI

Indice

PARTE PRIMA

Premessa: il fenomeno del *data mining* ed il potere dei dati[1].

"*I Big Data sono una grande promessa. Quella di una risorsa inesauribile per il business*":
così recita un passo della pubblicità promozionale di una delle più note ed importanti società nel settore dell'ICT. Tale affermazione consente di ritenere meritevole di attenzione, sul piano della tutela dei dati personali, il fenomeno di trattamento che si pone alla base dei *big data*, *rectius*, il fenomeno del cd. *data mining*.
Tale disciplina sarà valutata alla luce della recente proposta di regolamento comunitario, tutt'ora in attesa di approvazione dal Consiglio dell'Unione Europea, così come recentemente modificato dalla Commissione Libertà Civili, Giustizia e Affari Interni del Parlamento Europeo, con gli emendamenti presentati dalla Commissione Europea.
Il trattamento di *data mining* non è un istituto espressamente disciplinato né dall'attuale proposta di regolamento comunitario, né tanto meno da precedenti

[1] La presente opera intende proporre delle prime considerazioni in tema di *data mining* sulla base del percorso legislativo tutt'ora in corso, improntato all'emanazione di un nuovo regolamento comunitario in tema di trattamento di dati personali. Pertanto, questa trattazione si basa prevalentemente sulla lettura, e quindi sull'analisi, della Proposta di Regolamento del Parlamento Europeo e del Consiglio, concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati, versione italiana del 25.01.2012, nonché degli emendamenti al testo approvati definitivamente in data 31.10.2013, e disponibili al momento solo in lingua inglese (da ora in avanti ogni riferimento a singole norme si intenderà riferito a tale normativa, se non diversamente disposto), nonché sulla lettura della recente opera di Viktor Mayer-Schonberger e Kenneth Cukier, *"Big Data. Una rivoluzione che modificherà il nostro modo di vivere e già minaccia la nostra libertà"*, ed. Garzanti, 2012. Con tale contributo non si intende affrontare in maniera analitica singole questioni inerenti il trattamento dei dati personali *tout court* considerato, bensì offrire uno spunto di riflessione sugli effetti di una normativa che, partendo da tale embrione legislativo, si potrebbero produrre rispetto al fenomeno del *data mining*. Per quanto riguarda la trattazione in maniera specifica dei singoli argomenti trattati dalle normative in materia di dati personali, dalla direttiva 46/957CE, al D.Lgs. n. 196/2003 passando dalla prima formulazione della L. n. 675/1996, si rinvia ai contributi che altri illustri Autori hanno proposto nel corso degli anni. In particolare, solo per citare alcuni testi che sono stati di ausilio allo scrivente, e consultati *in parte qua* rispetto al tema principale, si rimanda alla lettura de: *"Il Codice in Materia di Protezione dei Dati Personali"*, a cura di Jury Monducci e Giovanni Sartor, ed. Cedam, 2004; *"La Protezione dei Dati Personali"*, a cura di Cesare Massimo Bianca e Francesco Donato Busnelli, ed. Cedam 2007; *"Libera Circolazione e Protezione dei Dati Personali"*, a cura di Rocco Panetta e Paolo Cendon, ed. Giuffrè Editore 2006; *"Il Codice del Trattamento dei dati personali"*, a cura di Vincenzo Cuffaro, Roberot D'Orazio e Vincenzo Ricciuto, ed. Giappichelli Editore, 2006; *"Statistical Data Mining Using SAS Applications, Second Edition"* di George Fernandez, CRC Press 2010, e *"Data mining nel social web"*, di Matthew A. Russell, Milano, ed. Tecniche Nuove, 2011.

normative, anche sul piano interno.
Tale mancanza non è dovuta ad una dimenticanza del legislatore, quanto piuttosto al fatto che la disciplina in tema di protezione di dati personali deve ricomprendere una serie di possibili *genera* di trattamento, senza poterne analiticamente distinguere le differenti tipologie specifiche.
In quest'opera si affronterà la disciplina teoricamente applicabile a tale tipo di trattamento di dati personali[2].
Quando si parla di *data mining* s'intende riferirsi, preliminarmente, ad un'operazione tipica del mondo dell'ICT, e dunque un fenomeno strettamente connesso con trattamenti di dati in forma automatizzata.
Il *data mining* in particolare è un "*powerful information technology tool*", che consiste nell'estrapolare[3] dati in formato elettronico dagli innumerevoli *database* che compongono la rete Internet.
L'operazione consiste, mediante l'utilizzo di determinati *software*, nel ricercare dati "grezzi" presenti nella rete e stabilire delle connessioni tra questi dati, in particolare per ricostruire schemi e disegni che permettano di addivenire a delle conclusioni ulteriori rispetto al dato di partenza.
L'utilizzo di specifici *software*, come le c.d. API[4] (*Application Program Interface*), consentono materialmente di sondare la rete alla ricerca di dati messi a disposizione dai vari *content provider* in forma liberamente accessibile o meno e sulla base del *range* di operazioni disponibili, mediante l'utilizzo di inferenze, addivenire a delle conclusioni nuove rispetto a dati singolarmente considerati.
Sotto il profilo formale, ci si potrebbe domandare se il trattamento di *data mining* consista nella mera operazione di ricerca del dato, oppure anche nella successiva operazione di creazione del risultato utile.
Ebbene tali operazioni sembrerebbero distinte, anche se non è facile riuscire ad individuare il momento in cui avviene questo passaggio.
Difatti, possono identificarsi quattro tipi di soggetti, a cui corrispondono diversi tipi di trattamento: il *content provider* che dispone dei dati, il soggetto che opera l'estrapolazione (il quale potrebbe già essere un nuovo responsabile, oppure un incaricato del responsabile - *content provider*), il soggetto che opera l'analisi dei

[2] L'art. 4 della bozza di regolamento definisce il trattamento come: *"qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la memorizzazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la cancellazione o la distruzione"*. La definizione offerta dal legislatore pare esaustiva nell'elencare le varie operazioni che caratterizzano un trattamento di *data mining*.
[3] Dall'inglese "*to mine*", scavare, estrarre, alludendo all'operazione tipica compiuta dai minatori.
[4] In generale il SAS Institute, una società con sede negli USA, North Carolina, è specializzata nello sviluppo di particolari *software*, chiamati per l'appunto in via generica SAS *software*, ovvero un complesso di prodotti *software* integrati che permettono ad un programmatore tutta una serie di operazioni, ed utilizzate appunto per il *data mining*.

dati grezzi (anche in questo caso potrebbe essere un nuovo responsabile o un incaricato), ed infine il soggetto che ne trae utilità.
Partendo dal presupposto che le normative in vigore disciplinano già la prima delle situazioni elencate, sembrerebbe preferibile ricomprendere all'interno del fenomeno del *data mining* le altre tre fasi per due ragioni, una di ordine giuridico, e l'altra di ordine tecnologico: la prima ragione consiste, in un'ottica giuspositivista, nel dover riempire quelle lacune che potrebbero crearsi nel lasciare all'arbitrio del mercato le successive fasi di operazioni compiute sui dati.
In secondo luogo, allorché nel mondo informatico si affronta la questione del *data mining* e dei *big data*, si tende a considerare le tre fasi successive come un *unicum*, altrimenti dovendosi considerare la mera estrazione dei dati come un'operazione priva di senso compiuto.
Ad ogni modo, nella pratica gli operatori di *data mining* scandagliano il *web* mediante il c.d. *crawler*, dei *software* che riescono ad analizzare i contenuti presenti in rete, insegnando a questi *software* come giudicare e valutare il sentimento (c.d. *sentyment analysis*) che emerge dalla rete, grazie all'opera dei linguisti computazionali, che attribuiscono valori differenti a differenti reazioni e stati d'animo che possono emergere a partire da un determinato fatto.
La rete offre già la possibilità di svolgere una serie di operazioni di ampia portata in grado di estrarre una grande quantità di dati, come la visione dei contenuti della posta elettronica, o piuttosto i messaggi rilasciati sui vari *social network*.
I dati della posta elettronica, come sostiene Russell nella sua opera "*Data mining nel social web*", sono sparsi in rete sotto forma di ricche discussioni su argomenti interessanti e, a differenza dei *social media*, le aziende hanno in genere il pieno controllo delle loro caselle postali e possono voler eseguire analisi aggregate per identificare particolari tipi di tendenze, e, ad esempio, capire quali sono gli argomenti maggiormente oggetto di discussione.
Come ricorda sempre Russel nella sua opera, Twitter, Facebook e Linkedin sono fonti inesauribili di dati e in quest'ottica la recente acquisizione da parte della società statunitense Facebook della *start-up* di messaggistica istantanea Whatsapp ad un prezzo elevatissimo, costituisce segno tangibile del valore che i dati portano con sé[5].

[5] Il riferimento è all'acquisto da parte di Facebook per la cifra record di 19 miliardi di dollari, suddivisi tra denaro e azioni della società WhatsApp, da www.ilsole24ore.com/art/notizie/2014-02-24/facebook-compra-whatsapp-19-miliardi-dollari-231641.shtml.

Grazie alle relative API, con il primo *social network* si possono effettuare analisi sia in merito alle relazioni tra gli utenti sia sul contenuto effettivo dei *tweet*, anche con riguardo alla posizione geografica degli utenti; con il secondo, definito la meraviglia "tutto in uno", è possibile svolgere qualsiasi operazione sociale immaginabile, fino ad arrivare anche alla creazione di applicazioni intelligenti e guidate dai dati.
Linkedin, a differenza dei primi due, si attesta su una politica più restrittiva rispetto all'accesso ai dati da parte di esterni, ma alcune informazioni sono comunque estraibili.
Inoltre, non si deve dimenticare che un trattamento di *data mining*, al di là della fruibilità pubblica del dato in sé, può essere effettuato anche a partire da dati messi a disposizione da determinati soggetti, nonostante l'inconsapevolezza degli utenti interessati.
Tali opportunità, quindi, rappresentano una fonte continua ed inesauribile di innovative strategie di business, ma lo scopo principale che può determinare un titolare del trattamento a procedere alla relativa operazione potrà consistere in finalità non lucrative[6].
Ad ogni modo, tale fenomeno rientra a pieno titolo nelle fattispecie considerate come trattamento di dati personali ai sensi delle normative comunitarie ed interne, meritevole di attenzione da parte del diritto.
Nel percorso di analisi della disciplina potenzialmente applicabile al trattamento di *data mining*, pare doveroso introdurre anche altri concetti che nel linguaggio informatico vi sono generalmente associati, ovvero i c.d. *big data* e gli *analytics*: con il termine *big data*[7], s'intende riferirsi alla grande e sterminata mole di dati presenti nella rete, a prescindere dalla grandezza o meno del *database* che li contiene, ovvero l'insieme, la somma di ogni singolo *database* che a sua volta contiene dei *database* più piccoli, che contengono a loro volta una certa mole di dati.
I *big data* rappresentano l'oggetto principale del trattamento di *data mining*.
Con l'espressione *analytics*, invece, si indica quel tipo di operazione che è parte integrante, ma successiva, del processo di *data mining*, ovverosia l'analisi e la scoperta di determinate connessioni rilevanti fra dati.
Gli scopi e le finalità che, in linea di massima, sono connesse a tale tipo di trattamento rappresentano uno dei motivi di interessamento per il giurista moderno.

---

[6] Matthew Russell, op. Cit., sottolinea come le tecniche di *data mining* (o estrazione dei dati), di analisi e di visualizzazione dei dati, applicate nel cd. *social web* consentono di rispondere a domande del tipo: *"Due persone si conoscono? E quali amicizie hanno in comune? Con quale frequenza determinate persone comunicano con altre? Qual'è il livello di simmetria nella comunicazione tra le persone? Chi sono i più chiacchieroni o i pù riservati in rete? Quali sono le persone più influenti o popolari in una rete? Di che cosa parla la gente? Che cosa ritiene interessante?".*

[7] *http://en.wikipedia.org/wiki/Big_data.*

Se è pur vero che l'intreccio dei dati può, da un lato, avere motivi d'interesse storico, statistico, o principalmente scientifico, è pur vero, dall'altro lato, che le implicazioni in termini di profilazione o comunque in termini economici possono, come è presumibile ritenere, essere le più rilevanti e meritevoli d'attenzione. Inoltre, al di là dello scopo, non si deve dimenticare che anche la natura stessa dei dati implica di per sé la necessità di un'attenzione particolare da parte del giurista.

La rete, e i *database* ivi presenti, possono contenere, al di là di un'elevata quantità di dati, anche dei dati di natura personale ed in particolare dati sensibili[8].

Il *Web* è un luogo virtuale dove, per sua natura, tutto è generalmente immanente[9], data la costante espansione ed affinamento delle tecnologie dell'informazione, pieno di dati che contengono sia informazioni di carattere giudiziario, magari attinenti a procedimenti penali, oppure di carattere sanitario, idonei a svelare aspetti inerenti lo stato di salute e psicofisico della persona.

Le possibili applicazioni che possono derivare da tali processi sopra brevemente descritti sono innumerevoli e l'unico limite è la fantasia di chi può entrare in possesso di tali dati[10].

Tali possibilità, come è logico intuire, permettono ai soggetti che si occupano di scandagliare la rete di entrare in possesso di un materiale prezioso e unico nel suo genere.

Le grandi aziende che offrono servizi o che si occupano della produzione e vendita di beni, possono osservare i comportamenti di una massa determinata o indeterminata di utenti della rete per sviluppare delle soluzioni di business mirate per ogni singolo soggetto, oppure anche per migliorare la propria offerta al pubblico.

---

[8] Sotto questo punto di vista, la scelta del legislatore comunitario, per risolvere il dubbio sull'inclusione o meno dei dati relativi alle persone giuridiche nella disciplina a protezione dei dati personali, ha stabilito che *"La protezione prevista dal presente regolamento si applica alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei dati personali. La protezione offerta dal presente regolamento non potrà essere invocata per il trattamento dei dati relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compreso il nome, la forma giuridica e i contatti. Ciò vale anche quando il nome della persona giuridica contiene il nome di una o più persone fisiche"* (considerando n. 12).

[9] Per tale motivo il legislatore europeo ha introdotto nell'attuale proposta di regolamento comunitario una sezione relativa al diritto all'oblio (al momento "retrocesso" a diritto di cancellazione), ovvero *"il diritto* [di ognuno] *ad ottenere la cancellazione di dati che lo riguardano"* (art. 17, categoria nata dalle elaborazioni della dottrina e poi recepita, al momento, come parte integrante dell'insieme di diritti propri dell'interessato dal trattamento di dati personali).

[10] Alcune di queste possibilità di sfruttamento dei dati sono previste espressamente anche da George Fernandez, op.cit., pag. 3:
-Increase customer acquisition and retention.
-Uncover and reduce fraud (determining if a particular transaction is out of the normal range of a person's activity and flagging that transaction for verification).
-Improve production quality and minimize production losses in manufacturing.
-Increase up-selling (offering customers a higher level of services or products, such as a gold credit card vs. a regular credit card) and cross-selling (selling customers more products based on what they have already bought).
-Sell products and services in combinations based on market basket analysis (by determining what combinations of products are purchased at a given time).

La profilazione del singolo sulla base dei suoi comportamenti in rete e quindi delle connessioni stabilite dallo stesso con gli altri utenti della rete, permetterebbe di offrire prodotti e servizi sempre più mirati rispetto alle esigenze del singolo, nella direzione di un vero e proprio *microtargeting*[11] sino al rischio di raggiungere situazioni di preoccupante ed inquietante controllo tecnologico[12].
Oppure, ancora, dall'analisi di una percentuale di acquisti di più prodotti correlati, si possono offrire sul mercato tali tipi di prodotti ad un prezzo agevolato, in modo da espandere ulteriormente i consumi.
Sotto un differente profilo, gli operatori commerciali potrebbero decidere di rifiutarsi di portare a compimento degli affari laddove è maggiormente probabile che si verifichino delle truffe o frodi informatiche[13].
L'analisi dei dati presenti nei *social network* potrebbe consentire di muoversi meglio all'interno del mercato dei titoli e quindi di prevedere con maggiore successo l'andamento della Borsa.
Si pensi ad esempio anche sul piano politico, ai possibili risvolti positivi da utilizzo di *analytics*: il politico candidato a ricoprire una carica pubblica potrebbe impostare e basare un discorso, oppure inserire nel proprio programma elettorale un determinato punto da perseguire nella campagna politica perché maggiormente in linea con il pensiero dell'elettorato.
Seppur tale caratteristica può ammettersi come pratica comune, l'analisi dei *big data* consentirebbe una certa anonimizzazione della procedura nonché una qualità del risultato maggiore, rispetto alla consapevole indagine di mercato effettuata mediante l'ausilio del telefono, del contatto fisico, oppure della posta elettronica.
L'Unione Europea, maggiormente sensibile sul tema della protezione dei dati personali nel periodo storico attuale, rispetto a realtà come gli USA[14], sta provvedendo ad emanare una normativa unitaria per tutti i paesi dell'Unione, con la speranza che il dibattito dottrinario e giurisprudenziale abbia contribuito ad aiutare il legislatore nella formulazione di un impianto normativo più in linea con le recenti innovazioni sul piano tecnologico.

---

[11] Per *microtargeting* s'intende l'utilizzo di tecniche predittive basate sulla combinazione di dati rispetto al singolo, inclusa la relativa ubicazione ed il comportamento personale; tale fenomeno ha avuto un grande impatto nell'ultima campagna elettorale statunitense, vinta dal presidente Barack Obama.

[12] Vedasi ad esempio il caso noto alle cronache del padre della giovane tredicenne che si indignò in seguito all'invio a casa di *coupon* relativi a prodotti per la maternità diretti alla figlia, salvo poi scoprire poco dopo, che la figlia era realmente in attesa di un bambino, come ricorda Daniela De Pasquale in *"La linea sottile tra manipolazione della rete e pubblicità"*, da Il Diritto Industriale n. 6/2012, pag. 4, che analizzando le varie tecniche di marketing *on line* riserva un'interessante paragrafo dedicato ai *big data* e alle tecniche di *predictive analytics*.

[13] Tale modalità di gestione del business sarebbe possibile laddove la struttura giuridica del negozio si identificasse con il cd. invito ad offrire, ovvero nella proposta di acquisto di beni o servizi.

[14] Per quanto la nascita di un interesse giuridico della dottrina ai temi della cd. *privacy* si collochi proprio negli Stati Uniti, con l'articolo di Warren e Brandeis, *"The right to privacy"*, in Harvard Law Review, 1890.

D'altronde, nella Relazione alla proposta di regolamento comunitario, si ravvisa una piena consapevolezza dell'entità del problema: "*Incalzanti sviluppi tecnologici hanno allontanato le frontiere della protezione dei dati personali. La portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso: la tecnologia attuale consente alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività e, sempre più spesso, gli stessi privati rendono pubbliche sulla rete mondiale informazioni personali che li riguardano. Le nuove tecnologie non hanno trasformato solo l'economia ma anche le relazioni sociali*".
D'ora in avanti, si dovrà vedere se gli strumenti giuridici adottandi saranno all'altezza della serietà delle premesse.

Il nodo della territorialità del trattamento ai tempi del *cloud*: le *big co.* statunitensi alla conquista del mercato europeo dei dati

La questione della territorialità, all'interno dell'annoso dibattito circa l'applicazione delle regole del diritto classico nelle controversie aventi ad oggetto la rete, riveste senza dubbio un'importanza centrale[15] recepita anche dal legislatore europeo: "*…i dati personali sono trasferiti attraverso le frontiere nazionali, sia interne che esterne, ad un ritmo sempre crescente…*"[16].

La presa di coscienza del legislatore rispetto alla natura sempre più volatile del dato personale, comporta una situazione necessitante la ricerca di accordi ed intese anche con paesi extra europei.

Si guardi, ancora, a quanto stabilito dal regolamento al considerando n. 20), in cui si sottolinea come i pericoli insiti nel trattamento operato da soggetti ubicati in altre parti del globo, spingano verso l'affermazione di un principio di extra-territorialità dell'applicazione della normativa.

Il legislatore europeo, sul piano dei principi ispiratori di un dettato normativo direttamente applicabile in maniera uniforme e cogente all'interno dei paesi membri dell'Unione Europea, si preoccupa, pertanto, che i diritti dei cittadini

[15] Già nel 1996, due autori come Johnson e Post, in "*Law and Borders*", sostenevano come*: "Il cyberspazio rende indeterminata la relazione tra le attività giuridicamente rilevanti svolte sulla rete e la localizzazione fisica. L'avvento della rete globale sta distruggendo il legame tra la localizzazione geografica e: 1)il potere dei governi locali di affermare il controllo sul comportamento tenuto sulla rete; 2) gli effetti del comportamento tenuto sulla rete sugli individui e sulle cose; 3) la legittimazione degli sforzi del potere territorialmente sovrano di rendere effettive regole applicabili a un fenomeno globale; 4) la possibilità della localizzazione fisica di rendere palesi le regole applicabili."* (trad. di Giovanni Pascuzzi in "Il diritto dell'era digitale", pag. 186, ed. 2002).

[16] Si aggiunge anche come: *"…esistono difficoltà pratiche nell'attuare efficacemente la normativa in materia di protezione dei dati e occorre stabilire una cooperazione tra gli Stati membri e le autorità nazionali a livello di Unione, per garantire uniformità nell'applicazione del diritto dell'UE. Infine, l'Unione si trova nella posizione migliore per garantire in maniera efficace e coerente lo stesso livello di protezione alle persone fisiche i cui dati personali siano trasferiti verso paesi terzi; – gli Stati membri non sono in grado da soli di risolvere i problemi posti dalla situazione attuale, in particolare dalla frammentazione delle legislazioni nazionali. Conseguentemente esiste la precisa esigenza di istituire un quadro armonizzato e coerente che consenta un agevole trasferimento transfrontaliero di dati personali all'interno dell'Unione europea e che garantisca nel contempo un'effettiva tutela di tutte le persone fisiche nell'intero territorio dell'UE;– le proposte legislative dell'UE risulteranno più efficaci rispetto ad analoghi provvedimenti adottati dai singoli Stati membri, a motivo della natura e della dimensione dei problemi che non sono confinati a uno o più Stati membri".*

europei siano rispettati anche al di fuori dei confini politici dell'Unione, per quanto tali affermazioni devono pur essere valutate alla luce delle legislazioni dei paesi extraeuropei, spostandosi, dunque, da un piano di diritto comunitario ad un piano di diritto internazionale.
La ricerca di intese sul piano internazionale è considerata un elemento da perseguire anche sul piano formale, come sottolinea l'art. 45 della bozza di regolamento (che prevede lo sviluppo di meccanismi di cooperazione internazionale per la protezione dei dati personali tra la Commissione e le autorità di controllo di paesi terzi, in particolare quelli che si ritiene offrano un adeguato livello di protezione).
Il regolamento comunitario, nel frattempo, cerca di porre rimedio alla disomogenea applicazione del diritto rispetto a trattamenti di dati tra paesi membri, creando, in quest'ottica, una scala di valori e principi unitari, così come nozioni, definizioni e procedure unitarie.
Innanzitutto, la bozza di regolamento all'art. 3 delinea il primo criterio di applicazione della normativa sotto il profilo territoriale, considerando soggetto alla disciplina del regolamento qualsiasi trattamento "*effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione* ***whether the processing takes place in the Union or not***".
Prima che intervenisse la modifica ad opera del Parlamento Europeo, poteva avere un senso chiedersi cosa dovesse intendersi per "stabilimento"[17].
Difatti, la proposta di regolamento offre soltanto la definizione di stabilimento principale, identificandolo come quel luogo di stabilimento, all'interno dell'Unione Europea, dove sono prese le principali decisioni sulle finalità, le condizioni e i mezzi del trattamento.
A contrario, sembra potersi identificare lo stabilimento come qualsiasi luogo in cui sono prese le decisioni "secondarie" in materia di dati, subordinate alle decisioni principali, quest'ultime adottate, appunto, presso lo stabilimento principale, e quindi focalizzando l'identificazione dello stabilimento in quel luogo in cui ogni soggetto svolga una determinata attività, seppur non principale rispetto all'attività intrapresa, ma comunque inerente un trattamento di dati personali.
Già da tale distinzione si intuisce come lo stabilimento principale nell'ottica

[17] Per quanto riguarda il concetto di responsabile del trattamento, l'art. 4, lo definisce come *"la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi del trattamento sono determinati dal diritto dell'Unione o dal diritto di uno Stato membro, il responsabile del trattamento o i criteri specifici applicabili alla sua nomina possono essere designati dal diritto dell'Unione o dal diritto dello Stato membro".* Come vedremo infra (cap. 6) soltanto la persona fisica che agisca individualmente, e per fini che esulano da scopi di lucro, non è considerato soggetto alla disciplina del regolamento, anche se è considerato pur sempre responsabile del trattamento posto in essere qualora ponga in essere una serie di operazioni ulteriori.

dell'applicazione della normativa in materia di protezione di dati personali, potrebbe non coincidere con lo stabilimento dove il soggetto svolga l'attività principale che caratterizza il suo business o la sua azione o scopo sociale.
L'impostazione del legislatore comunitario deve far riflettere, allora, se si considera che la normativa ad oggi in vigore, e che trova le sue radici nella direttiva 95/46/C.E., riteneva come la nozione di stabilimento dovesse coincidere proprio con quella in cui il responsabile (titolare) del trattamento esercitasse effettivamente e realmente l'attività economica principale.
In sostanza si sarebbe compiuto un ribaltamento dell'impostazione che lega l'applicabilità della normativa sui dati personali all'attività del soggetto responsabile del trattamento, all'applicabilità della normativa focalizzando l'attenzione sui dati stessi.
Se prima la nozione di stabilimento, come delineata dalle disposizioni interne sulla scia di quella comunitaria, doveva rileggersi in base alle pronunce della corte di Giustizia delle Comunità Europee, con la nuova normativa sarà possibile individuare due differenti tipologie dello stesso concetto di stabilimento.
La definizione utilizzata dal legislatore nella nuova bozza di regolamento sembrerebbe onnicomprensiva rispetto a soggetti che operano all'interno dell'Unione Europea, sia che il trattamento sia effettuato all'interno dei confini dell'Unione, sia all'esterno.
Sotto tale profilo, si potrebbe ricomprendere il trattamento effettuato da soggetti che agiscano in qualità di responsabili o anche solo di incaricati, che abbiano una sede o una succursale fisica all'interno dell'Unione[18].
Quando invece vi siano dei trattamenti automatizzati posti in essere da macchine comandate da soggetti situati, *rectius*, stabiliti in paesi extraeuropei, come ad esempio se in un paese comunitario si trovassero dei *server* che operano effettivamente il processo dei dati, sembrerebbe sempre l'art. 3, c. 1, a dover trovare applicazione.
La presente fattispecie riguarderebbe casi in cui le macchine processanti il dato si trovano fisicamente nei confini dell'Unione Europea, ed interesserebbe sia fenomeni di *input* posti in essere da soggetti fisicamente stabiliti altrove, ma anche fenomeni di c.d. intelligenze artificiali, in cui le macchine pongono in essere un trattamento sulla base di processi euristici in cui solo l'aspetto di programmazione e linguaggio conoscitivo è offerto dalla persona fisica, oppure anche da altri tipi di intelligenza.
E ciò in quanto il trattamento sarebbe comunque posto in essere "nell'ambito" di uno stabilimento presente sul territorio dell'Unione.

[18] Alla luce della presente opera ci si riferirà al responsabile del trattamento come nuova figura che racchiude ed unifica le due differenti figure previste dal D.Lgs. n. 196/2003, ovvero il titolare ed il responsabile del trattamento.

Tale espressione presenta sicuramente dei risvolti problematici: come può definirsi l'ambito di uno stabilimento? Cosa deve intendersi per ambito?
La versione in lingua inglese della bozza di regolamento utilizza l'espressione "*... in the context of the activities of a establishlment of a controller...*".
Poniamo che un responsabile con sede principale al di fuori dei confini dell'Unione Europea, ma con una sede anche all'interno dell'UE, affermi che le decisioni principali in materia di trattamento sono prese dalla sede all'estero.
In tale caso, è probabile che non possa applicarsi la normativa comunitaria, almeno sotto il profilo dell'art. 3, c. 1[19].
Poniamo, invece, il caso in cui il responsabile del trattamento non abbia alcuno stabilimento nell'Unione Europea così come l'incaricato del trattamento, ed altresì che non vi siano processori automatici di dati presenti fisicamente all'interno dei confini fisici dell'Unione Europea.
In tale fattispecie è l'art. 3, c. 2 a coprire la lacuna normativa.
Difatti, si considererà applicabile il regolamento comunitario anche a quei trattamenti di dati personali "*...nell'Unione effettuato da un responsabile* ***or a processor*** *del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti residenti nell'Unione* ***irrespective of whether a payment of the data subject is required****, oppure b) il controllo* ***of such data subjects***" (art. 7, c. 2).
Tale enunciato non sembrerebbe iscriversi nel solco del fenomeno della profilazione, intesa come analisi del comportamento della persona ai fini dell'ottimizzazione del soddisfacimento di gusti personali, basato unicamente su un trattamento automatizzato (disciplinato appositamente dall'art. 20 della bozza di regolamento), quanto piuttosto a ciò che caratterizza lo stesso fine ultimo del trattamento di *data mining*.

[19] Volgendo uno sguardo alle pronunce della giurisprudenza di merito, si registra una pronuncia importante che affronta varie questioni legate sia al D.Lgs. n. 70/2003 (di applicazione della dir. 31/2000/C.E. relativa a taluni aspetti giuridici dei servizi della società dell'informazione) sia al D.Lgs. n. 196/2003. Il riferimento è alla sentenza della Corte di Appello di Milano, sentenza n. 8611/2012, sul caso cd. *Google-Vividown*, relativa alla pubblicazione su Google Video di un *file* video contenente immagini altamente lesive della dignità personale di un ragazzo down, in cui diversi coetanei e compagni di scuola si divertono riprendendo con un telefono cellulare le vessazioni compiute ai danni del ragazzo disabile. Google Inc, rispetto al reato *ex* art. 167 D.Lgs. n. 196/2003, aveva sostenuto la non applicabilità della normativa sul presupposto che era Google Inc., con sede in USA a prendere decisioni in materia di dati personali, e non invece Google Italy srl. Rispetto a tale questione, la Corte di Appello senza entrare direttamente nel merito, ha ritenuto che, seppur il luogo di stabilimento rilevante non potesse essere rilevato in Google Italy srl, il Codice in materia di trattamento di dati personali dovesse comunque trovare applicazione sul disposto dell'art. 5, c. 2, che menziona "*l'utilizzo di strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo al fine di transito nel territorio dell'Unione Europea*". Ed ancora, riprendendo quanto sostenuto dal Gruppo art. 29 dei Garanti Europei, il Collegio milanese ha affermato che "nonostante il centro direzionale di Google si trovi negli Stati Uniti, Google ha l'obbligo legale di attenersi alle normative europee , ed in particolare alle normative sulla *privacy*, dato che i servizi di Google vengono forniti a cittadini europei e che svolge le attività di trattamento dati in Europa", anche se tale argomento è stato appunto alla base del comma secondo della nuova bozza di regolamento tutt'ora in fase di approvazione.

L'ultimo comma dell'art. 3, infine, ricomprende all'interno dell'applicazione del regolamento anche i luoghi in cui il diritto nazionale di uno Stato membro dell'Unione esplica i suoi effetti cogenti[20].
Sino ad ora si è offerta una panoramica circa le principali norme relative all'applicazione territoriale del presente regolamento.
Sotto tale aspetto, quindi, si concentra quello che è considerato il vero limite del diritto rispetto alla presente era digitale, ovvero il dover disciplinare fenomeni spesso d'inconsistenza materiale, laddove il fulcro della situazione giuridica non è rappresentato da componenti di facile, così come di fisica, rilevabilità.
Ciò nonostante, la caratteristica classica della statalizzazione del diritto, prova faticosamente ad arginare le falle dettate dalla smaterializzazione del dato e del relativo trattamento.
Come già anticipato, però, tale tendenza accentratrice del diritto statuale (ed ora comunitario) si scontra con la realtà degli operatori materiali che effettuano trattamenti di dati, i quali sono spesso sottoposti a legislazioni differenti e forse meno rispettose dei diritti fondamentali della persona, come invece avviene per l'Unione Europea.
Le grandi società situate nei paesi statunitensi dovrebbero potenzialmente essere sottoposte alla normativa comunitaria, ma logiche di puro carattere politico si scontrano con le logiche del mercato, così da determinare un quadro decisamente precario.
Il Garante per la Protezione dei Dati Personali italiano ha recentemente sottolineato come "*miliardi di informazioni vengono raccolte in tutto il mondo, analizzate attraverso la rete fino ad arrivare a dei server che sono sparsi ovunque e il cui pieno controllo è nelle mani sostanzialmente di un piccolo oligopolio che le gestisce e che ha un potere enormi*"[21].
Nel corso dell'intervista, il Garante si sofferma sui temi più rilevanti nel dibattito internazionale, dai *big data* al noto caso *Prism*[22], sostenendo come "*i grandi provider americani hanno un regime di tutela dei dati personali assolutamente più basso rispetto a quello europeo e questo produce uno svantaggio competitivo per cui le imprese del Vecchio Continente non riescono a concorrere...*".
I timori espressi dal legislatore europeo sono presenti e richiamati nelle parole del Garante nazionale.

---

[20] *"Il presente regolamento si applica al trattamento dei dati personali effettuato da un responsabile del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto nazionale di uno Stato membro in virtù del diritto internazionale pubblico".*
[21] Tali affermazioni sono state rilasciate nell'intervista del 29 agosto 2013 all'Huffington Post da Antonello Soro, attuale Presidente del Garante per la Protezione dei Dati Personali.
[22] Il riferimento è allo scandalo di dimensioni internazionali che ha coinvolto la *National Security Agency* statunitense, e indirettamente lo stesso governo degli Stati Uniti, a seguito delle rivelazioni di Edward Snowden, ex analista di dati della *Central Intelligence of America*, in cui lo stesso Presidente USA ha ammesso che l'Agenzia ha violato determinate procedure di intercettazioni di dati e metadati relativi a cittadini americani e non.

In questo quadro, al di là delle affermazioni di principio, la realtà dei trattamenti si scontra con la diversa, e forse più bassa, attenzione al diritto alla *privacy*, alla riservatezza, nonché alla dignità personale di altri paesi, come in questo caso gli Stati Uniti, paese in cui sono concentrati il maggior numero di operatori che compiono operazioni rilevanti in rete, sia sotto il profilo del numero della quantità che sotto il profilo della qualità delle informazioni[23].
Harper Reed, uno degli elementi di punta dello staff della campagna presidenziale del neo eletto Presidente degli USA, Barack Obama, ha affermato che "*esiste un problema di trasparenza legato al data mining...*", spostando però l'attenzione sul maggior numero di rischi per la *privacy* derivato dall'utilizzo dei dati da parte dei grandi operatori che offrono servizi di *social network*, rispetto ad operatori che si limitano ad un uso della rete nell'ottica di trattamenti di *data mining*[24].
L'aspetto del fenomeno territoriale è, quindi, determinante nell'approccio critico ad una prospettiva di analisi giuridica del fenomeno, anche se la consapevolezza della territorialità dei fenomeni connessi all'utilizzo della rete deve ricondurre ad un minor ottimismo nell'ottica di una disciplina efficace per il contrasto a trattamenti di natura illecita, o comunque contrari ad un generale principio di correttezza.
La realtà computazionale odierna, in cui vi sono grandi *data center* in cui sono fisicamente racchiusi centinaia di *server* che elaborano informazioni sparse nelle più differenti zone del pianeta, oppure intelligenze artificiali in grado di svolgere autonomamente operazioni aritmetiche sui dati per poi trasferirli altrove, è la realtà in cui una normativa comunitaria che intenda imporsi con i caratteri della cogenza, della effettività ed efficacia, deve e dovrà confrontarsi in un futuro neanche più così prossimo.
Anche nell'ottica di sanare il divario di forza – economica, ma anche politica – che deriva dalle capacità predittive dall'analisi dei *big data*, il legislatore europeo deve essere stimolato ad adottare delle contromisure, non solo tecnologiche, ma anche e prima di tutto giuridiche, per ottenere il rispetto, da parte degli operatori non stabiliti nell'Unione, dei principi stabiliti dal futuro regolamento comunitario in tema di trattamento di dati personali.

---

[23] Un'interessante trattazione circa l'analisi dei *big data* è offerta da Alessandro Mantelero, *"Big data: i rischi della concentrazione del potere informatico digitale e gli strumenti di controllo",* Diritto dell'informatica, pagg. da 125 a 134, in cui tra l'altro si sottolinea come "*L'analogia fra l'epoca del main frame e quella attuale del cloud computing e dei big data è significativa, poiché nuovamente ...le grandi risorse informatiche si concentrano in mano a pochi soggetti e risultano anche fisicamente aggregate in enormi data center"*, volendo con ciò alludere al potere maggiormente nelle mani delle *big company* statunitensi, definite veri e propri "signori dei dati", il cui vantaggio nell'elaborazione consente di sfruttare appieno le potenzialità offerte dall'analisi dei dati.
[24] Dall'intervista rilasciata a Wired US, tradotta e riportata su Wired Italia, p. 69, Febbraio 2013.

PARTE TERZA

I principi applicabili al trattamento di *data mining*

"*Il diritto alla protezione dei dati personali è sancito dall'articolo 8 della Carta, dall'articolo 16 del TFUE e dall'articolo 8 della convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU)*": così la Relazione d'apertura alla proposta di regolamento inquadra fin da subito il contesto in cui è valorizzato il dato personale, *rectius*, l'interesse alla protezione del dato nei confronti della varie ipotesi di trattamento, a cui si aggiunge il considerando n. 1) di apertura della proposta di regolamento[25].

Subito dopo, però, si precisa che "*il diritto alla protezione dei dati personali non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale*", sulla scorta delle elaborazioni giurisprudenziali della corte di Giustizia Europea; ma anche che la protezione dei dati è "*strettamente legata al rispetto della vita privata e familiare*", all'interno di un quadro in cui l'Unione Europea intende conferire rilevanza primaria ai diritti e alle libertà fondamentali delle persone fisiche.

Nel solco della migliore dottrina europea, quindi, il legislatore comunitario conferma il valore di diritto primario, fondamentale, del diritto alla riservatezza, alla *privacy*, o quanto meno al rispetto della sfera d'intimità che ogni persona fisica ha il diritto di avere, seppur nell'ambito della sua funzione sociale.

Tale sottolineatura, soprattutto agli occhi del giurista nostrano, ricorda le considerazioni che l'art. 41 Costituzione Italiana riserva al concetto di iniziativa economica privata (piuttosto che alla funzione sociale della proprietà privata), la quale è libera, ma non può svolgersi in contrasto con l'utilità sociale od in modo da recare danno alla sicurezza, alla libertà, e alla dignità umana.

[25] Il considerando n. 1) esordisce difatti ritenendo che *"La tutela delle persone fisiche con riguardo al trattamento dei dati personali è un diritto fondamentale"*. Anche il Considerando n. 2, con espressione molto forte, sottolinea come *"Il trattamento dei dati personali è al servizio dell'uomo; i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali devono rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato..."*

Con tale affermazione, il legislatore europeo, che si appresta ad emanare un regolamento unitario all'interno dei confini dell'UE di grande impatto e rilevanza in tutti i campi ed i settori delle attività conosciute, dimostra di essere consapevole dell'esistenza di un interesse contrapposto nel trattamento dei dati, il quale rientra a pieno titolo in quel tipo di operazioni a cui l'Unione Europea deve attribuire importanza, sia per incentivare la fiducia nell'economia digitale, sia per ottimizzare i rapporti fra Stato e cittadini nell'ottica di *best practice* in materia di *e-government*.
L'atteggiamento del legislatore, teso a proteggere i diritti fondamentali dell'individuo rispetto a propri dati personali, non contrasta, dunque, con un interesse verso la libera iniziativa economica e le sue forme di sviluppo nell'era digitale.
In quest'ottica, nel considerando n. 24, si sottolinea come: "*When using identifiers provided by devices, applications, tools and protocols, such as Internet Protocol addresses, cookie identifiers and Radio Frequency Identification tags, this Regulation should be applicable to processing involving such data, unless those identifiers do not relate to an identified or identifiable natural person*".
Il legislatore comunitario, in questo considerando, privo di per sé di efficacia normativa, si è spinto addirittura oltre, arrivando a sostenere che la tracciabilità delle operazioni compiute in rete dal singolo, sarà meritevole di attenzione da parte della normativa sulla protezione dei dati, solo e soltanto se l'insieme delle operazioni porterà a ricondurre tali tracce ad un univoco soggetto.
Tale inciso agevola senza dubbio i soggetti che intendano utilizzare i dati dei singoli per i loro scopi, consentendo un margine di manovra rispetto al trattamento di tali dati, al di fuori dei limiti del nuovo regolamento, anche se pare di difficile interpretazione.
Gli *identifiers* menzionati nel considerando si caratterizzano proprio per essere essenzialmente volti all'identificazione del soggetto, almeno in via di potenziale identificabilità (ma la questione dell'anonimizzazione dei dati si affronterà più avanti).
Il legislatore, più avanti richiama, in maniera sintetica, i diritti maggiormente rilevanti nella struttura della proposta di regolamento.[26]
L'importanza dei dati personali rispetto alle prime dissertazioni d'ambito giuridico del secolo scorso, in cui il potere computazionale del dato non può essere

[26] Così il par. 3.3 sulla *"Sintesi degli aspetti inerenti ai diritti fondamentali"*: *"La Carta sancisce altri diritti fondamentali, potenzialmente interessati: libertà di espressione (articolo 11); libertà d'impresa (articolo 16); il diritto di proprietà e, in particolare, la tutela della proprietà intellettuale (articolo 17, paragrafo 2); il divieto di qualsiasi forma di discriminazione fondata, tra l'altro, sulla razza, l'origine etnica, le caratteristiche genetiche, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, la disabilità, o l'orientamento sessuale (articolo 21); i diritti del minore (articolo 24); il diritto a un elevato livello di protezione sanitaria (articolo 35); il diritto d'accesso ai documenti (articolo 42); il diritto a un ricorso effettivo e a un giudice imparziale (articolo 47)".*

paragonato a quello relativo del periodo odierno, nonché futuro, è sintetizzata anche da un breve passo del considerando n. 67), in cui, a proposito dell'innovazione relativa all'obbligo di notifica di eventuali *breach* all'interno dei *database* interni propri del responsabile del trattamento, si avverte che "*Una violazione di dati personali può, se non affrontata in modo adeguato e tempestivo, provocare un grave danno economico e sociale all'interessato, tra cui l'usurpazione dell'identità*".
Il quadro offerto dal legislatore si caratterizza, in sostanza, per un livello di attenzione molto forte, sul piano dei valori, per quanto riguarda il diritto alla protezione dei dati personali, considerandone il trattamento come un aspetto essenziale che dovrà svolgersi nell'ambito dei limiti, delle regole e dei principi dettati a garanzia dell'interessato, stanti i grandi rischi connessi ad un illegittimo trattamento, se non proprio del responsabile, anche posto in essere da terzi.
L'*incipit* dell'art. 5, recita che i dati dovranno (da notare l'utilizzo di *shall*, meno duro rispetto al *must* della precedente formulazione) essere trattati "*in modo lecito, equo e trasparente nei confronti dell'interessato*".
Il principio di liceità, primo e più importante tra i principi applicabili al trattamento (su cui la dottrina più rilevante in materia si è espressa con orientamenti anche molto distanti fra loro), era già presente nella direttiva n. 46/1995 C.E. ed è ora richiamato[27].
A tali basilari principi sono ora aggiunti altri importanti corollari del trattamento, ovvero il principio di trasparenza, la precisazione del principio di minimizzazione dei dati e l'introduzione di una responsabilità generale del responsabile del trattamento, mentre si ribadiscono altri concetti già noti come il principio di necessità e proporzionalità, oppure il principio di finalità.
L'aspetto relativo alla trasparenza è ciò che maggiormente colpisce, se analizzato alla luce delle clausole generali con cui giuristi ed interpreti si confrontano quotidianamente.
Tale concetto si pone sulla scia delle rinnovate spinte che emergono dalla società civile, che costituiscono l'*humus* del movimento teso alla richiesta di trasparenza amministrativa e alla diffusione del concetto di *open data*.
Nell'ottica del trattamento di dati personali, il principio di trasparenza potrebbe

[27] In dottrina si è molto discusso circa i confini di questo fondamentale principio del trattamento, vd. ad esempio, Fabio Bravo e Jury Monducci, op. cit. pagg. da 35 a 119, sottolineano come "*...Il concetto di liceità … non va apprezzato come mera conformità al precetto giuridico, poiché altrimenti si sovrapporrebbe al diverso concetto di "legalità", ma va rilevato nel suo duplice aspetto di conformità al vincolo giuridico e di rispetto dell'ordinamento protetto dall'ordinamento"* (pag. 39); Fabrizio Piraino, invece, in *"Libera Circolazione e Protezione dei Dati Personali"*, op cit., pagg. da 743 a 914, riassume le varie posizioni tese ad attribuire, da un lato (Rodotà, Alpa, Ferrari, Busnelli, Navarretta) una bivalenza lessicale del termine, per cui la liceità andrebbe identificata con il suo opposto di illiceità come trasgressione di una norma che sanziona *a priori* un divieto, e in senso più ampio come realizzazione di una condotta *non iure* e quindi contraria alla clausola generale di buona fede e correttezza; mentre dall'altro lato (Iamiceli, Romano, Frosini, Carresi, Betti, Barba, Roppo) si preferisce identificare il concetto di liceità con una categoria unitaria che ricomprenda le nozioni di correttezza e di finalità, e dunque come rispetto dei limiti posti dall'ordinamento alla liberi esplicazione dell'autonomia degli individui.

porsi, ad avviso dello scrivente, come una specificazione della clausola generale di buona fede e correttezza, e dunque come requisito ulteriore che il soggetto titolare del trattamento dovrà soddisfare oltre ad essere già connotato da liceità, necessità e proporzionalità rispetto agli scopi da raggiungere per il tempo strettamente necessario.
La trasparenza, sotto tale aspetto, si pone come vincolo più stringente e diretto nei confronti del responsabile, il quale non dovrà occultare all'interessato nessuna informazione di cui sia a conoscenza.
La violazione del principio di trasparenza, rispetto ad un trattamento che in linea generale si conforma ai canoni richiesti *ex lege*, potrebbe comportare, così come già discusso in dottrina circa la violazione del principio di correttezza, comunque ad esporsi ad un eventuale risarcimento del danno da illegittimo trattamento di dati personali, sulla scorta di quanto l'art. 15 D.Lgs. n. 196/2003 prevede in caso di violazione dell'art. 11 del medesimo decreto.
Maggiori difficoltà potrebbero aversi, invece, nel definire i confini dell'equità di cui all'art. 5, c. 1, lett. a) della bozza di regolamento, anche se la versione in lingua inglese della normativa emendata aiuta a fare un po' di chiarezza.
Sotto questo punto di vista, infatti, il legislatore ritiene che i dati personali dovranno essere trattati in modo lecito e trasparente, ma anche "*fairly*".
Si noti allora, che mentre la precedente dir. 46/95/C.E. disponeva che i dati personali fossero "*processed fairly and lawfully*", nella versione attuale sarebbe stato aggiunto soltanto il principio di trasparenza ("*...and in a trasparent manner...*").
Evidentemente, in sede di traduzione, allo stato attuale si è preferito tradurre il sostantivo "*fair*" con il termine "equo", anche se tale scelta desta più di qualche perplessità, soprattutto perché se è vero che il legislatore interno, in sede di attuazione della direttiva con il rinnovato D.Lgs. n. 196/2003, ha deciso di identificare quei concetti con i principi di liceità e correttezza (creando non poche fatiche agli interpreti), non si vede il motivo per cui debba introdursi il criterio della "equità", di difficile collocazione nell'ambito di un trattamento di dati personali.
Seguendo quest'ordine di idee, ad esempio, non si capisce se l'equità debba porsi in contrapposizione rispetto alle finalità del trattamento, andando, però, in quel caso a coincidere con lo stesso principio di finalità, oppure, diversamente, a collidere con il principio di proporzionalità; ciò senza considerare l'implicazione dell'istituto processuale dell'equità come scelta discrezionale del giudicante al di fuori delle norme di diritto, in quanto situazione sarebbe priva di senso alla luce della *ratio* del legislatore.
L'auspicio, sotto tale profilo, sarebbe quello di avere maggiore chiarezza in sede di traduzione del regolamento definitivamente approvato.

L'aspetto relativo all'anonimizzazione dei dati, di cui all'art. 5, c. 1, lett. e), assume rilevanza limitata, allorché i principi posti alla base del trattamento, come ad esempio il principio di necessità, già spingevano e spingono tutt'ora nella direzione di ritenere conforme a tale principio un trattamento in cui si utilizzino dati personali soltanto se strettamente necessario al raggiungimento di un determinato obiettivo, oppure che consenta l'identificazione solo se non sia possibile celare l'appartenenza dei dati ad un determinato soggetto.
Il legislatore comunitario, nella bozza di regolamento, però, si spinge oltre, elencando all'art. 6 le condizioni senza le quali un trattamento deve, altrimenti, considerarsi illecito[28].
Valutando sommariamente l'ampio raggio di principi tracciati dal legislatore ai fini di un corretto trattamento, soprattutto alla luce di analisi del trattamento di *data mining*, emerge anzi tutto un importante distinzione sul tipo di soggetto che svolge il trattamento, considerato che il regolamento comunitario intende trovare applicazione sia nei confronti dei pubblici poteri che nei confronti di soggetti privati.
Allorquando ci si riferisce ad un soggetto pubblico, sovviene l'art. 6, lett. e) a ricordare che il trattamento è lecito se "*è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento*".
Senza aver la pretesa di indagare gli scopi e le finalità dell'azione pubblica, sembra potersi intravedere in tale formulazione un'eccessiva vaghezza nei limiti.
Si potrebbe considerare lecito un trattamento di *data mining* posto in essere da un ente pubblico locale, come un Comune che scandaglia la rete alla ricerca di informazioni sulle abitudini dei propri cittadini? La risposta potrebbe essere positiva, probabilmente, se l'analisi del *sentyment* consentisse di ricercare in forma anonima elementi utili alla gestione del verde pubblico, magari per decidere su quali tipi di strutture concentrare un maggior numero di finanziamenti; ma al tempo stesso potrebbe sembrare poco lecito analizzare i *trend* delle lamentele nei confronti dell'amministrazione per concentrare determinati tipi di controlli da parte della polizia locale, in merito a determinate fattispecie di violazioni.

[28] *"...l'interessato ha manifestato il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali prese su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del responsabile del trattamento,* ***or in case of disclosure, by the third party to whom the data is disclosed, and which meet the reasonable expectations of the data subject based on his or her relationship with the controller*** *a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali. Ciò non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esercizio dei loro compiti".*

E, difatti, proprio lo stesso art. 6, c. 3, prevede che "*La base su cui si fonda il trattamento dati di cui al paragrafo 1, lettere c) ed e), deve essere prevista: a) dal diritto dell'Unione, o b) dalla legislazione dello Stato membro cui è soggetto il responsabile del trattamento. Il diritto dello Stato membro deve perseguire un obiettivo di interesse pubblico o essere necessario per proteggere i diritti e le libertà altrui, rispettare il contenuto essenziale del diritto alla protezione dei dati personali ed essere proporzionato all'obiettivo legittimo*".
L'importante principio espresso nel comma 3 riporta nella giusta direzione un trattamento posto in essere dal soggetto pubblico che, stando alla lettera e), rischiava di essere eccessivamente permissivo in termini di possibili obiettivi e finalità dell'azione pubblica, anche se la questione interpretativa resta aperta.
Ad ogni modo, da un'analisi preliminare delle condizioni di liceità di cui all'art. 6, il trattamento di *data mining* posto in essere da un privato non sembrerebbe soddisfare nessuno dei criteri elencati, né tanto meno il principio di trasparenza, vera novità della bozza di regolamento.
Mediante l'utilizzo di appositi *software*, infatti, è possibile raccogliere dati relativi ad un vasto numero di persone, senza che vi sia una legittimo consenso alla base (vd. infra sulla tematica del consenso), in quanto non vi è stata alla radice un'accettazione delle condizioni generali di contratto che permetta all'operatore privato di estrapolare dati sulla base del legittimo scambio dei consensi.
È pur vero, come recita l'art. 11, che "*Il responsabile del trattamento applica politiche **concise**, trasparenti, **clear** e facilmente accessibili con riguardo al trattamento dei dati personali e ai fini dell'esercizio dei diritti dell'interessato*", e che "*Il responsabile del trattamento fornisce all'interessato tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in forma intelligibile, con linguaggio semplice e chiaro...*", ma il vero problema del trattamento di *data mining* è che il singolo non è in grado di comprendere come e da chi è posto in essere il trattamento.
Prima di analizzare la liceità o meno, alla luce dei vari principi generali sopra elencati, nell'ambito dei rapporti fra responsabile (e/o incaricato) e interessato nel quadro di una manifestazione di volontà "libera" nell'accettazione di condividere i propri dati, sul piano dei principi ispiratori del trattamento in generale, se si guarda all'analisi predittiva dei *big data*, l'aspetto maggiormente preoccupante è costituito proprio dal carattere generalmente occulto delle operazioni compiute dagli addetti ai lavori.
Il legislatore, nella relazione d'apertura alla bozza di regolamento sottolinea come il principio di trasparenza consiste nell'obbligo per i responsabili del trattamento di "*fornire informazioni trasparenti, comprensibili e facilmente accessibili*", e addirittura si arriva a sostenere come il responsabile debba essere "*obbligato*

ad informare esplicitamente l'interessato sui legittimi interessi perseguiti, che deve documentare, e sul diritto di opporsi al trattamento dei dati".
La vera questione è che sul piano applicativo il singolo dovrebbe porsi risposte al quesito sul destino dei propri dati personali.
Considerato che la maggior parte dei soggetti che offrono servizi *on line* sono utilizzabili senza il pagamento di un corrispettivo per l'utilizzo, è implicito che il profitto ottenuto da tali soggetti nasca dal valore dei dati personali raccolti.
Ma la trasparenza non risulta pienamente realizzata in tal senso nel momento iniziale di accettazione delle condizioni contrattuali, così come durante l'esercizio dei diritti dell'interessato.
Sul piano dei valori, il vero nodo cruciale e critico nell'ambito del trattamento di *data mining* è costituito dalla mancanza di trasparenza che caratterizza tale procedura, per quanto i fini realmente perseguiti possano, *ex se*, essere ritenuti meritevoli di tutela da parte dell'ordinamento giuridico.

PARTE QUARTA

La questione centrale del consenso

Il consenso dell'interessato, almeno sul piano del diritto interno, è considerato il presupposto principale affinché un responsabile del trattamento possa compiere una serie di operazioni aventi ad oggetto dati personali, e torna ad assumere un ruolo centrale anche nella bozza di regolamento comunitario.
Come visto nel precedente paragrafo, in mancanza di un consenso esplicitato nelle modalità di cui all'art. 7 della proposta di regolamento, è lo stesso legislatore comunitario a dettare regole rigide ai fini di una valutazione di liceità del trattamento (ma sul punto vd. anche art. 6), in quanto tale disposizione chiarisce a quali condizioni il consenso deve ritenersi validamente espresso.
Il considerando n. 25), invece, elenca delle fattispecie specifiche, attinenti alla manifestazione del consenso *on line*, precisando sin dal principio le caratteristiche fondamentali che compongono tale istituto: esplicito, libero, specifico, informato.
Tali caratteristiche sono riportate nell'art. 4, n. 8, relativo alle "definizioni" dei vari termini del trattamento, in cui si menzionano le modalità di manifestazione di un consenso ritenuto idoneo a soddisfare le suddette caratteristiche, ovverosia mediante una *dichiarazione* o una *azione positiva inequivocabile.*
In dottrina, sulla scia delle speculazioni inerenti il concetto di manifestazione di volontà del privato, si sono affermate, nel corso degli anni, delle posizioni che hanno portato alla creazione di nuovi negozi giuridici sconosciuti al legislatore del 1942, come il *factoring* o il *franchising*, ad esempio, prendendo come riferimento legittimante e fondante l'art. 1322 c.c. che santifica l'autonomia privata nel rispetto della realizzazione di interessi meritevoli di tutela secondo l'ordinamento giuridico.
Forse anche a causa di tale atteggiamento teso all'allargamento dei confini dell'autonomia privata, nel D.Lgs. n. 196/2003 il consenso riveste un ruolo ancor maggiore rispetto alla direttiva n. 46/1995 C.E., pur costituendo solo una

tra le varie ipotesi di trattamento lecito[29].
Per tale motivo, la proposta di regolamento comunitario non parrebbe così rivoluzionaria, agli occhi del giurista nostrano, nell'ottica di un accresciuto valore del consenso.
Il legislatore europeo, con la presente proposta di regolamento, si spinge ulteriormente nel senso di accrescere l'importanza di tale istituto, anche se, guardando al caso specifico del trattamento di *data mining*, non rappresenta un elemento pienamente soddisfacente.
Vediamo, innanzi tutto, come il legislatore comunitario disciplina l'istituto del consenso:
art. 7 – Condizioni per il consenso
1. ***Where processing is based on consent****, l'onere di dimostrare che l'interessato ha espresso il consenso al trattamento dei suoi dati personali per scopi specifici incombe sul responsabile del trattamento.*
2. Se il consenso dell'interessato deve essere fornito nel contesto di una dichiarazione scritta che riguarda anche altre materie, l'obbligo di prestare il consenso deve essere presentato in forma distinguibile dalle altre materie. ***Provisions on the data subject's consent which are partly in violation of this Regulation are fully void****.*
3. ***Notwithstanding other legal grounds for processing****, l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.* ***It shall be as easy to withdraw consent as to give it. The data subject shall be informed by the controller if withdrawal of consent may result in the termination of the services provided or of the relationship with the controller****.*
4. ***Consent shall be purpose-limited and shall lose its validity when the purpose ceases to exist or as soon as the processing of personal data is no longer necessary for carrying out the purpose for which they were originally collected. The execution of a contract or the provision of a service shall not be made conditional on the consent to the processing of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1), point (b)****.*

[29] Sul punto, Comandé, in artt. 11, 12, in *"La tutela dei dati personali. Commentario alla legge 675/1996"*, Padova, Cedam, 1997, già commentava come *"[i]l requisito del consenso rappresenta l'espressione più compiuta di quella libertà positiva di controllare i dati riferiti alla propria persona ed usciti dalla propria sfera di riservatezza in cui si sostanzia la libertà informatica intesa come diritto di autotutela della propria identità informatica"*; Salvatore Mazzamuto, *"Libera Circolazione e Protezione di dati personali",* op.cit.*,* invece, riassume, nel capitolo dedicato al principio del consenso, le posizioni formatesi in dottrina circa la natura giuridica del consenso, da un lato considerato come vero e proprio atto di disposizione (Oppo), secondo cui il sostrato oggettivo di riferimento sarebbe caratterizzato da *"ogni negozio giuridico produttivo del trasferimento, della modificazione o dell'estinzione di una preesistente situazione giuridica patrimoniale"* (così aprendo la strada a concezioni di ripensamento del dato in funzione di sfruttabilità sul piano economico), e dall'altro lato come mero auto di autorizzazione (Messinetti, Fici-Pellecchia), posizione imperniata invece sul carattere oggettivamente non patrimoniale del dato personale.

Nei casi di trattamento di *data mining*, come detto, spesso si prescinde dal consenso dell'interessato.
Pertanto, un trattamento massivo di dati, compiuto su una serie indistinta di persone, difficilmente si baserà sull'acquisizione di un consenso libero, esplicito, informato e specifico.
Poniamo il caso in cui un soggetto sia partecipe di discussioni su differenti *forum* o *chat* inerenti i più vari argomenti.
Accettando le regole imposte dal gestore della piattaforma *on line* (sempre che vi siano), l'utente è consapevole che i contenuti espressi sono visibili ad un numero determinato di persone.
Il mero comportamento concludente del soggetto che accetta le regole (sociali? giuridiche?) delle pubbliche discussioni, potrebbe essere letto, in quest'ottica come un'azione positiva inequivocabile che i suoi dati siano oggetto di trattamento?
E quali dati possono essere utilizzati realmente?
Prima di suddividere l'operazione di trattamento a seconda della qualità del responsabile, è bene rimarcare che la mera disponibilità pubblica del dato in rete non può tradursi *a priori come* legittimità di un'analisi di altro tipo.
Ciò in quanto il dato personale, che è definito dall'art. 4 come "*qualsiasi informazione concernente l'interessato*", per il solo fatto di essere presente materialmente o immaterialmente, ma comunque disponibile, è pur sempre soggetto, anche nelle more dell'approvazione della proposta di regolamento comunitario, alla disciplina del trattamento dei dati personali in vigore.
La peculiarità delle attività materiali caratterizzanti il c.d. *Web 2.0* consta di un accrescimento della produzione di *user generated content*, tale che determinati operazioni di *data mining* possono arrivare ad analizzare informazioni, contenenti dati personali, che il singolo utente decide di rendere pubbliche agli altri utenti.
Anche in questo caso, l'utente che pubblica dei dati personali, nella maggior parte dei casi, ha accettato quelle regole poste a presidio dell'utilizzazione lecita della piattaforma *on line*, e quindi la mera disponibilità pubblica del dato non dovrebbe di per sé rendere legittima l'operazione di *data mining,* tornando dunque a riespandere i propri confini la disciplina generale in materia di trattamento di dati personali.
Al contrario, però, dovrebbero ravvisarsi gli estremi di un trattamento consentito, qualora la fattispecie dovesse sussumersi nel caso di cui all'art. 2, c. 2 lett. d), cioè il trattamento effettuato da una persona fisica senza finalità di lucro per l'esercizio di attività esclusivamente personali o domestiche.
Sotto il profilo del responsabile, la fattispecie di trattamento dovrebbe distingue-

re la situazione di un soggetto esterno che acquisisca un insieme di informazioni dalla massa indistinta degli utenti, da quella del gestore del sito, il quale riporta l'analisi della figura di intermediario di cui alla direttiva n. 31/2000 C.E..
Tra l'altro, non si deve dimenticare come l'art. 2 sottolinei come il regolamento non debba pregiudicare l'applicazione della direttiva 2000/31/C.E., "*in particolare le norme relative alla responsabilità dei prestatori intermediari di servizi di cui ai suoi articoli da 12 a 15*".
Con tale asserzione, il legislatore ha voluto sottolineare come il *provider* (in particolare quello che svolge attività di *caching* e di *hosting*), sarà sottoposto, oltre alle norme in materia di protezione di dati personali, anche alla responsabilità in qualità di prestatore di servizi tipica della direttiva di cui 2000/31/C.E..
Tale precisazione si impone allorquando si venga a creare una situazione di possibile conflitto di norme, deciso dal legislatore nel senso della autonomia tra le diverse discipline, dato che diverso può essere il tipo di lesione prodottasi.
Se si considerano le caratteristiche del consenso come disciplinato nella bozza di regolamento, un trattamento di *data mining* in tal senso operato da un soggetto esterno non si basa su un consenso esplicito, libero, informato e specifico.
Le peculiarità della diffusione di dati personali disponibili in rete, può allora trovare una diversa legittimazione nei confronti del singolo in maniera indiretta, giacché l'interessato, come presente nella maggior parte delle condizioni generali di contratto relative all'utilizzo di un servizio *on line*, accetta di prestare il proprio consenso anche alla diffusione dei propri dati a terzi.
In particolare, allorquando sia un soggetto esterno ad operare un massivo intervento sui dati, difficilmente si potrà ritenere legittimo il trattamento posto in essere, a meno che non sia autorizzato dal soggetto che ha recepito il consenso dell'interessato.
Anche perché il legittimo interesse di cui all'art. 6, lett. f) della proposta di regolamento, ai fini della effettuazione di un trattamento conforme a liceità, dovrebbe essere valutato di volta in volta sulla base dello specifico obiettivo da realizzare, soprattutto allorquando sia caratterizzato da un interesse economico ultimo (anche perché, vd. *infra*, il trattamento individuale senza scopo di lucro è tendenzialmente libero, e quindi non soggetto ai vincoli della normativa in materia).
Differente discorso potrebbe porsi per quei tipi di trattamento di *data mining* che realizzino scopi storici, scientifici o statistici (vd. ancora *infra*).
Dallo spiraglio lasciato aperto dall'ordinamento, parrebbero legittimamente posti in essere tutti i trattamenti di grandi moli di dati per soddisfare le più varie finalità riconducibili a motivi didattici, nelle tre differenti forme descritte.
Il potere concesso da tale peculiare finalità del trattamento, legittimerebbe una

ampia casistica di possibilità, e consentirebbe di porre in essere le più differenti ricerche e tecniche di *data mining*.
Per tale ragione dovrà essere molto peculiare l'analisi relativa al trattamento, spostandosi da un piano di valutazione sulla legittimità ad un piano di effettiva indagine concreta sulle reali finalità dello stesso.
Inoltre, si consideri che a seguito di un trattamento di *data mining*, nulla vieta che determinate informazioni siano fornite in qualche modo per scopi diversi ulteriori, per i quali invece è richiesto uno specifico consenso.
Per quanto riguarda invece il trattamento realizzato dal soggetto responsabile che abbia acquisito un consenso, inteso come accettazione delle condizioni generali di contratto, sia quando si accetti con apposito *click* sulla corrispondente casella relativa alla presa visione (ed accettazione) delle suddette previsioni, sia quando si abbia accettazione generica nel momento di *download* di una determinata *app* su dispositivi come *smartphone* o *tablet*, le considerazioni da fare devono distinguersi a seconda della necessità o meno del consenso.
Da un lato, difatti, si dovrà valutare i casi in cui il consenso espresso è valido come accettazione di tali condizioni, dall'altro lato i casi in cui tale consenso non è espresso, ma il trattamento deve considerarsi comunque lecito nell'ambito dell'esecuzione di un contratto.
Nel primo caso, al di là di aspetti relativi alla profilazione dell'individuo, in particolare da parte dei gestori di *social network*, per il momento basti rilevare la fragilità di tale tipo di consenso, che difficilmente potrà rivestire quelle caratteristiche delineate dalla bozza di regolamento[30].
Allorché l'utente possa prestare il proprio consenso all'utilizzo dei propri dati personali, spesso anche a favore di soggetti terzi, non possono ritenersi idonee, in particolare riguardo alle caratteristiche di specificità e corretta informazione, quelle clausole con cui si autorizza il responsabile a cedere informazioni che lo riguardano, ad un terzo, seppur celate sotto la panacea dell'anonimizzazione dei dati, oppure con l'esca dell'utilità nei confronti dell'interessato.
Il soggetto che aderisce alle condizioni generali di contratto predisposte da determinate piattaforme non ha alternative, quindi la sua posizione si pone tra l'alternativa di accettare *tout court* la cessione di informazioni che lo riguardano, oppure di non usufruire del servizio.
La situazione necessitante, in tale contesto, differisce invece da quella, ad esempio, di un professionista, per il quale il trattamento di determinati dati è essenziale per lo svolgimento dell'attività principale, conseguentemente se l'interessa-

[30] In dottrina si è manifestata l'insufficienza del mero requisito del consenso ai fini della liceità del trattamento, sottolineando, appunto, l'aspetto di consenso "costretto" rispetto all'avvalersi di determinati servizi o prestazioni (così commenta Giulia Laddaga, in *"Il Vademecum della Privacy"*, dossier del Il Sole 24 Ore, , anno XX, numero 6, luglio-agosto 2013, riprendendo quanto sostenuto da Comandé).

to richiede un determinato servizio, non sussistono alternative all'effettuazione o meno del trattamento di quei determinati dati.
Diverso, appunto, è il caso in cui la concessione a terzi di operare trattamenti di *data mining*, pur non intaccando l'esecuzione principale dell'obbligazione contrattuale, ovverosia la fornitura di un determinato servizio (*blog*, *chat*, giochi, *et cetera*), attiene, invece, ad una pura scelta lucrativa del responsabile del trattamento, gestore della piattaforma.
Sotto un secondo profilo, si consideri il caso in cui il consenso dell'interessato non è richiesto né dovuto, giacché è necessario per l'esecuzione di obblighi derivanti dal contratto, tanto da poterlo considerare, con una sorta di *fictio iuris*, implicitamente prestato[31].
La fattispecie *de quo* deve essere inquadrata in un contesto in cui il trattamento dei dati personali si considera come una naturale conseguenza dello svolgimento dell'obbligazione principale, come nel caso dell'avvocato che deve svolgere la propria attività difensiva, oppure del datore di lavoro rispetto ad alcuni aspetti previsti per legge, come ad esempio a fini fiscali per operare le dovute trattenute nei confronti del dipendente.
La ricerca di un margine di manovra per le situazioni di analisi massiva di dati, sembra condurre, pertanto, ad un vicolo cieco, a meno che l'oggetto del contratto non sia costituito proprio dalla cessione delle informazioni.
Altro aspetto innovativo riguarda l'onere probatorio rispetto alla manifestazione del consenso, che realizza un importante *favor* nei confronti dell'interessato.
Sotto questo aspetto, sarà il responsabile del trattamento a dover dimostrare che vi è stata l'espressione di volontà in tal senso, dal momento che dispone dei mezzi tecnologici idonei alla conservazione della dichiarazione o dell'azione attiva inequivocabile di manifestazione del consenso.
L'ultimo comma dell'art. 7, infine, è stato modificato interamente, considerata l'oscura formulazione precedente, secondo cui "*Il consenso non costituisce una base giuridica per il trattamento ove vi sia un notevole squilibrio tra la posizione dell'interessato e del responsabile del trattamento*".
Il problema, soprattutto nell'ambito del mondo digitale, consiste nel capire quando l'utente possa considerarsi in una posizione di squilibrio – notevole, evidente – nei confronti del *provider*, gestore di una piattaforma, di una servizio, *et cetera*.
La figura dell'interessato, considerata alla luce della normativa in tema di protezione di dati personali, lo colloca *a priori* in una posizione di inferiorità, tanto da assimilarlo quasi alla posizione del consumatore nei confronti del professionista.

[31] L'art. 6 lett. b), *"Il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali prese su richiesta dello stesso".*

Ma è pur vero che se si dovesse interpretare il concetto di squilibrio in tal senso, si svuoterebbe di significato ogni aspetto relativo ai presupposti di liceità del trattamento, nonché tutti gli obblighi ad esso relativi, dato che il singolo utente potrebbe sempre ricorrere a questo tipo di posizione d'inferiorità di partenza.
La nuova formulazione, invece, modifica totalmente il raggio d'azione, spostando l'attenzione sul limite costituito dallo scopo del trattamento rispetto al consenso, stabilendo, in maniera quasi pleonastica, che il consenso a compiere un determinato trattamento cessa al raggiungimento dello scopo o nel momento in cui tale scopo non è più raggiungibile, così riproponendo i principi generali di finalità, di necessità e di proporzionalità.

PARTE QUINTA

I diritti dell'interessato

Ai diritti dell'interessato è dedicato l'intero Capo III° della proposta di regolamento comunitario.
All'interno di tale capo sono racchiuse cinque importanti sezioni: sulla trasparenza e sulle modalità del trattamento, sull'informazione (o informativa) all'interessato e sull'accesso ai dati, sulla rettifica e sulla cancellazione dei dati personali (tra cui si registra l'innovazione data dall'introduzione del diritto all'oblio, poi sostituito dal mero diritto alla cancellazione), sul diritto di opposizione e profilazione (considerata come pratica adesso riconosciuta anche a livello normativo), e, infine, sulle limitazioni che Unione Europea e stati membri possono introdurre rispetto alla portata degli obblighi e dei diritti previsti dal regolamento.
La scelta del legislatore europeo in tale senso va nella direzione di attribuire grande risalto ai poteri dell'interessato che si pongono come veri e propri diritti a difesa del titolare del trattamento.
Nel presente ambito si registrano pertanto anche molti spunti interessanti nell'ottica del trattamento di *data mining*.
Partendo in ordine logico e cronologico nell'analisi delle varie fattispecie, nell'art. 11 si intravede una caratteristica importante e basilare del trattamento lecito di dati personali, nel suo aspetto speculare di diritto dell'interessato, ovvero il diritto alla trasparenza.
In quest'ottica, il responsabile del trattamento dovrà comunicare all'interessato "*...tutte le informazioni e le comunicazioni relative al trattamento dei dati personali in forma intelligibile, con linguaggio semplice e chiaro e adeguato...*".
Il diritto a ricevere tutte le informazioni, in forma chiara e comprensibile, in merito al destino dei propri dati, è, sul piano dei valori, di grande rilevanza circa i trattamenti di *data mining*, in quanto dovrebbe obbligare il responsabile che recepisce le informazioni a comunicare a quali entità esterne e per quali scopi possono essere ceduti i dati, quale tipologia di dati (sia sotto il profilo quantita-

tivo che qualitativo), oppure ancora per quanto tempo e quante volte possono essere ceduti, per quali scopi verranno trattati i dati, *et cetera*.
Nel campo dei *big data* non è dato conoscere *a priori* le potenzialità insite nei dati stessi, tanto che la combinazione di diversi *database* può portare a risultati che un primo analista non potrebbe neanche immaginare.
Secondo quest'ordine d'idee, e considerato che il consenso (al di là dei casi specifici in cui non è necessario ottenerlo) deve sempre espresso preventivamente o contestualmente rispetto al trattamento, si potrebbe concludere che quei dati non saranno utilizzabili per il trattamento ulteriore, oppure che il responsabile dovrà ottenere un consenso ulteriore.
L'art. 12 (sulla scorta anche del considerando n. 47), delinea quelle che saranno le modalità di esercizio dei diritti dell'interessato, le procedure, nonché i tempi di risposta ed un importante corollario è costituito dalla gratuità delle relative azioni difensive.
Altro aspetto degno di nota aggiunto alla bozza di regolamento era costituito dall'obbligo introdotto, a carico dei responsabili del trattamento, di predisporre delle modalità di esercizio dei diritti per via elettronica; la commissione del Parlamento Europeo che ha emendato il testo, invece, ha previsto tale procedura soltanto "*where possible*", svuotando di significato il precetto.
L'art. 14 della proposta di regolamento specifica il diritto di informativa, che nell'ottica dell'impianto normativo, ha sempre occupato un posto di rilievo, dato che in esso sono elencate tutte le informazioni che l'interessato ha il diritto di ricevere dal responsabile del trattamento, sempre in linea con una più corretta gestione del flusso informativo[32].
Ai fini della presente trattazione, si consideri in particolare quanto disposto dall'art. 14, lett. f): il responsabile del trattamento dovrà comunicare ed informare l'interessato, anche riguardo i "*destinatari o le categorie di destinatari dei dati personali*".
Quest'obbligo di comunicazione è parzialmente in linea con i migliori principi in tema di trattamento di dati personali, ma rischia di essere sminuito dall'utilizzo della congiunzione alternativa, che autorizza a ritenere le due possibilità di comunicazione sostanzialmente equiparate.
La necessità di massima trasparenza richiesta dal legislatore non sembra essere

[32] Altresì è il considerando n. 51) a stabilire i principi in merito alle informazioni che il responsabile ha l'obbligo di riferire all'interessato: *"Ogni persona deve avere il diritto di accedere ai dati raccolti che la riguardano e di esercitare tale diritto facilmente, per essere consapevole del trattamento e verificarne la liceità. Occorre pertanto che ogni interessato abbia il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità del trattamento, al periodo* ***estimated*** *di conservazione, ai destinatari, alla logica* ***general*** *che presiede al trattamento e alle possibili conseguenze. Tale diritto non deve ledere i diritti e le libertà altrui,* ***such as in relation to*** *il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, queste considerazioni non devono portare a negare all'interessato l'accesso a tutte le informazioni".* Piccoli correttivi sono stati apposti, rispetto al precedente testo, dal Parlamento Europeo.

rispettata allorché si consente al responsabile del trattamento di comunicare le "categorie" di destinatari dei dati personali.
Un approccio maggiormente attento alle necessità dell'analisi dei *big data*, piuttosto che alla tutela della *privacy*, sicuramente si pone favorevolmente rispetto ad una normativa di impatto minimo rispetto alle potenzialità del *data mining*. In realtà, tale critica sarebbe priva di fondamento.
La costruzione di un impianto normativo intorno al responsabile del trattamento, il quale deve rispettare tutta una serie di parametri per un trattamento lecito, proporzionato e necessario, mal si concilia con la possibilità concessa allo stesso di comunicare all'interessato a quali "categorie" di destinatari potranno essere comunicati i dati.
Il dato personale, ovvero quel dato che caratterizza e contribuisce a identificare una persona, in particolare nell'era digitale, è volatile, facilmente riproducibile ma al tempo stesso difficilmente controllabile.
Le società che offrono beni o servizi *on line*, sia le grandi società, sia le realtà minori, hanno a disposizione dei *database* che contengono una quantità di informazioni sempre più elevata e sempre più appetibile per qualsiasi soggetto, dall'ente pubblico che si occupa di ricerca fino alle aziende di marketing.
In linea di principio, un trattamento di *data mining* è un'operazione utile che consente dall'analisi di centinaia, migliaia o piuttosto milioni di dati, di giungere a conclusioni da cui il soggetto può trarre beneficio.
Per tali motivi, sarebbe preferibile, in un'ottica di trattamento "*in a trasparent manner*", obbligare il responsabile del trattamento a specificare in maniera chiara tutti quei soggetti a cui i dati sono o saranno conferiti, o almeno a cui possono essere conferiti.
Ad ogni modo, i nuovi emendamenti proposti dalla commissione del Parlamento Europeo si pongono in funzione di attenuare gli effetti derivanti dalla precedente formulazione.
In particolare la lettera ga), ha imposto, pur sempre "*where applicable*", di informare "*...about the existence of profiling, of measures based on profiling, and the envisaged effects of profiling on the data subject...*".
Se realmente tale obbligo fosse imposto al soggetto responsabile del trattamento, il principio di trasparenza sarebbe rispettato a pieno.
Il problema, invece, risiede nell'espressione *where applicable* che nell'attuale traduzione del testo inglese risulta come "appropriato"oppure come "possibile".
La differenza non è di poco conto, se si pensa che in un caso si lascerebbe al responsabile una valutazione soggettiva di opportunità, mentre nel secondo la valutazione potrebbe essere oggettiva nel senso di effettiva possibilità materiale di comunicare se vi sono in atto misure basate sulla profilazione.

Altro aspetto critico è costituito dal comma 4, art. 14, in base al quale "*Il responsabile del trattamento fornisce le informazioni di cui ai paragrafi 1, 2 e 3: a) al momento in cui i dati personali sono ottenuti dall'interessato,* ***or without undue delay where the above is not feasible****, oppure b) quando i dati personali non sono raccolti direttamente presso l'interessato, al momento della registrazione o entro un termine ragionevole dopo la raccolta, in considerazione delle specifiche circostanze in cui i dati vengono raccolti o altrimenti trattati,* ***or***, ***if a transfer to another recipient is envisaged, and at the latest at the time of the first transfer***, ***or***, ***if the data are to be used for communication with the data subject concerned, at the latest at the time of the first communication to that data subject***; ***or (bb) only on request where the data are processed by a small or micro enterprise which processes personal data only as an ancillary activity***".
In particolare, sempre considerando che il responsabile del trattamento potrebbe disporre dei dati, ma cederli (gratuitamente, anche se è molto più probabile a titolo oneroso) ad altri soggetti dotati di competenze o intenzioni di effettuare analisi predittive sugli stessi, il mero concedere la possibilità di comunicare tutte le informazioni di cui all'art. 14 par. 1, 2 e 3 "*at the latest at the time of the first transfer*", o comunque "*if the data are to be used for communication with the data subject concerned, at the latest at the time of the first communication to that data subject*", sembra esulare da ogni migliore *best practice* in materia.
Da un lato, la comunicazione entro un termine ragionevole dalla raccolta sembra voler disciplinare quelle situazioni in cui, per motivi di necessità ed urgenza, il responsabile non ha potuto comunicare preventivamente le informazioni *ex* art. 14.
In questi termini, la clausola generale potrebbe essere vista come un modo per non appesantire burocraticamente quelle situazioni (particolari e limitate) in cui non è possibile materialmente comunicare le informazioni su dette.
Dall'altro lato, invece, se è pur vero che l'interessato ha il diritto di conoscere, preventivamente rispetto alla manifestazione del consenso, tutte le informazioni necessarie a comprendere (anche in forma chiara ed intellegibile) quale sorte toccherà ai dati forniti al responsabile, *a fortiori* non si comprende come lo stesso possa essere edotto in merito alle informazioni fondamentali del trattamento dei suoi dati, soltanto nel momento stesso in cui sono forniti.
La versione originale della proposta di regolamento, prima dell'emendamento, utilizzava l'espressione *disclosure* invece di *transfer*.
Tale distinzione non è, ad avviso dello scrivente, di poco conto.
La *disclosure* può anche consistere in una mera operazione di rivelazione dei dati senza necessariamente che venga un passaggio tracciabile.
Al contrario, un trasferimento di dati personali, implica sempre un atto di di-

vulgazione dei dati stessi.
L'emendamento presentato dal Parlamento Europeo sembra voler decisamente venire incontro a metodi di passaggio di informazioni senza che venga informato l'interessato, forse in modo da non voler appesantire i compiti del responsabile, ma così pregiudicando i diritti dello stesso interessato.
Inoltre, di ancor maggiore interesse, sempre in questa direzione, risulta l'emendamento all'art. 14, c. 4, che ha introdotto la lettera (bb).
Il requisito dimensionale del responsabile diventa fondamentale per escludere che sia fornita *a priori* l'informativa, se non dietro apposita richiesta dell'interessato: tale beneficio riguarderebbe le imprese piccole (ad esempio, ditte individuali) quando il contatto con dati personali avvenga, è da immaginare, in maniera marginale.
Una corretta lettura di tale emendamento può allora portare a dover ritenere escluse dall'obbligo di informativa quelle realtà economiche in cui la comunicazione delle informazioni *ex* art. 14 appesantirebbe lo svolgimento dell'attività economica principale e dunque tale norma non interesserebbe un'operazione di *data mining*.
In generale, al di là del reale senso che il legislatore europeo abbia voluto conferire a tale norma, pare certo doversi affermare il principio che, di regola, il responsabile del trattamento dovrà comunicare finalità e modalità del trattamento, così come i diritti dell'interessato, le sue modalità di esercizio, e tutte le altre informazioni, preventivamente rispetto al recepimento del consenso.
Allo stesso modo, dovrà comunicare preventivamente e specificamente sia i destinatari (non probabili, ma identificati) sia per quali motivi i dati saranno comunicati a terzi.
Ciò, in quanto il principio di trasparenza impone che il responsabile non celi nulla di quanto è a sua conoscenza rispetto al trattamento di dati personali.
L'art. 15, invece, elenca e specifica tutti i diritti dell'interessato nei confronti del responsabile[33].
In maniera simile all'art. 14, tale disposizione conferma, specularmente all'obbligo di informativa per il responsabile, il diritto per l'interessato di richiedere quali siano i destinatari a cui i dati personali sono stati o saranno comunicati, inclusi i destinatari di paesi terzi.
Tale norma però, vista proprio la criticità dell'espressione "categorie di destinatari", a seguito dell'emendamento del Parlamento Europeo ha visto decurtata tale menzione, che però adesso, rimane presente all'art. 14.
Il paradosso creato dal legislatore (almeno in questa fase) consiste nell'aver cre-

[33] Anche il considerando n. 55, ora 51a, elenca alcuni tipi, poi ripresi dall'art. 15, di diritti legittimamente esercitabili dall'interessato, come il diritto all'ottenimento di una copia dei dati personali in formato elettronico.

ato un obbligo in capo al responsabile di comunicare obbligatoriamente le categorie di destinatari a cui i dati possono o saranno comunicati (*rectius*, trasferiti), ma non esiste un diritto speculare dell'interessato di conoscere quelle categorie, qualora sia omessa la comunicazione da parte del responsabile.
Ancora, una delle principali novità rispetto alla precedente direttiva, è rappresentata dall'introduzione a livello normativo del diritto alla cancellazione dei dati, che ha sostituito totalmente l'espressione del diritto all'oblio, eliminata dall'emendamento del Parlamento Europeo, che costituiva una delle più grandi innovazioni, almeno sul piano semantico, rispetto al precedente testo normativo[34].
Il tema del diritto all'oblio ("*the right to be forgotten*") nell'ottica della protezione dei dati personali, meriterebbe una trattazione specifica, data l'estrema importanza di riflettere sul concetto di "oblio", termine che rappresenta una situazione di irrecuperabilità del ricordo, di dimenticanza eterna, laddove invece il dato digitale (e personale) può sopravvivere in rete in eterno ed anche restare immodificato[35].
Nel caso del *data mining*, ad ogni modo, vi sono altri spunti interessanti nella bozza di regolamento che vale la pena analizzare.
L'interessato, *ex* art. 17, ha "*il diritto di ottenere dal responsabile del trattamento la cancellazione di dati personali che lo riguardano e la rinuncia a un'ulteriore diffusione di tali dati* ***and to obtain from third parties the erasure of any links to, or copy or replication of that data***, *se sussiste uno dei motivi seguenti: a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si fonda il trattamento, di cui all'articolo 6, paragrafo 1, lettera a), oppure il periodo di conservazione dei dati autorizzato è scaduto e non sussiste altro motivo legittimo per trattare i dati; c) l'interessato si oppone al trattamento di dati personali ai sensi dell'articolo 19;* ***(ca) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;*** *d)* ***the data has been unlawfully processed***".

[34] L'art. 16, invece, prevede la possibilità per l'interessato di richiedere la rettifica di dati inesatti o parziali.
[35] Secondo il precedente testo del considerando n. 53 *"Ogni persona deve avere il diritto di rettificare i dati personali che la riguardano e il "diritto all'oblio", se la conservazione di tali dati non è conforme al presente regolamento. In particolare, l'interessato deve avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è particolarmente rilevante se l'interessato ha dato il consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare questo tipo di dati personali, in particolare da Internet. Tuttavia, occorre consentire l'ulteriore conservazione dei dati qualora sia necessario per finalità storiche, statistiche e di ricerca scientifica, per motivi di interesse pubblico nel settore della sanità pubblica, per l'esercizio del diritto alla libertà di espressione, ove richiesto per legge o quando sia giustificata una limitazione del trattamento dei dati anziché una loro cancellazione"*. Tale considerando, adesso, vede sostituita l'espressione "diritto all'oblio" con quella di "diritto di cancellazione".

La norma generale offre diverse possibilità all'interessato per far valere i propri diritti, tanto da poter ritenere sufficientemente esaustivo l'elenco dei vari diritti. In particolare può vedersi di buon auspicio l'introduzione della lettera ca) da parte dell'emendamento della commissione *ad hoc* del Parlamento Europeo.
Maggiormente degno di rilievo, però, è il comma 2, secondo cui: "*Quando ha reso pubblici dati personali,* ***without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties***, ***without prejudice to Article 77*** *il responsabile del trattamento* ***shall inform the data subject, where possible, of the action taken by the relevant third parties***".
Restando inteso che il responsabile del trattamento è l'unico potenziale titolare del diritto alla cancellazione (o all'oblio), qualora i dati rimangano confinati all'interno dell'ambito di dominabilità del soggetto stesso, allorché il responsabile abbia fornito un insieme di dati ad un soggetto terzo, sarà lo stesso responsabile a doverlo poi informare sulla volontà dell'interessato di cancellare i propri dati.
La formulazione attuale, alla luce dell'emendata disposizione, vede il responsabile maggiormente costretto a dover prendere tutte le misure ragionevoli per evitare un pregiudizio dell'interessato, tanto che il comma 3 prevede l'obbligo di portare avanti la cancellazione dei dati "senza ritardo", e tale onere è imposto al terzo soltanto "*where applicable*", quindi laddove appropriato o possibile, secondo l'interpretazione autentica che verrà fornita.
In quest'ottica, qualora il terzo non volesse adeguarsi alla nuova volontà dell'interessato, il responsabile del trattamento non subirebbe alcuna conseguenza: tale affermazione pare conforme ai più elementari principi in tema di responsabilità civile, intesa come attribuibilità e rimproverabilità della condotta posta in essere, dato che materialmente il responsabile non avrebbe accesso alle strutture *hardware* e *software* del terzo per operare operazioni di cancellazione permanente del dato.
L'art. 17 prevede anche degli importanti casi in cui il responsabile può opporre all'interessato un diritto di pari valore rispetto a quello teso alla cancellazione dei dati.
I casi previsti dalla proposta di regolamento si identificano nel diritto alla libertà di espressione (vd. art. 80 della proposta di regolamento), nei motivi di interesse pubblico nel settore della sanità pubblica (art. 81), per finalità storiche, statistiche e di ricerca scientifica (art. 83, nonché vd. *infra*), nella necessità di adempiere a un obbligo legale di conservazione di dati personali previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il responsabile del trattamento, nonché nei casi in cui non sia necessario provvedere ad una cancellazione soltan-

to parziale dei dati (par. 4 della stessa disposizione).
Le presenti fattispecie sono interessanti per capire entro quali limiti un trattamento di *data mining* effettuato da un determinato soggetto possa ritenersi esentato dall'obbligo di cancellazione dei dati personali.
L'analisi di grandi quantità di dati, trova una sua logica allorché i dati siano relativamente recenti e quindi più conformi a delineare realmente i soggetti che rappresentano.
La logica dell'oblio o cancellazione, da questo punto di vista, risponde a tale criterio perché il soggetto richiede di essere rappresentato come in quella determinata fase storica, e non come qualcuno che non riconosce più, perché il tempo è passato portando con sé dei cambiamenti.
È pur vero, però, che un analista di *big data* potrebbe avere interesse ad operare su masse di dati nel corso di anni diversi, e quindi anche molto addietro nel tempo.
Per tale motivo diventerà importante capire se il trattamento rientra nel campo delle opposizioni (pur sempre parziali e limitate, così come previsto dal par. 7) al diritto all'oblio o alla cancellazione dell'interessato oppure no.
L'ultimo aspetto degno di nota, è costituito dai diritti di opposizione e profilazione: l'art. 19 conferisce all'interessato di opporsi a quei trattamenti considerati leciti ma in cui si prescinde dalla volontà dello stesso, dato che la propria giustificazione si rinviene in altre cause.
Il diritto di opposizione, in tal caso, potrà essere esercitato "*...salvo che il responsabile del trattamento dimostri l'esistenza di motivi preminenti e legittimi per procedere al trattamento che prevalgono sugli interessi o sui diritti e sulle libertà fondamentali dell'interessato...*".
Degno di rilievo è anche il comma 2, in cui l'emendato testo della bozza di regolamento incontra il *favor* dei soggetti che si occupano di marketing.
Difatti, in precedenza era stabilito che l'interessato avesse sempre il diritto di opporsi, e gratuitamente "*...qualora i dati personali siano trattati per finalità di marketing diretto...*".
In questo caso, non si ravvisavano grandi problemi sul piano teorico, anche perché la vera rivoluzione dell'analisi predittiva di grandi quantità di dati, o comunque di processazione dei dati in forme innovative, difficilmente porta a concepire l'utilizzo di quei dati personali come forma di marketing diretto[36].
Spesso, risulta più comune la pratica per cui terzi dispongono di dati che poi offrono ad altre società o enti, i quali a loro volta li processano (oppure delegano tale operazione a terzi).

[36] Anche se alcuni dubbi residuerebbero nei casi comuni dei cd. suggerimenti che le società di *e-commerce* riservano ai propri clienti sulla base dei precedenti acquisti.

E, difatti, nella formulazione attuale, si sostiene come "***Where the processing of personal data is based on point (f) of Article 6(1), the data subject shall have at any time and without any further justification, the right to object free of charge in general or for any particular purpose to the processing of their personal data***".

Ciò porta direttamente a trattare del cd. fenomeno della profilazione[37].

Una delle altre grandi novità nel lessico normativo utilizzato dal legislatore, tipico delle operazioni che vengono compiute *on line*, è costituita proprio dall'introduzione del termine "profilazione".

Tale concetto è fortemente legato a quello di *big data*, e di *data mining*, in quanto l'accrescere della quantità di dati a disposizione in rete, oppure archiviati nei vari *server* sparsi per il mondo, unita alla sempre maggiore e costante implementazione delle strutture *hardware* e dei *software* in grado di gestire informazioni, portano a ritenere le attività di profilazione come molto frequenti, e, se non regolamentate, sempre più rischiose.

A tale riguardo, anche la 34° Conferenza mondiale delle Autorità Garanti in materia di dati e di *privacy*, nell'ottobre del 2012, ha redatto una dichiarazione incentrata sul "*profiling*"[38] *("…the collection of personal information into large databases and the subsequent use presents risks to the protection of personal data and privacy. This is especially the case if large data collections are used for analysis and profiling in order to, among others, carry out risk analyses, which help organisations and companies to target persons")*.

L'articolo 20, come stabilisce la relazione d'apertura alla bozza di regolamento, sancisce il diritto di non essere sottoposto a misure basate sulla profilazione, riprendendo, seppur con alcune modifiche, l'articolo 15, paragrafo 1, della direttiva 95/46/C.E. relativo alle decisioni individuali automatizzate, e tenendo conto della raccomandazione del Consiglio d'Europa sulla profilazione.

E, difatti, il concetto di profilazione specifica ciò che nel contesto della direttiva in vigore era considerato il "trattamento automatizzato di dati" al fine di ricostruire il profilo di una persona.

La rinnovata attenzione per un aspetto del trattamento tipicamente inerente l'utilizzo del *Web*, è confortato anche dalla specificazione, *ex* art. 20, c. 3, che l'interessato gode del diritto di ottenere informazioni sul trattamento di dati che

[37] In merito alle prime opinioni sul concetto di profilazione si rimanda a quanto sostenuto da Bravo e Monducci, op. cit., pagg. 30 e ss., in cui si ripercorrono i principali timori sollevati in dottrina (tra cui il Bellavista) circa la pericolosità insita nella profilazione dell'individuo.

[38] Preso atto dei possibili effetti positivi del *profiling* (in ambito sanitario come energetico), i garanti hanno stabilito come il *"purpose limitation"*, ovvero l'importanza dello scopo sia fondamentale per la disciplina della profilazione (da *Uruguay Declaration on Profiling, Punta del Este / Canelones, Uruguay - 26 October 2012*).

lo riguardano, incluso il diritto ad avere tutte le notizie circa eventuali aspetti di profilazione relativi.
L'art. 20, c. 1, così stabilisce: "***Without prejudice to the provisions in Article 6 every natural person shall have the right to object to profiling in accordance with Article 19. The data subject shall be informed about the right to object to profiling in a highly visible manner***".
Con l'emendato testo sulla profilazione, per cui si passa dalla dizione di "Misure basate sulla profilazione" alla "Profilazione" vera e propria, cambia anche la prospettiva visuale sul significato della stessa, adesso inserita direttamente nelle definizioni generali *ex* art. 4 come "***any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour***".
Questa la norma generale, a cui poi fanno seguito le deroghe dei commi seguenti, ed in particolare dal par. 2: "***2. Subject to the other provisions of this Regulation, a person may be subjected to profiling which leads to measures producing legal effects concerning the data subject or does similarly significantly affect the interests, rights or freedoms of the concerned data subject only if the processing: (a) is necessary for the entering into, or performance of, a contract, where the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied, provided that suitable measures to safeguard the data subject's legitimate interests have been adduced; or (b) is expressly authorized by a Union or Member State law which also lays down suitable measures to safeguard the data subject's legitimate interests; (c) is based on the data subject's consent, subject to the conditions laid down in Article 7 and to suitable safeguards***".
In realtà, l'ipotesi di profilazione secondo cui un trattamento è posto "unicamente" in essere in maniera automatizzata, costituisce una fattispecie di difficile comprensione, se presa alla lettera, dovendo ricomprendere quelle situazioni in cui è la macchina a gestire in autonomia il trattamento di dati, e ciò parrebbe aprire la strada alla profilazione posta in essere da intelligenze artificiali.
Pertanto, pare corretto intendere come profilazione, allo stato attuale, quel trattamento di dati personali in cui non vi sia un contatto diretto con l'interessato, ma in cui i dati siano analizzati soltanto tramite apparecchiature di processazione automatica, con un soggetto fisico che decide le operazioni che la macchina deve compiere.
Un'operazione di *data mining*, seguendo questo ragionamento, rientra a tutti gli effetti in una possibile forma di profilazione.

Di scarsa concretezza, invece, pare l'espressione "incidere significativamente sulla persona" ("*significantly affect*"), mentre, di contro, la produzione di effetti giuridici parrebbe eccessivamente generica.
Prescindendo dall'espressione utilizzata, le autorizzazioni di cui al comma 2, privano il dibattito di ogni possibile e reale interesse, giacché si indirizza la questione sulla liceità del trattamento di profilazione ad un piano di ricerca del consenso, nonché nell'ambito degli accordi inseriti dalle parti nelle varie clausole contrattuali.
Rebus sic stantibus, nel disciplinare il *profiling*, il legislatore si è limitato a prendere atto di una delle più importanti modalità in concreto di trattamento del dato, spostando il campo d'interesse, come sottolineato dai garanti dei vari paesi mondiali, dal mezzo al fine.
Non deve sottacersi, però come *the right to object to profiling* venga considerato parte dei diritti dell'interessato rispetto al trattamento di dati portato avanti dal responsabile, così come previsto dall'art. 10A, c. 2, del testo emendato.

PARTE SESTA

Lo scopo del trattamento

Ipotizzare una possibile disciplina giuridica di un trattamento di *data mining*, alla luce della proposta di regolamento comunitario in fase di approvazione, porta inevitabilmente a considerare quelli che sono gli scopi principali alla base delle operazioni di analisi dei dati, in particolare di dati
personali.
Sotto quest'aspetto diventa importante capire, ad esempio, se i dati inerenti la persona siano trattati per scopi di ricerca o di studio ed altresì se tali fini rientrino nell'ambito di enti pubblici che condividono i risultati ottenuti con la collettività, o piuttosto se invece il fine ultimo sia quello relativo alla massimizzazione dei profitti di una determinata società, sia in prospettiva del singolo utente consumatore, sia nell'ottica di un miglioramento della capacità produttiva o di vendita.
Capire quale direzione in concreto assumerà il trattamento di *data mining* diventa fondamentale per
capire se un trattamento sarà da ritenere lecito oppure illecito *a priori*, oppure invece se sarà lecito a
determinate condizioni, come ad esempio anche in mancanza del consenso espresso dell'interessato.
a)*Data mining* e trattamento a scopi commerciali[39].
Mayer-Schonberger e Cukier, elencano un grande quantità di casi in cui l'analisi dei comportamenti degli utenti in rete può aiutare le aziende a capire quali siano i gusti e le preferenze del pubblico, per poi poter decidere se promuovere o meno determinati prodotti, oppure le probabilità di successo di una determinata campagna promozionale, ma gli esempi potrebbero essere molteplici.
Sul piano giuridico, è bene precisare, nulla osta ad un effettuazione ricerche di mercato mediante operazioni di *data mining*.

[39] Un primo commento alla disposizione che disciplinava il trattamento esclusivamente automatizzato di dati personali è stato proposto da Jury Monducci e Fabio Bravo, capitolo III, op. cit.

Sotto questo profilo, le classiche ricerche di mercato, condotte col mezzo del telefono, mediante la posta elettronica oppure con indagini cd. "porta a porta", oltre ad essere maggiormente dispendiose in termini economici, nonché strettamente legate al mondo analogico o al massimo del *Web 1.0*, possono anche far emergere risultati spesso differenti ed incompleti.
Analizzare i comportamenti di utenti spesso inconsapevoli di essere controllati (*rectius*, dell'effettivo ambito di trattamento dei dati rilasciati in rete), anche in modalità remota, e quindi pescando impronte digitali lasciate nel tempo da una moltitudine di persone, grazie all'ausilio di macchinari sempre più potenti, porta inevitabilmente le imprese a preferire metodi innovativi, magari più economici e più proficui, per utilizzare dati a scopi commerciali.
La questione principale consiste nella consapevolezza del concetto di titolarità dei dati personali, ovvero che i dati sono la proiezione dell'individuo nel mondo reale e virtuale[40].
È diritto di ognuno decidere a chi e per quali motivi cedere le informazioni che lo riguardano.
Tale aspetto prescinde dall'altro problema, di notevole rilevanza, costituito dai grandi squilibri informativi che si creano tra chi dispone dei dati da analizzare, chi delle tecnologie in grado di compiere tali operazioni e chi invece necessita solo dei risultati utili che emergono dalle analisi di tali dati.
Sotto questo profilo, analizzando la situazione attuale, nel futuro prossimo saranno i detentori di dati ad avere un forte peso nell'ambito dei rapporti giuridico – economici tra gli operatori del mercato, e, al momento, sono le grandi società americane a detenere il maggior numero di informazioni, anche in termini qualitativi.
Il vero problema rispetto all'impianto normativo comunitario della proposta di regolamento (ma anche guardando all'ordinamento interno, sulla base del vigente D.Lgs. n. 196/2003) è costituito dalla menzione del trattamento basata sull'esecuzione di un contratto, come anche sulla base del consenso dell'interessato.

[40] La necessità di un nuovo *habeas data* (il riferimento è all'*habeas corpus* della Magna Charta Libertatum, il documento emanato dal re d'Inghilterra noto come Giovanni Senzaterra nel 1215, e considerato il primo embrione dei diritti universali della persona), e quindi di concedere la stessa attenzione per la tutela del corpo fisico anche alla tutela del corpo elettronico, costituisce uno dei grandi sforzi intellettuali del giurista ed ex Presidente dell'Autorità Garante della Protezione dei Dati Personali Stefano Rodotà, espresso nella maggior parte delle sue opere. Se ne può trarre un esempio nel discorso di chiusura alla 26° "Conferenza Internazionale sulla Privacy e la Protezione dei Dati Personali" del 2004: *"Ogni trattamento di singoli dati dev'essere considerato come se si riferisse al corpo nel suo insieme, ad una persona che deve essere rispettata nella sua integrità fisica e psichica. È nata una nuova concezione integrale della persona, alla cui proiezione nel mondo corrisponde il diritto al pieno rispetto di un corpo che ormai è, al tempo stesso, "fisico" ed "elettronico..."* (doc. *web* n. 1049293 disponibile sul sito *www.garanteprivacy.it*).

L'art. 20, difatti, rimanda alla liceità della profilazione allorché l'interessato abbia fornito il proprio consenso, fatti salvi i diritti di cui all'art. 7 della bozza di regolamento.
Il nodo cruciale rispetto ad un trattamento di *data mining* operato al fine di porre in essere la vendita di beni o servizi, sia in via diretta mediante una pubblicità mirata, sia indiretta, mediante l'utilizzo di tali informazioni per migliorare le strategie promozionali su larga scala, si pone rispetto al notevole squilibrio tra la posizione dell'interessato e quella del responsabile del trattamento.
Il Garante della Protezione dei Dati Personali è intervenuto più volte in merito a fenomeni come quello della profilazione dei comportamenti delle persone fisiche[41].
In tutti questi casi, sulla base delle raccomandazioni del Garante alla luce delle normative applicabili, le operazioni di profilazione sono consentite, anche in assenza della preventiva acquisizione del consenso dell'interessato, purché il responsabile adotti una serie di accorgimenti rivolti al mantenimento dell'anonimato dei soggetti interessati, oltre alla chiara specificazione del tipo di operazioni che il responsabile intende porre in essere, nonché delle modalità con cui intende raggiungere un determinato scopo.
Le grandi società (considerate tali dal punto di vista della mole di dati che gestiscono, ed oramai anche del fatturato realizzato) che offrono servizi di *social media*[42] possiedono un quantità di dati che mettono a disposizione di terzi, ben al di là di profili interni miglioramento dei propri prodotti o servizi.
Queste società godono di quella che si può definire una posizione dominante nel mondo digitale, in quanto il cd. effetto di rete ha portato tali soggetti a governare in maniera quasi totalitaria i rispettivi ambiti di servizi offerti, con la conseguenza che gli utenti si trovano costretti tra il subire gli effetti di un *digitale divide*, o quelli di subire una schedatura massiva da parte di coloro che vorranno attingere a quelle informazioni, per vendere un paio di scarpe quanto piuttosto per offrire la possibilità di investire in determinate operazioni finanziarie.
Ma, come detto, vi sono altre innumerevoli possibilità di utilizzo dei dati a fini commerciali, anche di gran lunga differenti del commercio classico.
Quale utente acconsentirebbe a far trattare i propri dati da soggetti che rivendono tali informazioni alle agenzie finanziarie?

---

[41] *Ex plurimis*, si vedano i provvedimenti del 03/02/2005 in materia di Tv interattiva e profilazione, del 25/06/2009 in cui si prescrivono gli accorgimenti necessari ai fornitori di servizi di comunicazione elettronica accessibili al pubblico che svolgono attività di profilazione, oppure anche provvedimenti mirati come quello del 15/03/2012, in risposta alle richieste di una società commerciale intenzionata ad effettuare trattamenti di profilazione.
[42] Solo tra i più conosciuti Facebook, Twitter, Linkedin, Whattsapp, nonché Google, che ottiene la maggior parte delle proprie informazioni dalle *query* del motore di ricerca.

Cosa succederebbe se una persona si vedesse negare un finanziamento perché l'analisi dei vari "*tag*", "Mi piace", *tweet*, status, foto e altro ancora, ha portato un soggetto che eroga prestiti a capire che tale persona gode di scarsa affidabilità nella restituzione del credito?
Probabilmente, guardando agli effetti positivi, ciò aiuterebbe le imprese sane ad essere più responsabili nella concessione dei prestiti, ma niente garantisce che il sistema abbia offerto la soluzione corretta, senza menzionare aspetti etici legati alla scomparsa dell'elemento umano a favore di risposte impostate esclusivamente sui dati.
Altro atteggiamento merita di essere citato per la possibilità di utilizzare i dati personali dell'utente per suggerire altri elementi connessi con precedenti acquisti dello stesso utente[43].
Nel mondo "fisico", allorché un soggetto dovesse porre in essere nuove operazioni commerciali presso un rivenditore della grande distribuzione, con cui già in precedenza aveva intrattenuto rapporti, difficilmente lo stesso sarà invitato ad effettuare un certo tipo di scelte sulla base delle scelte compiute in passato (ciò senza considerare, ad esempio, le strategie di neuro marketing, o le ultime tecniche di profilazione indiretta tramite i sistemi di videosorveglianza).
Nel mondo di Internet, le società di *e-commerce* registrano tutte le informazioni veicolate attraverso i propri *server*, venendo incontro alle sue preferenze suggerendo all'utente altri elementi che possono soddisfarne i gusti.
Per quanto possa costituire un'ipotesi non gradita, oppure invece un'opportunità innovativa e ben vista dall'utente-consumatore, almeno, in tale ultima fattispecie, vi sarà la consapevolezza di quale soggetto e per quali fini sono trattati quei determinati dati.

b)Scopi storici, statistici e scientifici.

La realizzazione di operazioni di *data mining*, anche mediante sistemi automatizzati è soggetta ad una diversa disciplina, allorché l'angolo visuale dato da scopi attinenti a motivi di ricerca e studio sia alla base del trattamento di dati personali.
Se nel precedente paragrafo, si è discusso circa il principale fine delle operazioni di estrazione ed analisi di grandi quantità di dati dalla rete, non si deve dimenticare che tali operazioni possono essere effettuate anche senza scopo di lucro.
L'art. 83 della bozza di regolamento, come già la precedente direttiva, lascia una porta aperta alla crescita collettiva della società grazie alle ricerche ed alle indagini di ambito storico, statistico e scientifico.

[43] Fra tanti, si veda la pratica di Amazon volta a suggerire i nuovi libri sulla scorta dei precedenti libri acquistati, oppure Google, che mediante il suo negozio suggerisce brani musicali o filmati video probabilmente graditi al soggetto interessato. Tali suggerimenti sono creati sulla base di potenti algoritmi, che associano risultati simili, ma anche sulla scorta di soluzioni difficilmente formulabili dall'essere umano.

Secondo la disposizione citata, quindi: "*Nei limiti del presente regolamento, i dati personali possono essere trattati per finalità storiche, statistiche e di ricerca scientifica solo se: a) tali finalità non possono essere altrimenti conseguite trattando dati che non consentono o non consentono più di identificare l'interessato; b) i dati che permettono di associare informazioni a un interessato identificato o identificabile sono conservati separatamente dalle altre informazioni,* ***under the highest technical standards, and all necessary measures are taken to prevent unwarranted re-identification of the data subjects***".

Il legislatore, nell'impianto generale della normativa, accoglie con favore il trattamento effettuato per tali finalità, sempre che avvenga nel rispetto dei limiti imposti sia dallo stesso regolamento sia dalle discipline specifiche in materia, nonché delle *best practice* in materia di sicurezza dei dati.

Difatti, anche per i cd. dati sensibili, definiti dalla normativa come "particolari categorie di dati personali", vige un divieto generale di trattamento, con la conseguenza che potranno essere trattati nei limiti dell'art. 83 per finalità storiche, statistiche o scientifiche.

In particolare, sono ribaditi alcuni concetti chiave della normativa in materia di trattamento di dati personali, come il principio di necessità e di proporzionalità, tali che il responsabile del trattamento potrà compiere soltanto quelle operazioni che si rivelino indispensabili, cercando di mantenere diversificati i *database* contenenti le informazioni, e provvedendo, ove possibile, all'anonimizzazione dei dati personali.

Tale aspetto è molto importante da sottolineare, proprio perché le possibilità concesse dall'analisi dei *big data*, come ampiamente sottolineato, sono molteplici[44].

Gli aspetti problematici intorno a tali tipi di trattamento ricadono essenzialmente sul tema della sicurezza e della reale verifica sulle intenzioni della ricerca. Inoltre, non si deve dimenticare che la ricerca scientifica, qualora fosse portata avanti da un ente privato, non dovrebbe rientrare nel particolare ambito dell'art. 83, quanto piuttosto nel caso di un trattamento a tutti gli effetti posto in essere per finalità economiche.

Tale fattispecie dovrebbe essere inquadrata nell'ambito della disciplina generale, con l'obbligo di acquisire il consenso dell'interessato, libero, informato, trasparente e preventivo e pur sempre nel rispetto delle *best practice* in materia

[44] Come descrivono nel loro libro Mayer-Schonberger e Cukier, op. cit., pp. 125 e 126, tal Sandy Pentland, che dirige lo Human Dynamics Laboratory del Massachussets Institute of Tecnology, ha sperimentato un trattamento di *data mining,* definito "*reality mining*", consistente nel processare enormi quantità di dati provenienti dai telefoni cellulari per trarne inferenze e previsioni sul comportamento umano: *"In uno studio, l'analisi degli spostamenti e delle chiamate li ha messi in condizione di identificare persone che avevano contratto l'influenza, ancor prima che queste sapessero di essere ammalate. Nel caso di un epidemia influenzale particolarmente virulenta, questa capacità potrebbe salvare milioni di vite in quanto consentirebbe alle autorità sanitarie si sapere in qualunque momento quali sono le zone più colpite".*

di trattamento di dati personali.
Altro aspetto importante sarà costituito dalla vigilanza del Garante, ed in generale della pubblica autorità, in merito al controllo del flusso di informazioni emerse e raccolte nell'ambito del trattamento *ex* art. 83.
Nulla vieta che i risultati ottenuti da enti di ricerca per finalità di pubblico dominio, ad esempio, siano rivenduti ad aziende farmaceutiche per poter essere sfruttate nella produzione di nuovi medicinali.
Ad ogni modo, il vero punto critico è costituito dalla sicurezza dei sistemi informativi.
I risultati della processazione automatica delle informazioni possono costituire un tesoro appetibile per una pluralità di soggetti e trattando spesso informazioni attinenti a dati sensibili (come ad esempio dati sanitari) la preoccupazione di predisporre adeguate garanzie sul piano della sicurezza dovrà essere ancor maggiore.

c)Il trattamento esclusivamente individuale.

Altro tipo di trattamento di *data mining* che esula dai limiti dell'applicazione della presente proposta normativa (fatta eccezione per il rispetto delle misure di sicurezza), come già per quanto concerne la precedente direttiva sulla cui base è stata costruita la disciplina del D.Lgs. n. 196/2003, è quello effettuato dal singolo persona fisica per un uso esclusivamente personale.
Gli emendamenti apposti dalla commissione del Parlamento Europeo, però, hanno modificato l'iniziale formulazione, simile a quanto già era espresso anche nel Codice Privacy del 2003.
L'art. 2, c. 2, lett. d) della proposta di regolamento, sancisce che "*...Le disposizioni del presente regolamento non si applicano ai trattamenti di dati personali: ...effettuati da una persona fisica per l'esercizio di attività esclusivamente personali o domestiche.* ***This exemption also shall apply to a publication of personal data where it can be reasonably expected that it will be only accessed by a limited number of persons****...*".
La cesoia dell'emendamento a tale paragrafo deve essere valutata in base anche a quanto disposto dal considerando n. 15): "*Il presente regolamento non deve applicarsi al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività esclusivamente personali,* ***family-related*** *o domestiche, quali la corrispondenza e gli indirizzari,* ***or a private sale*** *e senza alcuna connessione con un'attività commerciale o professionale. However this regulation should apply to controllers and processors which provide the means for processing personal data for such personal or domestic activities*".
Innanzitutto si può notare la scomparsa della finalità di lucro, a favore della possibilità di effettuare anche una vendita privata.

Tale parziale modifica potrebbe allora voler allargare i confini di quel principio di ragionevolezza secondo cui non si può gravare il singolo che si trovi a trattare dati personali solo in via incidentale[45].
Tale disposizione, già presente anche nel precedente testo normativo, identifica quel tipo di trattamento in base al quale i dati personali di altri individui, seppur trattati senza un preventivo consenso, ad esempio, non sono resi pubblici, rimanendo nella sfera privata del soggetto che li tratta.
L'inciso normativo, però, richiede come *condicio sine qua non* del trattamento libero da vincoli, la mancanza di finalità commerciali (e non più lucrative, nei termini anzi detti).
Inoltre, il singolo persona fisica, potrebbe, per puro spirito di conoscenza, effettuare un trattamento di dati al fine di scoprire le connessioni sociali tra gli utenti di una determinata rete sociale, oppure analizzarne gli stati d'animo rispetto ad un particolare fatto di cronaca o di vita quotidiana.
Il particolare *favor* concesso dal legislatore rispetto a tali trattamenti, si fonda sulla sfera d'azione del trattamento.
La disciplina generale in materia di protezione dei dati personali tende a prevenire un indebito utilizzo dei dati personali della persona fisica, poiché i pregiudizi che potenzialmente possono derivare al singolo dalla circolazione di informazioni che lo riguardano sono caratterizzati da un elevato indice di dannosità, allorquando tali informazioni siano rese pubbliche.
Diversamente, se tali dati rimangono racchiusi nella sfera personale del soggetto trattante, l'interessato (in teoria) non dovrebbe subire conseguenze negative, sempre che, appunto, quei dati non siano utilizzati per finalità commerciali.
Un trattamento di *data mining* effettuato nei limiti così definiti potrebbe definirsi lecito.

[45] A mero titolo di esempio, tale formulazione potrebbe far pensare ad una norma tesa a minimizzare le incombenze su quei privati che offrono beni e servizi mediante piattaforme che hanno il solo scopo di fare da intermediari tra domanda e offerta. Solo per fare un esempio, il privato che vendesse un bene personale ad un altro privato tramite la piattaforma E-bay, non sarebbe sottoposto, per il solo fatto di entrare in contatto con dati personali altrui, alle disposizioni in materia di trattamento di dati personali. Diversamente dovrebbe concludersi per il soggetto che opera sulla piattaforma con modalità di operatore commerciale oppure per lo stesso E-bay.

PARTE SETTIMA

Web semantico, *Web 3.0 predictive analytics*: i trattamenti da parte di intelligenze artificiali

Gli interrogativi che il giurista deve porsi rispetto allo scenario del trattamento dei *big data* devono essere rivolti allo spazio che il diritto può occupare per arginare la marea di innovazione scaturente dalle diverse spinte nel mondo della scienza e della tecnologia.
Un atteggiamento in partenza rinunciatario è fuorviante, oltre che sbagliato, ed allo stesso tempo non è proficuo delegare all'autocontrollo e all'autogoverno della rete la regolamentazione di fenomeni invasivi e dalle plurime potenzialità.
Come sostengono Mayer-Schonberger e Cukier, ogni cosa si sta "datizzando", prima ancora che digitalizzando.
Ma una volta "datizzate" tutte le informazioni e inserite in un processore, queste informazioni rischiano di essere disperse, sfruttate per scopi illeciti, oppure ancora carpite da soggetti istituzionali per fini, più che di sicurezza nazionale, di controllo globale (come ha dimostrato il recente caso *NSA-gate*).
Con il passare del tempo, la capacità computazionale dei processori aumenta in misura tale che i dispositivi elettronici possono analizzare una mole sempre più grande di dati, in un tempo sempre più ridotto, tanto da offrire soluzioni su misura per il singolo persona fisica in un lasso di tempo pressoché nullo.
Il *Web* si sta trasformando rapidamente in un luogo (non luogo) in cui le macchine, intese come struttura *hardware* e come programmi per elaboratore, vedranno aumentate sempre più le proprie capacità di potenza e di elaborazione, non solo grazie al lavoro dei programmatori, *data analyst*, *data scientist*, e tutte le altre figure specializzate, ma principalmente estraendo informazioni mediante *crawler* sparsi in rete.
In sostanza la tecnologia sarà sempre più invasiva, ed i nostri dati personali, tutte le informazioni che riguardano la persona, saranno a disposizione sparsi in

qualche *database* (o *dataset*) sparso sul globo, all'interno di qualche *server* difficilmente localizzabile.
Gli algoritmi di Google, che hanno garantito il successo a tale società sino ad oggi, si migliorano costantemente grazie anche agli stessi utenti che digitando sul motore di ricerca le varie *query* consentono al sistema di crescere, di rimodellarsi di continuo.
Ancora, società come Google e Facebook stanno iniziando a promuovere sempre più una terminologia incentrata sui grafi, piuttosto che sulla rete, proponendo, per i trattamenti di *data mining*, delle API basate sui grafi, tanto che, secondo Tim Berners Lee, addirittura si potrebbe già parlare di *Giant Global Graph*, ovvero un grafo globale gigante, per sostituire il termine *World Wide Web*[46], perché il *Web* si sta arricchendo sempre più di dati sociali[47].
Maggiori saranno le connessioni create, maggiori probabilità ci saranno che la *query* riferita al sistema di Google risponda esattamente alle richieste dell'utente.
Anche Russell, nella sua opera "*Data mining nel social web*", conferma che il "*web* semantico" potrebbe conferire una spinta importante per lo sviluppo delle intelligenze artificiali, perché le informazioni potrebbero essere condivise in un modo comprensibile alle macchine e sufficientemente inequivocabile, tanto da permettere a un agente utente evoluto, come un *Web Robot*, di estrarre, interpretare e usare le informazioni per prendere importanti decisioni.
Se sussistono preoccupazioni inerenti la protezione di dati personali nel momento attuale, in cui piccole, medie o grandi società possono analizzare grandi quantità di dati, incrociando anche diversi archivi di dati, operazioni di *data mining* poste in essere da sistemi d'intelligenza artificiale non saranno da meno. I risultati di tali operazioni possono sempre essere resi pubblici, e quindi conoscibili ad altre persone fisiche.
Gli accorgimenti per tutelare la dignità personale, ed il diritto naturale alla protezione dei dati personali saranno di primaria importanza nell'insegnamento e nella progettazione di sistemi d'intelligenza artificiale, anche se il compito si presenta difficile, stante la natura dei dati e l'incertezza spesso presente a livello d'interpretazione delle situazioni concrete.

[46] Tim Berners Lee, inoltre, uno degli inventori del *Wordl Wide Web* è stato anche uno degli inventori del termine "*web* semantico", definito come *"la trasformazione del Wordl Wide Web in un ambiente dove i documenti pubblicati (pagine HTML, file, immagini, e così via) sono associati ad informazioni e dati (metadati) che ne specificano il contesto semantico in un formato adatto all'interrogazione e l'interpretazione (es. Tramite motori di ricerca) e, più in generale, all'elaborazione automatica. Con l'interpretazione del contenuto dei documenti che il Web semantico impone, saranno possibili ricerche molto più evolute delle attuali, basate sulla presenza nel documento di parole chiave, e altre operazioni specialistiche come la costruzione di reti di relazioni e connessioni tra documenti secondo logiche più elaborate del semplice collegamento ipertestuale"*, da *https://it.wikipedia.org/wiki/Web_semantico*.
[47] Google, ad esempio, sta sviluppando il cd. *Knowledge Graph*, un sistema che raccoglie informazioni creando connessioni tra cose, come propone sulla stessa pagina dedicata al progeto su *www.google.com.*

Oltre a ciò, il *Web 3.0* sta portando con sé anche altre fenomenologie, come la realtà aumentata degli occhiali *smart*, che acquisiscono dati dal mondo esterno per suggerire soluzioni adeguate, nonché per agevolare le interazioni con il mondo stesso e con le altre persone, *devices* tecnologici in grado di processare tanti dati, ma soprattutto di analizzarli per offrire una forte presenza nella vita quotidiana, tanto che le nostre stesse scelte potranno essere condizionate dai suggerimenti di tali macchine.
Il legislatore europeo, nella proposta di regolamento europeo in tema di *profiling*, sembra aver dedicato un'attenzione particolare a tale tipo di trattamento automatizzato, tale da considerarlo particolarmente pericoloso data la potenzialità del dato materiale costituito dai processori esistenti (nonché futuri)[48].
Sul piano del diritto interno, in dottrina si è già ampiamente dibattuto, tra l'altro, sul concetto di pericolosità insita nel trattamento, rispetto ai mezzi utilizzati, visto e considerato il rimando dell'art. 15 D.Lgs. n. 196/2003 all'art. 2050 c.c. relativo alla responsabilità per l'esercizio di attività pericolose[49].
I progressi nel campo delle intelligenze artificiali permetteranno, in uno scenario non molto lontano, di effettuare in autonomia una serie di operazioni sempre maggiori, e grazie ai progressivi miglioramenti delle tecnologie disponibili, e al lavoro dei programmatori semantici, i robot saranno in grado di analizzare i *big data*, senza poter prevedere fino a quale limite.
Il dibattito circa i profili di responsabilità civile e penale collegata all'azione (od omissione) dei sistemi di intelligenza artificiale è una questione che, nell'ottica del *data mining*, avrà rilievo soltanto qualora la dottrina risolverà le questioni principali legate agli indirizzi anche politici che dovrà prendere questo ramo dell'ordinamento[50].
Senza voler prendere posizione sul piano etico, rispetto al panorama che si prospetta, e accogliendo anche con favore tali innovazioni, si dovrà comprendere quale destino è riservato ai dati personali.

---

[48] Anche se non si deve dimenticare che al considerando n. 13 si fa presente come *"La protezione delle persone fisiche deve essere neutrale sotto il profilo tecnologico e non dipendere dalle tecniche impiegate; in caso contrario, si correrebbero gravi rischi di elusione. La protezione delle persone fisiche deve applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati sono contenuti o destinati ad essere contenuti in un archivio"*.

[49] Tale argomento, data la vastità delle questioni coinvolte, dal tema della responsabilità contrattuale ed aquiliana astrattamente collegabile ad un trattamento illegittimo, passando alla questione della risarcibilità del danno non patrimoniale, richiederebbe una trattazione a parte, per cui si rimanda alla lettura dei più autorevoli esponenti in materia.

[50] Per una disamina delle principali questioni in materia di intelligenza artificiale si rimanda ai preziosi contributi di Sartor, *"Gli agenti software e la disciplina giuridica degli strumenti cognitivi"*, in Diritto dell'Informazione e dell'informatica, 2003, p. 55; *"Gli agenti software: nuovi soggetti del cyberdiritto?"*, in Contratto e Impresa, Padova, 2002, 2, pp. 466 e ss., e infine *"L'intenzionalità dei sistemi informatici e il diritto"*, Bologna, 2002, dattiloscritto.

Il diritto all'oblio, *the right to be forgotten*, è un concetto di grande importanza che già ha trovato applicazione anche nella giurisprudenza di legittimità interna[51].
Se sostenuto da appositi strumenti sanzionatori in caso di violazione e dalle strumentazioni tecniche adeguate, è sicuramente da ritenersi un solido principio da cui ripartire.

[51] Il riferimento è alla sentenza Sez. III, 5 aprile 2012, n. 5525, Corte di Cassazione, su diritto all'oblio e diritto di cronaca.

PARTE OTTAVA

Considerazioni finali

La disciplina sul trattamento dei dati personali, così come affrontata in sede di proposta di regolamento del Parlamento Europeo e del Consiglio dell'Unione Europea, non tratta in maniera specifica operazioni di trattamento come quella del *data mining*, così come altre possibili operazioni specifiche che l'uomo (o la macchina) possono compiere sui dati.
Tale atteggiamento del legislatore europeo non sorprende, se si considera la volontà di disciplinare *tout court* la fattispecie del trattamento di dati personali, in quanto, come si ricorda nel considerando n. 13), si preferisce proteggere la persona in maniera neutrale rispetto al profilo tecnologico e alle tecniche impiegate, eventualmente presenti nel trattamento.
Ad ogni modo, la disciplina sul trattamento dei dati personali, così come analizzata *in parte qua* rispetto alla fattispecie tipica dell'operazione di estrazione degli stessi dalla rete, pare sufficientemente esaustiva, pur nei limiti sopra descritti.
Oltre ad un'analisi meramente giuridica, poi, esiste anche la possibilità, seppur limitata, di implementare una protezione tecnologica all'interno dei confini giuridici attuali che può spingere nella direzione di una maggiore consapevolezza e autocontrollo delle proprie informazioni personali.
Per tale ragione possono essere proposti alcuni accorgimenti, sia sotto il profilo tecnico, sia, in un ottica *de jure condendo*, sotto il profilo giuridico.
In prima battuta, è doveroso essere consapevoli delle opportunità concesse dallo stato della tecnica rispetto alla possibilità di impedire che i propri dati personali siano estratti dai vari angoli della rete e successivamente utilizzati.
Attualmente sono già presenti, sul mercato dei programmi per elaboratore, diversi *software* in grado di bloccare il tracciamento da parte di soggetti terzi dei dati personali lasciati in rete.
Tali *software*, generalmente disponibili in concessione con licenze *open source*, si propongono di mettere in condizione l'utente di riappropriarsi del destino dei propri dati, decidendo con chi condividerli, a chi farli trattare, anche in

prospettiva di sapere per quali motivi possono essere successivamente utilizzati, e così esercitare tutti i diritti concessi all'interessato in merito ai propri dati, attualmente elencati dall'art. 11 all'art. 21 della bozza di regolamento[52].
La consapevolezza dell'utente sul destino dei propri dati ed il relativo controllo nelle fasi successive all'acquisizione sono i cardini che ispirano tali programmi, nonché lo stesso impianto normativo della normativa comunitaria in materia di protezione dei dati personali, almeno per quanto concerne i dati comuni.
Tale opportunità costituisce un passo avanti nell'ottica di una *self-regulatory policy* in materia di trattamento di dati personali, o meglio di una *privacy by design*, in quanto il singolo utente può stabilire con chi condividere i propri dati nell'ambito di un sistema trasparente, essendo edotto sui possibili fini del trattamento di *data mining*, nonché della successiva possibile operazione di incrocio dei risultati ottenuti dall'estrazione dei dati da differenti *database*.
Pur considerando la possibilità di sfruttare le potenzialità promesse da tali programmi, la questione relativa al consenso prestato dall'utente per il trattamento dei propri dati da parte del gestore del sito (per fini spesso non chiari e determinati preliminarmente) non è risolta, e forse tale spazio potrà essere riempito dal diritto in senso lato.
Passando, perciò, ad affrontare quelle che possono essere delle possibili prospettive future legate ad ipotesi di normazione positiva, il punto di partenza preliminare per affrontare tale questione è costituito dalla necessità che gli stessi cittadini, così come gli operatori del diritto e le istituzioni, siano maggiormente consapevoli del "valore" insito nei dati.
L'utente della rete deve essere edotto sulle reali opportunità che i propri dati personali offrono ai soggetti a cui vengono ceduti, ovvero come possono operare su quei dati.
I dati personali sono definiti, nella bozza di regolamento, come "*qualsiasi informazione che riguarda l'interessato*".
In realtà, per utilizzare una metafora, i dati personali (ma non soltanto quelli) sono come l'oro presente nel terreno, e come l'estrazione costituisce l'operazione idonea e necessaria da compiere per sfruttare tutto il valore del materiale, allo stesso modo il *data mining* deve identificarsi con quell'operazione che consente di dare un valore ai *big data* presenti in rete, estraendoli dai vari *dataset*, per

[52] Uno tra questi è ad esempio il programma Ghostery, disponibile gratuitamente dal sito *www.ghostery.com*. Come specificato sulla pagina dedicata al funzionamento del programma, dopo aver individuato quali sono i soggetti che hanno avuto l'accesso ai dai personali direttamente dal gestore del sito visitato, l'utente ha la possibilità anche di decidere da chi far trattare i propri dati ("*After you've seen what's tracking you, you can decide whether or not you want to block any or all of the companies in Ghostery's library*"), visto e considerato che lo stesso utente può comunque trarre dei benefici da quel trattamento, o comunque condividere le finalità del responsabile del trattamento di analisi dei dati. Ma la gamma di *free software* è ampia, e tali programmi sono facilmente disponibili sotto forma di *plugin* messi a disposizione dai relativi *browser* di navigazione Internet.

ottenere risultati di grande utilità, seppur dopo una certa lavorazione ed affinamento del materiale ottenuto.
Il singolo dovrebbe comprendere a pieno che le informazioni che lo riguardano, e tra questi i dati personali protetti come diritto fondamentale dell'individuo, interessano una moltitudine di soggetti, dalle singole persone fisiche che nutrono interessi riconducibili alla sfera personale, alle società multinazionali che offrono beni e servizi su scala mondiale, sia per motivi di ricerca scientifica o piuttosto per esigenze di marketing.
Tale tipo di rinnovata consapevolezza dovrà essere accompagnata, da un lato, da un nuovo spirito di attenzione e premura da parte della giurisprudenza e, dall'altro lato, da una maggiore implementazione di politiche di protezione del soggetto e dei dati che lo riguardano.
Pur non avendo affrontato nello specifico il profilo sanzionatorio relativo ad un illecito trattamento di dati personali, le cui regole comunque restano proprie del singolo ordinamento giuridico di ogni stato membro dell'Unione Europea, si potrebbe iniziare ad assegnare al pregiudizio consistente nel danno non patrimoniale nei suoi vari aspetti un determinato valore.
L'innovazione consistita nell'attribuire un punteggio d'invalidità, permanente e temporanea, in sede di liquidazione del danno biologico, potrebbe iniziare ad applicarsi anche in materia di protezione di dati.
Le tabelle di liquidazione del danno biologico sono invalse nella prassi del diritto giurisprudenziale per trovare rimedio ad una esigenza fondamentale, ovvero risarcire in maniera pienamente satisfattiva il danneggiato, di modo che il risarcimento ottenuto potesse compensare la perdita subita.
Rebus sic stantibus, e considerato che il danno non patrimoniale deve sempre essere risarcito in presenza di previsione di legge (previa dimostrazione del pregiudizio patito)[53], proprio come disposto, almeno sul piano interno dall'art. 15 D.Lgs. n. 196/2003, si tratterebbe di attribuire un punteggio in base al tipo di valutazione dell'illecito, che può portare ad un danno (esistenziale, alla vita di relazione, d'immagine, morale, *et cetera*) più o meno elevato, così come avvenuto per quanto concerne il danno "fisico" alla persona.
Tale prospettiva, seppur non direttamente influente sul trattamento di *data mining*, rappresenta comunque un passo verso cui il nostro ordinamento dovrà tendere, se ci sarà l'intenzione di conferire ai dati personali una tutela giuridica intensa, visto e considerato che in ambito comunitario il diritto alla *privacy* e alla protezione dei dati personali è un diritto fondamentale.

[53] Così come confermato anche dalla oramai nota sentenza n. 26972/2008 della Corte di Cassazione a Sezioni Unite.

Oltre alla necessità di una rinnovata attenzione da parte del diritto vivente verso la protezione dei dati personali, anche in un'ottica istituzionale si potrebbero apportare delle innovazioni.
Il Garante per la Protezione dei Dati Personali, figura chiave in ogni stato membro dell'UE, potrebbe veder accresciuta la sua autorità ed i suoi poteri[54].
L'attribuzione di poteri cautelari più incisivi, o comunque un potenziamento della struttura dell'organo, sarebbero segnali importanti nella direzione di una maggiore garanzia per i diritti dell'interessato.
I compiti a cui sono chiamati tali garanti, in una società dove il trattamento dei dati avviene sempre più (e talvolta anche esclusivamente) mediante l'uso di strumenti automatici, con informazioni che risiedono nei vari *server* di diverse dimensioni presenti in ogni parte del mondo, si accrescono a mano a mano con il passare del tempo.
Tale figura istituzionale può affrontare le nuove sfide in materia di protezione dei dati con una sensibilità maggiore della giurisprudenza, più legata ad una concezione in senso classico del diritto.
Ma il vero punto nevralgico della normativa comunitaria risiede nella manifestazione del "consenso".
Secondo Mayer-Schnonberger e Cukier, nell'era dei *big data* "*le tre strategie di base impiegate da sempre per garantire la privacy – consenso informato, dissociazione e anonimizzazione – hanno perso gran parte della loro efficacia*"[55].
Le operazioni di dissociazione e anonimizzazione, sono tecniche pur sempre utili per celare l'attribuibilità di determinati dati personali al singolo individuo, ma sicuramente, come sottolineano gli Autori, incrociando i dati ottenuti da vari *database* potrebbero essere vanificate, rendersi cioè ininfluenti, superflue.
Le operazioni di *data mining* compiute mediante *software* con una capacità di elaborazione dei dati sempre più potente possono effettivamente eludere questa garanzia tecnica di anonimato.
Ciò che propongono gli Autori, quindi, va nella direzione di un passaggio dalla *privacy* su consenso alla "*privacy tramite responsabilizzazione*", ovverosia un approccio in direzione di una "*privacy differenziale*"[56]
L'atteggiamento di responsabilizzazione del titolare del trattamento creerebbe un equilibrio più adatto per l'era dei *big data*, ovvero uno scenario in cui gli operatori economici possono sfruttare più a lungo i dati, in cambio di un'accre-

[54] Tale ipotesi è stata caldeggiata, tra le tante, anche dai garanti riuniti nella conferenza di Punta del Este, Uruguay nel 2012, la cd. *"Uruguay Declaration on profiling"*.
[55] Addirittura gli Autori si spingono fino a sostenere che *"in presenza di un quantitativo sufficiente di dati la totale anonimizzazione è assolutamente impossibile";* p. 210, op. cit.
[56] Ad esempio, si possono confondere deliberatamente i dati in modo che la singola *query* sul motore di ricerca offra in cambio dei risultati approssimativi, come suggerito a p. 236, op. cit.

sciuta responsabilità sulla loro circolazione e dell'obbligo di cancellazione dopo un certo periodo di tempo.
Tale prospettiva è senza dubbio meritevole d'attenzione, in particolare per quanto concerne il diritto all'oblio, argomento fondamentale in tema di dati personali.
Anche il concetto di *privacy* per responsabilizzazione assume una valenza importante, ma il vero problema relativo al consenso informato, risiede proprio in un differente approccio verso i dati personali e in una scelta chiara di politica legislativa.
Il singolo utente, in particolar modo quando diffonde e carica dati personali sui vari *social network*, come già spiegato sopra, accetta tutti i termini di un contratto di cui non ha la possibilità di contrattare il contenuto, limitandosi ad accettare le condizioni generali imposte dall'altra parte.
L'atteggiamento di responsabilizzare i soggetti che trattano dati personali è corretto, soprattutto quando dispongono di una grande mole di dati, ma ciò non preclude che quel singolo soggetto stia trattando i suoi dati per fini non comunicati preventivamente all'utente, oppure che li stia cedendo a soggetti terzi.
Seguendo questa logica, un accorgimento utile sul piano normativo, di minimo impatto sullo stato delle cose, sarebbe costituito dall'introduzione dell'obbligo di specificare tutti i soggetti a cui sono ceduti i propri dati personali (anche se ceduti in forma anonimizzata), e per quali fini saranno ceduti quei determinati dati.
Come già detto, non solo le categorie di destinatari, come prevede l'attuale art. 14 della proposta di regolamento, ma i destinatari effettivi.
Inoltre, preliminarmente rispetto ad un'azione positiva dell'interessato, sarebbe lo stesso responsabile a farsi carico di specificare anche i fini per cui questi dati sono trattati, di modo che tale compito non gravi ulteriormente sull'utente.
Riappropriarsi dei propri dati personali, però, significa anche prendere consapevolezza del valore dei dati.
Nulla vieta che in futuro il legislatore possa considerare i dati personali alla stregua di un diritto costituzionale, come sul piano interno è ritenuto tale il diritto alla salute[57].
È ovvio che tali questioni non siano di poco conto, soprattutto alla luce del sistema delle fonti tra diritto interno e diritto comunitario.

[57] Una riflessione ad ampio raggio, che parte dalle pronunce della *Supreme Court* statunitense per arrivare sino alla prospettiva di una costituzionalizzazione del diritto alla *privacy* è stata proposta da Andrea Putignani, *"Libera Circolazione e Protezione dei Dati Personali"*, op. cit., pag. 131. L'Autore, si sofferma a riflettere sulla possibilità di inquadrare il diritto alla *privacy* in senso lato nell'ambito di alcune disposizioni della Carta, anche se, considerando il D.Lgs. n. 196/2003 si allora recentissima emanazione, sostiene che: *"...non è senza conseguenze rilevare che i caratteri fondamentali di questa nuova privacy costituzionale si ritroverebbero già espressi nelle tecniche di bilanciamento utilizzate nel codice in materia di protezione dei dati personali."*

Ad ogni modo, seguendo questo percorso, il legislatore potrebbe stabilire, come previsto dal legislatore del 1942 per l'art. 5 del Codice Civile, che il singolo non possa liberamente privarsi dei propri dati personali.
Come nel mondo fisico il corpo ha ottenuto una tutela dal legislatore, prima ancora dell'entrata in vigore della carta costituzionale, così per il mondo digitale potrebbe essere introdotto un principio-limite costituito da un indice di tollerabilità sull'utilizzo dei dati rispetto al fine del loro trattamento, proprio nell'ottica di un nuovo *habeas data*, come auspicato da Rodotà.
Tanti *provider* in rete offrono la possibilità di usufruire dei propri servizi senza dover pagare alcuna somma come controprestazione, anche se, in realtà, la controprestazione è data dall'utilizzo di quei dati personali che si condividono con la piattaforma, che possono fruttare al gestore molto più in termini economici rispetto alla richiesta di corresponsione di un canone mensile e che talvolta possono costituire la base, seppur in forma anonimizzata, di inserzioni pubblicitarie mirate[58].
Gli utenti di tali piattaforme sono inclini a pubblicare materiali spesso contenenti dati sensibili nella consapevolezza che tali dati sono protetti, o comunque che saranno resi conoscibili ad una ristretta cerchia di persone.
Tali tipi di dati non dovrebbero essere utilizzati, neanche in forma anonimizzata, né da soggetti terzi, né allo stesso modo dal soggetto titolare del trattamento (ovviamente al di fuori dei casi in cui tali dati siano necessari per l'esecuzione l'oggetto del contratto), oppure utilizzati soltanto nel rispetto di garanzie determinate, in quanto godono giustamente di uno *status* privilegiato rispetto ai dati comuni, perché inerenti aspetti fondamentali della vita di ognuno, meritevoli di essere protetti in via primaria in quanto maggiore è il pregiudizio che il singolo può subire da un trattamento illecito delle relative informazioni.
Oltre all'aspetto relativo alla tutela della persona, difatti, non si deve dimenticare la prospettiva di utilizzo che dei dati possono fare le imprese nonché altri soggetti.
Le opportunità che offrono i *big data* sono infinite, e tra queste ve ne sono tante che possono essere di beneficio alla collettività.
Anche gli operatori economici, nel rispetto dei termini di legge, possono beneficiare di nuove *chance* per affinare i propri prodotti od anche per migliorare le proprie strategie comunicative.

[58] Molto evocativa a tale riguardo è l'esempio fornito da Eugeny Morozov in merito ai timori per la *privacy*, sopratutto dopo lo scandalo *NSA-gate*: *"Alcuni liquidano questi timori sostenendo che le nostre comunicazioni via email sono troppo personali per essere vendute come un prodotto commerciale. È vero. Eppure non abbiamo nulla da ridire se l'algoritmo di Google setaccia le nostre email per presentarci annunci pubblicitari mirati. È questa pubblicità personalizzata, che si basa sull'analisi e la classificazione immediata e automatica, a mantenere gratuito il raffinato e costoso sistema di posta elettronica di Google"*. Da un articolo pubblicato sul Frankfurter Allgemeine Zeitung, e tradotto in Italia da Internazionale, 6/12 settembre 2013, n. 1016, pag. 38.

Ma, allo stato attuale, un oligopolio di pochi grandi compagnie statunitensi gode di un vantaggio enorme rispetto a tutti gli altri soggetti presenti sul mercato e, tale potere derivante dalla grande quantità di dati raccolti, i *big data*, non è destinato a diminuire nel breve periodo, piuttosto ad aumentare[59].
La cooperazione internazionale in tal senso è indispensabile, considerato che tali aziende hanno a disposizione dati che le aziende nazionali possono ottenere magari a prezzi ridotti rispetto ai concorrenti europei, o magari possono avere a disposizione informazioni qualitativamente differenti.
Tali doverose preoccupazioni possono e debbono essere risolte anche mediante una collaborazione tra le istituzioni mondiali.
Governare il controllo delle operazioni di *data mining* è in pratica un'operazione impossibile, soprattutto in un ottica di prevenzione materiale, ma la necessità di disciplinare tale fenomeno, per tutti i motivi su descritti, si impone come necessaria per evitare che il *digital divide* già presente nell'attuale fase storica si trasformi ed evolva in un *data divide*, e che il singolo sia protetto da un uso dei dati personali non in linea con le sue reali volontà, o comunque non conforme al principio di autodeterminazione delle proprie scelte di vita.
D'altronde, anche i garanti riuniti a Varsavia, Polonia, per la 35° Conferenza Internazionale sulla Protezione dei Dati dei Garanti hanno sostenuto come: "*Realising that it is challenging to understand the complexities of the digital environment as information technology changes at rapid speed, the actors involved in this ecosystem and the business model on which it is based. Thus, users and policymakers are not in position to understand all the risks and all the opportunities for innovation and economic growth offered by digital technology*".

[59] E in quest'ottica la recente acquisizione di Whatsapp da parte di Facebook pare dare adito ancor maggiore a tali timori.