DIRITTO MERCATO TECNOLOGIA

INDICE DEL FASCICOLO N. 1
(gennaio – aprile 2016)

FOCUS
IL SISTEMA IMPOSITIVO NELL'ECONOMIA DIGITALE

BIG DATA E POTERE DI MERCATO
APPUNTO SUL CONTROLLO DELLE INFORMAZIONI

Gustavo Ghidini
Università di Milano

Marta Ghiglioni
Università di Milano

Anche in Europa è maturata la consapevolezza del mondo delle imprese e di quello delle istituzioni circa il "potere di mercato" conferito dalla raccolta e dal trattamento di dati personali, anche sensibili, di utenti acquisiti attraverso le reti web[1].

In particolare, per quanto riguarda i servizi della società dell'informazione, il potere sul mercato si costituisce attraverso la raccolta e l'aggregazione dei dati degli utenti nella misura in cui i dati stessi divengono base per l'erogazione di servizi ulteriori. La raccolta avviene attraverso l'offerta on-line di servizi, ora a pagamento ora a titolo (apparentemente: infra) gratuito, attraverso i quali raccolgono dagli utenti dati di diversa natura (personali, identificativi, dati di viaggio o informazioni relative a interessi e preferenze).

Il potere di mercato si genera così dal momento in cui molti di questi dati, una volta raccolti, entrano nella disponibilità di grandi compagnie[2],

Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.

[1] Attraverso Internet è, infatti possibile ottimizzare i meccanismi di raccolta, elaborazione e sfruttamento economico dei dati relativi a consumatori e clienti attuali o potenziali. I dati divengono sia strumento per prevedere e influenzare i comportamenti dei consumatori, sia vero e proprio "prodotto" offerto sul mercato. Come fu detto da M. Porter *"Internet technology provides better opportunities for companies to establish distinctive strategic positionings than did previous generations of information technology."* Porter, M. (2001), Strategy and the Internet, Harvard Business Review, March 2001.

[2] Di dimensione crescente grazie a funzioni come quelle che ha segnalato l'acquisto da parte di Facebook della piattaforma, leader della messaggistica istantanea, Whatsapp. Tali fusioni

rendendo difficile, se non impossibile per chi volesse fare il suo ingresso sul mercato, offrire servizi alternativi o comunque competitivi.

Questo nuovo tipo di competizione si basa, come si è sostenuto a Bruxelles[3], su due fattori: a) la diffusione tra gli utenti della piattaforma che raccoglie i dati; b) la quantità e natura dei dati che la piattaforma è idonea ad acquisire.

Sotto il primo profilo, il potere di mercato è caratterizzato dalla "*non replicabilità"*: i dati raccolti e aggregati per poter costituire potere di mercato devono essere acquisiti dalle imprese della società dell'informazione attraverso piattaforme che necessariamente dovranno raggiungere il medesimo grado di diffusione per offrire un servizio competitivo.

Per quanto invece attiene alla natura e alla quantità dei dati raccolti, il potere di mercato viene a costituirsi sulla base delle *privacy policies*: le imprese hanno frequentemente approfittato di una certa leggerezza degli utenti per raccogliere dati eccedenti le finalità del trattamento, o comunque ulteriori e non necessari all'erogazione del servizio offerto.

Va sottolineato un dato poco analizzato: la stessa acquisizione di potere di mercato può essere facilitata da abusi commessi ai danni dei consumatori. Ciò sia nell'ipotesi in cui i dati degli utenti, fonte del potere di mercato, fossero: a) raccolti o b) utilizzati (trattati) in modo non conforme alle normative nazionali ed europee.

Quanto al punto a) (fase di raccolta ed elaborazione), tra le diverse modalità con le quali i dati possono essere raccolti su internet, la registrazione attraverso "moduli (digitali)", cd. *forms*, è senz'altro il metodo più trasparente, poiché prevedendo che sia l'utente a immettere le proprie informazioni in appositi campi predisposti, garantisce che l'entità dei dati conferiti sia volontaria e consapevole. Tuttavia, questa modalità è oggi in corso di superamento: il tempo necessario a immettere le informazioni

permettono un grande accentramento di dati, difficilmente reperibili ed aggregabili allo stesso modo da soggetti i quali desiderino fare il loro ingresso sul mercato.

[3] Nel workshop del 2 giugno 2014 *"Privacy, Consumers, Competition and Big Data"* organizzato dall'European Data Protection Supervisor, Peter Hustynx, presso il Parlamento Europeo.

necessarie scoraggia gli utenti dal procedere nella registrazione. Si sono così creati meccanismi "rapidi" di registrazione, come la compilazione automatica dei moduli, predisposta dai browser, e la registrazione attraverso social network[4].

Se la prima soluzione risolve un'esigenza di rapidità, senza privare comunque l'utente della puntuale visione e possibile modifica dei dati conferiti in sede di registrazione, la seconda "aggira" l'utente, attingendo le informazioni richieste dal prestatore dei servizi direttamente da un account, come fosse un "contenitore" da cui attingere i dati necessari. Da compilazione manuale di diversi campi la registrazione diventa con questa modalità possibile con un unico "click" (o potremmo dire oggi "tocco", vista la diffusione di strumenti per la navigazione internet dotati di tecnologia *touchscreen*). Il diminuire di azioni necessarie a conferire i propri dati ingenera nell'utente l'impressione di compiere un'azione "banale" e pertanto poco importante.

La raccolta dati attraverso l'utilizzo di *forms* è solo uno dei metodi oggi esistenti e, per le ragioni illustrate pocanzi, uno dei meno efficaci per le aziende. Pensiamo, infatti, alla raccolta dati attraverso la tecnologia *cookies*[5], che permette di raccogliere informazioni riguardo la navigazione compiuta dall'utente in rete o tramite i social network, che sfruttando il desiderio degli utenti di comunicare, immagazzinano un gran numero di informazioni.

Ancora, i dati possono oggi essere raccolti attraverso applicazioni *mobile*, particolarmente efficaci nel rilevare non solo i luoghi visitati

[4] Ad esempio ciò avviene nella fase di registrazione della stragrande maggioranza delle piattaforme di commercio elettronico, tra le quali spicca per notorietà Amazon.it, ovvero a siti web dedicati a eventi, iniziative e prenotazioni di locali, tra i quali BlueNoteMilano.com. Lo stesso meccanismo viene adoperato anche da social network, quali ad esempio LinkedIn, Klout, e molti altri.

[5] Sono righe di testo usate per eseguire autenticazioni automatiche, tracciatura di sessioni e memorizzazione di informazioni specifiche riguardanti gli utenti che accedono al server, come ad esempio siti web preferiti o, in caso di acquisti via internet, il contenuto dei loro "carrelli della spesa".

"virtualmente" sulla rete ma anche i luoghi fisici dai quali gli utenti comunicano o per i quali chiedono, ad esempio, informazioni stradali.
Si pensi ai prestatori di servizi dell'informazione quali gestori di newsletter, di social network e di motori di ricerca come ad una scala in cui al crescere della quantità di dati trattati, diminuisce il tempo di conferimento e la sua percezione: un utente interessato a date informazioni di una rivista online compilerà un form con nome, cognome, email e, tendenzialmente in modo facoltativo, data di nascita o titolo di studio; un utente che entra a far parte di un social network comunicherà attraverso un form alcune informazioni di base, per poi continuare ad immettere dati sotto forma di comunicazione con i propri contatti, senza talvolta percepirli a pieno come conferiti e trattati dal social.

Tuttavia riferendosi ai social network è senz'altro l'utente a immettere dati su di una piattaforma, diversamente accade invece per i dati di navigazione[6]: non immettendo informazioni in spazi identificati come di "comunicazione", ma come di "navigazione", viene a mancare totalmente la consapevolezza non solo dell'utilizzo dei dati o del soggetto cui vengono conferiti, ma in generale dell'intera esistenza di un conferimento.[7]

---

[6] Come si legge nella stessa informative privacy del sito web dell'Autorità Garante per la protezione dei dati personali: «*I sistemi informatici e le procedure software preposte al funzionamento - dei siti web - acquisiscono, nel corso del loro normale esercizio, alcuni dati personali la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di Internet. Si tratta di informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti. In questa categoria di dati rientrano gli indirizzi IP o i nomi a dominio dei computer utilizzati dagli utenti che si connettono al sito, gli indirizzi in notazione URI (Uniform Resource Identifier) delle risorse richieste, l'orario della richiesta, il metodo utilizzato nel sottoporre la richiesta al server, la dimensione del file ottenuto in risposta, il codice numerico indicante lo stato della risposta data dal server (buon fine, errore, ecc.) ed altri parametri relativi al sistema operativo e all'ambiente informatico dell'utente*».

[7] Sul tema si muoveva la Direttiva 2009/136/CE, precisamente al considerando 66: «*Possono verificarsi tentativi da parte di terzi di archiviare le informazioni sull'apparecchiatura di un utente o di ottenere l'accesso a informazioni già archiviate, per una varietà di scopi che possono essere legittimi (ad esempio alcuni tipi di marcatori, «cookies») o implicare un'intrusione ingiustificata nella sfera privata (ad esempio software*

Per trarre maggiori utilità dai dati, una volta raccolti, è necessario procedere alla loro elaborazione. Compiendo operazioni di profilazione e aggregazione le aziende possono ottenere i c.d. *big data* [8].

Il Financial Times, nel 2013, ha stimato che i dati di mille individui abbiano un valore di mercato compreso tra 0,50$ e i 0,75$ [9], a seconda che riguardino informazioni generiche, come sesso, età o residenza, o che, invece, svelino interessi, avvenimenti importanti o ricorrenze. Nonostante

spia o virus). Conseguentemente è di fondamentale importanza che gli utenti siano informati in modo chiaro e completo quando compiono un'attività che potrebbe implicare l'archiviazione o l'ottenimento dell'accesso di cui sopra. Le modalità di comunicazione delle informazioni e di offerta del diritto al rifiuto dovrebbero essere il più possibile chiare e comprensibili. Eccezioni all'obbligo di comunicazione delle informazioni e di offerta del diritto al rifiuto dovrebbero essere limitate a quei casi in cui l'archiviazione tecnica o l'accesso siano strettamente necessari al fine legittimo di consentire l'uso di un servizio specifico esplicitamente richiesto dall'abbonato o dall'utente. Il consenso dell'utente al trattamento può essere espresso mediante l'uso delle opportune impostazioni di un motore di ricerca o di un'altra applicazione, qualora ciò si riveli tecnicamente fattibile ed efficace, conformemente alle pertinenti disposizioni della direttiva 95/46/CE. L'esecuzione di detti requisiti dovrebbe essere resa più efficace tramite i maggiori poteri conferiti alle autorità nazionali competenti».

Tuttavia per dare attuazione a questi principi ci si è limitati ad aggiungere ingombranti e fastidiosi banner, che disturbando la navigazione, spingono gli utenti ad accettare indiscriminatamente qualsiasi policy. L'unico paradossale risultato di questa Direttiva parrebbe essere oggi - in tutta Europa - un appesantimento della navigazione che porta gli utenti a percepire la privacy e il consenso al trattamento dei propri dati come inutili, macchinosi e fastidiosi.

[8] «*Big data refers to the exponential growth both in the availability and in the automated use of information: it refers to gigantic digital datasets held by corporations, governments and other large organizations, which are then extensively analyzed (hence the name: analytics) using computer algorithms. Big data can be used to identify more general trends and correlations but it can also be processed in order to directly affect individuals. With all its potential for innovation, big data may also pose significant risks for the protection of personal data and the right to privacy. How the general compatibility assessment and the specific provisions on 'further processing for historical, statistical or scientific purposes' can be applied to big data, including appropriate safeguards that may help data controllers meet the compatibility test, will be further discussed in Annex 2*.» Article 29 Working Party Opinion 03/2013 on purpose limitation p. 35

[9] Emily Steel, June 12, 2013 *Financial Times*

prezzi così apparentemente irrisori, va rilevato come il valore dei dati si accresca durante le operazioni di profilazione ed aggregazione, facendo proporzionalmente aumentare il potere di mercato che da essi deriva.

Quanto al punto b) (trattamento/utilizzazione), l'abuso potrebbe configurarsi qualora una impresa sfruttasse l'inconsapevolezza dell'utente per compiere trattamenti che non rispettino i principi fondamentali di *pertinenza*, *competenza* e *non eccedenza.*

Tale inconsapevolezza è spesso imputata alla negligenza dell'interessato. Ma le *privacy policies* non risultano di facile comprensione, sia per la loro eccessiva lunghezza, sia perché redatte, guarda caso, in un linguaggio giuridico poco accessibile. Si è calcolato che ogni utente avrebbe bisogno di 244 ore ogni anno, più della metà del tempo che normalmente passa su Internet, per leggere le policy privacy di ogni sito web che visita[10].

Peraltro, uno studio del 2012 ha rilevato come una gran parte delle applicazioni per smartphone, sempre più presenti nella quotidianità del consumatore, non richiedano affatto all'utente l'approvazione di alcuna informativa in materia di protezione dei dati personali.

In tali circostanze, l'utente non comprende quale uso sarà fatto dei suoi dati, lasciando alle imprese titolari la libertà di trattarli, sfruttando possibilità di impiego diverse da quelle per cui furono richiesti e comunicati dall'interessato. E così, pure, non essendo a conoscenza dei termini del trattamento, l'utente non potrà esercitare, o far esercitare dalle autorità di settore, le garanzie teoricamente previste.

Le conseguenze di tale opacità si traducono quindi in un aumento dei dati raccolti dalle imprese così come della possibilità di sfruttare i dati raccolti in misura pressoché sconfinata, anche offrendo servizi a pagamento basati sullo sfruttamento dei dati acquisiti tramite offerte "gratuite". E sfruttandoli a 360 gradi, senza limiti di mercati di destinazione specifici, ne consegue un potere di mercato di profilo *confidenziale*. Vantaggi competitivi, va sottolineato, conseguiti violando per più di un verso il *principio di non eccedenza* sancito dall'art 6 dalla Direttiva 95/46/CE [11].

[10] McDonald, A. M. and Cranor, L. F., 'The Cost of Reading Privacy Policies', A Journal of Law and Policy for the Information Society 2008, Privacy Year in Review, p.17

[11] Art 6. Gli Stati membri dispongono che i dati personali devono essere:

E così, dunque, ove da ciò consegua la costituzione o il rafforzamento di una posizione dominante, potrebbe dirsi non solo che l'effettivo sfruttamento di tali dati, a fini di *foreclosure* di concorrenti, rappresenti un abuso di detta posizione, bensì che si sia costituita una posizione dominante grazie ad un abuso dei diritti di privacy degli utenti (più esattamente: un abuso del diritto di libero esercizio di iniziativa economica in quanto compiuto in contrasto con i valori tutelati dall'art.41.2 co Cost., la tutela della "sicurezza e libertà umana" e più ampiamente della "utilità sociale" [categoria cui certamente si riconduce anche il godimento dei diritti di privacy dei cittadini]). L'abuso di dominanza si somma "a monte" alla costituzione o al rafforzamento della dominanza da abuso.

E si noti come, in considerazione della peculiarità di Internet, l'abuso della posizione dominante di colui che operi lo sfruttamento commerciale dei *big data* possa essere tale da determinare l'effetto escludente non solo nei confronti di imprese che operino nel settore di mercato direttamente concorrente (la commercializzazione dei *big data*, appunto) ma anche in ambiti merceologici differenti, ad esempio là dove l'accesso al mercato di questi operatori si intenda realizzare (anche o esclusivamente) mediante il commercio elettronico, che, nel mercato odierno, non può appunto

a) trattati lealmente e lecitamente;
b) rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri forniscano garanzie appropriate;
c) adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati e/o per le quali vengono successivamente trattati;
d) esatti e, se necessario, aggiornati; devono essere prese tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati;
e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.

prescindere dalla fruizione dei servizi pubblicitari che si fondino sul trattamento dei *big data.*

Su questo complesso fronte, che intreccia privacy e concorrenza, il diritto appare in ritardo. Sino ad oggi, quel mercato - e quel potere - sono stati individuati (come attesta la pronuncia della CGE rispetto al caso Google/DoubleClick)[12] in relazione alla massa e tipo di dati raccolti attraverso l'adesione degli utenti a servizi offerti a *pagamento,* non anche per il vasto e crescente mercato dei dati raccolti grazie all'adesione a offerte almeno apparentemente "gratuite". Apparentemente perché l'utente dà il proprio profilo, i dati personali, la sua "storia" sfruttabile per diverse utilizzazioni specie attraverso la profilazione dei dati.

In conclusione, e in via riassuntiva, il risultato di questa situazione è un doppio indebolimento: a) della tutela della privacy e dell'affidamento del consumatore, esposto a acquisizioni ed utilizzazioni non chiaramente conosciute e accettate dei suoi dati, usati anche per scopi diversi da quelli dichiarati; b) dell'azione antitrust, affievolita da una limitazione aprioristica, del tutto ingiustificata, della valutazione della eventuale situazione di dominanza e dello stesso "mercato rilevante" operata in relazione alla sola acquisizione di dati attraverso offerte a pagamento.

Tuttavia a Bruxelles si è anche rilevato che le politiche di protezione dei dati sono divenute recentemente nuovo strumento di competizione: offrire una maggiore protezione potrebbe infatti invogliare gli utenti a modificare le proprie abitudini in rete, prediligendo quelle aziende che offrano servizi nel modo più sicuro. Se da una parte, questa situazione potrebbe spingere il mercato a realizzare competizione riguardo a un miglioramento delle misure di sicurezza e di riservatezza dei dati degli utenti, dall'altra parte, ci si è chiesti se il mercato sia realmente in grado di realizzare tale tutela, o non sia invece opportuno un intervento normativo.

Giustamente, pertanto, lo *European Data Protection Supervisor* viene da tempo sollecitando una "*congiunta attenzione, ed una congiunta azione"* delle autorità di difesa della privacy, dei consumatori e della concorrenza

[12] Case No COMP/M.4731 – Google/ DoubleClick

onde rimediare a quella duplice situazione di debolezza di tutele poste a presidio di interessi collettivi e della persona.

È in quest'ottica che peraltro si muovono i più recenti provvedimenti delle autorità europee.

In particolare è già stato approvato il Capitolo V della proposta di Regolamento del Parlamento Europeo e del Consiglio in materia di tutela di trattamento e circolazione dei dati, il quale prevede che l'applicazione del regolamento sia territorialmente estesa al trasferimento dei dati personali di residenti nell'Unione effettuato da un responsabile[13] del trattamento terzo rispetto all'Unione. Oltre a definire una regolamentazione europea uniforme, tale previsione si pone come base per l'ampliamento delle tutele in ambiti regolamentari esterni all'Unione stessa.

Inoltre la Commissione europea si è recentemente dedicata al tema del *cloud computing*, rendendo disponibili le prime linee guida (*Service Level Agreement*) cui si sono obbligati gli operatori del settore. Tali SLA forniranno alcuni degli elementi chiave per uniformare i servizi, vincolando gli operatori ad adoperare una terminologia comprensibile e non ambigua nella contrattualistica[14].

Ma ancora, la Commissione europea, in un paper dello scorso luglio[15], occupandosi di *big data* e delle prospettive di applicazione di queste nuove tecnologie in una collaborazione tra PA e privati, ribadisce più volte come sia necessario che gli utenti di internet ed i cittadini europei acquistino fiducia nelle istituzioni e nelle imprese che utilizzeranno i dati.

Pur ritenendo doverosa questa evoluzione del sentire comune, come rilevato in precedenza, la malfidenza del cittadino nasce oggi da una mancanza di chiarezza, trasparenza e tutela.

Una soluzione può senz'altro essere quella di attuare un meccanismo di *notice and take down*, già più volte valutato da giurisprudenza e dottrina come situazione ottimale di compromesso tra esigenze di imprese dei servizi

[13] Equivalente in Italia del titolare del trattamento.

[14] Con particolare riguardo di alcuni punti fondamentali, tra cui: disponibilità e affidabilità del servizio cloud, livelli di sicurezza garantiti, oltre ad indicazioni su come gestire i dati nel cloud in maniera ottimale

[15] Commissione Europea, *Verso una florida economia basata sui dati*, etc etc

internet e tutela degli utenti della rete[16]. Attraverso tale tutela sarebbe possibile agli utenti, conosciuti i propri diritti, segnalare direttamente alle autorità garanti attraverso portali semplici e snelli, facilmente accessibili, gli abusi compiuti dalle imprese relativamente ai propri dati, permettendo di sanzionare le imprese che acquisiscano in modo non trasparente i dati e li riutilizzino non in conformità con i termini sottoscritti dagli utenti.

Pertanto, per quanto riguarda l'AGCM, appare opportuna una approfondita ricognizione della attività di raccolta e trattamento dei *big data* come fattore di costituzione e/o rafforzamento di posizioni dominanti, nonché di abusi delle medesime.

Altresì, è necessario che la stessa AGCM promuova una reciproca consultazione e collaborazione con APDP sulla falsariga di quanto EDPS propone sul piano comunitario, al fine di un'incisiva azione congiunta a tutela dei consumatori e degli utenti dei servizi della Società dell'Informazione.

[16] cfr. Regolamento AGCOM in materia di tutela del diritto d'autore sulle reti di comunicazione elettronica e procedure attuative ai sensi del d.lgs. aprile 2003, n. 7 (AGCOM Delibera n. 680/13/CONS del 12 dicembre 2013).