CONSUMERS' FORUM

PRESENTA

Consumerism 2017.
Decimo rapporto annuale.

"Dalla sharing alla social, alla data economy. Big data, fake news, privacy e pubblicità"

IN COLLABORAZIONE CON

ROMA TRE
UNIVERSITÀ DEGLI STUDI

CONSUMERS' FORUM

e

UNIVERSITÀ DEGLI STUDI ROMA TRE

presentano

CONSUMERISM 2017

Decimo Rapporto annuale

Dalla sharing alla social, alla data economy.

Big data, fake news, privacy e pubblicità

Il lavoro riflette esclusivamente le opinioni dei singoli Autori e non rappresenta le posizioni ufficiali di Consumers' Forum.

INDICE

Introduzione

I Consumatori nella *social economy* tra Big Data e *fake news* pag. 7

(Fabio Bassan – Maddalena Rabitti)

PUBBLICA AMMINISTRAZIONE **pag. 11**

(Maria Letizia Magno)

La gestione dei dati da parte della pubblica amministrazione: il difficile equilibrio tra trasparenza, *privacy* e sicurezza

1. Introduzione
2. Il contesto europeo e la politica del digitale
3. La pubblica amministrazione digitale in Italia
4. L'*eGovernment* nei rapporti con i cittadini: la trasparenza della PA
5. L'Autorità Nazionale Anticorruzione e il Garante della *Privacy*
6. La sicurezza delle banche dati pubbliche

ANAC **pag. 22**

(Cristiana Lauri)

PA – *e-procurement*

I dati e le informazioni nelle procedure di *e-procurement*

1. Il ruolo dell'ANAC e degli altri soggetti nel nuovo Codice dei Contratti Pubblici
2. La gestione dei dati nelle procedure di *e-procurement*
3. Gli effetti diretti sulle imprese e gli effetti indiretti sulla collettività

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO **pag. 29**

(Marco Cappai, Sara Perugini)

***Social economy* e tutela del consumatore: il ruolo dell'AGCM**

(Sara Perugini)

1. Premessa
2. Il valore economico dei Big Data nel diritto dei consumi
3. La sussistenza di un rapporto di consumo tra social media e utenti: gli interventi dell'AGCM nei confronti di WhatsApp
4. *Influencer Marketing*: il fenomeno e le iniziative assunte a livello internazionale
5. Segue: l'intervento dell'Autorità
6. *Fake news* e tutela del consumatore
7. Conclusioni

***Social economy*, gestione dei dati e tutela della concorrenza**

(Marco Cappai)

1. La rilevanza dei Big Data nel diritto della concorrenza: le questioni aperte e le iniziative sinora assunte dall'AGCM
2. Big Data e *Big Analytics*, profilazione e prezzi personalizzati: una possibile ipotesi di prezzi discriminatori ex artt. 102, lett. c) TFUE e 3, lett. c) legge n. 287/1990?
3. Abuso di sfruttamento ex artt. 102, lett. a) e 3, lett. a) legge n. 287/1990. Il caso avviato dal Bundeskartellamt contro Facebook
4. Conclusioni

AUTORITÀ DI REGOLAZIONE DEI TRASPORTI **pag. 49**

(Aldo Corvino, Paolo Occhiuzzi)

1. Gli utenti dei servizi di trasporto, tra Big Data e *fake news*, alla ricerca di un'Autorità *(Paolo Occhiuzzi)*
2. La gestione dei dati personali nel settore dei trasporti: problemi e prospettive *(Aldo Corvino)*
3. Big Data, trasporti e regolazione *(Paolo Occhiuzzi)*

AUTORITÀ PER L'ENERGIA ELETTRICA, IL GAS E IL SISTEMA IDRICO **pag. 59**

(Cristiana Lauri, Maria Chiara Sole)

I dati e le informazioni sui consumi energetici nel mercato *retail*

(Cristiana Lauri)

1. Gli interventi regolatori sui sistemi di *smart metering*
2. La gestione dei dati per lo sviluppo competitivo del mercato. Disintermediazione e soggetti coinvolti
3. Il valore dei dati e delle informazioni per il consumatore energetico nel paradigma della *social economy*

I Big Data nel settore delle risorse idriche

(Maria Chiara Sole)

1. I Big Data: una rapida evoluzione
2. Big Data e settore pubblico: la disintermediazione nella gestione dei Big Data dei servizi idrici
3. La tutela dell'utente finale nel settore idrico da parte dell'Autorità
4. Criticità e margini di miglioramento

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI **pag. 76**

(Valentina Angelini, Francesca Pellicanò, Rosaria Petti)

L'ecosistema digitale tra *fake news*, *hate speech* e *cyberbullismo*: l'intervento dell'Autorità per le garanzie nelle comunicazioni

I temi di interesse: le questioni all'attenzione del regolatore

1. I Big Data e i nuovi bisogni di protezione del cittadino digitale: stato dell'arte e questioni aperte *(Valentina Angelini)*
2. I fenomeni devianti del *web*: la responsabilità delle piattaforme e i poteri di intervento del regolatore *(Francesca Pellicanò)*
3. L'informazione *online* e il valore dei dati *(Rosaria Petti)*
4. I principi fondamentali applicati all'informazione *online* e l'inquadramento del fenomeno *fake news (Rosaria Petti)*

***Policy* regolatoria dell'Autorità per le garanzie nelle comunicazioni e soluzioni prospettiche**

1. Il ruolo dell'AGCom nella lotta alle principali problematiche legate all'utilizzo dei Big Data *(Valentina Angelini)*
2. L'evoluzione normativa in corso e la necessità di strumenti flessibili. Possibili scenari di intervento del regolatore *(Francesca Pellicanò)*
3. Potestà di intervento di AGCom nel contrasto alla diffusione di *fake news* e disinformazione *online (Rosaria Petti)*

BANCA D'ITALIA **pag. 94**

(Alfonso Affinito, Giorgia Biferali, Vincenzo Floccari)

I Big Data nel settore bancario: tra opportunità e rischi per i consumatori

(Antonio Affinito, Vincenzo Floccari)

1. Introduzione
2. La descrizione del fenomeno: i Big Data
3. Rischi ed opportunità derivanti dall'utilizzo dei Big Data nel settore bancario
4. La legislazione attuale e l'azione delle autorità

I Big Data nel *peer* to *peer lending* con e senza *bitcoin*
(Giorgia Biferali)

1. Premessa
2. Sistemi di informazione creditizia e tutela della *privacy*
3. *Peer to peer lending* e tutela della *privacy*
4. *Bitcoin peer to peer lending* e tutela della *privacy*

CONSOB **pag. 117**
(Francesco Della Rocca, Alfonso Ingenito)

Il mercato finanziario nell'era delle *fake news* e dei Big Data

Il ruolo della CONSOB nel "nuovo" fenomeno delle "*fake news*"
(Francesco Della Rocca)

I Big Data nelle attività e nei sevizi di investimento
(Alfonso Ingenito)

1. Premessa. Lo scambio di informazioni "alla" e "dalla" platea degli investitori
2. Lo scambio di informazioni "alla" platea degli investitori. L'obbligo di comunicazione al pubblico delle "informazioni privilegiate"
3. Lo scambio di informazioni "dalla" platea degli investitori: la profilatura del clienti nel regime della MiFID I
4. Big Data e FinTech: la Robo-advisory
5. Benefici e rischi dell'approccio "*data driven*" nei servizi di investimento

IVASS **pag. 130**
(Alessandra Camedda, Andrea Luberti)

Big Data e assicurazioni. Profilazione degli assicurandi e problemi di tutela della *privacy*

1. I profili di asimmetria informativa nel contratto di assicurazione *(Andrea Luberti)*
2. Le innovazioni legislative *(Andrea Luberti)*
3. Insurtech: la rivoluzione tecnologica nel settore assicurativo. L'approccio delle Authorities *(Alessandra Camedda)*
4. Profili di criticità: profilazione e tutela della *privacy*. Il nuovo Regolamento europeo in materia di protezione dei dati personali (Regolamento 2016/679/UE) *(Alessandra Camedda)*
5. Conclusioni *(Alessandra Camedda)*

PRIVACY **pag. 138**
(Angelica Saccoccio, Susanna Sandulli)

La *privacy* nella social *economy* fra Big Data e *fake news*

***Social economy* e Big Data, tra opportunità e minacce**
(Angelica Saccoccio)

1. La gestione dei Big Data. Il problema della condivisione delle informazioni
2. *Big Data* e nuove frontiere del *marketing*
1. Tra progressi tecnologici e tutela della *privacy*

***Fake news*: il mercato delle informazioni**
(Susanna Sandulli)

1. Il complesso fenomeno delle *fake news* e il ruolo del Garante per la protezione dei dati personali
2. I tentativi di regolamentazione a livello nazionale ed europeo
3. Utenti, operatori economici e *fake news*: quali tutele?

Gli Autori pag. 149

INTRODUZIONE

I Consumatori nella *social economy* tra Big Data e *fake news* *(Fabio Bassan, Maddalena Rabitti)*

Siamo giunti al decimo rapporto **Consumerism**. Dieci anni di studi al servizio dei consumatori e dei mercati. Una tradizione consolidata, fondata su uno sviluppo progressivo dell'attività di ricerca, sempre 'di frontiera', condotta affrontando in modo orizzontale i tradizionali silos regolatori verticali. Un grandangolo non deformante, è il compromesso che abbiamo ricercato in questi anni.

La ricerca di questo 'anniversario' si caratterizza per una continuità e una frattura. Si continua ad approfondire l'evoluzione dei mercati sulla base delle tecnologie e degli strumenti nuovi che la realtà digitale mette a disposizione dei consumatori, non solo delle aziende. Ma su questa linea la ricerca produce ora una crasi perché concentra l'esame su un profilo particolare; una prospettiva unica da cui osservare e valutare le evoluzioni. Per garantire un punto di osservazione solido la prospettiva ha bisogno di due fuochi (*big data* e *fake news*) che individuano un punto di fuga, diverso a seconda che si privilegi la libertà dei mercati o la democrazia; ed è amaro doverli considerare due estremi, ma non abbiamo l'ambizione di restituire l'immagine resa da Michelangelo nella Cappella Sistina con la Sibilla Cumana, in cui la contrapposizione e lo scontro delle masse trova una sintesi a suo modo armonica.

Questa scelta ci è apparsa necessaria per tentare di evitare l'effetto '*floating*' di chi è costretto a orientare la ricerca sulla base delle evoluzioni dei mercati. Tipico, questo, di chi studia la regolazione, che interviene quando gli eccessi evidenziano ciò che non necessita dimostrazione: i mercati non si autolimitano e oggi le forze contrapposte non sono simili o complementari. Ordini di grandezza separano le potenzialità delle imprese e le capacità di risposta dei consumatori e dei regolatori e non è solo asimmetria informativa. Questa divaricazione progressiva è in gran parte imputabile a un fattore di moltiplicazione rappresentato dalla capacità di alcune imprese di gestire una gran mole di dati e renderla disponibile in tempo reale per un numero potenzialmente illimitato di utilizzi. La scelta della prospettiva per la ricerca ci è apparsa dunque ovvia.

Acquisizione e gestione dei dati. Questo è il tema da cui muovere. Nei mercati troviamo enti e imprese che ottengono una mole di informazioni; alcuni sono anche in grado di gestirli, altri devono imparare. Ma il periodo di apprendimento non è consentito e comporta un arretramento inevitabile nel *tapis roulant* del mercato attuale, a velocità e pendenza crescenti. L'utilizzo dei dati dipende dalla finalità degli aggregatori: quelli che, ricordate, abbiamo individuato lo scorso anno come ragni nella tela (*web* questo significa, anche) e ci avevano indotto a qualificare non più *sharing* ma *social* l'economia digitale, dove le fonti di informazione si aggregano e scompongono con la velocità – controllata - di un *timelapse*. Attenzione poi ai ragni sociali, che non sono un ossimoro. L'uso può essere diretto o indiretto ad esempio, mediante vendita a terzi del dato grezzo o – più utilmente – di una sua modalità aggregata. La finalità può consistere nella penetrazione di un mercato, certo. Ma anche nella limitazione della capacità del concorrente, minandone la reputazione mediante diffusione di notizie verosimili. Con le *fake news*, il passaggio dai mercati alla politica è quasi inavvertito, e comporta conseguenze non affrontate perché solo parzialmente prevedibili.

Questa tensione - sul mercato ma ormai anche nella società - determina effetti diversi a seconda dell'autorità di settore che è costretta ad occuparsene, per gestire criticità attuali o prevenirne di potenziali. Le due principali autorità intersettoriali (Concorrenza e *Privacy*) hanno per vocazione e tradizione un approccio diverso su questo versante. Da un lato, il Garante per la protezione dei dati vede l'Europa staccarsi sempre più come un'isola alla deriva - in quella che si spera sia una fase congiunturale ma si teme sia un'evoluzione del ciclo storico - per la tutela dei dati personali, subordinati nel resto del mondo a una serie di condizioni, diverse a seconda della tradizione giuridica e del contesto geopolitico. Dall'altro lato, l'Autorità per la concorrenza non può ostacolare *newcomers* (per quanto grandi siano) che abbattono le barriere dei diversi mercati e aumentano le prospettive di concorrenza, potenziale almeno. A meno di considerare l'acquisizione e gestione dei dati un mercato a sé.

Nel mezzo, le Autorità di settore. Ciascuna studia, affronta il fenomeno e previene o combatte le patologie, diverse a seconda della tipologia dei prodotti e dei servizi regolati, della struttura del mercato, della sensibilità all'evoluzione tecnologica, della capacità degli operatori, della rigidità delle barriere all'ingresso (sul mercato certo, ma anche e soprattutto sul piano giuridico, delle autorizzazioni e licenze). Ciascuna autorità si aggrappa al proprio 'silos regolatorio' che però, all'inseguimento delle evoluzioni dei mercati – vere o false che siano - e della presunta economia reale, si

stacca progressivamente dal sistema delle norme e quindi, per quanto paradossalmente, per aumentare il livello delle garanzie (specifiche), rischia di ridurle (quelle generali); che le regole sono nulla senza sistema. Lo diceva nel secondo dopoguerra del '900 Carlo Schmid del diritto internazionale, utilizzando l'immagine della tela del ragno (appunto): che ferma gli insetti ma non può nulla contro le bombe. Il rischio è ancora maggiore in un sistema – quello europeo – ancora in mezzo al guado: la postazione più pericolosa da cui guardare la tempesta (e ormai purtroppo non abbiamo più bisogno dell'immaginazione). Sistema incompleto, in parte indefinito, immaginario, che invade i sistemi nazionali e poi si ritrae come un'onda, che definisce in dettaglio norme e scenari ma affida poi alle autorità una discrezionalità ampia di applicazione, se non anche di integrazione e la differenza è lasciata all'interpretazione, spesso. Con tutele e garanzie a geometria variabile in ragione (anche) dello stato membro in cui vengono (o meno) assicurate.

A metà, tra autorità e mercato, lo Stato. Superato in parte, da una costruzione sovranazionale claudicante e disintermediato in parte, nella produzione normativa, da un sistema delle fonti evoluto e una rete di regolatori organizzata ormai su base europea, lo Stato torna protagonista insospettato nel mercato. Da operatore si è trasformato rapidamente in questi anni in regolatore e poi in finanziatore (in conformità alle regole sugli aiuti di stato, *of course*), in garante e poi di nuovo in operatore, in una circolarità laica vichiana. E si, perché il principale detentore di dati personali è lo Stato. I meno avveduti se ne sono accorti ora con i modelli 730 precompilati. Ma è dal 2003 che la Commissione europea considera l'*eGovernment* un profilo centrale e strategico dello sviluppo dell'economia europea. Ed è qui che si avverte più forte la tensione tra trasparenza (su questo si concentra la recente riforma dell'*eProcurement* nel codice dei contratti pubblici e la conseguente azione dell'ANAC) e riservatezza dei dati, tra autonomia degli enti e uso funzionale dell'informazione, con la sicurezza informatica garanzia decisiva (al punto da ipotizzarsi un'agenzia europea); la fragilità delle banche dati è evidenziata quotidianamente da atti dimostrativi, per ora.

Veniamo all'attività delle Autorità. L'indagine ha seguito uno schema preciso, diretto a restituire omogeneità di analisi, per quanto possibile, consentire di individuare sovrapposizioni e lacune e metterle 'a sistema', proponendo soluzioni idonee e adeguate sulla base dell'analisi svolta. Partiamo dalle due 'intersettoriali' (AGCM e Garante Privacy) per proseguire con le Autorità di settore.

Responsabilità delle piattaforme online, profilazione degli utenti mediante l'impiego di tecnologie *Big Data* & *Big Analytics*, diffusione delle *fake news*, nuove strategie pubblicitarie come l'*influencer marketing*, (oggetto di linee guida specifiche negli Stati Uniti e nel Regno Unito, da cui originano specifiche '*advisory letters*' inviate a noti *influencers*), il valore economico delle informazioni generate o condivise dagli utenti (sul punto: la Commissione europea sull'acquisizione di WhatsApp da parte di Facebook), rappresentano i principali temi al centro dell'attività dell'AGCM per individuare un ruolo possibile del *public enforcement*. Ma la pubblicità occulta per l'*influencer marketing* e la pratica commerciale scorretta per le *fake news* sono strumenti che colgono solo in parte nel segno. Analogamente per le possibili applicazioni della disciplina sull'abuso di posizione dominante per l'uso dei dati profilati: oggi sono le condizioni tecniche, non più quelle economiche, il centro dell'azione. Misure comportamentali preventive, più che sanzioni *ex post*, servono quindi a ribilanciare il sistema, superando le asimmetrie del mercato. Ad oggi però, questi strumenti sono utilizzabili solo al verificarsi di determinati eventi (fusioni/acquisizioni) o comportamenti (abusi).

La *data driven innovation* è il punto di partenza dell'azione del garante dei dati, che ha adottato misure generali (Linee guida) e specifiche (Google). Ma sulla gestione dei dati i poteri del garante, nazionale ma anche europeo, sono ancora in parte impliciti. Né la recente riforma europea affida loro strumenti più adeguati. Certo, in sede di recepimento (per la direttiva) e di applicazione (per il regolamento) un margine di manovra resterebbe aperto, anche in considerazione del fatto che il coordinamento tra enti, autorità e imprese è indicato dal Garante uno strumento essenziale per reagire in tempo reale a violazioni o all'uso non corretto delle informazioni (*fake news*). La nozione stessa di dato personale e di identità digitale richiedono peraltro una revisione. L'indagine congiunta avviata dal Garante con AGCM e AGCom dovrebbe produrre risultati anche in questa direzione.

L'AGCom è in prima linea nell'affrontare i temi che nascono dall'uso delle tecnologie digitali: dalla protezione dell'utente e del cittadino, alla prevenzione e repressione dell'uso distorto dei dati e delle informazioni, sul piano non solo dei mercati ma anche della libertà di informazione, attiva e passiva (di essere informati correttamente). La disciplina sulla responsabilità delle piattaforme, che pure risale al 2010 (*notice and take down*) è strumento parzialmente idoneo, nei limiti di volumi contenuti, ma andrebbe integrato da un lato con le tipologie attuali (*social network* e piattaforme *on line*) non sempre riconducibili a quelle originarie (*mere conduit*, *caching e hosting*) e dall'altro con profili di responsabilità più incisivi che sanzionino eventuali inadempimenti, almeno nei casi più gravi. La Comunicazione della Commissione europea del 2016 sulle piattaforme on line e la successiva indagine conoscitiva dell'AGCom sono

un passo in questa direzione; l'impressione però è che il movimento verso una disciplina compiuta debba essere più rapido. Analogamente, in tema di *fake news* si attende la proposta della Commissione europea, che dovrebbe contemperare esigenze e interessi contrapposti; nel frattempo in alcuni paesi (Francia, tra tutti) avanza una disciplina di autoregolazione (di *fact checking*) sotto la vigilanza pubblica. L'AGCom propende per un intervento normativo che affidi all'autorità poteri specifici sul settore *on line*. Per il resto, il TUSMAR conferisce già all'AGCom potere di intervento a garanzia della correttezza dell'informazione nel rispetto del pluralismo. Di nuovo, la realtà muta prima non solo delle regole, ma anche delle scelte su quali utilizzare, tra *soft* e *hard law*.

La gestione dei dati è al centro anche delle evoluzioni nel sistema dei trasporti, che a parte poche aree di concorrenza 'nel mercato' è caratterizzato da una concorrenza 'per il mercato', con operatori che gestiscono in regime di monopolio il servizio messo a gara, e usufruiscono così di informazioni utili non solo per godere di una posizione privilegiata nella partecipazione alla gara successiva per il medesimo servizio (rimodulando l'offerta per rendere più efficiente il servizio), ma anche per profilare i clienti ottenendo informazioni ulteriori per campagne di *marketing* mirate. Questioni specifiche presenta poi l'evoluzione del servizio di trasporto non di linea, che ha ormai spostato la competizione sulle piattaforme tecnologiche, portando il legislatore e il regolatore ai confini delle competenze, territoriali e dei poteri attribuiti, rispettivamente. Da cui, l'esigenza di interventi sempre più armonizzati sul piano europeo, normativo (all'insegna della multimodalità) e regolatorio, mediante la rete delle autorità ormai consolidata sul trasporto ferroviario (IRG-rail). Ma come dimostrato da una ricerca specifica consegnata da *Consumers' Forum* all'ART sulle carte dei servizi nei trasporti, vi sono aree e ambiti ancora non aperti alle tutele, con resilienza minima, incapaci di sostenere un confronto con operatori in grado di acquisire e gestire dati. E qui, davvero, la debolezza delle barriere all'entrata del mercato digitale può essere utilizzata dall'Autorità per aprire alla concorrenza il mercato dei servizi reale, utilizzando i poteri a disposizione, ad esempio qualificando gli obblighi di servizio pubblico.

L'AEEGSI si trova ad affrontare questioni analoghe per i servizi energetici e idrici. Gli *smart metering* offrono numerosi vantaggi in termini di certezza, sicurezza e risparmio, ma pongono anche quesiti sulla concorrenza del mercato retail (*energy footprint*), che l'Autorità contribuisce a stimolare proprio avvalendosi delle piattaforme tecnologiche, utilizzate a tal fine, come messo in valore nel rapporto dello scorso anno. Tra le priorità dell'Autorità: l'accesso ai dati di consumo; la definizione dei requisiti funzionali dei misuratori di energia elettrica ("misuratori 2G"); la fatturazione sulla base dei consumi effettivi o delle autoletture. Il Sistema Informativo Integrato (SII), che consente una condivisione di talune informazioni e supera le vischiosità del sistema (ad esempio, nei passaggi dei clienti da un operatore a un altro) costituisce un *benchmark* da cui si potrebbe trarre spunto anche per settori diversi in cui si dovrebbe però, evidentemente, superare un'integrazione verticale ormai antistorica, frutto di un'impostazione antiquata che, per frenare la concorrenza nazionale, ha indebolito il sistema e reso le aziende facili prede di concorrenti più strutturati. Analogamente, per l'uso della tecnologia *blockchain* e la disciplina dei dati per la domotica. Il mercato si amplia e la concorrenza viene garantita da misure minimamente invasive.

In ambito bancario, assicurativo e finanziario la capacità di gestire i dati acquista un ruolo decisivo per la definizione del perimetro del mercato futuro e dei soggetti che vi operano. L'impressione è che in questi settori si giochi la partita più importante e decisiva: per la velocità del cambiamento, per l'arretratezza del comparto - provato da anni di crisi e dunque di bassi investimenti tecnologici - e per la sua frammentazione (da cui, l'assenza di standard tecnologici ampiamente condivisi, ma anche la scarsa condivisione delle informazioni), che ne evidenziano la resilienza minima in caso di concorrenza aggressiva. Peraltro questi mercati, soggetti a una disciplina normativa (di primo livello) e regolamentare – mediante gli interventi delle Autorità settoriali europee e nazionali, che indirizzano i mercati mediante atti tipici e atipici, produttivi di effetti giuridici, spesso anche vincolanti, di fatto – sperimentano per primi le potenzialità del nuovo approccio europeo, che da un lato reagisce in tempo reale alle dinamiche del settore e dall'altro rischia però di minare la certezza del diritto. Un punto d'incontro deve essere individuato rapidamente.

Le FinTech sono oggetto di studio di gruppi di lavoro congiunti cui partecipano anche Banca d'Italia, CONSOB, IVASS, ma non sono che un assaggio di quel che il mercato potrà fare, quando le *start up* di settore saranno sostituite (o meglio, secondo il capitalismo anglosassone) acquisite dai grandi *players*. Un certo grado di sostituzione tra gli operatori tradizionali e quelli *web native* esiste già ora, ma va rapidamente crescendo: Alibaba ha costituito un proprio circuito di pagamento (Alipay) superando in pochi mesi la soglia dei 400 milioni di clienti. E così Amazon, che ha costituito una propria piattaforma per i prestiti ai rivenditori (*Amazon lending*); Paypal con *working capital*, ecc.... Si riduce proporzionalmente la capacità delle autorità di garantire un controllo adeguato, nella fase sia iniziale, di autorizzazione, sia di operatività e soprattutto, di sanzione, in un ambiente che non ha limiti territoriali quanto alla fornitura dei servizi, e ne ha – ma nei confini dell'Unione – quanto ai poteri di controllo. Le linee guida pubblicate da BCE a settembre

mirano a garantire il cd. *level playing field*, ma anche a promuovere l'utilizzo di questi strumenti da parte delle banche.

Nel settore bancario ci si concentra ora principalmente sui temi della *privacy*, dei servizi a distanza e della *governance* dei prodotti. Il sistema bancario più degli altri soffre il dilemma della transizione. Ancora forte è l'attenzione su temi classici di riservatezza dei dati personali: ne è prova l'ampio filone di decisioni dell'Arbitro bancario finanziario sul problema delle banche dati e delle segnalazioni in centrali rischi, sia private sia in quella gestita da Banca d'Italia, che precludono l'accesso al credito quando si tratta di segnalazioni negative. Ed ecco che nella gestione di queste banche dati occorre considerare interessi diversi, che meritano tutela ma che è difficile bilanciare senza assumere scelte di fondo che coinvolgono il mercato del credito e la persona.

Già vecchio, quasi, il tema dei *bitcoins*, e più in generale delle monete virtuali, che Banca d'Italia monitora attentamente con le altre Autorità europee, ma che ancora una volta pone un problema di dati, oltre che di legalità. Piuttosto, nel *deep web* chi gestisce i dati? Chi garantisce i diritti?

La ricerca di equilibrio tra diritti e tecnologia è poi del tutto evidente nella *product governance*. Si inizia con il garantire contenuti e modalità con cui vengono forniti. La possibilità di profilazione puntuale rende peraltro questi prodotti 'orizzontali' rispetto ai silos regolatori 'verticali', e pone un tema di disciplina applicabile, su cui a tutt'oggi non v'è condivisione.

Nel mercato assicurativo, una profilazione così puntuale rischia anche di pregiudicare le stesse basi del sistema mutualistico, che si aggiungono alle asimmetrie tipiche e specifiche dei contratti di assicurazione, che la recente riforma nazionale (nella legge sulla concorrenza, n. 124 del 4 agosto 2017) tenta di ridurre. L'attuazione della legge da un lato, e del Regolamento UE in materia di protezione dei dati personali (2016/679/UE) assume pertanto nel settore un rilievo decisivo. L'impegno delle aziende del settore verso un più radicale uso della tecnologia appare più consapevole rispetto al mercato bancario. Nell'ottica di una integrazione tra i due settori, questo può essere un indizio, se non una prova.

Nei mercati finanziari, al documento per la consultazione del 2016 sull'uso dei *big data* nelle istituzioni finanziarie ha fatto seguito in Italia il recepimento delle direttiva MAR e MIFID II, che hanno aumentato i vincoli informativi a tutela degli investitori, anche in relazione alla profilatura di questi ultimi e alla comunicazione delle 'informazioni privilegiate'. L'applicazione specifica nel settore delle Fintech viene affrontata sul piano della *digital advise* e dell'attività dei *robo-advisors*. L'impressione è che si sia ancora lontani da una comprensione del fenomeno nella sua complessità, manifestandosi questo ogni volta con forme diverse e parziali. Da cui, la difficoltà di una regolazione, sul piano europeo ancor prima che nazionale. Si vedrà se la flessibilità normativa e regolatoria tipica dei mercati ESAs sarà sufficiente per consentire di prevenire o almeno reprimere efficacemente eventuali violazioni o distorsioni.

Certo, nel frattempo spetta in primo luogo alle *Authorities* lavorare per l'educazione del consumatore. L'educazione diviene sinonimo di autonomia e responsabilità delle scelte. E l'autonomia delle scelte di mercato è essenziale per contrastare le spinte alla classificazione, alla sorveglianza e in ultima analisi alla profilazione (almeno) della nostra identità.

Stefano Rodotà già qualche anno fa ammoniva: "*le reti sociali nascono dall'idea di cercare il modo migliore per sfruttare economicamente l'iperconnessione di milioni di persone che generano altrettanti milioni di dati. Bisogna discutere sulle pre-condizioni della democrazia sul web a fronte della rapidità dell'innovazione tecnologica. Il controllo dei poteri sociali da parte dei big del web è una discussione aperta e non va dimenticato il concetto di diritti dei nuovi popoli del web*". E dunque? Il filo che unisce *big data* e *fake news* è la conoscenza, che ancora Rodotà qualifica come la via per acquisire non solo valore aggiunto sul mercato, ma anche la libera costruzione della personalità di ciascuno di noi.

PUBBLICA AMMINISTRAZIONE

(Maria Letizia Magno)

La gestione dei dati da parte della pubblica amministrazione: il difficile equilibrio tra trasparenza, *privacy* e sicurezza

*Il settore nel quale l'utilizzo delle moderne tecnologie ha mostrato sin da subito il suo potenziale ruolo di motore del rilancio economico è stato quello pubblico. Già nel 2003 la Commissione ha considerato l'*eGovernment *quale ambito centrale e strategico dell'intera economia europea. Il legislatore italiano, seguendo gli indirizzi europei, ha avviato dal 2005 una serie di riforme volte a realizzare la digitalizzazione degli apparati pubblici. In particolare il c.d. FOIA introduce un nuovo concetto di trasparenza dell'agire pubblico. L'attuazione di detto principio richiede però particolare cautela da parte delle PA nella gestione dei dati e dei documenti oggetto di trasparenza. Mentre sembra adeguatamente garantito il bilanciamento di interessi tra pubblicità e tutela della riservatezza, numerose possibili violazioni dei diritti fondamentali potrebbero invece verificarsi sul fronte della sicurezza cibernetica.*

SOMMARIO: 1. INTRODUZIONE. – 2. IL CONTESTO EUROPEO E LA POLITICA DEL DIGITALE. – 3. LA PUBBLICA AMMINISTRAZIONE DIGITALE IN ITALIA. – 4. L'*EGOVERNMENT* NEI RAPPORTI CON I CITTADINI: LA TRASPARENZA DELLA PA. – 5. L'AUTORITÀ NAZIONALE ANTICORRUZIONE E IL GARANTE DELLA *PRIVACY*. – 6. LA SICUREZZA DELLE BANCHE DATI PUBBLICHE.

1. INTRODUZIONE

Negli ultimi dieci anni l'umanità ha prodotto più dati di quanto non abbia fatto nella sua intera storia[1]. I dati personali sono solo una parte delle informazioni che quotidianamente vengono prodotte e trattate, e rappresentano indubbiamente la parte più significativa, specialmente quando vengono utilizzate dalle amministrazioni pubbliche. Ad oggi, infatti, la gestione dell'informazione detenuta dal soggetto pubblico viene esteriorizzata per dar conto dell'agire amministrativo e per contribuire allo sviluppo socio-economico della comunità. Le pubbliche amministrazioni sono destinate a diventare i più importanti centri di aggregazione ed elaborazione dei dati dei cittadini: questo enorme *database* di informazioni, tuttavia, solleva numerosi dubbi sia per quanto riguarda la possibilità di una perdita di democrazia e libertà sia per ciò che attiene alla sicurezza pubblica e individuale. Si rischia, da un lato, che i cittadini vengano identificati, profilati, rielaborati e, dall'altro, che i relativi dati in uso alle pubbliche amministrazioni vengano a queste sottratti e

[1] "Nel 2003 i ricercatori della School of Information Management and Systems di Berkeley hanno stimato che l'umanità abbia accumulato approssimativamente 12 *esabyte* di dati un *esabyte* corrisponde a 1018 *byte*, ovvero a un dvd lungo 50.000 anni, nel corso della sua storia fino alla commercializzazione dei computer. Tuttavia, hanno anche calcolato che i mezzi di immagazzinamento a stampa, su pellicola, magnetici e ottici, hanno già prodotto più di 5 *esabyte* di dati soltanto nel 2002. (…) Secondo uno studio più recente, tra il 2006 e il 2010 la quantità globale di dati digitali è cresciuta più di sei volte, da 161 esabyte a 988 *esabyte*". Cfr., L. Floridi, *La rivoluzione dell'informazione*, Torino, 2012. 6-7.

sfruttati per scopi molto diversi dal benessere della comunità. Per bilanciare gli interessi economici intorno alle infinite possibilità di sfruttamento dei dati personali degli utenti e rispettarne i fondamentali diritti di libertà, occorre non solo una forte politica di protezione in tema di riservatezza ma soprattutto in materia di sicurezza pubblica dei sistemi di gestione e conservazione di detti dati. Il processo di trasformazione digitale della pubblica amministrazione, di cui si da conto nel presente contributo, se da un lato favorisce l'efficienza e l'efficacia dell'agire pubblico traducendosi in un miglioramento dei servizi ai cittadini, dall'altro comporta per la stessa amministrazione un maggior grado di responsabilità nella tutela dei privati, in considerazione della maggiore vulnerabilità dei sistemi informatici di gestione dei dati rispetto ai "vecchi" archivi cartacei.

2. IL CONTESTO EUROPEO E LA POLITICA DEL DIGITALE

Sin dalla Strategia di Lisbona del 2000 il ricorso alle moderne tecnologie digitali[2], specie nel settore pubblico, è stato considerato la miglior risorsa spendibile per il rilancio dell'economia europea[3]. Da allora, le istituzioni europee hanno mostrato crescente attenzione nei confronti della società dell'informazione, basata sulle tecnologie della comunicazione e grazie ad esse in grado di produrre conoscenza e ricchezza in modo veloce, economico e sostenibile. Per la creazione dell'Europa digitale sono stati adottati negli anni numerosi piani di azione[4] e attualmente si assiste alla realizzazione della Strategia Europa 2020[5].

La politica del digitale, benché non espressamente contemplata nel Trattato sul funzionamento dell'Unione europea, appare il presupposto per il raggiungimento degli obiettivi in, praticamente, tutti gli ambiti di politica europea.

Nel 2003 la Commissione ha elaborato la Comunicazione "*Il ruolo dell'eGovernment*[6] *per il futuro dell'Europa*", con-

---

[2] Il linguaggio digitale è quel linguaggio basato sul codice binario, composto dei numeri 0 e 1, ed è il linguaggio utilizzato da tutte le apparecchiature elettroniche che, in quanto basate su tale linguaggio, vengono a loro volta definite digitali esse stesse. Digitale è, dunque, lo strumento e, contemporaneamente, l'apparecchio che utilizza tale strumento nonché il prodotto realizzato dall'apparecchio. Il digitale, unito all'infrastruttura internet, rendono possibile il collegamento e la messa in rete di tutti i dati e generano, a loro volta, dati. Internet è il luogo della terra dove si parla la lingua digitale. Sull'utilizzo del termine digitale nell'ambito della riforma della pubblica amministrazione, cfr., B. Carotti, *L'amministrazione digitale: le sfide culturali e politiche del nuovo Codice*, in *Giorn. dir. amm.*, 1, 2017, 7 ss.

[3] La Strategia di Lisbona è stata adottata dal Consiglio Europeo in Data 23 e 24 marzo del 2000 con l'obiettivo di creare entro il 2010 un'economia della conoscenza europea che fosse la più competitiva e dinamica del mondo e in grado di realizzare una crescita economica sostenibile con nuovi e migliori posti di lavoro e una maggiore coesione sociale. La prima iniziativa di *eEurope* della Commissione europea risale al dicembre 1999.

[4] "La spiegazione all'utilizzo di un detto metodo (i Piani di azione) potrebbe essere ricercata non solo nella peculiarità della materia, ma anche (e probabilmente soprattutto nella prima fase di costruzione della politica di *eEurope*) nella mancanza delle basi giuridiche idonee a consentire alle Istituzioni una regolazione più specifica", cfr. C. Leone, *Il ruolo del diritto europeo nella costruzione dell'amministrazione digitale*, in *Riv. it. dir. pub. com.*, 3-4, 2014, 868.

[5] La Strategia Europa 2020 è stata elaborata dalla Commissione europea con lo scopo di garantire una crescita economica intelligente, sostenibile e inclusiva, al fine di rilanciare l'economia europea e di porre rimedio alla crisi che in soli due anni ha "cancellato un ventennio di risanamento del bilancio". La Strategia si compone di sette "Iniziative Faro" tra le quali è compresa l'Agenda digitale, che mira a stabilire il ruolo chiave delle tecnologie dell'informazione e della comunicazione nel raggiungimento degli obiettivi 20/20/20. In particolare, l'agenda digitale europea individua sette aree tematiche nelle quali intervenire: mercato digitale unico e dinamico; interoperabilità e standard; fiducia e sicurezza; accesso ad internet veloce e superveloce; ricerca e innovazione; alfabetizzazione, competenze e inclusione nel mondo digitale; vantaggi offerti dalle ITC nelle società dell'UE. Per ciascuna area tematica vengono chiariti gli specifici obiettivi da raggiungere e indicate le azioni da svolgere per il loro positivo raggiungimento. Cfr., Comunicazione della Commissione europea, Bruxelles 3 marzo 2010, COM (2010) 2020, *Europa 2020. Una strategia per una crescita intelligente, sostenibile e inclusiva*, in *http://eur-lex.europa.eu/legal-content/it/ALL/?uri=CELEX%3A52010DC2020.*

[6] La Comunicazione chiarisce che per *eGovernment* si intende: "l'uso delle tecnologie dell'informazione e della comunicazione

siderato l'ambito centrale e strategico dell'intera economia europea[7]. L'*eGovernment* garantirebbe un miglioramento dei servizi ai cittadini con conseguente aumento della qualità della vita; un miglioramento dei servizi alle imprese promuovendo la competitività, e un aumento dei servizi tra amministrazioni rafforzandone la cooperazione. Più di recente l'*eGovernment* **è stato considerato uno degli ambiti applicativi –** in specie quello più importante e determinante – di realizzazione delle *smart cities*[8], intese come lo spazio fisico integrato con i soggetti che le abitano, in grado di offrire un'elevata qualità della vita e di favorire la crescita personale, sociale ed economica dei cittadini[9].

3. LA PUBBLICA AMMINISTRAZIONE DIGITALE IN ITALIA

Seguendo gli indirizzi europei, il legislatore italiano sin dal 2005 ha avviato un processo di riforma della pubblica amministrazione con lo scopo di favorire la realizzazione dell'*eGovernment*. Da allora gli interventi legislativi si sono susseguiti senza sosta e ancora oggi, a distanza di oltre 12 anni, tale processo non solo non può dirsi compiuto ma è stato di recente interamente riprogrammato. Infatti, il codice dell'amministrazione digitale, di cui al d.lgs. n. 82 del 7 marzo del 2005 è stato modificato – anche in ossequio agli indirizzi europei –, dapprima, con il d.lgs. n. 235 del 30 dicembre 2010, e da ultimo con il d.lgs. n. 179 del 26 agosto del 2016. *Medio tempore* si sono succeduti una serie di decreti, volta a volta dedicati alla semplificazione, alla crescita, al fare e alla trasparenza amministrativa, che a vario titolo hanno inciso su alcuni aspetti specifici del processo di digitalizzazione dell'apparato amministrativo[10].

Nel 2015 con l'adozione della legge delega n. 124 per la riorganizzazione dell'apparato amministrativo si è dato avvio ad un progetto organico di riforma con lo scopo di semplificare e coordinare tra loro i vari provvedimenti stratificatisi nel corso degli anni. La riforma più che introdurre nuovi istituti interviene in massima parte su discipline già esistenti al fine di garantirne un'efficace applicazione. Essa non incide soltanto sul codice dell'amministrazione digitale la cui delega **è contenuta all'art. 1, comma 1,** bensì sull'intero sistema amministrativo, spaziando dalla conferenza dei servizi, al riordino delle camere di commercio, passando attraverso la disciplina del lavoro pubblico, delle partecipazioni societarie

---

nelle Pubbliche Amministrazioni, coniugato a modifiche organizzative e all'acquisizione di nuove competenze al fine di migliorare i servizi pubblici e i processi democratici e di rafforzare il sostegno alle politiche pubbliche". Cfr., Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni, *Il ruolo dell'eGovernment per il futuro dell'Europa*, del 26.09.2003.

[7] Si legge nella Comunicazione che: "Il settore pubblico è chiamato a svolgere un ruolo di primo piano nella modernizzazione dell'economia e della società europee, affinché l'Europa sia più competitiva e dinamica, caratterizzata da una crescita sostenibile ed in grado di aumentare la quantità e la qualità dei posti di lavoro e di rafforzare la coesione sociale".

[8] Il termine *smart cities* compare ufficialmente per la prima volta nel 2011 con l'iniziativa *Smart cities and communities* avviata dall'Unione europea allo scopo di ottimizzare l'utilizzo delle risorse energetiche nelle città. Nel 2014 il Parlamento europeo ha pubblicato il documento *Mapping smart cities in the EU* nel quale chiarisce che affinché si possa parlare di *smart city* come sistema integrato di ambienti intelligenti, devono essere considerati i seguenti ambiti di intervento: *Governance*; *Economy*; *Mobility*; *Environment*; *People*; *Living*. La concreta realizzazione di una città *smart* deve sviluppare contemporaneamente e in maniera integrata tra loro, tutti i predetti ambiti.

[9] Cfr. Commissione Europea, Comunicazione della Commissione, *Smart Cities and communities – European Innovation Partneship*, Bruxelles, 10.07.2012, 4701, reperibile al seguente indirizzo: *http: //ec.europa.eu/Energy/technology/initiatives/doc/2012_4701_smart_cities_en.pdf*.

[10] Si tratta, in particolare del: d.lgs. n. 5 del 2012, c.d. decreto "semplificazione", recante disposizioni urgenti in materia di semplificazione e di sviluppo, convertito nella L. n. 35/2012 la quale istituisce l'Agenda Digitale Italiana; d.lgs. n. 83 del 2012, c.d. decreto "crescita", recante misure urgenti per la crescita del paese, convertito nella legge n. 134 del 2012 la quale ha stabilito il subentro dell'Agenzia per l'Italia Digitale alla DigitPA; d.lgs. n. 179 del 20120, c.d. decreto "crescita 2.0", recante ulteriori misuri urgenti per la crescita del paese, convertito nella legge n. 221 del 2012, la quale introduce numerosi istituti volti a raggiungere gli obiettivi europei in tema di *eGovernment* (il documento digitale unificato, la carta di identità elettronica, la tessera sanitaria, l'anagrafe nazionale della popolazione residente e il sistema pubblico di connettività); d.l. n. 69/2013, c.d. decreto "del fare", recante disposizioni urgenti per il rilancio dell'economia e, da ultimo, del d.l. n. 90/2014 recante misure urgenti per la semplificazione e la trasparenza amministrativa e per l'efficienza degli uffici giudiziari.

nelle pubbliche amministrazioni, della dirigenza pubblica e della prevenzione della corruzione e tutela della trasparenza amministrativa; nel complesso la legge contiene ventotto deleghe dalle quali sono attualmente derivati venti decreti attuativi[11]. L'ampiezza e l'eterogeneità delle diverse deleghe conferite ha suscitato molteplici dubbi interpretativi sulla bontà della Riforma[12], richiedendo in ultima istanza l'intervento della Corte Costituzionale la quale, con sentenza n. 125 del 25 novembre 2016, da un lato ha dichiarato l'illegittimità costituzionale degli artt. 11, 17, 18 e 19 della legge delega, dall'altro ha ritenuto legittimi i principi e i criteri di cui all'art. 1, lett. b), c) e g)[13].

Nonostante l'ampiezza della delega, la riforma non esaurisce il processo di realizzazione dell'*eGovernment*, così come il nuovo codice non esaurisce il sistema delle fonti dell'amministrazione digitale. Infatti, quanto ai rapporti con le imprese, ad esempio, mentre alcune norme di carattere generale sono contenute nel CAD[14], la completa realizzazione del

---

[11] Alla Data del 27 luglio 2017 risultano emanati i seguenti decreti attuativi (elencati secondo l'ordine delle deleghe e non in ordine cronologico): d.lgs. 26 agosto 2016, n. 179, Modifiche ed integrazioni al Codice dell'amministrazione digitale; d.lgs. 30 giugno 2016, n. 127, Norme per il riordino della disciplina in materia di conferenza di servizi; d.lgs. 30 giugno 2016, n. 126, Attuazione della delega in materia di segnalazione certificata di inizio attività; d.lgs. 25 novembre 2016, n. 222, Individuazione di procedimenti oggetto di autorizzazione, segnalazione certificata di inizio di attività (SCIA), silenzio assenso e comunicazione e di definizione dei regimi amministrativi applicabili a determinate attività e procedimenti; d.lgs. 25 maggio 2916, n. 97, Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione, pubblicità e trasparenza; d.lgs. 4 agosto 2016, n. 169, Riorganizzazione, razionalizzazione e semplificazione della disciplina concernente le Autorità portuali; d.lgs. 19 agosto 2016, n. 177, Disposizioni in materia di razionalizzazione delle funzioni di polizia e assorbimento del Corpo forestale dello Stato; d.lgs. 27 febbraio 2017, n. 43, Riorganizzazione delle amministrazioni pubbliche, concernente il Comitato italiano Paralimpico; d.lgs. 29 maggio 2017, n. 95, Disposizioni in materia di revisione dei ruoli delle Forze di polizia; d.lgs. 29 maggio 2017, n. 97, Disposizioni recanti modifiche al decreto legislativo 8 marzo 2006, n. 139, concernente le funzioni e i compiti del Corpo nazionale dei vigili del fuoco; d.lgs. 29 maggio 2017, n. 98, Razionalizzazione dei processi di gestione dei dati di circolazione e di proprietà di autoveicoli, motoveicoli e rimorchi, finalizzata al rilascio di un documento unico; d.lgs. 25 novembre 2016, n. 219, Riordino delle funzioni e del finanziamento delle camere di commercio, industria, artigianato e agricoltura; d.lgs. 20 giugno 2016, n. 171, Attuazione della delega di cui all'articolo 11, comma 1, lettera p), della legge 7 agosto 2015, n. 124, in materia di dirigenza sanitaria; d.lgs. 25 novembre 2016, n. 218 Semplificazione delle attività degli enti pubblici di ricerca; d.lgs. 20 giugno 2016, n. 116, Modifiche all'articolo 55 *quater* del decreto legislativo 30 marzo 2001, n. 165, in materia di licenziamento disciplinare; d.lgs. 25 maggio 2017, n. 74, Modifiche al d.lgs. 27 ottobre 2009, n. 150; d.lgs. 25 maggio 2017, n. 75, Modifiche e integrazioni al decreto legislativo 30 marzo 2001, n. 165, in materia di riorganizzazione delle amministrazioni pubbliche; d.lgs. 19 agosto 2016, n. 175, Testo unico in materia di società a partecipazione pubblica; d.lgs. 16 giugno 2017, n. 100, Disposizioni integrative e correttive al decreto legislativo 19 agosto 2016, n. 175, recante testo unico in materia di società a partecipazione pubblica; d.lgs. 26 agosto 2016, n. 174, Codice di giustizia contabile e d.lgs. 22 gennaio 2016, n. 10, Modifica e abrogazione di disposizioni di legge che prevedono l'adozione di provvedimenti non legislativi di attuazione. Cfr., www.parlamentoitaliano.it.

[12] "Alla eterogeneità delle materie – che non è una buona cosa per una legge – si aggiunga la lunghezza delle regole adottate che dilagano in commi ed articoli interminabili (l'articolo più lungo occupa ben 5 pagine della Gazzetta Ufficiale) e si dipanano in un precipitare di proposizioni subordinate e coordinate che troppo spesso costringono il lettore a ritornare, anche più volte, sui suoi passi per trovare il filo di quel discorso legislativo che, secondo il saggio ammonimento di Tommaso Campanella, dovrebbe essere "breve e chiaro" così, I. F. Camazza, *Le regole dell'azione amministrativa: dalla L. 7 agosto 1990 n. 241 alla L. 7 agosto 2015 n. 124*, in *Dir. amm.*, 2, , 2015, 570; Cfr., inoltre, B. G. Mattarella, *Il contesto e gli obiettivi della riforma*, in *Giorn. dir. amm.*, 5, 2015, 621 ss.; G. Melis, *Una buona legge e molto da* fare, in *Giorn. dir. amm.*, 5, 2015, 581.

[13] Sul giudizio di legittimità avente ad oggetto una legge delega la Corte precisa che "non si riscontrano ostacoli all'esame nel merito delle censure promosse, per il sol fatto che esse sono contenute in una legge delega (…) la legge di delegazione, in quanto atto avente forza di legge, non si sottrae, ai sensi dell'art. 134 Cost., al controllo di costituzionalità in via principale, di cui può divenire oggetto, quando sia possibile riscontrare una lesione dell'autonomia regionale", cfr., Sent. Corte Cost. n. 125 del 26 novembre 2016 in *www.pluriscedam.it*. Sul riparto di competenze e sul valore dell'intesa come strumento di raccordo tra Stato e Regioni, cfr., B. G. Mattarella, *Delega legislativa e principio di leale collaborazione*, in *Giorn. dir. amm.*, 2, 2017, 179 ss.; A. Spadaro, *La pericolosa anomalia della "contrattazione" Stato-Regioni: una storia senza fine,* in *www.federalismi.it,* 28 agosto 2013. Sulla portata innovativa della sentenza in merito all'ambito di applicazione del principio di leale collaborazione, anche nella prospettiva delle fonti del diritto cfr., R. Bifulco, *L'onda lunga della sentenza 251/2016 della Corte costituzionale*, in *www.federalismi.it*, 1 febbraio 2017. Cfr., inoltre, J. Marshall., *La Corte costituzionale, senza accorgersene, modifica la forma di Stato?*, in *Giorn. dir. amm.*, 6, 2016, 705 ss.; G. D'Amico, *Il seguito della sentenza 251/2016 della Corte costituzionale tra "suggerimenti", "correzioni" e nuove impugnative*, in *Giorn. dir. amm.*, 3, 2017, 287 ss.

[14] Ci si riferisce, ad esempio, all'art. 5-*bis* rubricato "Comunicazioni tra imprese e pubblica amministrazione", introdotto con il d.lgs. n. 235

c.d. *eProcurement*[15] *è invece affi*data al nuovo Codice dei Contratti Pubblici[16] che, nella sua versione vigente non risulta affatto coordinato con le disposizioni generali di cui al CAD stesso[17].

Quanto, invece, al rapporto con i cittadini, la nuova disciplina della trasparenza amministrativa non si rinviene all'interno del CAD bensì nel c.d. *Freedom of information act*, adottato con d.lgs. 25 maggio 2016, n. 97, ai sensi dell'art. 7 della legge delega 124/2015, il quale integra e modifica il precedente d.lgs. 14 marzo 2013, n. 33 (c.d. Decreto trasparenza) e si affianca, e in alcuni casi sovrappone, alla legge sulla trasparenza amministrativa n. 241 del 1990, tuttora in vigore. Ne deriva, dunque, che anche nell'ambito dell'*Open government*, si assiste ad una dispersione delle fonti responsabile di antinomie e conseguenti incertezze applicative.

4. L'EGOVERNMENT NEI RAPPORTI CON I CITTADINI: LA TRASPARENZA DELLA PA

Come anticipato, benché il CAD contenga alcune norme di carattere generale relative alla trasparenza, accessibilità e partecipazione democratica dei cittadini all'agire amministrativo, la disciplina organica sul diritto di accesso alle informazioni detenute dalla pubblica amministrazione non si rinviene all'interno di esso, bensì in un separato decreto, che deve quindi essere adeguatamente coordinato con le altre fonti dell'amministrazione digitale. Se, infatti, da un lato il codice introduce principi[18] quali il diritto all'uso delle tecnologie (art. 3), l'alfabetizzazione informatica di cittadini (art.

---

del 2010, il quale dispone che la presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni deve avvenire esclusivamente utilizzando tecnologie dell'informazione e della comunicazione. Con le stesse modalità le amministrazioni adottano e comunicano atti e provvedimenti amministrativi alle imprese. Ancora, all'art. 6-*bis* introdotto nel 2012, – a seguito dell'obbligo, di cui all'art. 16 della legge n. 2 del 2009, per le imprese e per i professionisti di dotarsi di un indirizzo di posta elettronica certificata – il quale dispone che gli indirizzi inseriti nell'indice costituiscono mezzo esclusivo di comunicazione e notifica con le pubbliche amministrazioni. L'accesso all'indice INI-PEC è consentito non solo alle pubbliche amministrazioni e alle imprese e professionisti, ma anche ai gestori o esercenti servizi pubblici, nonché a tutti i cittadini. Quanto all'uso esclusivo del sistema PEC per le comunicazioni tra imprese e pubbliche amministrazioni – utilizzato anche nell'ambito delle procedure disciplinate dal codice dei contratti pubblici-, Cfr., G. Carullo, *Posta elettronica certificata e domicilio digitale: futuro e incertezze in una prospettiva europea*, in *Riv. it. dir. pubb. com.*, 1, 2016 51 ss.e. e videnti si veda in dottrinlusivamente italiana.
tratti pubblici-ottata da nessun altro paese. e videnti si veda in dottrin..e. e videnti si veda in dottrinlusivamente italiana.
tratti pubblici-ottata da nessun altro paese. e videnti si veda in dottrin

[15] L'*eProcurement*, così come l'*Open government* per quanto riguarda i rapporti con i cittadini, rappresenta uno degli ambiti di realizzazione dell'*eGovernment* e si riferisce alle modalità di acquisto di beni e servizi da parte delle pubbliche amministrazioni grazie a procedimenti di gara interamente gestiti in modalità digitali.

[16] Con la legge delega n. 11 del 2016, emanata al fine di dare attuazione alle Direttive europee nn. 23, 24 e 25 del 2014, il Governo è stato delegato ad adottare il nuovo codice dei contratti pubblici. Il d.lgs. 18 aprile 2016, n. 50 sostituisce, dunque, il precedente d.lgs. n. 163 del 2006 e costituisce una tappa fondamentale per la piena realizzazione dell'*eProcurement*.

[17] Ad esempio, nella nuova versione del Cad entrata in vigore a settembre 2016 – posteriormente, quindi, alla riforma del codice dei contratti pubblici – compare ancora l'art. 62-*bis*, introdotto nel codice del 2005 con il d.lgs. n. 235 del 2010, il quale prescrive che per favorire il controllo dell'azione amministrativa e il rispetto della legalità si utilizza la banca dati nazionale dei contratti pubblici istituita presso la relativa autorità di vigilanza. Tuttavia, la predetta autorità, costituita con la legge n. 109 del 1994, e successivamente riorganizzata a seguito dell'approvazione del d.lgs. n. 163 del 2006, è stata soppressa nel 2014 con il d.l. n. 90, e le sue funzioni e strutture sono confluite nell'Autorità nazionale anticorruzione (ANAC) la quale oggi assomma in sé le competenze relative sia ai contratti pubblici sia alla trasparenza; cfr., C. Lauri, *I dati e le informazioni nelle procedure di* e-procurement, in questo Rapporto.

[18] L'introduzione di norme che favoriscono il dialogo digitale tra pubblico e privato tuttavia non vale di per sé stessa a colmare il *deficit* di competenze digitali registrato dall'Italia rispetto agli altri Paesi europei. Dal rapporto DESI 2016 emerge che una delle situazioni più gravi, che collocano l'Italia tra gli ultimi Paesi della classifica, riguarda proprio la diffusione di una adeguata cultura digitale, laddove il 57 % della popolazione risulta avere competenze del tutto assenti o comunque inferiori a quelle considerate base. L'importanza della competenza digitale quale competenza chiave per l'apprendimento è stata riconosciuta dal Parlamento europeo sin dalla Raccomandazione del 2006, intitolata "*Competenze chiave per l'apprendimento permanente*", che la colloca tra le otto competenze essenziali (insieme a comunicazione nella madrelingua; comunicazione nelle lingue straniere;

8), la partecipazione democratica elettronica (art. 9) [19], prevedendo istituti come il domicilio digitale, l'identità digitale e la carta di identità elettronica, dall'altro è nel *Freedom of information act* che si rinvengono le disposizioni operative e concrete destinate a cambiare il rapporto tra cittadini e pubblica amministrazione specie in tema di accesso alle informazioni pubbliche[20].

In virtù della delega più volte citata, il d.lgs. n. 97 del 2016 procede infatti al riordino della disciplina riguardante gli obblighi di pubblicità e trasparenza delle pubbliche amministrazioni, di cui al precedente d.lgs. n. 33 del 2013 (c.d. Decreto trasparenza)[21]. Esso, in particolare, prevede un obbligo generale di pubblicazione di tutti i dati e i documenti detenuti dalle pubbliche amministrazioni cui si contrappone il correlativo diritto di chiunque di conoscere detti dati e di fruirne gratuitamente, nonché di utilizzarli e riutilizzarli[22].

Al concetto di pubblicità, intesa come conoscibilità da parte dei cittadini delle attività poste in essere da soggetti pubblici si affianca un ulteriore e nuovo concetto di trasparenza, quale vero e proprio diritto del singolo di richiedere ed ottenere informazioni sull'operato pubblico[23]. Con la previsione del diritto di accesso civico il nuovo FOIA mira a garantire a garantire la piena attuazione del principio generale di trasparenza, al fine di promuovere la partecipazione degli interessati all'attività amministrativa e di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche[24]. Il d.lgs. n. 97 del 2016 dunque introduce un diritto di accesso civico molto diverso da quello di accesso agli atti già disciplinato nella legge sul procedimento amministrativo[25]. Il confronto tra il nuovo diritto e quello precedente evidenzia il mutamento del concetto di trasparenza amministrativa, dalla mera conoscibilità degli atti alla piena accessibilità ad ogni documento detenuto o elaborato dalla pubblica amministrazione. Infatti, nonostante l'art. 22, comma 2, della legge n. 241 del 1990, così come modificato dalla legge n. 69 del 2009, prescriva che l'accesso ai documenti amministrativi, attese le sue rilevanti finalità di pubblico interesse, costituisce principio generale

---

competenza matematica e di base in scienza e tecnologia; imparare a imparare; competenze sociali e civiche; spirito di iniziativa e imprenditorialità; consapevolezza ed espressione culturale). Per competenza digitale si intende il saper utilizzare con dimestichezza e spirito critico le tecnologie della società dell'informazione per il lavoro, il tempo libero e la comunicazione. Nella raccomandazione, inoltre, la sua importanza è riconosciuta non soltanto in termini assoluti ma anche e soprattutto in quanto competenza strettamente interconnessa e funzionale a tutte le altre.

[19] Si tratterebbe di situazioni giuridiche soggettive meramente strumentali e non direttamente coercibili, tanto che più che di diritti dovrebbe parlarsi di mere norme di principio. Cfr., F. Cardarelli, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. dell'informazione e dell'informatica*, 2, 2015, 239 ss.

[20] Cfr., I. F. Caramazza, *Le regole dell'azione amministrativa: dalla L. 7 agosto 1990 n. 241 alla L. 7 agosto 2015 n. 124*, in *Dir. amm.*, 2-3, 2015, 569 ss.; M. C. Cavallaro, *Garanzie della trasparenza amministrativa e tutela dei privati*, in *Dir. amm.*, 1, 2015, 121 ss.; E. Tedeschi, *Il diritto di accesso: il nuovo dovere di collaborazione dell'amministrazione*, in *Giorn. dir. amm.*, 6, 2016, 805 ss.; P. Canaparo, *L'ambito soggettivo di applicazione del decreto legislativo 33/2013 dopo l'attuazione della Riforma Madia: più o meno trasparenza pubblica*, in *www.federalismi.it.*, 8 febbraio 2017; S. Villamena, *Il cosiddetto FOIA (o accesso civico 2016) e il suo coordinamento con istituti consimili*, in *www.federalismi.it.*, 30 novembre 2016

[21] Con l'adozione di un *Freedom of information act*, l'Italia si allinea agli oltre 90 paesi democratici i quali riconoscono, anche in conformità alla CEDU, come fondamentale il diritto di accesso all'informazione detenuta dai governi. Per un'analisi in chiave comparata cfr., D. Galetta, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione: un'analisi storico-evolutiva, in una prospettiva di diritto comparato europeo*, in *Riv. it. dir. pubb. com.*, 5, 2016, 1019 ss.

[22] Cfr., combinato disposto artt. 3 e 5.

[23] Vi sarebbe differenza tra pubblicità e trasparenza: "la pubblicità implica un'attività dell'amministrazione, la quale, per pubblicizzare un'informazione deve prima individuarla, distinguerla dalle altre notizie, per poi tradurla all'esterno all'attenzione degli utenti o di chi ne faccia richiesta; la trasparenza presuppone invece uno sforzo organizzativo che consenta la visibilità dell'azione amministrativa", così M.C. Cavallaro, *Garanzie della trasparenza amministrative e tutela dei privati*, in *Dir. amm.*, 1, , 2015, 122.

[24] Cfr., art. 1, comma 2: "*La trasparenza (…) concorre ad attuare il principio democratico e i principi costituzionali di eguaglianza, di imparzialità, buon andamento, responsabilità, efficacia ed efficienza nell'utilizzo di risorse pubbliche, integrità e lealtà nel servizio alla nazione. Essa è condizione di garanzia delle libertà individuali e collettive, nonché dei diritti civili, politici e sociali, integra il diritto ad una buona amministrazione e concorre alla realizzazione di una amministrazione aperta, al servizio del cittadino*".

[25] Si ricordi tuttavia che le disposizioni del FOIA non abrogano le norme di cui alla legge 241 del 1990 e ciò crea notevoli difficoltà di coordinamento tra le due discipline, tanto che potrebbe dubitarsi dell'opportunità della perdurante vigenza della legge 241 del 1990.

dell'attività amministrativa al fine di favorire la partecipazione e di assicurarne l'imparzialità e la trasparenza, il diritto di accesso agli atti – a differenza dell'accesso civico – è comunque sottoposto ad una serie di requisiti e condizioni[26] e non ha, per espressa previsione di legge, la funzione di consentire la partecipazione degli interessati all'azione amministrativa ma soltanto quella, ben più ristretta, di garantire la mera conoscibilità dei documenti che possono incidere su una determinata situazione giuridica soggettiva[27].

Diversamente, lo scopo del diritto di accesso civico, introdotto dal FOIA, è proprio quello di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere, quindi, la partecipazione di tutti i cittadini all'attività amministrativa[28]. Ci si trova, dunque, in presenza di un concetto di trasparenza amministrativa del tutto innovativo, che richiede la partecipazione del cittadino proprio al fine di migliorare l'efficienza dell'agire pubblico.

D'altra parte è altresì evidente che per poter assolvere al principio di trasparenza e garantire ai cittadini l'accesso civico le istituzioni pubbliche devono poter disporre di adeguate infrastrutture ed altrettante competenze per la gestione dei relativi dati[29]. Se da un lato, la previsione del generale obbligo di pubblicità unitamente alla trasparenza dovrebbero concorrere ad aumentare la qualità della vita dei cittadini, consentendo loro di partecipare attivamente alla gestione pubblica, dall'altro l'attuazione del principio di trasparenza implica e presuppone che la stessa pubblica amministrazione sia prima di tutto in grado di assicurare ai medesimi cittadini il pieno rispetto di altri e più importanti diritti, quali quelli di rilevanza costituzionale relativi alla tutela della riservatezza, della dignità e della libertà[30]. Per fare ciò non basta ricorrere al giudizio di bilanciamento degli interessi, ma occorre predisporre adeguate infrastrutture tecnologiche in grado di prevenire gli abusivi e scongiurare i rischi derivanti dalla messa in rete di informazioni e dati personali.

In conclusione, l'attuazione del principio di trasparenza richiede molteplici cautele, che sono affidate alla regolazione secondaria posta in essere dalle diverse autorità, a vario titolo competenti in materia. L'ANAC, la Privacy, l'AgId e il Dipartimento della funzione pubblica hanno il difficile compito di collaborare per garantire la sicurezza in termini tecnici del nuovo sistema di pubblicità da un lato e la certezza in termini giuridici dei nuovi diritti di trasparenza.

---

[26] Infatti, può essere esercitato soltanto dai soggetti interessati, ovvero da coloro che hanno un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso. Inoltre, ai sensi dell'art. 25, comma 2, la richiesta di accesso ai documenti deve essere motivata e deve essere rivolta all'amministrazione che ha formato il documento o che lo detiene stabilmente. Infine, ai sensi dell'art. 24, comma 3, non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni.

[27] Come si legge nella Determinazione ANAC n. 1309 del 28.12.2016: "La finalità dell'accesso documentale *ex* l. 241/90 è, in effetti, ben differente da quella sottesa all'accesso generalizzato ed è quella di porre i soggetti interessati in grado di esercitare al meglio le facoltà – partecipative e/o oppositive e difensive – che l'ordinamento attribuisce loro a tutela delle posizioni giuridiche qualificate di cui sono titolari".

[28] L'esercizio del diritto non è sottoposto ad alcuna limitazione quanto alla legittimazione soggettiva del richiedente né è richiesto di motivare la relativa istanza. Inoltre, l'accesso può essere esercitato nei confronti di tutti i dati, i documenti e le informazioni non soltanto detenute dalle pubbliche amministrazioni ma anche da queste elaborate, e può avere ad oggetto anche le informazioni che non sono sottoposte alla pubblicazione obbligatoria; cfr. combinato disposto degli artt. 3, 5 e 7.

[29] Ci si riferisce al sistema pubblico di connettività che, per effetto delle modifiche introdotte agli artt. 73 ss. CAD, non solo garantisce il coordinamento informativo tra le PA nazionali ma anche nei confronti dei sistemi dell'Unione europea nonché dei gestori di servizi pubblici e dei soggetti privati. Sul SPC cfr., G. Santucci, P. Minasi, *Il Sistema pubblico di connettività (spc) quale strumento di* governance*, razionalizzazione e valorizzazione delle basi di dati pubbliche*, in *www.cnipa.it*; G. Carullo, *Big Data e pubblica amministrazione nell'era delle banche dati interconnesse*, in *htpps://ssrn.com/abstract=2929660*; C. D'Orta, *Il SPC: un approccio nuovo alle esigenze della rete delle pubbliche amministrazioni*, in *Giorn. dir. amm.*, 7, 2005, 693 ss.

[30] Non sempre alla maggiore trasparenza corrisponde una maggiore libertà di azione del privato. Non è solo il privato, infatti, ad esercitare nuove forme di controllo sul pubblico ma è anzi quest'ultimo a gestire e poter manipolare dati su ogni aspetto della vita privata dei cittadini.

5. L'AUTORITÀ NAZIONALE ANTICORRUZIONE E IL GARANTE DELLA PRIVACY

A dimostrazione della diversa funzione attribuita al concetto di trasparenza dell'agire pubblico, il FOIA affida all'Autorità nazionale anticorruzione la vigilanza sull'applicazione delle proprie disposizioni.

Nell'ambito della sua attività in materia di anticorruzione e trasparenza, l'Autorità in data 28 dicembre 2016 ha adottato: la Determinazione n. 1309 contenente Linee Guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5, comma 2, del d.lgs. n. 33 del 2013, nonché la Delibera n. 1310 contenente le Prime Linee Guida recanti indicazioni sull'attuazione degli obblighi di pubblicità, trasparenza e diffusione di informazioni.

La prima, adottata d'intesa con il Garante per la protezione dei dati personali, procede a chiarire e definire alcuni concetti chiave della nuova disciplina della trasparenza, distinguendo ad esempio l'accesso civico da quello generalizzato e da quello documentale, nonché delineando gli ambiti di applicazione oggettivo e soggettivo della disciplina e il regime delle eccezioni dei limiti. La *ratio* sottesa al provvedimento è quella di fornire a tutte le amministrazioni dei criteri univoci per evitare comportamenti disomogenei. La seconda delibera è, invece, principalmente dedicata a definire gli obblighi di pubblicità, relativi dunque all'accesso generalizzato. Si tratta, dunque, di una regolazione secondaria che ha il primario scopo di agevolare l'applicazione delle norme di rango superiore specificandone i relativi campi di applicazione e le modalità operative[31]. Essa, tuttavia, si occupa esclusivamente di garantire il pieno rispetto del diritto di trasparenza senza considerare i possibili rischi di abuso degli altri diritti fondamentali che potrebbero derivare sia da un distorto uso della pubblicità, sia da un inadeguato sistema infrastrutturale di trasparenza[32].

Tali aspetti sono piuttosto regolati dal Garante della Privacy il quale ha, fin dalle prime declinazioni del principio di trasparenza, predisposto norme generali e linee guida. Ci si riferisce, in primo luogo, alle norme contenute nel Codice della *privacy*, di cui al d.lgs. 30 giugno 2003, n. 196, e in secondo luogo ai provvedimenti emanati a partire dal 2007[33]. Quanto alle prime occorre ricordare che oltre ai principi di esattezza e aggiornamento, pertinenza e completezza, provvisorietà e di proporzionalità allo scopo, si applicano ai dati raccolti dai soggetti pubblici le regole specifiche di cui agli artt. 18 e 19. Esse dispongono che il trattamento dei dati da parte dei soggetti pubblici è consentito solo per lo svolgimento delle funzioni istituzionali e che non è richiesto il previo consenso dell'interessato (salvo per gli organismi sanitari pubblici)[34]. Inoltre, il trattamento dei dati da parte di un soggetto pubblico è consentito anche in mancanza

---

[31] Oltre ai compiti di indirizzo e regolazione, come già accennato, competono all'ANAC anche i compiti di controllo e sanzionatori disciplinati dal Capo VI del FOIA agli artt. 43 ss. In tal modo l'ANAC assomma in sé compiti di regolazione e controllo sia a scopo preventivo sia a scopo sanzionatorio e ciò se, da un lato, potrebbe essere avere il merito di garantire una maggiore coerenza nell'applicazione della disciplina, dall'altro, potrebbe invece determinare una sovrapposizione dei vari piani di tutela. Sugli ambigui poteri dell'ANAC interessante è l'articolo di B. Manfellotto, *Il cantone dimezzato*, comparso su *L'Espresso* del 30 luglio 2017.

[32] Si allude alla sicurezza non solo della gestione delle banche dati – dalle quali il cittadino ha diritto di estrarre informazioni e documenti – ma anche del sistema di scambio delle informazioni tra le varie amministrazioni. Cfr., L. Califano, *Brevi riflessioni su privacy e costituzionalismo al tempo dei* Big Data, in *www.federalismi.it*, 3 maggio 2017; G. Buttarelli, Privacy*, sicurezza e nuove tecnologie al bivio di nuove scelte strategiche*, in *www.federalismi.it*, 14 gennaio 2015.

[33] Cfr., Deliberazione n. 17 del 19 aprile 2007 contenente le Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione di atti e documenti di enti locali.

[34] La non previsione del consenso preventivo è connaturata allo stesso rapporto tra pubblico e privato. La comunicazione dei dati del privato al soggetto pubblico spesso infatti non avviene affatto su base volontaria, così come il trattamento dei dati dei privati da parte delle amministrazioni spesso è essenziale per l'esercizio della funzione pubblica. Anche per tali motivi si rende ancor di più necessario apprestare adeguati sistemi di sicurezza di gestione dei dati da parte delle pubbliche amministrazioni, sia perché il conferimento dei dati personali spesso non può essere evitato dal privato, sia perché conferendo un proprio dato al sistema pubblico il privato è portato ad adottare un atteggiamento di fiducia nel sistema stesso che lo spinge a disattendere le cautele che altrimenti utilizzerebbe in un contesto dichiaratamente imprenditoriale.

di espressa previsione di legge. Quanto alla comunicazione dei dati tra soggetti pubblici, essa è ammessa in generale quando è prevista da una norma di legge o di regolamento. In mancanza di espressa previsione è tuttavia ammessa quando è comunque necessaria per lo svolgimento di funzioni istituzionali. Diversamente, la comunicazione di dati da parte di un soggetto pubblico a un soggetto privato è ammessa unicamente quando prevista da una norma di legge o di regolamento.

Alle norme generali si affiancano quelle contenute nelle Linee guida adottate, in particolare, con i provvedimenti del 15 maggio 2014 e del 2 luglio del 2015 relativi rispettivamente al "*trattamento dei dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici*" e alle "*misure di sicurezza da adottare per le banche dati pubbliche e sulle modalità relative allo scambio dei dati personali tra amministrazioni*"[35]. In entrambi si afferma il principio cardine del trattamento dei dati da parte delle amministrazioni pubbliche rappresentato dalla necessità di uno stretto legame tra il trattamento stesso e la funzione pubblica direttamente esercitata dalla medesima amministrazione[36].

Lo stesso principio viene da ultimo disciplinato con il Regolamento 2016/679/UE il quale, pubblicato in Gazzetta ufficiale il 4 maggio 2016, diventerà immediatamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018. Non è possibile in questa sede procedere ad una disamina puntuale delle disposizioni del nuovo regolamento[37], la cui entrata in vigore chiederà di certo un'opera di adeguamento delle disposizioni interne; tuttavia, si può sin da ora notare che molti dei principi e delle regole introdotte trovano, già allo stato attuale, opportuna corrispondenza nell'attività regolamentare sino ad oggi prodotta dal Garante della Privacy. Ciò che, invece, difetta nel nostro ordinamento, così come in quello europeo, è una disciplina organica in grado di garantire l'effettiva ed efficace sicurezza dei sistemi di gestione delle banche dati.

6. LA SICUREZZA DELLE BANCHE DATI PUBBLICHE

Come anticipato, la possibilità di violazione dei diritti fondamentali quali la riservatezza e la libertà personale non deriva soltanto dalle ipotesi di abuso o di trattamento illecito dei dati; esistono, invero, molteplici altre fattispecie che sfuggono al controllo sia pubblico sia privato. Le banche dati, specie se connesse in rete, rappresentano luoghi dei quali è molto difficile garantirne l'inviolabilità. Le notizie relative ad attacchi da parte di *hacker* nei confronti delle banche date pubbliche sono sempre più frequenti[38] tanto che, a seguire attentamente i fatti di cronaca, si ha la sensazione che la difesa sia non già difficile ma del tutto impossibile.

Alcune importanti previsioni in materia di sicurezza sono contenute nelle Linee guida del Garante Privacy di luglio 2015,

---

[35] Quanto alle attività dei privati meritano menzione inoltre le Linee Guida in materia di trattamento dei dati personali per profilazione *online* del 19 marzo 2015.

[36] Cfr., delibera n. 393 del 2 luglio 2015, adottata in attuazione dell'art. 58 Cad.

[37] Sia consentito rinviare a M.L. Magno, *Verso una nuova economia*, in *Consumerism 2016. Nono rapporto annuale. Dalla sharing alla social economy*, in www.consumersforum.it, 20 ss. Nel presente volume si rimanda inoltre al capitolo dedicato alla *Privacy* curato da S. Sandulli e A. Saccoccio.

[38] In un solo mese, a partire dalla metà di luglio alla metà di agosto 2017, dai giornali e telegiornali si è venuti a conoscenza di un attacco ai sistemi di gestione dei codici iban di una delle principali banche italiane, di un attacco alla piattaforma *online* di uno dei partiti politici e, infine, delle falle dell'intera infrastruttura informatica della difesa italiana i cui *server* che custodiscono le informazioni vitali del Paese sono protetti da software per i quali non esiste più possibilità di aggiornamento (Cfr., La Repubblica, 13 agosto 2017). Da ultimo, la Sogei – società *in house* del Ministero dell'Economia e delle Finanze, che gestisce i servizi informatici per la pubblica amministrazione e per l'Agenzia delle Entrate – ha mostrato una falla nel sistema telematico che ha permesso a chiunque avesse le credenziali per entrare, commercialisti o anche semplici contribuenti, di consultare liberamente i dati fiscali degli altri cittadini.

specie in tema di *data breach*[39]; tuttavia, nonostante si debba riconoscere all'Autorità il merito dell'aver affrontato il tema della sicurezza, non si può non considerare come lo spazio cibernetico[40] necessiti di un suo sistema di difesa speciale, che vada ben oltre la semplice protezione della *privacy* dei cittadini.

La digitalizzazione dell'apparato pubblico comporta efficienza ma produce dei rischi. Quanto più si è connessi tanto più si è vulnerabili, sia a livello individuale sia a livello statale.

La protezione del *cyber* spazio è una delle questioni affrontate dall'Unione europea con la Direttiva n. 2016/1148 del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, anche nota come Direttiva NIS (*Network and Information Security*). La Direttiva ha lo scopo di stabilire i requisiti minimi di sicurezza informatica per gli operatori dei servizi essenziali e dei servizi digitali; tuttavia, lascia impregiudicata la possibilità, per ciascuno Stato membro, di adottare le misure necessarie per assicurare la tutela degli interessi essenziali della sua sicurezza, salvaguardare l'ordine pubblico e la pubblica sicurezza. Si tratta, dunque, di una Direttiva che prescrive regole di armonizzazione minima, come espressamente sancito dall'art. 3, così pregiudicando l'effettiva tutela dello spazio digitale europeo[41].

Per quanto riguarda la legislazione italiana occorre ricordare che il Comitato interministeriale per la sicurezza della Repubblica (CISR) nel dicembre 2013 ha elaborato il Quadro strategico nazionale per la sicurezza dello spazio cibernetico e il Piano nazionale per la protezione cibernetica e la sicurezza informatica, che contengono gli obiettivi strategici e operativi della *cyber security* italiana. In particolare, il Piano nazionale per la protezione cibernetica e la sicurezza informatica prevede la creazione e lo sviluppo dei c.d. CERT-PA (*computer emergency response team*) e l'avvio di un CERT Nazionale. Nonostante la previsione, però, la maggior parte delle pubbliche amministrazioni non ha ancora provveduto ad istituire un CERT, mentre a livello regionale soltanto una delle regioni italiane (il Friuli Venezia Giulia) ha istituito, già dal 2005, il CERT-RAFVS.

Da ultimo, occorre ricordare che l'Autorità Garante per la Protezione dei dati personali e il Dipartimento delle informazioni per la sicurezza (Dis) hanno di recente firmato un documento che tiene conto della recente Direttiva del Governo in materia di protezione cibernetica e sicurezza informatica nazionali (cosiddetta "Direttiva Gentiloni") e si propone di mettere a sistema e rendere più efficaci le verifiche del Garante, già previste dalla normativa vigente.

In conclusione, l'attuazione dei nuovi valori di accessibilità totale, trasparenza, partecipazione e informazione dei cittadini se da un lato rappresenta una conquista fondamentale per la società civile, dall'altro cela il pericolo di altrettante innovative violazioni dei diritti della personalità. Il processo di digitalizzazione della pubblica amministrazione coinvolge le competenze di due autorità indipendenti, un'agenzia e un dipartimento ministeriale[42]: a nessuno di detti soggetti,

---

[39] Si intende, l'obbligo per le amministrazioni pubbliche di comunicare all'Autorità Garante, entro 48 ore dalla conoscenza del fatto, tutte le violazioni dei dati o gli incidenti informatici che possono avere un impatto significativo sui dati personali detenuti nelle banche dati stesse.

[40] Nel *summit* della NATO, tenutosi a Varsavia nel luglio del 2016, il *cyber* spazio è stato riconosciuto come quinto spazio operazionale dopo aria, terra, mare e spazio (atmosferico).

[41] Ai sensi dell'art. 1, la direttiva stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno. A tal fine la direttiva: a) fa obbligo a tutti gli Stati membri di adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi; b) istituisce un gruppo di cooperazione al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri e di sviluppare la fiducia tra di essi; c) crea una rete di gruppi di intervento per la sicurezza informatica in caso di incidente ("rete CSIRT") per contribuire allo sviluppo della fiducia tra Stati membri e promuovere una cooperazione operativa rapida ed efficace; d) stabilisce obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali; e) fa obbligo agli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT (*Computer security incident response team*) con compiti connessi alla sicurezza della rete e dei sistemi informativi.

[42] Non è in questa sede possibile soffermarsi sul ruolo e le funzioni dell'AgId e del Dipartimento della funzione pubblica. Sinteticamente si ricordi però che alla prima competono la definizione di alcune norme tecniche cui il Cad fa rinvio (ad esempio in materia di fatturazione elettronica, nodo dei pagamenti, anagrafe nazionale delle persone residenti, sistema pubblico di identità digitale, etc.), mentre al secondo è affidato il presidio delle politiche di riforma e modernizzazione delle pubbliche

però, è direttamente attribuita la funzione di predisporre, monitorare e aggiornare gli strumenti di protezione dei sistemi informatici pubblici.

amministrazioni. In particolare, il Dipartimento assicura il supporto al Ministro per la semplificazione e la pubblica amministrazione nello svolgimento dei compiti delegati dal Presidente del Consiglio dei Ministri in materia di trasformazione della PA.

ANAC

(Cristiana Lauri)

PA – E-PROCUREMENT

La disponibilità dei dati e delle informazioni assume particolare rilievo tra le novità delineate nel nuovo Codice dei Contratti Pubblici. La prospettiva di un passaggio totale alla digitalizzazione delle procedure rappresenta negli intenti del legislatore garanzia di trasparenza e di legalità. In questo scenario, un ruolo di primo ordine è svolto dall'Autorità di riferimento – l'ANAC – e dagli altri soggetti istituzionali con cui essa dialoga. In un sistema ancora in via di assestamento e connotato da forti novità sotto i profili soggettivi, procedurali e gestionali, la trasparenza è valore imprescindibile sia per un leale confronto concorrenziale tra imprese, sia nell'ottica di garantire un approvvigionamento di beni e servizi vantaggioso per la cosa pubblica e per il buon andamento della stessa.

I dati e le informazioni nelle procedure di *e-procurement*

(Cristiana Lauri)

SOMMARIO: 1. IL RUOLO DELL'ANAC E DEGLI ALTRI SOGGETTI NEL NUOVO CODICE DEI CONTRATTI PUBBLICI. – 2. LA GESTIONE DEI DATI NELLE PROCEDURE DI *E-PROCUREMENT*. – 3. GLI EFFETTI DIRETTI SULLE IMPRESE E GLI EFFETTI INDIRETTI SULLA COLLETTIVITÀ.

1. IL RUOLO DELL'ANAC E DEGLI ALTRI SOGGETTI NEL NUOVO CODICE DEI CONTRATTI PUBBLICI

Dalla loro comparsa nell'ordinamento italiano le *Authorities* hanno progressivamente avocato a sé funzioni e competenze settoriali che nel tempo ha visto assestamenti e ampliamenti più o meno significativi. Ad esse, forse più che ad altri soggetti istituzionali, è toccato il compito di gestire alcuni fenomeni complessi, molti tra i quali determinati dall'applicazione delle nuove tecnologie relativamente a beni e servizi indirizzati a cittadini e consumatori, ma anche alle PA stesse. Tra questi compiti rientra anche il tema in oggetto del presente Rapporto e cioè la gestione dei dati e delle informazioni nel momento in cui transitano nei mercati e si fanno valore per i soggetti che in quei mercati agiscono.

Tuttavia, se per quanto riguarda il settore dei servizi di interesse economico generale e i compiti delle relative Autorità – AGCom, AEEGSI, ART – l'impostazione della questione risulta ormai sufficientemente lineare, altrettanto non sembra potersi dire per il particolare settore che in questa parte di Rapporto si vuole esaminare: la gestione dei dati nei contratti pubblici e, segnatamente, nelle procedure di *e-procurement*.

In primo luogo, risulta primaria l'analisi del ruolo dell'ANAC e il rapporto di questa con altri soggetti istituzionali, in ragione delle numerose mutazioni genetiche vissute nel tempo, che l'hanno condotta a divenire soggetto indipendente e titolare di alcune funzioni non dissimili dalle altre *Authorities*[43].

[43] Vd. N. Longobardi, *Autorità indipendenti di regolazione dei mercati e autorità atipiche*. L'autorità Nazionale Anticorruzione, in www.giustamm.it, n. 5/2016, laddove viene evidenziata la differenza con le Autorità amministrative indipendenti divise tra autorità di regolazione dei mercati con funzioni principalmente regolatorie e autorità regolative giustiziali con funzioni di

In secondo luogo, vale precisare che nonostante il tema non riguardi i cittadini-consumatori in via diretta, ma indiretta, per il tramite della pubblica amministrazione, il sistema di approvvigionamento di beni e servizi da parte della PA ha delle ricadute certe su cittadini, consumatori e utenti destinatari dell'azione della PA di volta in volta considerata.

Infine, una considerazione più ampia: il recupero nel Rapporto una parte dedicata alla PA e alle imprese, nelle ultime edizioni non affrontata, enfatizza la centralità che il valore dei dati e delle informazioni assume nel sistema complessivamente inteso nonché la capacità di investire tutti i settori in modo trasversale e di rafforzare le relazioni dei consumatori nella loro veste di cittadini e utenti con le imprese e con i soggetti pubblici[44].

Quali sono, dunque, i soggetti istituzionali coinvolti? La risposta è contenuta nel titolo II del d.lgs. n. 50/2016[45], "*Governance*". L'art. 213 opera un rafforzamento del ruolo e delle funzioni dell'ANAC[46]. L'Autorità garantisce un generale compito di vigilanza e controllo sui contratti pubblici[47] e una regolazione del settore attraverso linee-guida, bandi-tipo, capitolati-tipo, contratti-tipo ed altri strumenti di regolazione flessibile. Ai fini dello svolgimento di tale attività di regolazione, all'ANAC è attribuita la gestione della Banca Dati Nazionale dei Contratti Pubblici[48], in cui confluiscono tutte le informazioni contenute nelle banche dati esistenti, anche a livello territoriale, con il fine di garantire accessibilità unificata, trasparenza, pubblicità e tracciabilità delle procedure di gara e delle fasi prodromiche e successive[49].

Con proprio provvedimento l'ANAC individua modalità e tempi entro i quali i titolari delle banche dati, previa stipula di protocolli di interoperabilità, garantiscono la confluenza dei dati nella Banca dati – unico archivio accreditato – di cui l'Autorità è titolare in via esclusiva[50].

La Banca dati è autonoma rispetto alla Banca dati nazionale degli operatori economici di cui all'art. 81[51], tenuta dal MIT, che erediterà le funzioni di AVCPASS – finora in capo all'ANAC – volto alla verifica dei requisiti degli operatori economici in fase di accesso alle gare. Pertanto, ANAC e MIT sono chiamati a cooperare: concordano le modalità di interscambio delle informazioni per garantire la funzione di prevenzione dalla corruzione e di tutela della legalità all'Autorità, nonché evitare sovrapposizioni di competenze e ottimizzare l'utilizzo dei dati nell'interesse della fruizione degli stessi da parte

---

vigilanza e *adjudication*. L'ANAC sembra racchiudere in sé i tratti di entrambe, sebbene vi siano contaminazioni in quanto per alcune funzioni sia previsto un esercizio di poteri congiunto al MIT o alla Cabina di Regia presso la Presidenza del Consiglio dei Ministri di cui all'art. 212.

[44] Sulla gestione dei dati da parte della PA e il difficile bilanciamento tra i differenti interessi in gioco si veda M.L. Magno, *La gestione dei dati da parte della pubblica amministrazione: il difficile equilibrio tra trasparenza, privacy e sicurezza*, in questo Rapporto.

[45] Codice dei Contratti Pubblici (d'ora in avanti anche CCP).

[46] Cfr. in dottrina i rilievi di R. Rolli-D. Sammarro, *Il nuovo Codice dei contratti pubblici: l'ANAC e l'Uomo di Vitruvio*, in www.giustamm.it, n. 4/2016. In generale all'ANAC vengono affidate funzioni di vigilanza di regolazione e decisorie, compresa la materia dell'inclusione e dell'esclusione delle imprese. L'A. si avvale di "linee guida" basate sulla regola del *command and control*. Sono previste anche norme vincolanti con le relative sanzioni, di cui l'ANAC può disporre irrogazione.

[47] V. d.lgs. 18 aprile 2016, n. 50, art. 213 "Autorità Nazionale Anticorruzione".

[48] Art. 213, comma 8.

[49] Con riferimento alle opere pubbliche la norma specifica che l'Autorità, il MEF, il MIT, la Presidenza del Consiglio dei Ministri e le Regioni e le Province autonome quali gestori dei sistemi informatizzati di cui al comma 4 dell'articolo 29 concordano le modalità di rilevazione e interscambio delle informazioni nell'ambito della banca dati nazionale dei contratti pubblici, della banca dati di cui all'art. 13 della legge 31 dicembre 2009, n. 196, della banca dati di cui all'art. 1, comma 5, della legge 17 maggio 1999, n. 144 e della banca dati di cui all'articolo 36 del d.l. 24 giugno 2014, n. 90, convertito, con modificazioni, dalla legge 11 agosto 2014, n. 114, al fine di assicurare, ai sensi del d.lgs. 29 dicembre 2011, n. 229, del d.lgs. 14 marzo 2013, n. 33 e del presente codice, il rispetto del principio di unicità dell'invio delle informazioni e la riduzione degli oneri amministrativi per i soggetti di cui all'articolo 1, comma 1, l'efficace monitoraggio dalla programmazione alla realizzazione delle opere e la tracciabilità dei relativi flussi finanziari o il raccordo degli adempimenti in termini di trasparenza preventiva.

[50] Per ulteriori rilievi v. G. Pizzanelli, *Il ruolo dell'ANAC nel nuovo Codice dei contratti pubblici: verso la compiutezza di un modello*?, in A. Fioritto (a cura di) *Nuove forme e nuove discipline del partenariato pubblico privato,* Torino, 2017, 134 ss.

[51] Secondo cui "*la documentazione comprovante il possesso dei requisiti di carattere generale, tecnico-professionale ed economico e finanziario, per la partecipazione alle procedure disciplinate dal presente codice e per il controllo in fase di esecuzione del contratto della permanenza dei suddetti requisiti, è acquisita esclusivamente attraverso la Banca dati centralizzata gestita dal Ministero delle infrastrutture e dei trasporti, denominata Banca dati nazionale degli operatori economici*".

degli operatori economici e delle stazioni appaltanti[52].

Per la gestione della Banca dati l'ANAC si avvale dell'Osservatorio dei contratti pubblici relativi a lavori, servizi e forniture – che opera mediante procedure informatiche sulla base di convenzioni anche attraverso il collegamento con i relativi sistemi in uso presso le sezioni regionali e presso altre Amministrazioni pubbliche e altri soggetti operanti nel settore dei contratti pubblici[53].

L'Autorità gestisce, inoltre, il Casellario Informatico dei contratti pubblici di lavori, servizi e forniture istituito presso l'Osservatorio, il quale contiene tutte le notizie, informazioni e dati relativi agli operatori economici riguardanti le iscrizioni previste *ex* art. 80 e garantisce collegamento con la banca dati di cui all'art. 81.

L'Autorità promuove l'efficienza e la qualità delle stazioni appaltanti, fornendo supporto volto a facilitare lo scambio di informazioni e favorendo omogeneità nei procedimenti e sviluppo delle migliori pratiche.

L'art. 78 riconosce inoltre all'ANAC il compito di gestire e aggiornare l'Albo Nazionale obbligatorio dei componenti delle Commissioni giudicatrici e l'elenco delle stazioni appaltanti che operano mediante affidamenti diretti nei confronti di proprie società *in house* ai sensi dell'art. 192[54].

Presso l'Autorità è, infine, istituito un elenco dei soggetti aggregatori, nell'ambito dell'Anagrafe Unica delle stazioni appaltanti[55].

Per quanto attiene alla collaborazione con altre Autorità indipendenti, è significativa la collaborazione tra ANAC e Autorità Garante della Concorrenza e del Mercato (AGCM) volta alla rilevazione di comportamenti aziendali meritevoli di valutazione al fine del c.d. "*rating* di legalità" delle imprese[56], che si coordina con il *rating* di impresa di cui all'art. 83, comma 10, il quale riconosce all'ANAC la gestione del sistema di qualificazione delle stazioni appaltanti e delle centrali di committenza. L'ANAC cura la gestione del sistema del *rating* di impresa e delle relative premialità e penalità ai fini della qualificazione delle imprese, relativamente al quale rilascia apposita certificazione. Il sistema è connesso a requisiti reputazionali valutati sulla base di indici qualitativi e quantitativi, oggettivi e misurabili, e sulla base di accertamenti definitivi che esprimono la capacità strutturale e di affidabilità dell'impresa, la cui definizione unitamente ai criteri di valutazione degli stessi e alle modalità di rilascio della relativa certificazione, avviene mediante linee guida adottate entro tre mesi dalla data di entrata in vigore del codice[57]. I requisiti reputazionali sui quali si basa il rating di impresa tengono conto del *rating* di legalità rilevato dall'ANAC in collaborazione con AGCM ai sensi dell'art. 213, comma 7, e dei precedenti comportamenti dell'impresa con riferimento al rispetto dei tempi e costi dell'esecuzione dei contratti, all'incidenza del contenzioso sia in sede di partecipazione alle procedure di gara che in fase di esecuzione del contratto e infine della regolarità contributiva, compresi i versamenti alle Casse edili, valutata con riferimento ai tre anni precedenti.

La preminenza del ruolo dei dati e l'affidamento ad un unico gestore delle banche dati in materia di appalti "*onde garantire accessibilità unificata, trasparenza e tracciabilità delle procedure di gara e delle fasi a essa prodromiche e successive*", rappresenta una delle novità più significative del nuovo Codice dei Contratti Pubblici[58].

Rilevanza strategica era peraltro già stata riconosciuta dalle Direttive 2014 al sistema elettronico *e-Certis*[59], volto allo

[52] Art. 213, comma 8

[53] Nel caso in cui un soggetto ometta, senza giustificato motivo, di fornire informazioni richieste o fornisca informazioni non veritiere, l'Autorità può irrogare sanzioni amministrative pecuniarie.

[54] Art. 213, comma 15.

[55] Art. 213, comma 16.

[56] V. Art. 5 ter, d.l. 24 gennaio 2012, n. 1.

[57] Inoltre ANAC determina misure sanzionatorie amministrative per i casi di omessa o tardiva denuncia obbligatoria delle richieste estorsive e corruttive da parte delle imprese titolari di contratti pubblici, comprese le imprese subappaltatrici e le imprese fornitrici di materiali, opere e servizi.

[58] In dottrina v. A. Camanzi, *I contratti pubblici*, Roma, 2013, 23 ss.

[59] Art. 61, Dir. 2014/24/UE; art. 88 ccp. Il sistema permette di rintracciare i certificati necessari per partecipare alle proce-

scambio di certificati e di altri documenti probatori richiesti dalle amministrazioni aggiudicatrici degli Stati membri, nonché successivamente al DGUE, il documento di gara unico europeo, che permette agli operatori di autocertificare la propria situazione, sburocratizzando le procedure[60] .

Per poter giudicare l'efficienza del passaggio a tale sistema fortemente accentrato occorrerà attenderne la piena implementazione[61]. Il tema del riordino della gestione dei dati permette tuttavia di introdurre un passo successivo: il potenziamento della digitalizzazione e degli strumenti di *e-procurement*[62]. A tal proposito, sul piano dei soggetti l'art. 212 del Codice, rubricato "Indirizzo e coordinamento" prevede l'istituzione di una Cabina di regia presso la Presidenza del Consiglio dei Ministri[63]. Significativo per la nostra analisi è la lett. d) laddove le viene attribuito il compito di "*promuovere la realizzazione, in collaborazione con i soggetti competenti, di un piano nazionale in tema di procedure telematiche di acquisto, al fine della diffusione degli strumenti informatici e della digitalizzazione delle fasi del processo di acquisto*".

Merita, infine, richiamare il ruolo dell'Agenzia per l'Italia Digitale che, nel generale espletamento dei propri compiti in tema di digitalizzazione dell'attività amministrativa, ai sensi del comma 10 dell'art. 58 è chiamata ad emanare regole tecniche aggiuntive per garantire il colloquio e la condivisione dei dati tra i sistemi telematici di acquisito e di negoziazione. A tal fine, a seguito di consultazione pubblica, l'Agenzia ha emanato la Circolare 6 dicembre 2016, n. 3 recante *"Regole e tecniche aggiuntive per garantire il colloquio e la condivisione dei dati tra i sistemi telematici di acquisto e di negoziazione"*.

Aprendo lo sguardo al panorama europeo è inoltre significativa è la creazione della rete Pan-European Public Procurement On-Line (Peppol), con l'obiettivo di creare un'infrastruttura comune per l'*e-procurement* in Europa. L'AgID assume il ruolo di *Authority* per l'Italia della rete e svolge un ruolo di *governance* sull'applicazione delle specifiche tecniche legate agli standard europei nell'ambito dell'*e-procurement* e di coordinamento degli *Access Point Provider* presenti sul territorio nazionale.

2. LA GESTIONE DEI DATI NELLE PROCEDURE DI *E-PROCUREMENT*

L'*e-procurement (electronic procurement)* nasce in ambito privatistico come processo di approvvigionamento elettronico di beni e servizi, dapprima tra aziende (*business to business* o B2B) e successivamente anche tra aziende e istituzioni pubbliche (*governance to business* o G2B) facendo leva su due caratteristiche fondamentali: il risparmio e la trasparenza. Il suo sviluppo è, dunque, fortemente dipendente dalla della rete internet e dal commercio elettronico, tanto che quando fu ideato (negli anni settanta) i costi – essenzialmente in termini di investimenti nelle reti – ne rendevano proibitivo l'uso da parte della maggior parte delle imprese. Con l'avvento della rete aperta e standardizzata le imprese

---

dure su scala europea.

[60] Art. 59, Dir. 2014/24/UE; art. 85 ccp. Il documento permette di adempiere telematicamente sia alla compilazione della documentazione necessaria alla partecipazione, che alla presentazione dell'offerta. Le imprese possono autocertificare la propria situazione finanziaria, abilità, idoneità, requisiti.

[61] G. Pizzanelli, cit., 138.

[62] Tra le modalità comuni alle procedure di affidamento, la novità più significativa del codice è costituita dall'art. 44 del d.lgs. 18 aprile 2016, n. 50 all'art. 44, rubricato "digitalizzazione delle procedure" il quale stabilisce che "*entro un anno dalla Data di entrata in vigore del presente codice, con decreto del Ministro per la semplificazione e la pubblica amministrazione, di concerto con il Ministro delle infrastrutture e dei trasporti e il Ministro dell'economia e delle finanze, sentita l'Agenzia per l'Italia Digitale (AGID) nonché dell'Autorità garante della privacy per i profili di competenza, sono definite le modalità di digitalizzazione delle procedure di tutti i contratti pubblici, anche attraverso l'interconnessione per interoperabilità dei dati delle pubbliche amministrazioni. Sono, altresì, definite le migliori pratiche riguardanti metodologie organizzative e di lavoro, metodologie di programmazione e pianificazione, riferite anche all'individuazione dei dati rilevanti, alla loro raccolta, gestione ed elaborazione, soluzioni informatiche, telematiche e tecnologiche di supporto*".

[63] Art. 83 Dir. 2014/24/UE.

hanno potuto iniziare ad utilizzare e spostare dati a proprio uso privato: in un primo momento attraverso la predisposizione di un catalogo elettronico per offrire e di una procedura di pagamento per acquistare; successivamente, con l'ampliamento di tale struttura, aggiungendo ulteriori funzionalità, fino a coprire l'intero processo: il controllo del ciclo produttivo; la gestione in tempo reale dei magazzini; la gestione dei contatti con i fornitori e con gli spedizionieri[64].

Il processo di digitalizzazione dei processi di acquisizione di beni e servizi da parte delle PA è considerato uno dei principali *driver* delle politiche della Commissione Europea, che ha come obiettivo di medio periodo quello di digitalizzare l'intero processo: dalla pubblicazione del bando, passando per l'aggiudicazione, fino a giungere alla fase di pagamento (si parla a tal proposito di appalti elettronici *end-to-end*).

Nel settore pubblico l'Italia è stata tra i primi paesi europei a regolare le procedure elettroniche[65]. Il Codice vigente disciplina gli istituti relativi nella sezione II: "Tecniche e strumenti per gli appalti elettronici e aggregati", delineando differenti strumenti di negoziazione, in particolare: l'art. 54 disciplina gli "accordi quadro"; l'art. 55 i "sistemi dinamici di acquisizione"[66]; l'art. 56 le "aste elettroniche"[67]; l'art. 57 i "cataloghi elettronici"[68]. L'art. 58, infine, rubricato "procedure svolte attraverso piattaforme telematiche di negoziazione" stabilisce che "*l'utilizzo dei sistemi telematici non deve alterare la parità di accesso agli operatori o impedire, limitare o distorcere la concorrenza o modificare l'oggetto dell'appalto, come definito dai documenti di gara*".

A seconda dell'importo contrattuale, sono definite le procedure per l'approvvigionamento elettronico di beni e servizi: il mercato elettronico per gli acquisti sotto soglia; le gare telematiche per gli acquisti di valore pari o superiore alla soglia.

Il Mercato elettronico della P.A. (MePA) si presenta come un vero e proprio mercato digitale in cui le Amministrazioni abilitate[69] possono fare acquisti, per valori inferiori alla soglia comunitaria, di beni e servizi offerti da fornitori abilitati a presentare i propri cataloghi sul sistema.

Il principale operatore pubblico italiano di *e-procurement* è Consip SpA, società *in house* del MEF. Accanto ad essa vi sono altre centrali di acquisto che possono esser costituite a livello regionale e operare come centrali di committenza, sebbene, come noto, la razionalizzazione alla base del nuovo Codice abbia previsto una decisa riduzione numerica. A Consip sono assegnati alcuni compiti di rilievo: definire con bandi le tipologie di beni e servizi e le condizioni generali di fornitura; gestire l'abilitazione dei fornitori e la pubblicazione e l'aggiornamento dei cataloghi. Le amministrazioni

---

[64] Lo ricorda D. Ielo, *Appalti e innovazione digitale nella nuova prospettiva del partenariato per l'innovazione*, in L'Agenda digitale: dalle parole ai fatti, Torino, 2015, 149.

[65] Vd. Legge n. 488/1999, con cui viene avviato un programma di razionalizzazione degli acquisti della PA. L'*e-procurement pubblico* compare per la prima volta nel Piano Nazionale per l'*e-governemt* approvato il 22 giugno 2000 (Azione 12) e nelle Linee guida in materia di digitalizzazione dell'amministrazione del 21 dicembre 2001. Riferimenti ulteriori si rinvengono anche nelle iniziative regionali e comunali.

[66] Il sistema dinamico di acquisizione, è un processo interamente elettronico, per acquisti di uso corrente, tipizzato e standardizzato, aperto per tutto il periodo di efficacia a qualsiasi operatore economico che soddisfi i criteri di selezione.

[67] La norma specifica che "*le stazioni appaltanti possono ricorrere ad aste elettroniche nelle quali vengono presentati nuovi prezzi, modificati al ribasso o nuovi valori riguardanti taluni elementi delle offerte. A tal fine, le stazioni appaltanti strutturano l'asta come un processo elettronico per fasi successive, che interviene dopo una prima valutazione completa delle offerte e consente di classificarle sulla base di un trattamento automatico*".

[68] La norma specifica che "*Nel caso in cui sia richiesto l'uso di mezzi di comunicazione elettronici, le stazioni appaltanti possono chiedere che le offerte siano presentate sotto forma di catalogo elettronico o che includano un catalogo elettronico. Le offerte presentate sotto forma di catalogo elettronico possono essere corredate di altri documenti, a completamento dell'offerta. I cataloghi elettronici sono predisposti dai candidati o dagli offerenti per la partecipazione a una determinata procedura di appalto in conformità alle specifiche tecniche e al formato stabiliti dalle stazioni appaltanti*".

[69] "Le amministrazioni statali, ivi compresi gli istituti e le scuole di ogni ordine e grado e le istituzioni educative; le aziende ed amministrazioni dello stato ad ordinamento autonomo; le regioni, le province, i comuni, le comunità montane e loro consorzi e associazioni; le istituzioni universitarie; le amministrazioni, le aziende del ssn; gli enti del ssn; le amministrazioni territoriali non regionali; gli organismi di diritto pubblico; gli iacp; le camere di commercia, industria, artigianato e agricoltura e le loro associazioni; gli enti pubblici non economici nazionali, regionali e locali; l'agenzia per la rappresentanza negoziale delle PA; le agenzie di cui al d.lgs. n. 300/1999; le onlus e le organizzazioni di volontariato; le stazioni appaltanti".

possono verificare l'offerta di beni e servizi accedendo alla "vetrina del mercato elettronico" o navigando sul "catalogo prodotti"; possono confrontare le proposte dei fornitori e scegliere quella più rispondente alle proprie esigenze e procedere con un Ordine diretto di acquisto o con una Richiesta di offerta. Le gare telematiche si basano sulla comparazione tra offerte alternative presentate mediante strumenti informatici e telematici; le procedure si articolano in quattro fasi: autorizzazione; pubblicazione degli avvisi di gara e degli inviti; espletamento della gara.

In un primo momento tali procedure sollevavano perplessità con riguardo ad alcuni profili in tema di *privacy* e sicurezza, tra cui la paternità dell'offerta, la non modificabilità dei documenti sottomessi, la segretezza, l'effettiva ricezione dell'offerta. Tali perplessità si sono attenuate a seguito dell'introduzione di uno strumento fondamentale quale la firma digitale e dal generale riordino assicurato dal CAD (tra cui figura l'art. 54, il quale prevede che ogni sito di PA riporti l'elenco dei bandi di gara). Per quanto riguarda la trasparenza delle procedure di affidamento, inoltre, a livello comunitario è significativa la creazione del TED (Tenders Electronic Daily)[70] e dell' Annual Public Procurement Implementation Review.

La tracciabilità in tal senso rappresenta un elemento fondamentale nel contrasto dell'illegalità: le novità in tema di gestione e controllo dei dati e della documentazione permettono chiaramente di massimizzare i profili di trasparenza e imparzialità[71]. Nelle procedure descritte, infatti, i dati e le informazioni rappresentano la linfa di un sistema il cui buon esito è estremamente dipendente dalla veridicità e dalla tracciabilità di tali elementi e, come si è cercato di delineare, il loro utilizzo si sostanzia in una serie di passaggi essenziali alla base del funzionamento dello stesso. Primo: l'utilizzo dei dati per la profilazione e la promozione delle aziende. Secondo: utilizzo dei dati nel sistema Banca dati Nazionale contratti pubblici/lavori/servizi/forniture. Terzo: utilizzo dei dati nelle piattaforme dedicate a progetti e gare.

3. GLI EFFETTI DIRETTI SULLE IMPRESE E GLI EFFETTI INDIRETTI SULLA COLLETTIVITÀ

I dati si atteggiano diversamente a seconda che vengano utilizzati nel settore pubblico o in quello privato (e a sua volta che il privato sia un consumatore o un'impresa) e diversi sono ad oggi i vantaggi per entrambe le parti.

Le amministrazioni possono godere di risparmi di tempo sul processo di acquisizione di beni e servizi sotto soglia; di un ampliamento delle possibilità di scelta poiché in grado di confrontare prodotti offerti da fornitori su ampia scala; sono in grado di soddisfare esigenze specifiche anche grazie alla possibilità di emettere richieste d'offerta.

L'*e-procurement* va, inoltre, inserito nel più ampio contesto di riforma del settore dei contratti pubblici, in cui una delle innovazioni accolta con maggior favore è consistita nel progetto di razionalizzazione delle stazioni appaltanti polverizzate sul territorio, attraverso i soggetti aggregatori: tale sistema "a rete", informatizzato e tracciabile nell'intero processo di acquisto, genererebbe significativi risparmi anche sulla spesa pubblica[72]. In dottrina era stato significativamente

[70] "Supplemento alla Gazzetta ufficiale dell'Unione europea", dove vengono pubblicati gli avvisi di appalti e i bandi di gara cui si applicano le norme dell'UE. Il TED consente un accesso gratuito alle opportunità commerciali ed è aggiornato più volte a settimana con circa 1500 avvisi di appalti pubblici.

[71] V. Direttiva 2014/24/UE, considerando 126; cfr anche CDS, V, 6018/2014.

[72] Anche in considerazione di tali rilievi il MePA, tra i mercati elettronici istituiti a livello europeo, è considerata una iniziativa di particolare efficienza e rappresenta un modello da valorizzare. Nel 2009, in occasione della manifestazione "*European eGovernment Awards*", il Mercato Elettronico è stato insignito del premio per la categoria "*eGovernment empowering Business*" in quanto "rappresenta un'iniziativa altamente innovativa. L'impatto verso le istituzioni governative è elevato, ma è altrettanto importante verso le PMI (...) Il progetto ha anche garantito l'adesione degli utilizzatori mediante piani di comunicazione e formazione che includono, tra l'altro, sportelli di formazione (...) Il premio dato a Consip è un riconoscimento del valore del MEPA nel migliorare l'accesso ai servizi pubblici da parte delle aziende, creando opportunità commerciali e generando risparmi per le imprese, in particolare le PMI".

affermato con lungimiranza che "la possibilità di trattamento elettronico delle informazioni trasforma a tal punto la struttura amministrativa nel suo complesso, da rendere necessaria la considerazione di nuove ripartizioni di potere al suo interno, rispondenti tanto alla necessità del migliore sfruttamento del mezzo tecnico impiegato, quanto di equilibri corrispondenti alle nuove possibilità di azione"[73].

In tal senso il rafforzamento dei poteri dell'ANAC verso un modello sempre più delineato e interconnesso con altri soggetti istituzionali rappresenta un primo passo per l'evoluzione di un settore tradizionalmente considerato volubile agli attacchi sotto il profilo della legalità e della trasparenza. Sembrano, pertanto, sussistere i presupposti per poter ampliare ancor più la portata delle novità già introdotte, ad esempio consentendo il ricorso alle procedure per l'affidamento telematico di appalti complessi[74], considerati non gestibili mediante sistemi di *e-procurement*.

Dall'altro lato vi sono significativi vantaggi per le imprese nel senso della riduzione degli oneri a loro carico: diminuzione dei costi commerciali e ottimizzazione dei tempi di vendita; accesso più ampio al mercato della PA; valorizzazione dell'attività svolta; concorrenzialità e confronto diretto con il mercato di riferimento; opportunità di offrire i propri prodotti su tutto il territorio più vasto; rinnovamento dei processi di vendita. Per le imprese le procedure di *e-procurement* comportano inoltre un processo di dematerializzazione che si traduce in una significativa riduzione degli oneri amministrativi e in una generalizzata semplificazione, generatrice di risparmio (si pensi agli strumenti della firma elettronica e della convalida dei documenti per l'ammissione alle procedure). Anche in questo caso è dirimente il profilo della trasparenza, nell'ottica di valorizzare un confronto concorrenziale documentato, pubblicizzato e tracciato nelle sue fasi. In una prospettiva evolutiva, seguendo il percorso finora tracciato, l'obiettivo per il futuro è rappresentato dagli appalti elettronici *end-to-end*.

Vale, infine, considerare che il settore dei contratti pubblici è diventato a tutti gli effetti uno strumento per l'incentivazione dell'innovazione, come dimostrato anche dal perfezionamento di alcuni istituti e dall'introduzione di nuovi (si pensi al partenariato per l'innovazione o all'appalto pre-commerciale e alla contestuale valorizzazione del ruolo dei privati). Anche alla luce di tale aspetto, la lettura di tali riforme non può dunque non tener in considerazione le significative ripercussioni sul sistema economico determinate dal mutato rapporto tra innovazione tecnologica e ruolo dei soggetti in campo.

Sebbene il nuovo codice abbia fornito impulso a trasparenza, razionalizzazione e legalità, l'utilizzo delle procedure elettroniche ancora può fare molto. Bisognerà ad esempio vedere se la gestione dei dati nell'intreccio tra ANAC e MIT sarà efficiente e se le risorse a ciò dedicate saranno sufficienti; se il passaggio da un sistema di gestione di dati frammentato ad uno accentrato sia davvero una delle chiavi di volta per combattere la corruzione nel settore dei contratti pubblici; se l'uso dei sistemi per l'interoperabilità e lo scambio di dati sia adeguatamente fruibile per i soggetti che vi si confronteranno. Inoltre, occorrerà potenziare tali strumenti anche nel contesto sovranazionale, in quanto negli altri Stati membri lo scenario si presenta ancora frammentato e disomogeneo[75]. In conclusione: come ricordato dal Consiglio di Stato "una riforma, per quanto ben costruita, è tale solo quando raggiunge un'effettiva attuazione, che sia in grado di incidere "in concreto" su cittadini e imprese, migliorandone il rapporto con il pubblico potere, semplificando l'esercizio delle attività private, modificando positivamente gli indicatori dell'economia e della qualità della vita"[76].

---

[73] Così S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, 119.

[74] In questo senso conclude D. Ielo, cit., 148.

[75] V. Comunicazione della Commissione, "*Appalti elettronici end-to-end per modernizzare la pubblica amministrazione*".

[76] Consiglio di Stato, Parere sullo schema del nuovo codice in materia di contratti pubblici, lavori, servizi e forniture, n. 855/2016.

AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

(Marco Cappai, Sara Perugini)

Social economy e tutela del consumatore: il ruolo dell'AGCM

*(Sara Perugini) **

In uno scenario come quello del mercato digitale caratterizzato da continui mutamenti, il presente contributo si prefigge di verificare, seppur di scorcio, se e in che misura i fenomeni che caratterizzano la c.d. social economy oggetto del presente Rapporto (Big Data, fake news *e* influencer*) siano riconducibili nell'ambito del quadro normativo esistente in materia di tutela del consumatore di competenza dell'Autorità Garante della Concorrenza e del Mercato.*

SOMMARIO: 1. PREMESSA. – 2. IL VALORE ECONOMICO DEI BIG DATA NEL DIRITTO DEI CONSUMI. – 3. LA SUSSISTENZA DI UN RAPPORTO DI CONSUMO TRA *SOCIAL MEDIA* E UTENTI: GLI INTERVENTI DELL'AGCM NEI CONFRONTI DI WHATSAPP. – 4. *INFLUENCER MARKETING*: IL FENOMENO E LE INIZIATIVE ASSUNTE A LIVELLO INTERNAZIONALE. – 5. SEGUE: L'INTERVENTO DELL'AUTORITÀ. – 6. *FAKE NEWS* E TUTELA DEL CONSUMATORE. – 7. CONCLUSIONI.

1. PREMESSA

Nell'ambito di una realtà come quella del mercato digitale europeo[77], accanto ai modelli di consumo collaborativo ricompresi nella c.d. *sharing economy* – sulla quale come si ricorderà si è incentrata la ricerca del 2016 – la c.d. *social economy* rappresenta il "*luogo*" in cui si sviluppano i principali fenomeni socio-economici oggetto di attenzione da parte di interpreti del diritto, organi di stampa e politica.

Responsabilità delle piattaforme *online,* profilazione degli utenti mediante l'impiego di tecnologie *Big Data & Big Analytics*[78]*,* diffusione delle *fake news*, nuove strategie pubblicitarie come il c.d. *influencer marketing*[79]*,* rappresentano i principali temi al centro del dibattito giuridico rispetto ai quali l'esigenza di ricercare e riscoprire un ruolo del *public*

[77] Come noto, l'Unione Europea ha intrapreso negli ultimi 4 anni un percorso volto a rafforzare ed integrare il mercato unico digitale europeo, sostenendo e accelerando la transizione verso una *Data-driven economy* europea, già incominciata da tempo in altri paesi (Stati Uniti e Cina). A tal fine, l'UE ha adottato una serie di misure e interventi per perseguire 3 macro obiettivi, vale a dire migliorare l'accesso ai beni e servizi digitali, creare un ambiente che favorisca lo scambio di tali beni e servizi e far diventare l'economia digitale il driver per la crescita futura dell'UE. Fra gli interventi che l'UE ha recentemente adottato, si evidenzia la Comunicazione della Commissione Europea, "*Costituire un'economia dei dati europei*", COM(2017) 9 final, 10 gennaio 2017, Bruxelles.

[78] In estrema sintesi i Big Data si differenziano dai "semplici" dati per (i) il volume, la quantità di dati raccolti è esplosiva; (ii) la velocità, i dati sono in continua evoluzione e necessitano di analisi just-in-time, effettuate tramite l'utilizzo di complessi algoritmi; (iii) la varietà, i dati cambiano a seconda del contenuto e del formato. In argomento, cfr. M. Huberty, *Awaiting the Second Big Data Revolution: From digital noise to value creation*, in *Journal of Industry, Competition and Trade*, Vol. 15 (2015), 35 ss.; Commissione Europea, 2 luglio 2014, COM(2014) 442 final, *Verso una florida economia basata sui dati* {SWD(2014) 214 final}; Id., *Building a european Data economy*, 10 gennaio 2017, COM(2017) 9 final Staff Working Document (2017) 2 final del 10 gennaio 2017 *On the free flow of Data and emerging issues of the European Data economy*.

[79] Cfr. infra § 4.

enforcement nella difesa dell'interesse pubblico alla correttezza del mercato, alla informazione e alla consapevolezza degli utenti nelle scelte di consumo si fa sempre più incessante.

In tale contesto, in assenza di una specifica cornice giuridica di riferimento, l'interprete è chiamato a verificare se e in che misura il diritto dei consumatori attualmente vigente sia in grado di definire e contenere i suddetti fenomeni, capacità alla quale fa da contrappasso la scelta, oggetto di annosi dibattiti, tra l'adozione di nuovi e specifici interventi normativi di natura regolatoria e la c.d. auto-regolamentazione del mercato[80].

La questione, per quanto qui di interesse, concerne la possibilità di ricondurre le suddette fattispecie in tutto o in parte nell'ambito delle norme a tutela del consumatore di competenza dell'Autorità Garante della Concorrenza e del Mercato che, è noto, accanto all'azione *antitrust* di tutela e promozione della concorrenza vanta attribuzioni esclusive in materia di pratiche commerciali scorrette[81], clausole vessatorie[82] e *consumer rights*[83].

In tale prospettiva, il presente contributo si prefigge di verificare, seppur per cenni, quali e quanti siano i passi in avanti sino ad oggi compiuti in sede di *enforcement pubblico* dall'*Antitrust* italiana nel contesto consumeristico e quali passi siano ancora da compiere rispetto ad un mercato tanto mutevole.

2. IL VALORE ECONOMICO DEI BIG DATA NEL DIRITTO DEI CONSUMI

Nel mercato digitale, le piattaforme *online*[84] svolgono un ruolo considerevole nella creazione del c.d. "*valore digitale*".

---

[80] L'autoregolamentazione, considerata a livello europeo una valida alternativa al processo legislativo, sembrerebbe essere la soluzione da privilegiare per combattere il fenomeno delle *fake news.*

[81] La letteratura in materia è vastissima. Per un aggiornamento sul tema, sia consentito rinviare a S. Perugini, *Le pratiche commerciali scorrette,* in *Diritto dei Consumi: Atto, attività, enforcement,* di Liliana Rossi Carleo (a cura di), Padova, 2015, Parte III, Capitolo I, pp. 161-202; tra i commentari più recenti, v. AA.VV: *Commentario breve al diritto dei consumatori (Codice del Consumo e legislazione complementare),* G. De Cristofaro e A Zaccaria (a cura di), Padova, 2013 nonché *ex multis AA.VV., Le modifiche al codice del Consumo*, E. Minervini e L. Rossi Carleo (a cura di), Torino, 2009; *AA.VV. Pratiche commerciali scorrette e codice del consumo*, G. De Cristofaro (a cura di), Torino, 2009; *AA.VV. Le pratiche commerciali sleali*, *Direttiva comunitaria ed ordinamento italiano* E. Minervini e L. Rossi Carleo (a cura di), Milano, 2007; *AA.VV., I decreti legislativi sulle pratiche commerciali scorrette. Attuazione e impatto sistematico della direttiva 2005/29/Ce,* a cura di A. Genovese, Padova, *2008; AA.VV., Pratiche commerciali scorrette e codice del consumo, Il recepimento della direttiva 2005/29/Ce nel diritto italiano (decreti legislativi nn. 145 e 146 del 2 agosto 2007),* G. De Cristofaro (a cura di), Torino, 2008*; AA.VV., Codice del consumo- Aggiornamento: pratiche commerciali scorrette ed azione collettiva,* G. Vettori (a cura di), Padova, 2009*;* P. Bartolomucci, *La proposta di direttiva sulle pratiche commerciali sleali: note a prima lettura*, in *Contratti*, 2005, 954 ss.; Id., *L'attuazione della direttiva sulle pratiche commerciali scorrette e le modifiche al codice del consumo*, in *Rass. dir. civ.*, 2008, 267 ss.; T. Broggiato, *La direttiva n. 2005/29 «sulle pratiche commerciali sleali»*, in *Dir. banc.*, 2006, II, 23 ss.; C. Chessa, *Le modifiche al codice del consumo introdotte dalla nuova agosto 2007, n. 146, attuativo della Direttiva 2005/29/CE),* in *Riv. giur. sarda,* 2007, 925 ss.; M. Dona*, Pubblicità, pratiche commerciali e contratti nel Codice del Consumo,* Torino, 2008.

[82] Sul punto si rinvia a L. Rossi Carleo, *La tutela amministrativa contro le clausole vessatorie*, in *Obbl. contr.*, 2012, 492 ss.; E. Minervini, *La tutela amministrativa contro le clausole vessatorie nei contratti del consumatore,* in questa *Rivista,* 2012, 563 ss.; A. Mirone, *Verso la despecializzazione dell'Autorità antitrust. Prime riflessioni sul controllo delle clausole vessatorie ai sensi dell'art. 37*-bis *cod. cons.*, in *AIDA*, 2012, 296 ss.

[83] Decreto Legislativo 21 febbraio 2014, n. 21 "*Attuazione della direttiva 2011/83/UE sui diritti dei consumatori, recante modifica delle direttive 93/13/CEE e 1999/44/CE e che abroga le direttive 85/577/CEE e 97/7/CE*". Per un'analisi, sia consentito rinviare a S. Perugini, *Il recepimento della Direttiva 2011/83/UE: prime riflessioni*, in *Giustizia Civile.com*, Giuffrè, 21 maggio 2014, 1-33.

[84] Le piattaforme presentano diverse forme e dimensioni, sono in continua evoluzione, e ricomprendono una vasta varietà di attività. Si distinguono, infatti, piattaforme pubblicitarie online, mercati, motori di ricerca, social media e punti vendita di contenuti creativi, piattaforme di distribuzione di applicazioni, servizi di comunicazione, sistemi di pagamento e piattaforme per l'economia collaborativa. Sui diversi modelli di *business* delle piattaforme *online* cfr. S. Perugini, *I mercati dell'innovazione e benessere dei consumatori. Nuovi scenari in ambito europeo e possibili riflessi sull'attività dell'Autorità Garante della Concorrenza e del Mercato,* in *Consumerism 2015, Ottavo Rapporto annuale, Il consumatore nell'era della condivizione,* § 6.

Tra queste i *social media* o *social networks* – in cui ciascun utente è invitato a creare la propria pagina e a offrire al giudizio degli altri i propri prodotti mettendo a disposizione del Professionista una mole ingente di informazioni collegate al proprio *account,* inclusi i dati personali e quelli dei propri contatti in rubrica[85] (Facebook, Twitter, YouTube, WhatsApp, Instagram) – si pongono al centro del noto dibattito concernente i cc.dd. Big Data oggetto del presente Rapporto.

In ambito consumeristico il tema cruciale è costituito dalla commercializzazione da parte delle piattaforme *social* dei dati e dei contenuti generati e condivisi dagli utenti (UGC*User's generated content*) e dalla loro rilevanza economica[86]. Nella maggior parte dei casi i *social media* offrono i propri servizi a titolo "*gratuito*".

Pertanto, in assenza di un corrispettivo pecuniario, la possibilità di sussumere le condotte tenute dalla piattaforma *social* nei confronti dei propri utenti nel quadro giuridico di competenza dell'*Antitrust* è condizionata alla sussistenza di un qualche vantaggio economico diretto o indiretto. Come noto, infatti, in assenza di un siffatto vantaggio il gestore della piattaforma non può considerarsi *professionista* di cui all'art. 18, lett. b) cod. cons. con conseguente esclusione di un *rapporto di consumo* con i propri utenti[87].

In proposito, occorre tener conto del clima di generale consapevolezza, maturato in ambiente sia europeo che nazionale[88], in ordine al fatto che i servizi offerti dalle piattaforme *online* apparentemente "*gratuiti*" presentino in realtà un costo: la cessione e/o l'accesso ai dati personali raccolti in esecuzione del rapporto.

Come già osservato nel contributo dello scorso anno, difatti, il modello di queste piattaforme sociali si basa sullo scambio di *privacy* contro servizi: il controvalore della prestazione fruita dal consumatore-utente è sovente costituito dalla possibilità per l'operatore di ricavare ricchezza dai dati personali sfruttandoli (o cedendoli) su mercati ulteriori o su altri versanti dello stesso mercato.

Le piattaforme *social* rappresentano, infatti, un *luogo privilegiato* di osservazione e archiviazione del comportamento degli utenti in rete, funzionale alla attività di *profilazione* che consente di individuare gli interessi e le preferenze di ciascun utente per fini commerciali e per finalità di *marketing*[89].

---

[85] Si tratta di soggetti che, come di recente evidenziato dalla Commissione europea nell'ambito della versione aggiornata delle linee guida sulle PCS, "*enable users to create profiles and communicate with each other, including sharing information and content, such as text, images and sound files. A social medium may be a chat room, a blog or a social network*" Cfr. SWD (2016) 163 final, del 25 maggio 2016, *Guidance in the implementation/application on directive 2005/29/EC on unfair commercial practices.* Secondo la stessa Autorità le piattaforme *social* "*svolgono oggi un ruolo di primo piano nella costruzione dei rapporti tra imprese e consumatori, grazie all'accessibilità, alla fruibilità dei contenuti e alla velocità con cui questi possono essere caricati e raggiunti dagli utenti*" Cfr. Relazione annuale dell'AGCM sull'attività svolta nel 2016, presentata il 31 marzo 2017.

[86] Un secondo interrogativo concerne il vantaggio competitivo eventualmente ricavabile dal possesso di tali dati. Non a caso l'AGCM ha deciso di avviare un'indagine conoscitiva diretta a comprendere se i Big Data possano essere considerati alla stregua di "*input o asset idonei a creare e/o rafforzare il potere di mercato di alcuni operatori, generare effetti di lock-in per gli utenti e costituire barriere all'entrata*" Cfr. delibera n. 26620 del 30 maggio 2017, di avvio della IC53 – *Big Data*. In dottrina, si rinvia a G. Pitruzzella, *Big Data, competition and privacy: a look from the antitrust perspective*, in *Concorrenza e mercato*, Vol. 23 (2016), 15 e ss.

[87] Trattandosi di una piattaforma occorre altresì dimostrare che la stessa svolga un ruolo attivo rispetto al servizio di memorizzazione delle informazioni fornite dagli utenti con conseguente esclusione della deroga sancita dall'art 14 della Direttiva n. 2000/31/CE. Come evidenziato nel Rapporto dello scorso anno, sotto tale profilo, il gestore della piattaforma *social* non si limita a fornire agli utenti in modo asettico un servizio di memorizzazione delle informazioni ma piuttosto un servizio di organizzazione e correlazione tra contenuti multimediali che in quanto tale dimostrerebbe l'assenza dell'elemento di neutralità. In tal senso cfr. S. Perugini, *I mercati dell'innovazione e benessere dei consumatori,* cit. § 6.

[88] "In molti casi, il consumatore accede al contenuto digitale gratuitamente, ovvero senza un esborso monetario: l'accesso, tuttavia, può essere retribuito attraverso la fornitura di dati personali dell'utente, ovvero tramite la rinuncia a diritti disponibili. Si tratta, in tali ipotesi, di contratti con prestazioni corrispettive, cui dovrebbe essere applicabile la disciplina a tutela del consumatore". E quanto si legge nella Relazione annuale dell'AGCM sull'attività svolta nel 2016, 252.

[89] Come rilevato in dottrina, negli ultimi anni si è registrato un fenomeno di accentramento delle forme di profilazione in capo a pochi soggetti *leader* del settore IT6. A differenza di quanto avveniva nel modello iniziale di *web* – incentrato su un pluralismo di offerte e di interlocutori – oggi poche Società, ciascuna leader nel proprio ambito, sembrano dominare il mercato. Di conseguenza questi pochi *Big players* detengono l'indiscusso controllo delle attività di profilazione dei propri utenti. I *Big*

Un siffatto patrimonio informativo acquista, in ragione di tale uso, un enorme valore economico e l'indubbia natura di controprestazione non pecuniaria del servizio fornito dal *social media*[90].

L'assunto sulla base del quale, lo vedremo a breve, l'AGCM è intervenuta nei confronti di WhatsApp azionando i poteri a lei attribuiti in materia di tutela del consumatore, è confermato da recenti ma consolidati orientamenti comunitari in sede consumeristica. La tesi presente nelle Linee Guida sulle PCS (*"Personal Data, consumer preferences and other user generated content, have a 'de facto' economic value and are being sold to third parties")*[91] è sviluppata anche nella proposta di direttiva 634/2015 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale, il cui art. 3 ("*Campo di applicazione*") recita: "*La presente direttiva si applica ai contratti in cui il fornitore fornisce contenuto digitale al consumatore, o si impegna a farlo, e in cambio del quale il consumatore corrisponde un prezzo oppure fornisce attivamente una controprestazione non pecuniaria sotto forma di dati personali o di qualsiasi altro dato*"[92].

---

players hanno, per loro natura, carattere sovranazionale.

[90] La dimostrazione della sussistenza di un vantaggio economico ottenuto dalla piattaforma mediante lo sfruttamento delle informazioni condivise dagli utenti per fini commerciali consente di qualificare anche il gestore della piattaforma "*social*" come *professionista* con ciò che ne deriva sul piano delle eventuali responsabilità. Cfr. in tal senso, S. Perugini, *I mercati dell'innovazione e benessere dei consumatori. Nuovi scenari in ambito europeo e possibili riflessi sull'attività dell'Autorità Garante della Concorrenza e del Mercato,* cit.

[91] Nella versione riveduta degli orientamenti relativi alla direttiva sulle pratiche commerciali sleali [SWD (2016) 163 final, del 25 maggio 2016], vengono descritti una serie fenomeni che caratterizzano l'attività dei *social media* o si sviluppano grazie ad essa e che, secondo la Commissione europea, potrebbero integrare pratiche commerciali scorrette. In particolare, si evidenzia che "*If a social media platform does not inform consumers that their personal Data will be processed for economic purposes it could be argued that it is omitting material information that the consumer needs to take an informed transactional decision. For such an omission to be unfair under Article 7 UCPD, it will have to be shown that it is likely to cause the average consumer to take a transactional decision he would not have taken otherwise*". Con ciò l'Esecutivo europeo mostra di riconoscere che la piattaforma trae un beneficio economico dal valore commerciale dei dati e delle informazioni fornite dagli utenti.

[92] Cfr. altresì il considerando (13) della Direttiva ove si legge: "*Nell'economia digitale, gli operatori del mercato tendono spesso e sempre più a considerare le informazioni sulle persone fisiche beni di valore comparabile al denaro. I contenuti digitali sono spesso forniti non a fronte di un corrispettivo in denaro ma di una controprestazione non pecuniaria, vale a dire consentendo l'accesso a dati personali o altri dati. Tali specifici modelli commerciali si applicano in diverse forme in una parte considerevole del mercato. Introdurre una differenziazione a seconda della natura della controprestazione significherebbe discriminare alcuni modelli commerciali e incoraggerebbe in modo ingiustificato le imprese ad orientarsi verso l'offerta di contenuti digitali contro la messa a disposizione di dati. Vanno garantite condizioni di parità eque. Inoltre, è possibile che una cattiva prestazione del contenuto digitale fornito in cambio di una controprestazione non pecuniaria abbia ripercussioni sugli interessi economici dei consumatori. L'applicabilità delle disposizioni della presente direttiva non dovrebbe pertanto dipendere dal pagamento o meno di un prezzo per il contenuto digitale in questione".* Il concetto viene ribadito anche nei paragrafi successivi. Il considerando (14) recita: "*Per quanto riguarda la fornitura di contenuto digitale non in cambio del pagamento di un prezzo ma di una controprestazione non pecuniaria, la presente direttiva dovrebbe applicarsi solo ai contratti in cui il fornitore richiede dati, quali il nome e l'indirizzo e-mail o foto e il consumatore glieli fornisce attivamente, in modo diretto o indiretto, ad esempio attraverso una procedura di registrazione individuale o sulla base di un contratto che consente l'accesso alle fotografie dei consumatori. La presente direttiva non dovrebbe applicarsi alle situazioni in cui il fornitore raccoglie i dati necessari affinché il contenuto digitale funzioni in conformità al contratto, ad esempio la localizzazione geografica se tale dato è necessario per il corretto funzionamento di un'applicazione mobile, o al solo scopo di soddisfare obblighi di legge, ad esempio nei casi in cui la registrazione del consumatore è obbligatoria ai fini di sicurezza e di identificazione. La presente direttiva non dovrebbe nemmeno applicarsi a situazioni in cui il fornitore raccoglie le informazioni, compresi i dati personali, quali l'indirizzo IP, o altre informazioni generate automaticamente, ad esempio le informazioni raccolte e trasmesse mediante un cookie, senza che il consumatore le fornisca attivamente, anche se accetta il cookie. Inoltre non dovrebbe essere applicata alle situazioni in cui il consumatore è esposto a messaggi pubblicitari esclusivamente al fine di ottenere l'accesso ai contenuti digitali*". Considerando (15): "*Il contenuto generato dai consumatori dovrebbe essere trattato alla stessa stregua di ogni altro contenuto digitale che il consumatore fornisce o memorizza per tutta la durata del contratto, quali musica e giochi, immagini, file video o applicazioni. Il contenuto generato dai consumatori comprende un'ampia gamma di esempi: che include immagini digitali, file video e audio, blog, forum di discussione, formati di testo collaborativi, chat, post, tweet, log, podcast, contenuti creati su dispositivi mobili, contenuti creati nel contesto di ambienti virtuali online, le sitografie e le valutazioni di contenuti on line*". Cfr. inoltre la "*Common position of national authorities within the CPC Network concerning the protection of consumers on social networks*", assunta ai sensi del Reg. (CE) 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa che tutela i consumatori e pubblicata il 17 marzo 2017, ove si legge che "*[s]ocial media operators supplying services to users residing in the European Union (and in other EEA countries) shall use terms of services in their contracts that are in conformity with Directive 93/13/EC on Unfair Contract Terms. This Directive applies to all contracts between consumers and businesses, regardless of whether they involve monetary consideration, including contracts where consumer generated content and profiling represent the counter-performance alternative to money*".

Del resto, oltre che in sede di tutela del consumatore l'orientamento della Commissione europea volto a riconoscere la natura di controprestazione non pecuniaria dei dati degli utenti dei *social media*, è, oramai, consolidato anche in sede di valutazione delle concentrazioni tra imprese. La Commissione, infatti, nell'esaminare i profili concorrenziali dell'acquisizione di WhatsApp da parte di Facebook[93], ha incluso numerose considerazioni sul valore economico dei dati degli utenti dei "*consumer communication services*"[94].

3. LA SUSSISTENZA DI UN RAPPORTO DI CONSUMO TRA SOCIAL MEDIA E UTENTI: GLI INTERVENTI DELL'AGCM NEI CONFRONTI DI WHATSAPP

In sede nazionale assumono indubbia rilevanza le decisioni dell'AGCM in materia di pratiche commerciali scorrette e clausole vessatorie nei confronti WhatsApp operatore che fornisce "*gratuitamente*" [95] i servizi di messaggistica istantanea e di chiamata utilizzando la connessione *internet* del dispositivo sul quale viene utilizzata l'applicazione WhatsApp Messenger.

Più nello specifico, come auspicato nel Rapporto dello scorso anno[96], l'Autorità ha adottato un primo provvedimento di scorrettezza[97] avente ad oggetto la condotta posta in essere da WhatsApp consistente nell'aver modificato, nel mese di agosto 2016, i termini di utilizzo, introducendo, tra le altre innovazioni, la condivisione con Facebook dei dati dell'*account* degli utenti WhatsApp e nell'aver invitato questi ultimi ad accettare i nuovi Termini rappresentando che, diversamente, essi non avrebbero più potuto continuare a utilizzare l'applicazione. A coloro che erano già utenti dell'applicazione alla data della modifica, WhatsApp offriva, tuttavia, la possibilità di accettarne "*parzialmente*" i contenuti. L'utente poteva, in particolare, decidere di non fornire l'assenso a condividere le informazioni del proprio *account* WhatsApp con Facebook. L'esistenza di un'opzione non veniva, però, rappresentata chiaramente nella schermata principale dedicata all'accettazione dei nuovi Termini di utilizzo in cui all'utente veniva genericamente indicato "leggi i termini e l'informativa sulla privacy per saperne di più sulle opzioni a tua disposizione"[98].

---

[93] Merger procedure, Case No. COMP/M.7217 – Facebook/WhatsApp, 3 ottobre 2014; 'Refining the EU merger control system', Speech by Commissioner Vestager, Studienvereinigung Kartellrecht, Brussels, 10 March 2016.

[94] Più nello specifico, è stato evidenziato come gli operatori di *social network* offrano i loro servizi, in genere, gratuitamente ricavando, tuttavia, una remunerazione non pecuniaria dalla pubblicità e dai servizi premium. La Commissione ha, inoltre, considerato il "*network effect*" quale elemento centrale per attribuire valore alle "*consumer communications apps*" valutando specificatamente l'impatto economico derivante dalla possibile integrazione tra WhatsApp e Facebook in termini di "*cross-platform communication*", finalizzata a consentire agli utenti dei due *social media* di comunicare tra loro, confermando, anche sotto tale aspetto, il valore economico attribuito ai dati a disposizione delle due piattaforme. La Commissione ha, poi, analizzato, sempre presupponendo il valore economico dei dati, l'effetto della concentrazione tra Facebook e WhatsApp in termini di "*Data collected from WhatsApp's users*" affermando che "[*t*]*his would have the effect of reinforcing Facebook's position in the online advertising market or sub segments thereof".* La Commissione ha, infine, considerato, nell'analisi economica svolta a fini concorrenziali, gli effetti migliorativi dell'utilizzo dei dati degli utenti di WhatsApp sull'attività di *advertising* di Facebook (cfr. caso No. COMP/M.7217 – FACEBOOK/WHATSAPP, §129 ss.).

[95] La gratuità, evidenziata, peraltro, nei *claim*s pubblicitari inseriti negli *stores* digitali che distribuiscono WM, si fonda sulla scelta del Professionista di fornire l'applicazione e i relativi servizi senza richiedere all'utente alcun pagamento ed è il risultato della mutata politica commerciale, adottata da WhatsApp a partire da gennaio 2016.

[96] Cfr. in tal senso S. Perugini, *I mercati della "condivisione sociale" in Europa e in Italia. Il ruolo cruciale dell'Autorità Garante della Concorrenza e del Mercato, ,* in *Consumerism 2016, Nono Rapporto annuale*, dalla *Sharing alla Social Economy*, § 6 & 7.

[97] Cfr. provv. n. 26597 dell'11 maggio 2017, PS/10601, *Whatsapp trasferimento dati a Facebook*, in *Boll.* 18/2017.

[98] Solo nella schermata successiva, alla quale si accedeva cliccando sul *link* che rimandava alla lettura dei Termini e dell'informativa sulla *privacy,* l'utente si accorgeva, in realtà, di avere una scelta alternativa che risultava, peraltro, pre-impostata, tramite spunta nell'apposita casella, sul consenso alla condivisione dei dati. Se l'utente non avesse voluto condividere i propri dati con Facebook avrebbe dovuto deselezionare la spunta. Nella schermata in cui appariva l'opzione "Facebook" l'utente veniva, inoltre, sommariamente informato dello scopo della condivisione, ossia "*migliorare*" le proprie esperienze *"con le inserzioni*

L'Autorità ha qualificato il comportamento dell'operatore come pratica commerciale aggressiva in violazione degli artt. 20, 24 e 25 cod. cons. [99] dopo aver evidenziato che "Il patrimonio informativo costituito dai dati degli utenti di WhatsApp, utilizzato per la profilazione degli utenti medesimi a uso commerciale e per finalità di marketing, acquista, proprio in ragione di tale uso, un valore economico idoneo, dunque, a configurare l'esistenza di un rapporto di consumo tra il Professionista e l'utente"[100].

Con un secondo provvedimento l'Autorità ha poi accertato la vessatorietà di una serie di clausole inserite nei "*Termini di utilizzo*" di WhatsApp Messenger riguardanti, in particolare, la facoltà di modifiche unilaterali del contratto da parte della società, il diritto di recesso stabilito unicamente per il professionista, le esclusioni e le limitazioni di responsabilità a suo favore, le interruzioni ingiustificate del servizio, la scelta del Foro competente sulle controversie stabilito esclusivamente presso Tribunali americani[101].

Entrambe le decisioni si fondano su una premessa: la rilevanza economica dei dati e delle informazioni fornite dagli utenti che rappresentano a tutti gli effetti la controprestazione del servizio offerto dal *social media*, assunto da cui discende quale diretto corollario la qualificazione del gestore della piattaforma "*social*" come *professionista* con ciò che ne deriva sul piano delle eventuali responsabilità e della sussistenza di un *rapporto di consumo* tra piattaforma *social* e utenti.

4. INFLUENCER MARKETING: IL FENOMENO E LE INIZIATIVE ASSUNTE A LIVELLO INTERNAZIONALE

I *social* e tra questi quelli utilizzabili con estrema facilità da cellulare e con una messaggistica istantanea (le cc.dd. piattaforme *mobile-first* come Instagram, Facebook, Snapchat) rappresentano anche il luogo dove viene attuata una nuova strategia pubblicitaria di grande attualità, preferenzialmente destinata alle generazioni del nuovo millennio (nativi digitali): il c.d. *influencer marketing*.

Tale strategia è caratterizzata da messaggi diffusi su *social network* da "*influencers*"[102] – personaggi di riferimento del

---

e i prodotti di Facebook". Il testo che descriveva l'opzione era formulato in modo tale da porre l'accento sul vantaggio recato all'utente, quasi a voler sottolineare una sorta di servizio aggiuntivo offerto gratuitamente dal Professionista al consumatore, in cambio dei suoi dati personali.

[99] In particolare, l'indebito condizionamento secondo l'A. deriva dall'aver, di fatto, forzato gli utenti di WhatsApp Messenger ad accettare la condivisione dei dati con Facebook, facendo loro credere che sarebbe stato, altrimenti, impossibile proseguire nell'uso dell'applicazione laddove coloro che erano già utenti alla data della modifica dei Termini, avevano, invece, la possibilità di accettarne "parzialmente" i contenuti. L'utente avrebbe potuto, in particolare, decidere di non fornire l'assenso a condividere le informazioni del proprio *account* WhatsApp con Facebook e continuare, comunque, a utilizzare WM. Secondo l'A. l'effetto di condizionamento è stato, determinato dal contenuto della prima schermata e dalla prespuntatura apposta sull'opzione di selezione del consenso nella seconda schermata, quindi dall'*opt-out*, a cui hanno avuto accesso coloro che, nonostante la conclamata necessità di accettazione, avessero desiderato conoscere i nuovi Termini di utilizzo del servizio.

[100] Sotto il profilo probatorio la rilevanza economica dei dati degli utenti di WhatsApp e la finalità stessa della pratica in esame è stata dimostrata prendendo in considerazione le dichiarazioni stesse rese dal professionista nel corso dell'istruttoria. In particolare, la Parte ha rappresentato che l'attività di condivisione dei dati con Facebook avrebbe migliorato l'attività di *advertising* della medesima e generato ricavi direttamente a Facebook.

[101] Cfr. Provv. n. 26596 dell'11 maggio 2017, CV/154, *Whatsapp clausole vessatorie*, in *Boll.* 18/2017. Peraltro, nella sua adunanza del 9 agosto 2017, l'. A. ha avviato nei confronti di WhatsApp un procedimento di inottemperanza per non aver dato seguito all'ordine di pubblicazione disposto dall'autorità.

[102] Gli *influencer* possono essere sia personaggi famosi sia persone comuni in grado di influenzare le decisioni di acquisto del pubblico. Possono diventare *influencer*, infatti, anche ragazzi e ragazze comuni che, per qualche motivo, suscitano interesse in un pubblico di massa senza avere la fama dei personaggi del mondo dello spettacolo. Nella generica categoria degli *influencers* può assumere rilievo la distinzione tra coloro che sono noti solo in virtù della loro presenza sui *social*, esercitando professionalmente l'attività di *fashion blogger o youtuber* di varia natura e derivando un reddito da tale attività, e coloro che sono invece noti per svolgere altra professione (attore, sportivo ecc.) e

mondo *online* che hanno un numero elevato di *followers* – che mostrano prodotti in evidenza con *brand* riconoscibili senza rappresentare in modo trasparente il loro carattere promozionale[103].

Il fenomeno che integra a tutti gli effetti una ipotesi di *pubblicità occulta*, è stato attenzionato in diversi paesi da parte delle Autorità a tutela del consumatore che hanno assunto iniziative per sollecitare imprese, agenzia pubblicitarie e *influencer* al rispetto dei principi contenuti nelle normative a tutela del consumatore in relazione all'obbligo di evidenziare in modo trasparente intenti commerciali nelle comunicazioni al pubblico. Gli interventi che nella maggior parte dei casi hanno assunto la forma di linee guida, lettere al mercato o "*moral suasion*" a una moltitudine di soggetti, hanno in comune la circostanza che la base normativa è quella generale a tutela del consumatore, senza che vi siano previsioni *ad hoc* per i *social network*.

E così, ad esempio, nelle linee guida[104] relative al fenomeno in esame rese pubbliche ad esito di un gruppo di lavoro dall'ICPEN – che raggruppa le Autorità preposte all'applicazione della normativa a tutela del consumatore di 60 Paesi – vengono fissati i principi che i diversi attori debbono rispettare quando diffondono *post*, *tweets*, *blog*, articoli sul *web*, video[105]. Gli *influencer*, i produttori e i professionisti del *marketing* devono rendere noto in modo chiaro ed evidente, da un lato, se il contenuto è stato diffuso a pagamento o se il bene o servizio è stato fornito gratuitamente dal produttore; dall'altro, se vi sono altri rapporti commerciali rilevanti con i produttori, ad esempio se il personaggio è, in generale, il *testimonial* del marchio oggetto del *post*, anche se non vi è stato un pagamento specifico per una singola foto o dichiarazione[106].

In US, la Federal Trade Commission (FTC) ha emanato "*Guides Concerning the Use of Endorsements and Testimonials in Advertising*", riferite ad ogni tipologia di mezzo di comunicazione che disciplinano in modo dettagliato come devono essere resi pubblici eventuali rapporti tra produttori e quei consumatori che rendono pubblico il loro sostegno e approvazione per un prodotto, su tutti i media. Tali rapporti assumono rilevanza se prevedono, oltre che un compenso, anche la fornitura gratuita di prodotti, l'esistenza di un interesse aziendale diretto, o di interessi di origine familiare[107].

---

pubblicano immagini sui propri profili social. Inoltre, quasi tutti i *fashion blogger*, hanno anche siti di *e-commerce* dove vendono alcuni dei prodotti posti in evidenza e che vengono citati talvolta nei post.

[103] "La forza trainante e peculiare del fenomeno è che gli *influencer* sono sinonimo di credibilità dato che riescono ad instaurare una connessione autentica con la loro audience. É infatti noto che quando il messaggio proviene dall'azienda, i consumatori sono più scettici e percepiscono la finalità di vendita promossa dalla pubblicità, mentre, quando il prodotto è presentato su un *social media*, si determina un diverso approccio che i consumatori vivono come un consiglio del personaggio". Cfr. il comunicato dell'AGCM pubblicato il 24 luglio 2017 sul sito www.agcm.it.

[104] "*Online reviews &endorsements*" ICPEN Guidelines for Digital Influencers, ICPEN Guidelines for Traders &Marketing Professionals (June 2016) https://www.icpen.org/for-consumer-experts/what-we-do/industry-participant-guidance.

[105] In tali linee guida si evidenza la rilevanza del fenomeno di "*online review and endorsements*", che dà alle imprese nuove possibilità di fare pubblicità ai propri prodotti tramite i "*digital influencers*" utilizzando "*native adverstising*", che è una pratica assolutamente legittima. Tuttavia, se l'informazione fornita non esprime le reali preferenze dell'*influencer*, ma è distorta da interessi economici, ciò deve essere rappresentato in modo appropriato, altrimenti il consumatore non comprende che si tratta di pubblicità, con pregiudizio per il consumatore e la concorrenza.

[106] I produttori e i professionisti del *marketing* devono assicurarsi che tutte le parti coinvolte nel processo di diffusione della pubblicità rendano manifesto in modo chiaro la presenza di contenuti sponsorizzati e non devono chiedere a *bloggers*, *vloggers*, *tweeters* e altri *influencers* digitali di nascondere i loro legami commerciali. Inoltre, debbono controllare che le istruzioni impartite ai dipendenti, le politiche interne e i contratti riflettano tali principi di trasparenza.

[107] Successivamente, nel 2015, la FTC ha dettagliato le modalità con cui tali principi debbono essere applicati in modo specifico ai "*social media*", con un testo nella forma di "*Questions & Answers*" nel quale si delineano varie casistiche possibili. Nel documento si evidenzia che: a) l'effetto pubblicitario si può produrre anche con una foto non accompagnata da commenti; b) è rilevante rendere esplicita l'esistenza di un legame tra l'influencer e il prodotto sia perché non è scontato che gli *influencer* ricevano sempre un compenso, sia perché solo alcuni consumatori più evoluti potrebbero riconoscere la natura pubblicitaria di un post, in assenza di indicazioni esplicite; c) al fine di individuare l'esistenza di una pubblicità occulta, occorre valutare se i consumatori sono consapevoli dell'esistenza di un rapporto economico tra *influencer* e produttore. Ad esempio, per uno sportivo che notoriamente è il *testimonial* di un marchio, o per un *influencer* che regolarmente cita marchi di moda sui *social*, potrebbe essere evidente l'intento promozionale.

Inoltre, nel maggio 2017 la FTC ha inviato "*advisory letters*" a circa 45 imprese e 45 influencers in relazione alle modalità con cui viene effettuato il "*product endorsement*", attraverso Instagram con riferimento specifico a singoli post allegati alle lettere stesse.[108] In tali lettere, aventi natura di raccomandazione, o *moral suasion*, viene sollecitato il rispetto di un serie di regole[109], allegando post esemplificativi di violazioni, secondo il principio generale che devono essere evidenziate in modo chiaro eventuali connessioni con il prodotto mostrato[110].

In UK, la *Competition and Market Authority* (CMA) ha effettuato un'indagine di settore relativa a "*online reviews and endorsements*", ad esito della quale ha pubblicato differenti "*open letters*"[111] a agenzie di pubblicità, ai loro clienti, e a chi pubblica contenuti editoriali *online*, come *influencers,* richiamando al rispetto sulla normativa a tutela del consumatore, la quale prevede che le comunicazioni commerciali, anche sui *social networks*, devono essere chiaramente riconoscibili.[112]

Altre Autorità come l'Autorità norvegese a tutela del consumatore (ForbrukerOmbudet) e quella FinaIndese (KKV) hanno pubblicato linee guida che richiamano al rispetto della normativa in tema di pubblicità trasparente anche sui *social media*.

In sintesi, da tali interventi emerge che la natura promozionale della comunicazione deve essere resa manifesta, sia che discenda da uno specifico pagamento per il singolo *post*/*blog*/video, sia nel caso in cui il prodotto sia fornito a titolo gratuito, sia se l'*influencer* è in generale il *testimonial* del marchio. Inoltre, la linea comune di detti interventi è che per rendere inequivocabilmente chiara la finalità pubblicitaria occorre inserire nella comunicazione diciture come "pubblicità/messaggio promozionale" e similari, o in ogni caso elementi formali[113]. Altro elemento rilevante desumibile dall'esperienza internazionale è che non sono stati definiti né criteri utili all'individuazione della natura occulta delle pubblicità, né rigide modalità per rendere palese l'intento commerciale.

5. SEGUE: L'INTERVENTO DELL'AUTORITÀ

Ciò posto, lo scorso luglio, in linea con le esperienze maturate in sede internazionale brevemente descritte, l'Autorità *Antitrust* italiana ha inviato lettere di *moral suasion* ad alcuni dei principali *influencer* e alle società titolari dei marchi

[108] http://www.socialmedialawbulletin.com/2017/05/ftc-instagram-posts-endorsement-guides/

[109] Nelle lettere, si precisa che "*se esiste un legame commerciale*" tra l'*influencer* e il *brand*, questo deve essere esplicitato. In particolare, poi, si invitano le imprese a verificare la correttezza delle politiche aziendali relative ai social media e a dotarsi di linee guida scritte di riferimento per i propri *influencer*.

[110] Ciò deve essere fatto inserendo negli hashtag in modo chiaro diciture come "*sponsorizzato*" "*partner*" "*pubblicità*" "*l'azienda X mi ha dato il prodotto da provare*". Vengono quindi dettagliati una serie di criteri relativi alla trasparenza informativa. Ad esempio, non è sufficiente che venga citato il nome del *brand* all'interno di una lunga serie di *hashtag*; l'*hashtag* deve essere visibile senza la necessità di dover abbassare una tendina non è sufficiente citare il nome del *brand* come sigla, ma per esteso.
È posto in capo alle imprese l'onere di inserire nei contratti con gli *influencers* regole che rendano il post sui *social* ottemperanti rispetto a tali indicazioni.

[111] https://www.gov.uk/government/collections/online-reviews-and-endorsements-information-for-businesses.

[112] Secondo la CMA, gli *influencer* non possono far credere di agire come consumatori quando in realtà stanno promuovendo un *brand*. Il fine commerciale dell'inserimento di un prodotto in un post deve essere chiaro e comprensibile, con diciture in evidenza nei *post* come "pubblicità". Anche la CMA non ha fornito indicazioni rigide e specifiche su come rendere esplicito l'intento commerciale. Si afferma tuttavia che, per esempio, gli *influencers* potrebbero mettere in evidenza nei *post* e video diciture come "Promozione Pubblicitaria" (*Advertisement Promotion),* "Informazione Pubblicitaria" *(Advertisement Feature)*. https://www.gov.uk/government/collections/online-reviews-and-endorsements-information-for-businesses.

[113] Elementi che, secondo la prassi interpretativa dell'Autorità in materia, potrebbero consistere anche in accorgimenti grafici e/o acustici di evidente percezione.

visualizzati senza l'indicazione evidente della possibile natura promozionale della comunicazione[114].

Nelle proprie lettere, l'Autorità dopo aver ricordato che la pubblicità deve essere chiaramente riconoscibile come tale, affinché l'intento commerciale di una comunicazione sia percepibile dal consumatore, ha evidenziato come il divieto di *pubblicità occulta* abbia portata generale e debba, dunque, essere applicato anche con riferimento alle comunicazioni diffuse tramite i *social network*, non potendo gli *influencer* lasciar credere di agire in modo spontaneo e disinteressato se, in realtà, stanno promuovendo un *brand*.

L'Autorità ha, pertanto, individuato criteri generali di comportamento e ha chiesto di rendere chiaramente riconoscibile la finalità promozionale, ove sussistente, in relazione a tutti i contenuti diffusi mediante social media, attraverso l'inserimento di avvertenze, quali, a titolo esemplificativo e alternativo, #pubblicità, #sponsorizzato, #advertising, #inserzioneapagamento, o, nel caso di fornitura del bene ancorché a titolo gratuito, #prodottofornitoda; diciture alle quali far sempre seguire il nome del marchio.

Inoltre, considerato che il fenomeno del *marketing* occulto è ritenuto particolarmente insidioso, in quanto è in grado di privare il consumatore delle naturali difese che si ergono in presenza di un dichiarato intento pubblicitario**,** l'Autorità ha contestualmente sollecitato con un comunicato rivolto al mercato, tutti gli operatori coinvolti a vario titolo nel fenomeno a conformarsi alle prescrizioni del Codice del consumo, "fornendo adeguate indicazioni atte a rivelare la reale natura del messaggio, laddove esso derivi da un rapporto di committenza e abbia una finalità commerciale, ancorché basato sulla fornitura gratuita di prodotti".

6. FAKE NEWS E TUTELA DEL CONSUMATORE

Come noto, le tematiche poste dalle cc.dd. *fake news* sono oggetto di un dibattito che vede schierarsi, da un lato, i promotori di sistemi di auto-regolamentazione da parte dei *Big* del *web* che hanno annunciato lo sviluppo di algoritmi finalizzati a rimuovere le informazioni false e virali[115]; dall'altro, i sostenitori di rimedi attuati attraverso interventi legislativi o regolamentari volti sia a costituire organismi deputati a definire regole per l'individuazione, la verifica e la rimozione delle informazioni false o calunniose, sia a fare obbligo alle piattaforme di rimuoverle[116].

La soluzione del fenomeno appare, almeno allo stato, ancora lontana.

Viene, pertanto, da chiedersi se e fino a che punto la vigente legislazione in materia di tutela del consumatore (costruita intorno a nozioni ben definite di professionista e consumatore) non trovi applicazione rispetto ad un fenomeno che

[114] È quanto si legge nel comunicato stampa pubblicato il 24 luglio 2017 sul sito www.agcm.it.

[115] Google ha annunciato modifiche all'algoritmo che regola il funzionamento del *searching*. Il motore *online* punterà a privilegiare sempre più pagine *web* di qualità, ad esempio assegnando un peso maggiore a fonti autorevoli, assegnando un ruolo chiave ai valutatori e tenendo sempre più conto delle segnalazioni "umane" sui contenuti inappropriati. Wikipedia ha creato Wikitribune, una piattaforma che promette di dare spazio solo a storie ed articoli scritti da giornalisti professionisti, grazie al ruolo di volontari che certificheranno la correttezza di notizie e dati. Facebook ha annuciato un nuovo strumento informativo per aiutare gli utenti a distinguere le notizie attendibili da quelle false, o satiriche. Facebook introdurrà un *tool* in alto al NewsFeed: quando si cliccherà, si potrà accedere a più informazioni e risorse all'interno del Centro Assistenza Facebook, dove sono presenti consigli e un decalogo su come individuare meglio notizie false, come ad esempio controllare l'Url del sito, investigare sulle fonti e cercare altre segnalazione sul tema.

[116] Depone a favore di un intervento normativo l'AGCom che, tuttavia, sottolinea come forme di controllo siano difficili da attuare in quanto dovrebbero essere condivise a livello globale. Per contro la sfiducia verso sistemi di autoregolamentazione deriva dal dubbio che in assenza di un controllo esterno e terzo, questi operatori siano effettivamente disponibili a sacrificare i ricchi introiti pubblicitari a favore di costi per il contenimento dei danni in reputazione depone a favore di un intervento normativo la preoccupazione per l'eccessivo potere delle piattaforme *online*. Cfr. Relazione annuale sull'attività svolta nel 2016.

si pone al di fuori dei tradizionali schemi sui quali si fonda tradizionalmente la normativa europea in ambito consumeristico.

In linea generale, l'opinione giuridica tende ad escludere che il problema delle *fake news* strettamente intese – ossia la diffusione voluminosa, istantanea e incontrollata di notizie deliberatamente falsificate o manipolate che nulla hanno a che fare con la vendita di un prodotto – possa essere ricondotto nella cornice giuridica a tutela del consumatore di competenza dell'Autorità.

A ben vedere, tuttavia, in alcune circostanze, la diffusione di *fake news* potrebbe integrare una pratica commerciale scorretta. Si pensi al caso in cui la tecnica della *fake news* venga impiegata su un sito un *blog* o la pagina *social* di una testata giornalistica per trarre profitto dai "*click*" su inserzioni pubblicitarie ivi collocate. Il comportamento potrebbe integrare una azione "*ingannevole*", in quanto l'utente verrebbe esposto a inserzioni pubblicitarie che non avrebbe visto in mancanza di "titoli" decettivi e artatamente suggestivi che ne hanno stimolato il *click*. In una ipotesi di questo tipo, la vera questione concerne il grado di responsabilità delle piattaforme, tema che, è noto, interessa l'intero mercato digitale.

In estrema sintesi, si ritiene che la piattaforma dovrebbe considerarsi responsabile non solo nel caso di predisposizione della pagina contenente la *fake news*, ma anche nel caso di omessa e/o inadeguata vigilanza sui contenuti editati da terzi e ospitati sui propri spazi al ricorrere a condizione che sia destinataria di uno specifico vantaggio economico e che ricopra una *posizione di controllo* tale da consentirgli di prevenire la realizzazione della pratica commerciale[117].

7. CONCLUSIONI

In conclusione, l'impressione è che nel corso degli ultimi anni l'*Antitrust* italiana nella sua funzione di garante della tutela del consumatore stia svolgendo, nel contesto della *social economy*, una efficacie attività di *enforcement* a protezione del consumatore e ricopra un ruolo cruciale nel mercato digitale europeo.

In un contesto dove lo sviluppo delle piattaforme digitali rende sempre più evidente l'intreccio tra questioni di tutela del consumatore e gestione dei dati personali e relative discipline[118], il riconoscimento formale da parte dell'AGCM del valore economico dei dati ceduti dagli utenti e della loro natura di controprestazione non pecuniaria così come le iniziative assunte rispetto al fenomeno degli *influencer*, rappresentano importanti passi avanti nell'applicazione degli

[117] In tal senso si pensi all'intervento dell'Autorità che nell'affrontare il problema delle cc.dd. *fake reviews* ha attribuito al gestore di un di strutture ricettive consultabili gratuitamente dagli utenti, la responsabilità per le cc.dd. false recensioni, riconoscendone la qualifica di professionista in considerazione del fatto che, la messa a disposizione di informazioni turistiche avviene in un contesto in cui la stipula di accordi per la vendita di spazi pubblicitari agli inserzionisti e la sottoscrizione di contratti per l'attivazione di profili *business* costituiscono la remunerazione del professionista (cfr. Provv. del 19 dicembre 2014, n. 25237, PS9345 in *Boll.* 50/2014). In forma analoga, nel settore dei comparatori assicurativi, l'Autorità ha individuato nel gestore della piattaforma una specifica responsabilità in merito alla diffusione di false informazioni in merito alla natura della prestazione e alla rappresentatività dei confronti, derivante dalla qualifica del gestore quale *broker* assicurativo destinatario di uno specifico vantaggio economico in considerazione della remunerazione concordata con le imprese di assicurazione (Provv. dell' 8 aprile 2015, n. 25420, in *Boll.* 14/2015). Cfr. in tal senso S. Perugini, *I mercati dell'innovazione e benessere dei consumatori. Nuovi scenari in ambito europeo e possibili riflessi sull'attività dell'Autorità Garante della Concorrenza e del Mercato,* in *Consumerism 2015*, *Ottavo Rapporto annuale*, *Il consumatore nell'era della condivisione*, 17 ss.

[118] Le istanze di tutela della riservatezza provenienti dagli utenti di fronte ai colossi della *social economy* restano poi prioritariamente affidate al Garante della privacy, soggetto con il quale tutte le Autorità di vigilanza dovranno necessariamente dialogare in tutti i casi in cui intendano intraprendere iniziative dirette a tutelare (anche) la *privacy* dei consumatori-utenti.

schemi di tutela consumeristica di sua competenza, in grado di garantire la salvaguardia dei diritti degli utenti anche facendo propri i principi elaborati in sede europea e internazionale.

Difatti, se, da un lato, il fenomeno delle *fake news* potrebbe essere ricondotto solo in parte e in modo *indiretto* nell'ambito del Codice del consumo, restando necessariamente affidato, in assenza di uno specifico intervento normativo, alla *auto-regolamentazione* da parte delle piattaforme *online* che si auspica divenire sempre più capillare e efficaci; dall'altro, i provvedimenti adottati in sede di *enforcement* pubblico, testimoniano l'efficienza del quadro normativo vigente a tutela del consumatore nel rispondere ai cambiamenti di mercato accompagnando la trasformazione tecnologica propria di una realtà come la *social economy*, dove i confini nazionali perdono di significato e la persona si pone al centro di una rete di relazioni in maniera sempre più "*circolare*".

Social economy, gestione dei dati e *tutela della concorrenza*

(*Marco Cappai*)

Come sovente accade di fronte alle principali innovazioni tecnologiche, anche il fenomeno dei Big Data & Big Analytics *è sorto in mancanza di un quadro normativo di riferimento, portando con sé il problema del regime giuridico da applicarvi. Ci si è allora chiesti se il diritto della concorrenza possa giocare un ruolo in questa partita, andandosi ad affiancare ad uno o più degli altri campi di disciplina oggi esistenti (tutela del consumatore e della* privacy*, proprietà industriale, regolazione economica, ecc.). Coerentemente con le finalità del presente Rapporto, si tenteranno di analizzare due possibili abusi di posizione dominante che, nell'era dei Big Data e della* social economy*, potrebbero in tesi avere un impatto diretto sui consumatori: quella della "discriminazione" realizzabile attraverso l'elaborazione di prezzi "personalizzati" e quella dell'imposizione di condizioni sulla privacy illegittime. Introdotto il tema e osservate le iniziative sin qui intraprese sul punto dai* competition enforcers*, si cercheranno di svolgere alcune prime considerazioni sugli ulteriori passi che le istituzioni della concorrenza potrebbero utilmente compiere.*

SOMMARIO: 1. LA RILEVANZA DEI BIG DATA NEL DIRITTO DELLA CONCORRENZA: LE QUESTIONI APERTE E LE INIZIATIVE SINORA ASSUNTE DALL'AGCM. – 2. *BIG DATA & BIG ANALYTICS*, PROFILAZIONE E PREZZI PERSONALIZZATI: UNA POSSIBILE IPOTESI DI PREZZI DISCRIMINATORI *EX* ARTT. 102, LETT. C) TFUE E 3, LETT. C) LEGGE N. 287/1990? – 3. ABUSO DI SFRUTTAMENTO *EX* ARTT. 102, LETT. A) TFUE E 3, LETT. A) LEGGE N. 287/1990. IL CASO AVVIATO DAL BUNDESKARTELLAMT CONTRO FACEBOOK. – 4. CONCLUSIONI.

1. LA RILEVANZA DEI BIG DATA NEL DIRITTO DELLA CONCORRENZA: LE QUESTIONI APERTE E LE INIZIATIVE SINORA ASSUNTE DALL'AGCM

La complessità dei fenomeni socio-economici analizzati nel presente Rapporto è attestata dal fatto che, per un verso, gli stessi si sono sviluppati e diffusi in assenza di una specifica cornice giuridica di riferimento e, per altro verso, non si registra uniformità di vedute su quali strumenti giuridici applicare tra quelli messi a disposizione dai campi di disciplina oggi esistenti.

Si è visto che alcune delle problematiche sollevate dalla *social economy* – tra cui la profilazione degli utenti attraverso l'impiego di tecnologie *Big Data & Big Analytics*, la diffusione di *fake news* e l'indebita attività di orientamento delle scelte di consumo talvolta esercitata dagli *influencer* – possono, in determinati casi, tamponarsi attraverso i poteri di tutela del consumatore affidati all'AGCM[119].

In questo contesto non è mancato chi ha auspicato un intervento di tipo complementare anche dei *competition officers* (e, tra questi, della stessa AGCM) per affrontare le sfide lanciate dalla *social economy*.

Più precisamente, mentre non si ravvisano, almeno in linea di principio, particolari criticità concorrenziali con rife-

[119] V. la Prima Parte del presente Capitolo.

rimento al problema delle *fake news*[120] e dei messaggi pubblicitari talvolta celatamente veicolati dagli *influencer*[121], alcuni studiosi (e con essi le medesime istituzioni di tutela della concorrenza) si stanno chiedendo a quali condizioni il fenomeno dei *Big Data & Big Analytics* possa dar luogo a comportamenti anticompetitivi e, se del caso, in che misura gli strumenti di *enforcement* ad oggi esistenti possano risultare utili a ristabilire l'equilibrio concorrenziale del mercato.

La constatazione di partenza è che stiamo assistendo ad una vera e propria "rivoluzione industriale" in cui le imprese accumulano ed elaborano ingenti masse di dati, prevalentemente personali, al fine di ricavarne come *output* una più mirata programmazione degli investimenti e delle strategie commerciali[122].

In questo rinnovato ambiente di mercato il primo, importante quesito da sciogliere è, dunque, se il possesso di tali *dataset* possa, di per sé, attribuire un vantaggio competitivo non replicabile alle imprese (e, pertanto, rilevare ai sensi della disciplina di tutela della concorrenza)[123].

È quanto si stanno chiedendo anche i *competition enfrocers*, i quali hanno raccolto le sfide lanciate dall'economia

---

[120] In linea di principio il problema delle *fake news* non sembra poter assumere, o almeno non in quanto tale, rilevanza anticoncorrenziale. La repressione del fenomeno potrebbe interessare l'AGCom, munita di poteri volti a garantire – e a preservare – il pluralismo informativo (su questo v. Cap. ? [Pellicanò – Angelini – Petti]), oppure potrebbe essere affidato, *de iure condendo*, un'agenzia *ad hoc*, come suggerito dal Presidente dell'AGCM Giovanni Pitruzzella in un'intervista rilasciata al Financial Times (https://www.ft.com/content/e7280576-cddc-11e6-864f-20dcb35cede2). In determinati casi potrebbe infine immaginarsi un intervento dell'AGCM in funzione di tutela dei consumatori (v. prima Parte, § 6).

[121] Come visto nella Prima Parte del presente Capitolo (§ 5), sulla scorta di un'interpretazione evolutiva della nozione di "*professionista*" di cui all'art. 18, lett. b) Codice del consumo, l'AGCM ha inviato una *moral suasion* ad alcuni *influencer* che avevano diffuso messaggi pubblicitari in modo occulto (cfr. http://www.agcm.it/stampa/comunicati/8853-antitrust-su-influencer-marketing-la-pubblicit%C3%A0-deve-essere-sempre-trasparente.html, Comunicato stampa del 24/7/2017).

[122] Cfr. M. Huberty, *Awaiting the Second Big Data Revolution: From digital noise to value creation*, in *Journal of Industry, Competition and Trade*, Vol. 15 (2015), 35 e ss.; OECD, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris, 2015, http://dx.doi.org/10.1787/9789264229358-en; R. Davies, European Parliamentary Research Service (EPRS), *Big Data and Data analytics. The potential for innovation and growth*, settembre 2016, http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589801/EPRS_BRI(2016)589801_EN.pdf; Commissione europea, 2 luglio 2014, COM(2014) 442 final, *Verso una florida economia basata sui dati* {SWD(2014) 214 final}; Id., *Building a european Data economy*, 10 gennaio 2017, COM(2017) 9 final e il relativo Staff Working Document (2017) 2 final del 10 gennaio 2017 *On the free flow of Data and emerging issues of the European Data economy*; Big Data Value Europe, *Big Data Value Strategic Research & Innovation European Agenda* (BDV-SRIA), Version 3.0, gennaio 2017, http://www.bdva.eu/sites/default/files/EuropeanBigDataValuePartnership_SRIA__v3.pdf.

[123] In senso contrario, D.D. Sokol – R. Comerford, *Does antitrust have a role to play in regulating Big Data?*, in *Cambridge Handbook of Antitrust, Intellectual Property and High Tech*, Cambridge University Press, 2016; Id., *Antitrust and regulating Big Data*, in *Geo. Mason L. Rev.*, Vol. 23 (2016), 1129 e ss.; A. Lambrecht – C. Tucker, *Can Big Data protect a firm from competition?*, Working paper, 18 dicembre 2015, https://papers.ssrn.com/sol3/papers2.cfm?abstract_id=2705530; D.S. Tucker – H. Welford, *Big mistakes regarding Big Data*, in *Antitrust Source*, dicembre 2014; A.V. Lerner, *The role of "Big Data" in online platform competition*, Working paper, 2014, https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2482780. Scetticismo viene inoltre espresso in G. Colangelo, *Big Data, piattaforme digitali e antitrust*, in *Mercato, Concorrenza, Regole*, Vol. 3(2016), 458-59. In senso favorevole, A. Ezrachi – M.E. Stucke, *Virtual Competition. The promise and perils of the algorithm-driven economy*, Harvard University Press, 2016; M.E. Stucke - A.P. Grünes, *Big Data and competition policy*, Oxford University Press, 2016; Id., *No mistake about it: the important role of antitrust in the era of Big Data*, in *Antitrust source*, Aprile 2015; G. Pitruzzella, *Big Data, competition and privacy: a look from the antitrust perspective*, in *Concorrenza e mercato*, Vol. 23 (2016), 15 e ss.; Id., *Big Data and antitrust enforcement*, in *Italian Antitrust Review*, Vol. 1(2017), 77 e ss.; B. Lasserre – A. Mundt, *Competition law and Big Data: the enforcers' view*, in *Italian Antitrust Review*, Vol. 1(2017), 87 e ss.; D.L. Rubinfeld - M. S. Gal, *Access barriers to Big Data*, in *Arizona Law Review*, Vol. 59 (2017), 339 ss.; N.P. Schepp – A. Wambach, *On Big Data and its relevance for market power assessment*, in *Journal of European Competition Law & Practice*, Vol. 7 (2016), Issue 2, 120 ss., https://doi.org/10.1093/jeclap/lpv091; I. Graef, *Market definition and market power in Data: the case of online platforms*, in *World Competition*, Vol. 38 (2015), Issue 4, 473 ss.

digitale rilasciando *public announcements*, commenti e interviste[124], pubblicando alcuni studi[125], avviando istruttorie[126] e indagini conoscitive mirate[127]. Questi primi passi sembrano tutti accumunati dalla generale consapevolezza della necessità di un intervento in materia. Ad essere meno chiaro è il *quomodo* dell'intervento stesso, soprattutto ove si consideri che la repressione di eventuali comportamenti illeciti non potrebbe comunque prescindere da un "*assessment case by case*", tipico del diritto della concorrenza (a meno di non voler optare, in tutto o in parte, per un approccio regolatorio).

Dal suo canto – s'è visto – l'AGCM ha per ora deciso di avviare un'indagine conoscitiva diretta a comprendere se i Big Data possano essere considerati alla stregua di "*input* o asset idonei a creare e/o rafforzare il potere di mercato di alcuni operatori, generare effetti di *lock-in* per gli utenti e costituire barriere all'entrata"[128]. Nella medesima delibera l'Autorità ha inoltre dichiarato di voler soppesare "il possibile impatto dei Big Data su fattori concorrenziali attinenti alla sfera qualitativa dei servizi offerti, come il livello di protezione dei dati garantito ai clienti, al fine di valutare se e in che misura aspetti relativi al livello di *privacy* possano assumere rilievo a fini concorrenziali"[129].

Questa, in breve, la panoramica di insieme.

All'interno della casistica dei comportamenti anticompetitivi in tesi derivanti dall'impiego dei *Big Data & Big Analytics*, in questa sede si tenterà di isolare due condotte suscettibili di impattare *in modo diretto e immediato* il benessere dei consumatori, al fine di verificare se gli strumenti di cui oggi dispone il diritto della concorrenza possano costituire la più opportuna e adatta risposta per fronteggiare simili preoccupazioni.

2. *BIG DATA & BIG ANALYTICS*, PROFILAZIONE E PREZZI PERSONALIZZATI: UNA POSSIBILE IPOTESI DI PREZZI DISCRIMINATORI EX ARTT. 102, LETT. C) TFUE E 3, LETT. C) LEGGE N. 287/1990?

Lo sguardo prospettico di alcuni studiosi ha visto nel fenomeno dei *Big Data & Big Analytics* la chiave per arrivare, in un futuro abbastanza prossimo e a costi relativamente contenuti, alla diffusione della tecnica commerciale dei "prezzi personalizzati"[130].

Attraverso le nuove tecnologie abilitanti l'operatore economico si troverebbe, infatti, nella possibilità di applicare ai consumatori dei prezzi ritagliati individualmente e riflettenti il massimo che, in base alle proprie preferenze e disponi-

---

[124] M. Vestager (commissario europeo per la concorrenza), *Refining the EU merger control system*, Studienvereinigung Kartellrecht, Bruxelles, 10 marzo 2016; Id., *Big Data and Competition*, EDPS-BEUC Conference on Big Data, Bruxelles, 29 settembre 2016; J. Hine (FTC), *Mergers and privacy promises*, 25 maggio 2015; D. Feinstein (FTC), *The not-so-Big news about Big Data*, 16 giugno 2015.

[125] Autorité de la concurrence (FR) – Bundeskartellamt (DE), *Competition Law and Data*, 10 maggio 2016, http://www.autoritedelaconcurrence.fr/doc/reportcompetitionlawandDatafinal.pdf; Competition & Markets Authority (UK), *The commercial use of consumer Data*, 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_Data/file/435817/The_commercial_use_of_consumer_Data.pdf; Monopolkommission (DE), *Competition policy: The challenge of digital markets*, Special report n. 68/2015.

[126] Cfr. *infra* § 3.

[127] Si pensi ad esempio all'indagine conoscitiva avviata dall'Autorità francese con la décision n° 16-SOA-02 del 23 maggio 2016 "*relative à une saisine d'office pour avis portant sur l'exploitation des données dans le secteur de la publicité en ligne*" e all'indagine conoscitiva relativa al settore dell'*e-commerce* lanciata dalla Commissione europea il 6.5.2015 (HT.4607) e avente ad oggetto, *inter alia*, la verifica di eventuali criticità concorrenziali nel settore in oggetto.

[128] Cfr. § 3 della delibera n. 26620 del 30 maggio 2017, di avvio della IC53 – *Big Data*.

[129] *Ibidem*.

[130] In tal senso, ad es., N. NEWMAN, *Search, Antitrust, and the Economics of the Control of User Data, in Yale Journal on Regulation*, Vol. 31 (2014), Issue 2, 443-444.

bilità economiche, un determinato individuo è pronto a pagare in un determinato momento per un determinato bene o servizio (c.d. prezzo di riserva)[131].

In questo scenario il quesito che è stato sollevato è se i prezzi personalizzati ricavabili attraverso i *Big Data & Big Analytics* possano dar luogo a una ipotesi di "*prezzi discriminatori*" ai sensi dell'art. 102, lett. *c)* TFUE e 3, lett. *c)* legge n. 287/1990 e, dunque, a una particolare forma di abuso di posizione dominante[132].

Come noto, la fattispecie in parola richiede una posizione dominante dell'agente; la scelta di questo di praticare prezzi (o condizioni) dissimili a fronte di prestazioni equivalenti; la produzione di una "svantaggio competitivo" per i *competitor* operanti a valle o a monte.

Il primo ostacolo giuridico alla configurazione dell'illecito qui analizzato potrebbe risiedere nel fatto che il concetto di "svantaggio competitivo", a rigore riferito ai "*rapporti commerciali con altri contraenti*" (e, dunque, a rapporti tra imprese), dovrebbe nella specie essere declinato come pregiudizio subito direttamente dai consumatori cui vengano imposti prezzi discriminatori, attraverso una lettura della norma che, per quanto evolutiva, non potrebbe ritenersi perfettamente aderente con il dato testuale.

Per sciogliere in senso positivo il quesito si potrebbe accogliere quelle autorevoli visioni che secondo cui "la tutela della concorrenza [deve intendersi] non più come tutela di una certa struttura di mercato ma come disciplina volta a realizzare l'obiettivo del massimo benessere del consumatore"[133].

Una simile risposta consentirebbe di sciogliere in senso positivo anche il secondo nodo interpretativo, strettamente connesso al primo, ossia se, in termini di benessere, la pratica dei prezzi personalizzati risulti realmente svantaggiosa per la comunità degli utenti.

Alcuni studiosi hanno infatti dimostrato che la risposta al quesito cambia a seconda che si adotti una prospettiva di "benessere totale" (*total* od *overall welfare*) o di "benessere dei consumatori" (*consumer welfare*).

Le simulazioni economiche evidenziano in particolare che, adottando il primo approccio, la risposta sarebbe negativa, in quanto attraverso i prezzi personalizzati l'impresa in monopolio aumenterebbe la produzione e innalzerebbe i livelli della domanda, rendendo accessibili i beni anche alle fasce meno abbienti, a fronte di un esborso maggiore per quelle più facoltose (o comunque più interessate all'articolo)[134]. Pertanto, anche se il "*surplus*" verrebbe in questo modo interamente drenato dall'impresa, si potrebbe comunque ritenere che l'allocazione delle risorse sul mercato sia stata più efficiente (*total* od *overall welfare*).

---

[131] I Big Data potrebbero infatti consentire di realizzare un comportamento fino ad oggi ritenuto virtuale o teorico: la discriminazione "perfetta" o, che dir si voglia, "di primo grado". Si registrano invece nella prassi commerciale svariate ipotesi di discriminazione "imperfette", ossia di c.d. secondo grado (o di "*menu pricing*", come ad es. gli sconti quantità) o di terzo grado (altrimenti dette "di gruppo", come ad es. il *geoblocking*).

[132] L'indagine circa la riconducibilità della pratica del prezzo personalizzato alle intese restrittive di cui agli artt. 101, lett. c) TFUE e 2, lett. d) legge n. 287/1990 sembra invece scarsamente utile: trattandosi di una forma di coordinamento sui prezzi, il comportamento darebbe luogo a una violazione c.d. per oggetto, ciò che renderebbe irrilevante l'accertamento della natura personalizzata o meno dei prezzi praticati (M. MAGGIOLINO, *Big Data* e prezzi personalizzati, in F. DI PORTO (a cura di), *Big Data* cit., 117-118).

[133] Così M. LIBERTINI, *La concorrenza degli antichi e la concorrenza dei moderni*, in AA. VV. C. RABITTI BEDOGNI, P. BARUCCI (a cura di), 20 *anni di antitrust. L'evoluzione dell'Autorità Garante della Concorrenza e del Mercato*, I, Torino, 2010, 109.

[134] Per questa tesi sembra propendere M. MAGGIOLINO, *Big Data e prezzi personalizzati* cit., 111-116 e 123-124, la quale ritiene che la posizione di "*disinteresse*" assunta al riguardo dalla Commissione europea "induce a supporre che essa potrebbe non procedere contro l'impresa in posizione dominante che si limitasse a drenare risorse dai consumatori". Giungono alla conclusione della tendenziale irrilevanza dei prezzi personalizzati agli effetti del diritto della concorrenza anche gli Studi condotti dall'EXECUTIVE OFFICE OF THE PRESIDENT, *Big Data and differential pricing*, febbraio 2015, in https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/docs/Big_Data_Report_Nonembargo_v2.pdf e dall'Autorité de la concurrence (FR) e Bundeskartellamt (DE), *Competition Law* cit., 21-22.

Adottando un approccio basato sullo *standard consumer welfare*[135], il comportamento presenterebbe invece criticità competitive, posto che tale prospettiva evidenzierebbe come il "*surplus*" realizzato non venga "distribuito" ai consumatori, ma trattenuto per intero dall'impresa in posizione dominante[136].

È in questo terreno scivoloso che dovrà muoversi l'AGCM, con modalità ancora da stabilire, sia nell'*an* che nel *quomodo*, e che si tenteranno di anticipare e tratteggiare nelle Conclusioni (v. § 4.2.1).

3. ABUSO DI SFRUTTAMENTO EX ARTT. 102, LETT. A) TFUE E 3, LETT. A) LEGGE N. 287/1990. IL CASO AVVIATO DAL BUNDESKARTELLAMT CONTRO FACEBOOK

Si è visto nella prima parte del Capitolo che l'AGCM ha imputato a WhatsApp la violazione della disciplina delle pratiche commerciali aggressive per aver indotto i propri utenti a credere, all'indomani della fusione con Facebook[137], che, contrariamente al vero, il trasferimento dei propri dati personali al *social network* sarebbe stato indefettibile per continuare a fruire del servizio (con un distinto procedimento l'Autorità ha inoltre accertato la vessatorietà di svariate clausole contrattuali predisposte da WhatsApp)[138].

È interessante notare che, mentre la Commissione europea ha irrogato alla società incorporante una sanzione di 110 milioni di euro per aver fornito informazioni reticenti nel corso del procedimento istruttorio all'esito del quale è stata autorizzata l'operazione[139], il Bundeskartellamt sta osservando il comportamento della piattaforma *social* attraverso i fari del diritto della concorrenza. L'autorità tedesca ha, infatti, avviato un procedimento per possibile abuso di posizione dominante, in questo caso nei confronti della *subsidiary* irlandese di Facebook[140].

Più precisamente, l'ipotesi accusatoria è che "*with its specific terms of service on the use of user Data, Facebook has abused its possibly dominant position in the market for social networks*", al fine di profilare gli utenti e, per l'effetto, "*enabl*[ing] *its advertising customers to better target their advertising activities*"[141]. Potrebbe, dunque, trattarsi di un puro

---

[135] R.A. WOODCOCK, Big Data, *price discrimination and antitrust, in Hastings Law Journal* (in corso di pubblicazione), disponibile in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2817523 nella versione aggiornata al 19 agosto 2017, 6. Meno netta la posizione espressa in M. BOURREAU, A. DE STREEL e I. GRAEF, *Big Data and competition policy: market power, personalised pricing and advertising*, Project report of the Centre on Regulation in Europe (CERRE), www.cerre.eu/sites/cerre/files/170216_CERRE_CompData_FinalReport.pdf, 16 febbraio 2017, 44, in cui, pur guardando il fenomeno in una prospettiva di *consumer welfare*, si evidenzia come le conseguenze della *price discrimination* sul benessere dei consumatori non siano univoche, potendo variare a seconda delle condizioni della domanda.

[136] La conclusione è confortata anche da studi più risalenti: A. ACQUISTI – H.R. VARIAN, *Conditioning prices on purchase history*, in *Marketing* Sci., Vol. 24 (2005), 367-372.

[137] L'operazione è stata autorizzata dalla Commissione con decisione COMP/M.7217 del 3 ottobre 2014.

[138] Cfr. § 3 della Prima Parte del presente contributo.

[139] Cfr. caso M.8228 - *Facebook/WhatsApp*, avviato ex articolo 14, § 1 del Reg. (CE) n. 139/2004 e concluso con decisione del 17 maggio 2015, C(2017)3192 final.

[140] In argomento, v. G. COLANGELO, M. MAGGIOLINO, *Big Data, Data protection and antitrust in the wake of the Bunderskartellamt case against Facebook, in Italian Antitrust Review*, Vol. 1/2017, 105 e 108, i quali esprimono sul punto "*deep skepticism*", in quanto "*if network effects and the like are what disincentives digital platforms from producing privacy-friendly services, economic regulation rather than antitrust law should intervene*"; nonchè A.B. HUTTENLAUCH, *How many "likes" for the German Facebook antitrust probe?*, in CPI *Antitrust Chronicle*, Vol. 1 (2016), B. LASSERRE – A. MUNDT, *Competition law* cit., 100 e N. ZINGALES, *Between a rock and two hard places: WhatsApp at the crossroad of Competition, Data Protection and Consumer Law*, 22 giugno 2017, in corso di pubblicazione in *Computer Law and Security Review* e disponibile alla pagina https://ssrn.com/abstract=2990939, 5.

[141] Cfr. Comunicato stampa del 2.3.2016, http://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2016/02_03_2016_Facebook.html?nn=3591568. Come si vede, il Bundeskartellamt ha deciso di definire il mercato del prodotto come quello dei "*social network*", così segmentando il (ben più ampio) mercato dell'"*advertising-financed internet services*", all'interno del quale sarebbe più complicato dimostrare la posizione dominante di Facebook.

abuso di sfruttamento *ex* art. 102, lett. *a)* TFUE (in Italia: art. 3, lett. *a* legge n. 287/1990), nella misura in cui l'utente "distratto" (o comunque attratto alla piattaforma in ragione dei considerevoli *network effect* che essa genera) finisca per accettare, più o meno consapevolmente, condizioni contrattuali che prevedano un trattamento dei dati personali particolarmente pervasivo e, secondo l'Autorità tedesca, "*in violation of Data protection provisions*".

A giudicare dal tenore del comunicato stampa, il procedimento sembra essere costruito come tentativo di rimediare *ex post* a quel calo dei livelli di "qualità" dell'offerta che talvolta può (patologicamente) discendere dalla concentrazione del potere di mercato in mano a uno o pochi soggetti.

L'istruttoria – certamente non banale nell'impianto e non scontata negli esiti – costituisce un vero e proprio "esperimento" e riflette la viva curiosità espressa da vari *competition officer* e studiosi in merito ai possibili punti di contatto esistenti tra diritto della concorrenza e tutela della *privacy*[142].

Anche in questo caso si tenterà di esprimere alcune (primissime e certamente non decisive) considerazioni in merito all'efficacia dell'impostazione che, almeno fino ad oggi, sembrerebbe aver seguito l'autorità tedesca (v. § 4.2.2).

4. CONCLUSIONI

4.1. Le questioni economiche e giuridiche poste dal fenomeno dei *Big Data & Big Analytics* sono plurime e in grado di destabilizzare le stesse fondamenta concettuali del diritto della concorrenza (v. § 1).

Di qui la condivisibile scelta dell'AGCM di avviare un'indagine conoscitiva in cui, anziché esplorare i confini di un ipotetico mercato dei *Big Data & Big Analytics*[143], verificare preliminarmente in che misura l'utilizzo di un *Dataset*, laddove inteso come "*input*" o "*asset*" produttivo, possa attribuire all'impresa che ne sia in possesso un vantaggio competitivo non replicabile (o replicabile in tempi e a costi eccessivamente elevati).

4.2 Su queste premesse, in linea con le finalità del presente Rapporto sono state analizzate due possibili ipotesi di illeciti concorrenziali posti in essere attraverso le tecnologie *Big Data & Big Analytics* e suscettibili di produrre, in tesi, ricadute dirette sui consumatori: *i)* quella dei prezzi "discriminatori" *ex* artt. 102, lett. *c)* TFUE e 3, lett. *c)* legge n. 287/1990 (e, più precisamente, dei prezzi "personalizzati" ritagliati attraverso la meta-elaborazione dei "profili" degli

[142] Sul tema dei possibili rapporti tra i due campi di disciplina cfr. Autorité de la concurrence (FR) e Bundeskartellamt (DE), *Competition Law* cit., 23-24, secondo cui "*privacy policies could be considered from a competition standpoint whenever these policies are liable to affect competition, notably when they are implemented by a dominant undertaking for which Data serves as a main input of its products or services*"; nonchè J. ALMUNIA, *Competition and personal Data protection*, Speech/12/860, "*Competition and Privacy in Markets of Data*", Bruxelles, 26 novembre 2012 e le *Preliminary Opinion* dell'EDPS di marzo 2014, "*Privacy and competitiveness in the age of Big Data: The interplay between Data protection, competition law and consumer protection in the Digital Economy*", https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_Big_Data_EN.pdf e n. 8 del 23 settembre 2016, "*Coherent enforcement of fundamental rights in the age of Big Data*", https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Eve.nts/16-09-23_BigData_opinion_EN.pdf. In dottrina, aprono alla possibilità di impiegare il diritto della concorrenza (anche) per realizzare obiettivi di tutela della privacy: A.P. GRUNES, *Another look at privacy, in George Mason law review,* Vol. 20 (2013), Issue 4, 1107 ss.; D.S. TUCKER, *The proper role of privacy in merger review*, in CPI *Antitrust Chronicle*, Vol. 2 (2015), *Big Data*!; S. VEZZOSO, *The interface between competition policy and Data protection, in Journal of European Competition Law & Practice*, Vol. 3 (2012), 225. Negano invece l'idoneità del diritto della concorrenza a perseguire finalità di tutela della privacy A.J. BURNSIDE, *No such thing as a free search. Antitrust and the pursuit of privacy goals*, in CPI *Antitrust Chronicle*, Vol. 2 (2015), Big Data!; G.A. MANNE - R.B. SPERRY, *The problems and perils* cit.; M.K. OHLHAUSEN – A.P. OKULIAR, C*ompetition, consumer protection, and the right [approach] to privacy, in Antitrust Law Journal*, Vol. 80 (2015), 121 ss.; N.P. SCHEPP - A.WAMBACH, *On Big Data* cit..

[143] In argomento, cfr. V. BAGNOLI, *The Big Data relevant market*, in F. Di Porto (a cura di), *Big Data* cit., 73 ss., secondo il quale il mercato in parola andrebbe segmentato in i) *Big Data Capture*; ii) *Big Data Storage* e iii) *Big Data Analytics*.

utenti: v. § 2); *ii)* quella dell'abuso di sfruttamento *ex* artt. 102, lett. *a)* TFUE e 3 lett. *a)* legge n. 287/1990 che l'impresa in posizione dominante potrebbe in ipotesi realizzare attraverso l'imposizione di condizioni sulla *privacy* non conformi alla normativa vigente (v. § 3).

4.2.1 Quanto alla prima fattispecie, si è visto che l'inquadramento della pratica dei prezzi personalizzati quale abuso di posizione dominante pone l'interprete di fronte ad alcuni interrogativi: per un verso, occorrerebbe ammettere che lo "svantaggio competitivo" cui alludono gli artt. 102 TFUE e 3 legge n. 287/1990 possa essere subito, oltre che da altre imprese, anche dai consumatori; per altro verso si dovrebbe considerare la concorrenza come strumento per massimizzare il "*consumer welfare*" (piuttosto che l'*overhall* o *total welfare*).

Se alcune posizioni ritengono di poter superare questi due ostacoli, vi potrebbe però essere un'obiezione più radicale alla tesi dei prezzi personalizzati come possibile ipotesi di "*price discrimination*". Potrebbe, infatti, ritenersi che, attraverso una simile tecnica di *pricing*, le imprese in realtà "differenzino", ma non "discriminino": a *tutti* i consumatori viene infatti praticato il massimo prezzo che ciascuno di essi, in base alle proprie disponibilità e ai propri gusti, è pronto a pagare per un determinato bene o servizio in un dato momento (c.d. prezzo di riserva). Se così è, si potrebbe allora pensare che le regole del gioco siano uguali per tutti (e, dunque, non discriminatorie). Un reale problema di "discriminazione", invece, potrebbe sorgere (solo) laddove l'impresa praticasse a taluni un prezzo personalizzato e ad altri un prezzo superiore al proprio prezzo di riserva (il che potrebbe denominarsi con l'espressione "discriminazione in senso proprio"). In definitiva, l'intero problema dei prezzi personalizzati potrebbe considerarsi, da un punto di vista concorrenziale, sovrastimato nella sua entità. A parità di *like*, infatti, i consumatori pagherebbero lo stesso prezzo. Le uniche "discriminazioni" che si potrebbero in tesi ravvisare sarebbero "di classe", in quanto per i soggetti con gli stessi gusti il *driver* suscettibile di far variare il prezzo sarebbe quello della loro disponibilità economica. Tale aspetto, però, sottende una più profonda valutazione di giustizia distributiva che, in quanto tale, non dovrebbe interessare i *competition enforcers*.

Vero è che studi di *marketing* hanno evidenziato che la maggior parte dei consumatori percepisce il prezzo personalizzato come una lesione delle proprie prerogative e, avendone contezza, non acquisterebbe il bene o servizio offerto con tali modalità. Ma allora – come correttamente rilevato – l'attenzione potrebbe più opportunamente spostarsi sui campi di disciplina contigui della tutela del consumatore e della *privacy*[144].

Assumendo che – eccettuato il limite sopra descritto della "discriminazione in senso proprio" – non esista un diritto soggettivo del consumatore a godere di prezzi *standard*[145], ma che ne esista uno a essere debitamente informato sull'esistenza di un eventuale prezzo personalizzato, si potrebbe dunque ragionare sui rimedi astrattamente idonei a raggiungere lo scopo.

La constatazione di partenza è che ad oggi la "filiera del dato" appare eccessivamente opaca e sfuggente: la normativa di tutela della *privacy* prescrive infatti di acquisire uno specifico consenso preventivo per l'attività di profilazione[146] (ciò che, almeno in linea teorica, dovrebbe esporre i soli soggetti consenzienti al rischio di un prezzo personalizzato); impone di acquisire un consenso espresso anche per la cessione dei dati a terzi per finalità commerciali[147]; sanziona l'inosservanza di tali obblighi di comportamento attraverso un apparato di sanzioni sia amministrative che penali. Tuttavia, a livello pratico la suddetta normativa non sembra consegnare al consumatore-utente efficaci strumenti per monitorare, in modo semplice e immediato, il "viaggio" compiuto dai propri dati personali in ambiente digitale.

---

[144] Questa, in sostanza, la conclusione raggiunta in M. MAGGIOLINO, *Big Data e prezzi personalizzati* cit., 127-135.

[145] Una simile convinzione, infatti, potrebbe essere anche essere considerata come un semplice portato del modello di "produzione di massa" affermatosi a partire dalla rivoluzione industriale.

[146] Cfr. Garante della privacy, *Linee guida in materia di trattamento di dati personali per profilazione on line*, doc. web n. 3881513 del 19 marzo 2015, § 2.6.3.

[147] Cfr. Garante della privacy, *Linee guida in materia di attività promozionale e contrasto allo spam*, doc. web n. 2542348 del 4 luglio 2013.

Con riferimento al problema in esame si potrebbe allora pensare di estendere ai dati personali, ancorché con i dovuti adeguamenti, la disciplina di tipo preventivo vigente in materia di "*sicurezza dei prodotti*", disciplina che – nel suo paradigma più moderno – fa del concetto di "*tracciabilità*" il proprio perno[148]. Sul piano pubblicistico, ciò renderebbe di più facile individuazione le violazioni della normativa posta a protezione dei dati personali, esponendo il professionista a un maggiore rischio sanzionatorio; sul piano privatistico, ciò consegnerebbe al consumatore-utente uno strumento per avere più agevole contezza delle lesioni eventualmente subite e per valutare se richiedere un risarcimento del danno (patrimoniale e non) ai sensi dell'art. 82 del regolamento (UE) n. 679/2016 (e dell'art. 15 del d. lgs. n. 259 del 2003) oppure, in virtù di un'interpretazione estensiva, anche ai sensi degli artt. 1 e 3, § 3 della direttiva n. 85/374/CEE (artt. 114 o 116 del Codice del consumo).

A completamento del suddetto intervento si potrebbe inoltre integrare la disciplina degli obblighi informativi precontrattuali, aggiungendo agli artt. 5 e 6 della direttiva n. 2011/83/UE (e 48 e 49 del Codice del consumo) una previsione che imponga al professionista di indicare in modo specifico quando il prezzo praticato sia "personalizzato".

4.2.3 Quanto al procedimento avviato dal Bundeskartellamt contro Facebook, si è detto che comportamenti sostanzialmente analoghi sono stati qualificati in Italia come pratiche aggressive e come clausole vessatorie. La vicenda per un verso dimostra la circolarità e complementarietà delle forme di tutela dell'individuo e i numerosi punti di contatto tra diritto della concorrenza e tutela del consumatore; per altro verso evidenzia l'assenza, almeno ad oggi, di orientamenti applicativi chiari su come fronteggiare le problematiche sollevate dalla *social economy*.

Nel merito, l'Autorità tedesca sembra legare l'ipotizzato abuso di sfruttamento a un fattore prettamente "qualitativo": l'impresa in posizione dominante, infatti, sarebbe destinataria di particolari obblighi, tra cui – lascia intendere il comunicato stampa – anche quello di assicurare il pieno rispetto della normativa di tutela della *privacy*.

In modo non dissimile, nella delibera di avvio dell'indagine conoscitiva IC-53 l'AGCM ha dichiarato di voler soppesare "il possibile impatto dei Big Data su fattori concorrenziali attinenti alla sfera qualitativa dei servizi offerti, come il livello di protezione dei dati garantito ai clienti, al fine di valutare se e in che misura aspetti relativi al livello di privacy possano assumere rilievo a fini concorrenziali".

L'atteggiamento delle due Autorità sottende un quesito di più ampia portata: il diritto della concorrenza, tradizionalmente inteso come strumento per raggiungere l'efficienza allocativa dei mercati e oggi riconsiderato, almeno nella visione di alcuni studiosi, come strumento per assicurare il benessere economico dei consumatori, può trasformarsi, nell'epoca dei Big Data e della *social economy*, in un mezzo per conseguire una nozione di benessere più ampia, estesa anche a componenti non economiche, quali il diritto dei consumatori a mantenere la riservatezza dei propri dati[149]?

Due considerazioni al riguardo.

In primo luogo, la questione della perseguibilità di una violazione della normativa sulla *privacy* anche alla stregua di un illecito concorrenziale sembra anzitutto porre un (non indifferente) problema di legalità. Può un'autorità della concorrenza accertare, per quanto incidentalmente, una violazione della *data protection law*? Il Bundeskartellamt sembra aver colto (in parte) il problema, laddove ha pubblicamente dichiarato di portare avanti l'istruttoria "*in close contact with the competent Data protection officers*".

In secondo luogo, ci si potrebbe chiedere se sia corretto costruire l'abuso di sfruttamento avente ad oggetto dati personali sul fattore "qualità" – come lascia trasparire l'Autorità tedesca e come ha dichiarato di voler approfondire anche l'AGCM – piuttosto che sull'elemento "prezzo" e/o sulle "condizioni economiche" ("quantità").

---

[148] In argomento, v. E. BELLISARIO, *La sicurezza dei prodotti: profili evolutivi e aspetti sostanziali*, in AA. VV. L. Rossi Carleo (a cura di), *Diritto dei consumi. Soggetti, atto, attività, enforcement*, Torino, 2015, 203 ss.

[149] In senso positivo, v. ad es. M.E. STUCKE - A.P. GRÜNES, *Big Data and competition policy*, Oxford University Press, 2016, 151-154 e 260-276. Possibilista, inoltre, la posizione espressa in G. PITRUZZELLA, *Big Data and antitrust* cit., 79; B. LASSERRE - A. MUNDT, *Competition law and Big Data* cit., 94.

A tale ultimo riguardo occorre infatti tener conto del fatto che servizi apparentemente gratuiti, come quelli offerti dalle piattaforme *online*, tali in realtà non sono ove si consideri che il controvalore della prestazione fruita dal consumatore-utente è sovente costituito dalla possibilità per l'operatore di ricavare ricchezza dai dati personali raccolti in esecuzione del rapporto, sfruttandoli (o cedendoli) su mercati ulteriori o su altri versanti dello stesso mercato. In definitiva, se l'autorizzazione a trattare un dato personale può davvero assumere valore economico e se, come ipotizzato nell'atto di avvio, la politica sulla *privacy* di Facebook è volta a massimizzare tale vantaggio attraverso l'imposizione di condizioni sulla *privacy* illegittime, ne viene che l'impresa in posizione dominante sta chiedendo un prezzo troppo alto (o, che dir si voglia, sta imponendo delle condizioni contrattuali troppo onerose) per il servizio offerto, lucrando un indebito extra-profitto a spese dei consumatori-utenti.

Ciò detto, si ritiene che l'impostazione di stampo "quantitativo" qui suggerita potrebbe forse sortire un maggiore effetto utile, permettendo di colpire (anche) comportamenti non sanzionabili in una prospettiva solamente "qualitativa": si pensi all'ipotesi in cui l'impresa in posizione dominante, pur rispettando formalmente la *data protection law*, finisca nondimeno per imporre, di fatto, condizioni sulla privacy fortemente intrusive, sfruttando gli errori cognitivi dei propri utenti e la scarsa inclinazione di questi a percepire il "valore" delle informazioni cedute.

AUTORITÀ DI REGOLAZIONE DEI TRASPORTI[150*]

(Aldo Corvino, Paolo Occhiuzzi)

I problemi sollevati dalla social economy, tra Big Data e fake news*, anche se parzialmente trasversali a tutti i settori, nel settore dei trasporti si colorano delle particolari caratteristiche dei dati coinvolti, relativi allo spostamento di merci e persone, richiedendo di tenerne conto nel bilanciamento della protezione dei dati personali con le ragioni dell'economia e della pubblica sicurezza.*

In questo quadro dinamico, è all'organismo di regolazione che si richiedono risposte tempestive alle domande poste dal vuoto normativo nel quale si muovono i fenomeni digitali legati ai Big Data.

La presente analisi mira, dunque, a tracciare le linee essenziali del rapporto tra mobilità, nuove tecnologie e Big Data, esaminando il tema delle tutele da differenti angolazioni soggettive: operatori e consumatori, individui e autorità di regolazione.

SOMMARIO: 1. GLI UTENTI DEI SERVIZI DI TRASPORTO, TRA BIG DATA E *FAKE NEWS*, ALLA RICERCA DI UNA AUTORITÀ. – 2. LA GESTIONE DEI DATI PERSONALI NEL SETTORE DEI TRASPORTI: PROBLEMI E PROSPETTIVE. – 3. BIG DATA, TRASPORTI E REGOLAZIONE.

1. GLI UTENTI DEI SERVIZI DI TRASPORTO, TRA BIG DATA E *FAKE NEWS*, ALLA RICERCA DI UNA AUTORITÀ

(Paolo Occhiuzzi)

La nostra società è destinata a produrre una sempre crescente quantità di dati: nei prossimi anni, a quelli già prodotti dagli utenti del *web* e dai *social network* andranno aggiunti i dati generati dai dispositivi e dai sensori dell'Internet delle Cose (*Internet of Things*) e quelli che saranno resi disponibili sotto forma di dati aperti (*Open Data*).

Non contano, tuttavia, tanto i Big Data quanto il loro utilizzo intelligente. Quello dei Big Data, infatti, è un fenomeno con una dimensione ambivalente: una *quantitativa* e l'altra prettamente *qualitativa*. Le caratteristiche dei Big Data, la loro ragguardevole quantità, la loro eterogeneità nelle forme e nelle fonti di produzione, la loro dimensione quantitativa appunto, hanno, infatti, reso obsolete gran parte delle tecnologie di conservazione ed elaborazione dei dati e hanno permesso lo sviluppo della prima dimensione qualitativa del fenomeno, cioè lo sviluppo di nuove tecnologie in grado di sfruttare pienamente le loro potenzialità[151] (il c.d. *smart data*).

Per cogliere il fenomeno, è agevole riferirsi a ipotesi concrete come lo strumento *Google Books* e alla sua capacità di indicizzare tutte le parole di tutti i testi digitalizzati e contenuti al suo interno, tanto da poter produrre dei grafici sull'utilizzo di determinate parole o di determinate frasi nel tempo.

Un altro esempio di "*datizzazione*", più vicino al settore dei trasporti, è la geolocalizzazione dei luoghi, delle persone

[150] *La parte I e la parte III sono di Paolo Occhiuzzi (le opinioni espresse dall'Autore non impegnano l'Istituzione cui appartiene); la parte II è di Aldo Corvino.

[151] V. A. W. Crosby, *The Measure of reality*, Cambridge University Press, Cambridge, 1996, tr. it., *La misura della realtà*, Bari, 1998.

e degli oggetti[152]. Il noto GPS (*Global Positioning System*), strumento che già permetteva da tempo di geolocalizzare i luoghi e gli oggetti, rappresenta allo stato solo uno strumento – tra gli innumerevoli – tramite il quale operare una raccolta dati.

E ancora si pensi al caso Moovit, un'applicazione gratuita nata nel 2013 che in pochi anni ha conquistato 50 milioni di utenti, diventando la *app* dedicata al trasporto più diffusa al mondo. Il suo punto di forza consiste nel combinare insieme diversi dati relativi al trasporto, per dare all'utente un'istantanea in tempo reale sul loro spostamento, indicando i percorsi più veloci e comodi in base alla destinazione desiderata. Le fonti dalle quali Moovit attinge le proprie informazioni provengono dalle aziende di trasporto che gratuitamente aderiscono a Moovit, da una *community* composta da 120 mila *editor*, dagli *open data* resi disponibili dalle pubbliche amministrazioni, oltre ai dati forniti in tempo reale dagli utilizzatori della *app*.

Fatta tale doverosa premessa, è, dunque, prioritario comprendere quale sia la ricaduta del fenomeno appena analizzato in termini di tutele nei mercati tradizionali, come quello dei trasporti.

Quando si parla di Big Data e tutele, infatti, si pensa principalmente ai profili di *privacy* e all'esigenza di protezione del consumatore interconnesso. Invero, rispetto a tale aspetto le regole europee già esistono. Il nuovo Regolamento Europeo n. 2016/679 in materia di protezione dei dati personali, che diverrà direttamente applicabile in tutti gli Stati membri UE il 25 maggio 2018, coglie perfettamente questi rischi nell'introdurre il principio di *privacy by design*, che si pone l'ambizioso obiettivo di individuare nuove forme di tutela per le persone basate sulla leva tecnologica, in aggiunta a quelle che tradizionalmente si sono realizzate intervenendo sulla leva giuridica[153].

Una volta superato il *problema privacy*, ecco che l'attenzione sul tema dei Big Data si sposta in terreni diversi: quello della regolazione, della concorrenza, della competenza fiscale al diritto d'autore.

A ben vedere, infatti, la capacità di acquisire e analizzare un grande volume di dati eterogenei in tempi ristretti riveste un ruolo sempre più centrale non solo nell'ecosistema digitale, ma anche nei settori più tradizionali dell'economia, come quello dei trasporti.

In questo settore, il fenomeno dei Big Data si intreccia strettamente con quello del potere di mercato dal momento che proprio la capacità di acquisire e analizzare ingenti quantitativi di informazioni può consentire ad alcune imprese di acquisire un significativo potere di mercato. È soprattutto in tali circostanze che emergono i rischi maggiori per il consumatore che vede limitare la propria offerta di servizi e la concorrenza.

Non è qui in discussione la circostanza che un buon impiego dei Big Data nel settore può concretamente rivoluzionare la mobilità offrendo numerosi vantaggi sia di ordine economico che sociale. In tale prospettiva i cittadini assumono un ruolo centrale, diventando anche loro sempre più *smart*, utilizzando sempre più le tecnologie mobili per interagire e fruire dei servizi della città. Si pensi all'acquisto del *ticket* per il bus o la metro, al pagamento del parcheggio, al pagamento dei permessi per l'accesso alle ZTL, effettuabili tramite cellulare, anche con addebito dell'importo sul credito telefonico.

---

[152] Sul tema si rimanda al secondo paragrafo.

[153] Sempre a livello europeo, è stata costituita la Digital Clearing House (DCH) istituita su iniziativa dello European Data Protection Supervisor (EDPS). Più specificamente, il DCH è un network volontario tra autorità di regolazione per la condivisione di informazioni – in maniera volontaria e nei limiti delle rispettive competenze – a proposito di possibili abusi nell'ecosistema digitale e dell'individuazione delle strategie per gestire tali abusi. V., sul punto, EDPS, *Opinion 8/2016, Opinion on coherent enforcement of fundamental rights in the age of Big Data*, 15 ss. L'obiettivo della DCH risiede nell'identificare le potenziali azioni di coordinamento o di sensibilizzazione a livello europeo che possano disincentivare l'attuazione di strategie imprenditoriali dannose; nel discutere soluzioni regolatorie per determinati mercati in cui i dati personali sono un *input* chiave, come alternativa efficiente a iniziative legislative che possano disincentivare l'innovazione; valutare l'impatto sui diritti ed interessi degli individui nel mondo digitale delle sanzioni e dei rimedi proposte per la risoluzione dei singoli casi; identificare le sinergie e promuovere la cooperazione tra le autorità di *enforcement* e la loro conoscenza delle regole applicabili, ivi incluso tramite contatti formali ed informali nell'ambito dello European Competition Network e del Consumer Protection Cooperation Network.

Questo alto potenziale va però ben gestito, consentendo una minimizzazione dei rischi correlati e un'equa distribuzione del *payoff*. A ben vedere, infatti, il fenomeno ha creato, nel tempo, delle profonde disparità all'interno di alcuni mercati, tra le aziende che possiedono i dati e producono le informazioni, in particolare informazioni in merito agli utenti e ai consumatori, e coloro che ne possiedono di meno o non ne possiedono affatto e, di conseguenza, hanno meno informazioni sui consumatori e sugli utenti[154]. Le situazioni di monopolio che si vengono a creare, infatti, sono fortemente legate alla produzione e alla gestione di informazioni sui consumatori e alla capacità delle aziende di "conoscere" il più possibile le preferenze e i comportamenti dei consumatori a cui ci si vogliono rivolgere. La capacità di ricostruire il profilo dei clienti o dei potenziali clienti che l'elaborazione dei Big Data permette di fare in maniera più semplice rispetto al passato, facilita il miglioramento dei servizi offerti o le capacità di pubblicizzare e vendere i propri prodotti a scapito della concorrenza, alcune volte, in maniera difficilmente reversibile. Un divario che stabilizza un vantaggio competitivo evidente a favore delle aziende che "conoscono" i consumatori e gli utenti[155].

Sotto il profilo delle tutele, questi aspetti hanno cominciato a fare emergere degli interrogativi rilevanti sulla capacità della disciplina della concorrenza di regolare le nuove dinamiche del mercato e frenare i monopoli che si stanno consolidando[156], in particolare ci si interroga sulla capacità del diritto antitrust di fare fronte ad un fenomeno fondamentalmente nuovo: al protagonismo, molte volte inconsapevole, dei consumatori nelle dinamiche concorrenziali tra le aziende[157]. Questi, infatti, fornendo continuamente e volontariamente dati personali, sulle proprie abitudini e sui propri comportamenti, contribuiscono per primi a creare e a rafforzare le posizioni dominanti nel mercato. In una situazione come quella appena descritta, ci si è domandati, per esempio, se definizioni come quella di mercato rilevante – contenuta nella disciplina europea e principio cardine della disciplina antitrust per la valutazione dell'esistenza di pratiche restrittive o di abuso della posizione dominante nel mercato unico europeo – possano essere ancora parametri guida, ad esempio in mercati come quello digitale, per ricostruire le caratteristiche del mercato e per individuare probabili posizioni dominanti.

Ed è dai casi concreti diffusi nel settore dei trasporti che si coglie la difficoltà di ricondurre alle categorie giuridiche della disciplina antitrust tutte le possibili patologie. Gli esempi non sono pochi.

Si pensi al trasporto ferroviario regionale ove i servizi vengono affidati ad un unico gestore che ha la possibilità di gestire ed immagazzinare un numero rilevantissimo di informazioni sulle abitudini dei clienti. In tali casi il monopolio nella prestazione del servizio contribuisce a formare un monopolio delle informazioni che ha effetti anche nel mercato del trasporto ferroviario nazionale ove operano solo pochi *players* nel mercato.

Al contrario, può succedere che il monopolista di fatto di un dato settore e/o servizio impedisca o cerchi di rallentare l'ingresso a nuovi operatori dell'ecosistema digitale, in mercati collegati.

Si pensi, ancora, al servizio taxi. Il servizio taxi ha precise caratteristiche che lo differenziano dal servizio di noleggio con conducente (anche servizio NCC). Tale servizio funziona mediante un sistema centralizzato nel quale una centrale operativa riceve le richieste telefoniche, ricerca via radio e localizza il taxi disponibile più vicino al luogo del prelevamento dell'utente al momento della chiamata e gli assegna la corsa. Per usufruire del servizio radiotaxi il singolo tassista paga una *fee* d'ingresso in cifra fissa ed un canone mensile, il cui ammontare è stabilito dal rispettivo gestore di radiotaxi. Ai canali tradizionali di raccolta della domanda del servizio taxi (richiesta diretta da parte dell'utenza di un taxi in transito o nei posteggi, chiamata telefonica alle colonnine situate nei posteggi) – e al c.d. servizio radiotaxi – si sono aggiunte recentemente nuove modalità di raccolta e smistamento della domanda che utilizzano le tecnologie basate sulla geolo-

[154] Per un approfondimento sul tema, v. G. Colangelo, *Big Data, piattaforme digitali e antitrust*, Mercato Concorrenza Regole, Fascicolo 3, dicembre 2016.

[155] OCSE, *Big Data: Bringing competition policy to the digital era*, DAF/Comp(2016)14, 12 ottobre 2016, Parigi.

[156] V. al riguardo C. Buzzacchi, *La politica europea per i Big Data e la logica del single market: prospettive di maggiore concorrenza?*, Concorrenza e Mercato, 2016.

[157] Cfr. Report OCSE, *Data-Driven Innovation. Big Data for Growth and Well-Being*, ottobre 2015.

calizzazione della domanda e dell'offerta. È il caso di MyTaxi che sta incontrando, in Italia, numerosi ostacoli all'ingresso nel mercato.

Si pensi, infine, al caso Uber: un operatore che può potenzialmente mettere in collegamento l'offerta di trasporto di migliaia di autisti privati ed NCC, con la domanda di milioni di potenziali clienti iscritti al servizio, con tariffe di trasporto preventivabili e pagabili con carta di credito attraverso il sito. Tale offerta rimane allo stato – in Italia – solo potenziale e non effettiva.

Ebbene, dopo tale parziale e sintetica panoramica del settore dei trasporti messo a confronto con le nuove sfide offerte dall'economia collaborativa, appare anche indispensabile un maggiore coordinamento delle Autorità, sia a livello nazionale tra le diverse *Authority*, di garanzia e settoriali, sia a livello sovranazionale. Sembra, infatti, che la complessità del fenomeno sia tale da non permettere di individuare il soggetto meglio posizionato per intervenire a correggere le (eventuali) distorsioni.

2. LA GESTIONE DEI DATI PERSONALI NEL SETTORE DEI TRASPORTI: PROBLEMI E PROSPETTIVE

(Aldo Corvino)

Il tema della gestione dei dati si è ormai imposto anche al di fuori del dibattito specialistico ed occupa una posizione centrale quale fenomeno culturale che caratterizza la società contemporanea. Anche se i pericoli derivanti dalla memorizzazione ed elaborazione di una quantità impressionante di dati personali difficilmente possono essere intesi in tutte le loro implicazioni, essi sono ormai generalmente avvertiti. In particolare, comincia ad essere oggetto di discussione il modello secondo cui alcuni servizi vengono offerti gratuitamente, o con una riduzione del corrispettivo, in cambio dell'autorizzazione ad utilizzare e condividere dati personali[158].

Come è stato osservato, l'identità riscostruita partendo dalla enorme quantità di dati personali rilasciati quotidianamente trasforma la persona da essere umano in un complesso di dati: la *natural person* in una *digital person*.

All'interno di tale complesso si distinguono i dati utilizzati per fornire servizi amministrativi (come la carta d'identità digitale, la patente automobilistica digitale, la tessera sanitaria digitale) e quelli che permettono di riscostruire le abitudini delle persone attraverso le operazioni economiche che compiono quotidianamente (*transaction identity*)[159].

La gestione dei dati, come è noto, non si pone come problema relativo ad uno specifico settore, ma è trasversale, in quanto riguarda tutti i settori.

L'incessante sviluppo tecnologico rende opportuna un'analisi volta ad individuare, in vista di ulteriori possibili distinzioni e prospettive di ricerca, le caratteristiche dei dati coinvolti in ciascun settore ed il loro trattamento.

Nel settore dei trasporti lo sviluppo tecnologico e la *social economy* hanno influito notevolmente sui modelli di *business*. Come sottolinea il Presidente dell'Autorità di regolazione dei trasporti "lo sviluppo della industria della mobilità è legato a quello dell'energia e del digitale", ed in questo nuovo contesto "non è scontato che continuino ad essere gli

[158] Sul punto, v. Consumerism 2016. Nono rapporto annuale. Dalla *sharing* alla *social economy*, ed ivi, in particolare, l'introduzione di F. Bassan, M. Rabitti, Dalla *sharing*, alla *social* verso la *shadow economy*: l'Europa in transizione. Cfr. G. Colangelo, *Big Data, piattaforme digitali e antitrust*, in Mercato, concorrenza e regole, 2016, 425 ss. Recentemente, il tema è frequentemente affrontato anche dalla stampa. Ad esempio, muovendo dalla premessa secondo cui "l'utopia della rete degli esordi – libera, decentralizzata, paritaria per natura – è morta" ci si interroga su come invertire la marcia, e si suggerisce che il punto centrale è smontare l'idea secondo cui è fisiologico che la moneta di scambio per fruire di servizi solo apparentemente gratuiti siano le nostre vite, in ogni più minuto dettaglio (F. Chiusi, in L'espresso, n. 38, anno LXIII, 17 settembre 2017, 76).

[159] G. Alpa, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contr. impr.*, 2017, 723 ss.

attori tradizionali ad orientarne la crescita; nuovi operatori globali, attivi anche nella raccolta e gestione dei dati essenziali per i servizi di mobilità sono già sulla scena"[160].

Paradigmatico, in questo senso, è ovviamente il caso di Uber. Un modello certamente innovativo e che genera una serie di problemi, ad esempio, anche nel campo della tutela dei lavoratori[161]. Altro esempio più recente è quello di Flixbus, società tedesca che si occupa di trasporti extraurbani su autobus in tutta Europa e che si basa su un modello economico secondo cui la predetta società non svolge direttamente il servizio di trasporto ma si occupa di *marketing*, politica dei prezzi e gestione della qualità.

Vi è anche da dire che alcune attività, anche se presentate come fortemente innovative, non sono poi così diverse dalle tradizionali, se non per la notevole attenzione al *marketing*[162].

Ma persino in questi casi, ciò che inevitabilmente cambia rispetto al passato è la maggiore accumulazione di dati personali, favorita dalla possibilità di effettuare trasporti intermodali utilizzando un semplice dispositivo[163].

Per individuare le specifiche problematiche relative alla gestione dei dati personali nel settore dei trasporti il punto di partenza non può che essere la nozione di "dato personale". Si tratta, come è noto, di "*qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")*"[164].

Orbene, con riferimento al trasporto, inteso, in via generale, quale attività umana che consente lo spostamento di persone o merci da un luogo ad un altro (avvalendosi di percorsi terrestri, aerei e marittimi, eventualmente tra loro combinati), come per qualsiasi altra operazione economica i dati rilasciati consentono di riscostruire il profilo dell'utente in relazione ai beni e servizi acquistati e dunque, in questo caso, consentono di ricostruire i suoi spostamenti.

Per inciso, lo stesso risultato viene raggiunto con la c.d. "geolocalizzazione", che consente, avvalendosi di varie possibili tecniche, di identificare la posizione di un dato oggetto (e, conseguentemente, la posizione di una persona o di un altro oggetto ubicato nei pressi di quello geolocalizzato). Il problema relativo alla quantità di dati coinvolti è evidente se solo si pensa a tutte le applicazioni che per funzionare, o per funzionare in modo più performante, hanno bisogno di raccogliere dati relativi, appunto, alla geolocalizzazione[165]. A questo proposito, infatti, il recente Regolamento Europeo, nel fornire la definizione di "dato personale" precisa che costituisce dato personale qualsiasi informazione riguardante una persona identificabile anche attraverso "dati relativi all'ubicazione"[166].

Tuttavia la c.d. "geolocalizzazione" si presenta probabilmente quale problema generale legato alla *privacy* e non ri-

---

[160] Relazione del Presidente dell'Autorità di regolazione dei trasporti Andrea Camanzi presentata alla Camera dei Deputati il 12 luglio 2017.

[161] La Repubblica, 25 giugno 2017, pag. 18, si legge la discussione sulla possibilità di equiparare le piattaforme digitali alle agenzie per il lavoro

[162] È il caso, ad esempio, di "Lyft Shuttle". Il servizio viene presentato come un modo "rapido e abbordabile" per viaggiare su tratte fisse, "senza fermate a sorpresa" e a un prezzo prestabilito. È stato notato che "al netto dell'aziendalese, Lyft pare solamente avere reinventato l'autobus" (F. Chiusi, in L'Espresso, n. 34, anno LXIII, 20 agosto 2017, 11).

[163] Da questo punto di vista la concentrazione dei dati rende il problema ancor più rilevante, e fa riflettere quanto si legge sull'Economia, Corriere della Sera, del 14 agosto 2017: "Parcheggi, pedaggi, benzina, multe, Biglietti dell'autobus, car sharing: un'applicazione unica per pagare tutti i servizi legati alla mobilità. A lanciarla è Telepass, che annuncia un piano digitale che porti, entro il 2018, il saldo invisibile del conto di qualsiasi servizio. Scaricando Telepass pay, insomma, non ci si accorgerà più di pagare: a fare tutto sarà l'*app*".

[164] Questa è la definizione che si legge nell'art. 4, comma 1, n. 1, del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/ce (regolamento generale sulla protezione dei dati).

165 Si pensi al prossimo aggiornamento della nota App di messaggistica istantanea WhatsApp che potrebbe introdurre un sistema di geolocalizzazione live dei contatti, che potrebbe peraltro essere già attivo di default.

[166] Ai sensi del Regolamento, infatti, "*si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*".

guarda in modo specifico il settore dei trasporti. Difatti, essa consente di conoscere l'ubicazione e lo spostamento di un oggetto, ma ciò a prescindere dal mezzo di trasporto utilizzato, e più a monte anche a prescindere dall'utilizzo di un servizio di trasporto.

Tornando alla c.d. *transaction identity*, e cioè all'identità digitale ricostruita attraverso le operazioni economiche compiute, il problema della gestione dei dati, che si pone con riferimento ad ogni modello di *business*, è particolarmente rilevante nelle c.d. piattaforme multi-versante (come, ad esempio, Uber e Blablacar), le quali, come è noto, operano come intermediari tra due o più gruppi di agenti economici fornendo loro un luogo virtuale di incontro per facilitarne le interazioni e gli scambi commerciali.

Il modello di *business* di tali piattaforme si basa infatti proprio sulle informazioni, e segnatamente "sulle esternalità che, attraverso la piattaforma, si generano tra i diversi gruppi di utenti di cui si agevola il contatto: in particolare, quelli derivanti dalla circostanza che due o più gruppi di agenti economici per interagire hanno bisogno di utilizzare la piattaforma e che il valore conseguito dal gruppo di agenti presente su un versante della piattaforma dipende dal numero degli agenti che partecipano sull'altro versante della piattaforma"[167].

Le informazioni veicolate in tali piattaforme generano poi un ulteriore ordine di problemi, relativamente ai *feedback* consegnati dall'utente alla piattaforma. Il tema è quello delle false recensioni. Esso sembra costituire l'omologo del problema delle *fake news*: come le notizie false di interesse generale (le *fake news*, appunto) costituiscono un problema per l'intera rete[168], le false recensioni costituiscono il corrispondente problema nelle piattaforme multiversante in cui l'informazione falsa si riferisce ad uno specifico tipo di servizio.

Infine, nel settore dei trasporti i dati personali hanno anche una rilevanza che potrebbe forse essere considerata più tradizionale, ma che si amplifica nella *social economy*. Questi, infatti, costituiscono informazioni importanti nell'ambito delle politiche di sicurezza e di contrasto al terrorismo. Così come per il trasporto aereo, si discute, allora, dell'estensione dell'obbligo di emettere biglietti nominativi anche ad altre modalità di trasporto. Qui il tema, forse più classico, è quello dei limiti ai poteri esercitati per finalità di pubblica sicurezza, che devono essere bilanciati, ovviamente, con il diritto alla *privacy*.

Tirando le somme, i problemi sollevati dalla *social economy*, tra Big Data e *fake news*, anche se parzialmente trasversali a tutti i settori, nel settore dei trasporti, qui esaminato, si colorano delle particolari caratteristiche dei dati coinvolti, relativi allo spostamento di merci e persone, richiedendo a chi pone le regole (ed a chi deve interpretarle ed applicarle) di tenerne conto nel bilanciamento della protezione dei dati personali con le ragioni dell'economia e della pubblica sicurezza.

3. BIG DATA, TRASPORTI E REGOLAZIONE

(Paolo Occhiuzzi)

Abbiamo osservato nelle precedenti pagine che la raccolta delle informazioni e la loro gestione con la logica dei Big Data, rivestono un ruolo strategico per le imprese, in particolare per quelle che operano con un modello di *business* tipico delle piattaforme *online* e che ricorrono sempre più spesso alle informazioni a carattere personale con l'obiettivo di creare nuove forme di valore. Di qui, il significativo e crescente ruolo svolto dai Big Data sulla concorrenza dei mercati e sul pluralismo dell'informazione.

[167] G. Colangelo, *Big Data, piattaforme digitali e antitrust*, cit., 434.

[168] Sul punto, v. G. Ghidini e A. Massolo, *Fake news: responsabilità, non censura*, in Dir. ind., 2017, 352 ss.

Tutto ciò posto la domanda che è opportuno porsi è relativa alla necessità di individuare delle regole settoriali per gestire il fenomeno.

La regolazione, invero, dei Big Data dovrebbe essere quanto più possibile di carattere orizzontale, lasciando dunque alla concorrenza il compito di gestire i rapporti tra gli attori del mercato. Ma abbiamo già osservato che la disciplina antitrust può non bastare e potrebbe essere comunque necessario un intervento per evitare una inutile distorsione in uno specifico mercato.

Pensiamo al settore dei trasporti. In tale aerea dell'economia, intermodalità e integrazione (anche tecnologica ed infrastrutturale) dei trasporti caratterizzano sempre più diffusamente le strategie industriali delle imprese del settore ed i bisogni di mobilità dei cittadini.

Non a caso, in ambito UE, la Commissione ha intitolato il 2018 alla multimodalità. Alla multimodalità sono, altresì, orientate le più recenti iniziative di *policy* dell'esecutivo comunitario, quali quella dedicata alla mobilità dei passeggeri[169]. In tale contesto, nel tracciare "l'agenda per una transizione socialmente equa verso una mobilità pulita, competitiva e connessa a favore di tutti", la Commissione evidenzia, fra l'altro, l'interazione e contestuale evoluzione di nuovi bisogni di mobilità e di quella che viene definita la "*rivoluzione della mobilità digitale*", enunciando il binomio multimodalità-digitalizzazione che caratterizzerà tale agenda negli anni a venire.

Anche in sede plurilaterale, nell'ambito del *network* degli organismi di regolazione denominato IRG-rail (Independent Regulators' Group), il binomio multimodalità-digitalizzazione è stato integrato nella strategia del prossimo triennio tra le principali sfide ed opportunità per il regolatore.

Queste tendenze pongono importanti sfide sia nella definizione delle politiche pubbliche che nella regolazione economica *ex ante.*

Ma quali possono essere degli efficaci interventi di regolazione settoriale? Senza alcuna pretesa di indicare soluzioni, la nostra analisi si può tuttavia concentrare su due esempi: il mondo ferroviario e i servizi di trasporto non di linea.

Il settore ferroviario è già entrato nel percorso della digitalizzazione; percorso che coinvolge tutti gli attori del mercato, dagli utenti finali alle imprese ferroviarie, ai gestori delle infrastrutture o ai fornitori del materiale rotabile.

A livello nazionale il gruppo Ferrovie dello Stato è una delle realtà italiane che sta puntando sull'innovazione e sulla trasformazione digitale, per coniugare due obiettivi fino a qualche anno fa difficilmente compatibili: migliorare sia l'efficienza che i livelli di servizio ai clienti.

A fine settembre il gruppo ha dato due segnali forti in questo senso. Il primo è il piano decennale 2017-2026, con cui punta a diventare operatore di mobilità nel senso più ampio: un unico punto d'accesso per tutti i tipi di trasporto, dai treni ai bus (trasporto pubblico locale, ma anche lunga percorrenza) fino al *car sharing*, grazie a una piattaforma digitale che accompagnerà il cliente "da porta a porta", con un unico titolo di viaggio. Il secondo è l'avvio della parte più innovativa di un grande progetto che riguarda Trenitalia, e che dimostra concretamente l'impegno sul digitale per cambiare profondamente gli approcci operativi e competitivi.

L'operatore può già raccogliere e combinare le informazioni che arrivano da biglietterie e tornelli. Le obliteratrici poi sono dotate di una carta sim: al momento serve a segnalare eventuali guasti, ma in prospettiva potrà leggere e comunicare il passaggio degli abbonati. Altre sperimentazioni riguardano il *Near field communication*. Piccoli *chip* installati nel telefono (Apple dovrebbe offrirlo per la prima volta con il nuovo modello di iPhone) e usati per i pagamenti elettronici dialogheranno con i tornelli alla stazione, scalando in automatico il costo del viaggio. Oppure, inseriti all'interno di un normale biglietto di carta, segnaleranno i dati al computer dei controllori, che potranno subito verificare le presenze in carrozza.

[169] Comunicazione della Commissione UE del 31 maggio 2017 [COM(2017)283 final], intitolata "*Europe on the move*"

L'opportunità è quella di rimodulare l'offerta secondo le esigenze dei clienti, comunicandola con campagne di *marketing* mirate. Di calibrare al meglio composizione e orari dei treni, in modo che non viaggino pieni o vuoti. E nel settore del trasporto merci, di rendere più efficienti le connessioni tra rotaie, porti e interporti.

Ma a ben vedere, una parte di dati che l'operatore Trenitalia può processare deriva dalla prestazione di servizi non in concorrenza e soggetti ad obblighi di servizio pubblico (si pensi al servizi di trasporto regionale e/o servizi prestati sulla base di contratti esistenti con il Ministero delle Infrastrutture, ad es. servizi Intercity).

In tali casi, si può immaginare che un operatore privato detenga un patrimonio informativo – acquisito non sulla base di un confronto concorrenziale – al quale operatori minori non riescono ad accedere, o il cui utilizzo è precluso a chi non ha le risorse per un uso competitivo dei dati.

L'importanza di tale patrimonio informativo è elemento certamente noto all'Autorità dei trasporti che ha avviato una consultazione pubblica su uno schema di atto di regolazione che stabilisce le condizioni minime di qualità dei servizi di trasporto passeggeri per ferrovia (nazionali e regionali) connotati da obblighi di servizio pubblico (OSP)[170].

Alla base della proposta vi è il processo di unificazione dei principali indicatori di qualità – regolarità, puntualità, comfort, pulizie, PRM, ecc. – e la definizione delle modalità per la loro verifica e monitoraggio, mediante responsabilizzazione delle imprese ferroviarie (certificazione dei dati), degli Enti affidanti (controllo attraverso strutture dedicate), ed il pieno coinvolgimento delle associazioni dei consumatori, il tutto con l'obiettivo di garantire maggiore omogeneità nelle condizioni di qualità per gli utilizzatori dei servizi di trasporto passeggeri per ferrovia.

Per quanto qui d'interesse, nell'opera di regolazione avviata dall'ART, rivestono particolare rilievo il tema della trasparenza e nonché la previsione del c.d. "Piano di Accesso al dato".

Quanto al tema della trasparenza, l'Autorità sembra aver colto appieno l'esigenza di rendere disponibili i dati al fine di definire gli indicatori e i livelli minimi di servizio. L'accesso ai dati, compatibilmente con il rispetto dei limiti per la tutela degli interessi rilevati, rappresenta, infatti, un elemento essenziale per un efficace controllo dei servizi erogati nonché per una più efficiente allocazione delle risorse pubbliche.

Nell'ottica della trasparenza, al punto 4, Misura 3, dell'atto di regolazione si introduce il "*Piano di Accesso al dato*", definito a cura dell'ente affidante in sede di stipula del contratto di servizio, nell'ambito del quale si individuano i dati disponibili, le modalità di rilevazione e le modalità di accesso da parte di terzi, open o tramite specifica istanza. Particolare enfasi viene posta sull'accesso ai dati real-time, considerati i potenziali utilizzi e i benefici per gli utenti del servizio, la cui esperienza di viaggio complessiva risulterebbe migliorata.

Lo schema di atto in commento testimonia l'estrema attenzione dell'Autorità su un tema estremamente sensibile. D'altro canto, le piattaforme digitali e l'emergere di nuovi operatori di mercato multimodale dovrebbero spingere gli organismi di regolamentazione a sviluppare competenze e strumenti per monitorare efficacemente i mercati dei passeggeri e dei trasporti ferroviari. Ciò al fine di valutare l'esigenza di un intervento regolatorio idoneo a far sì che il diseguale accesso alle informazioni e la non uniforme capacità di estrarre da esse elementi di accrescimento della propria competitività non determinino fenomeni di concorrenza sleale e di distorsione della concorrenza vera e propria.

Ulteriori e più strutturate misure potrebbero essere adottate anche in sede di attuazione dei principi del regolamento UE 2016/2338, che modifica il regolamento CE 1370/2007, in base al quale le Autorità competenti di ogni Stato membro dell'Unione Europea (Stato, Regioni, Enti locali) dovranno stabilire per il trasporto, sia su ferro sia su strada, le specifiche degli obblighi di servizio pubblico.

[170] Il riferimento è qui alla delibera ART n. 88/2017, consultabile all'indirizzo *http://www.autorita-trasporti.it/wp-content/uploads/2016/04/Allegato-A-delibera-n.-8_2017.pdf*

Se è vero, infatti, che compito della politica di concorrenza sia difendere il mercato contro se stesso[171], e quindi governare e correggere i processi spontanei dei mercati, che tendono a chiudersi in assetti monopolistici e ad allontanarsi da quel dinamismo che garantisce la continuità dello sviluppo[172], tale difesa avviene anche, e soprattutto, da parte degli apparati pubblici, attraverso gli strumenti di regolazione.

La correzione dei vantaggi competitivi, acquisiti in relazione al possesso ed all'elaborazione delle informazioni e suscettibili di alterare la concorrenza, si qualifica, allora, come l'obiettivo che la politica della concorrenza deve darsi, e che può tradursi in un'azione efficace se riveste la forma della regolazione.

Nel settore dei trasporti non di linea, nell'ultimo decennio si sono osservati irreversibili fenomeni di allargamento e diversificazione dell'offerta dei servizi di mobilità non di linea, idonei ad aumentare l'offerta e a ridurre i prezzi del servizio, con indubbi vantaggi per il consumatore.

Rispetto a questo processo di evoluzione del mercato, gli operatori tradizionali, dotati di licenza taxi emessa dai comuni e operanti sulla base di una rigida regolamentazione del numero di licenze, dei turni, degli orari ecc., rappresentano la categoria più vulnerabile. Sono stati ormai già evidenziati[173] i benefici concorrenziali per i consumatori finali derivanti da una generale affermazione delle nuove piattaforme di comunicazione fra domanda e offerta di servizi di mobilità non di linea in termini di maggiore facilità di fruizione del servizio di mobilità, migliore copertura di una domanda spesso insoddisfatta, miglioramento della qualità del servizio e riduzione dei costi per l'utenza, e, nella misura in cui si disincentiva l'uso del mezzo privato, in termini di decongestionamento del traffico urbano, con un miglioramento delle condizioni di offerta del servizio di trasporto pubblico di linea e di circolazione del traffico privato.

In particolare, sono state espresse valutazioni concorrenziali sia con riferimento a quella tipologia di servizi che utilizzano piattaforme digitali per connettere autisti professionisti dotati di licenza taxi o autorizzazione NCC con la domanda finale (come UBER Black o Mytaxi), sia con riguardo all'altra tipologia di servizi che, tramite la piattaforma, mette in connessione autisti non professionisti e la domanda finale (come il servizio UBER Pop, attualmente inibito sull'intero territorio nazionale da alcune decisioni del Tribunale civile di Milano)[174].

Con riferimento al primo tipo di servizi, è d'obbligo procedere ad un'interpretazione delle norme vigenti costituzionalmente orientata e dunque rispettosa del principio di libertà di iniziativa economica privata di cui all'articolo 41 della Costituzione. L'Autorità di settore dovrebbe sostenere l'inapplicabilità agli autisti dotati di autorizzazione NCC che si servono di piattaforme digitali per il procacciamento della clientela delle norme della legge 21/92 che ne vincolano l'operatività all'esistenza ad una rimessa all'interno del comune che ha rilasciato l'autorizzazione (ed in particolare degli articoli 3 e 11 della legge 21/92).

Non a caso, l'Autorità di Regolazione dei Trasporti già nel 2015 ha adottato il noto "*Atto di segnalazione al Governo e al Parlamento sull'autotrasporto di persone non di linea: taxi, noleggio con conducente e servizi tecnologici per la mobilità*", nell'ambito dell'esercizio delle funzioni di segnalazione di interventi legislativi correlati alla evoluzione del settore dei trasporti e, nello specifico, del trasporto pubblico non di linea.

Con tale atto, l'ART ha già fornito prime indicazioni "con l'obiettivo di promuovere la concorrenza e garantire adeguati livelli di qualità ed efficienza dei servizi di autotrasporto di persone non di linea".

Le indicazioni contenute nella segnalazione riguardano alcune proposte di modifica normativa proprio relative alla legge quadro n. 21/92, anche alla luce del già discusso impiego delle piattaforme tecnologiche che svolgono attività

[171] S. Mannoni, *La regolazione delle comunicazioni elettroniche,* Bologna, 2014, 11

[172] M. Libertini, *Diritto della concorrenza dell'Unione Europea,* Milano, 2014, 42 ss.

[173] Cfr. AGCM, Segnalazione al Parlamento e al Governo sulla "*Legge quadro per il trasporto di persone mediante autoservizi pubblici non di linea*" in bollettino AGCM n. 39/2015.

[174] Cfr. ordinanza del 25 maggio 2015, R.G. n. 16612/2015, in primo grado; ordinanza del 2 luglio 2015, R.G. nn. 35445/2015 e 36491/2015, in sede di reclamo.

di intermediazione tra domanda e offerta di mobilità, proponendo di inserire nella legge quadro n. 21/92 un nuovo articolo contenente la disciplina delle nuove forme di mobilità che si svolgono grazie ad applicazioni *web* che utilizzano piattaforme tecnologiche per l'interconnessione dei passeggeri e dei conducenti (i cc.dd. "servizi tecnologici per la mobilità" o anche STM).

È certamente da ammirare, dunque, il lavoro dell'ART che prima tra tutte le Autorità ha tentato di dare risposte alle domande poste dal vuoto normativo nel quale si muovono i fenomeni digitali nel settore dei trasporti, ponendo all'attenzione del legislatore la necessità di superare le obsolete norme recate dalla l. 21/92.

Con riferimento a quei servizi di mobilità che utilizzano autisti non professionisti collegati ad una piattaforma digitale, è forse necessaria l'adozione di una regolamentazione minima, alla luce dell'esigenza di contemperare interessi meritevoli di tutela: concorrenza, sicurezza stradale e incolumità dei passeggeri, definendo un "terzo genere" di fornitori di servizi di mobilità non di linea (in aggiunta ai taxi ed agli NCC). Tale regolamentazione dovrebbe essere tuttavia la meno invasiva possibile, limitandosi a prevedere una registrazione delle piattaforme in un registro pubblico e l'individuazione di una serie di requisiti e obblighi per gli autisti. In questo contesto, appare necessario evitare soluzioni che, pur rappresentando una apertura a questi servizi, ne potrebbero sancire, di fatto, un'operatività ridotta, non in grado di aumentare la concorrenza sui servizi di trasporto non di linea.

In un'ottica di massimizzazione del benessere sociale, la strada da perseguire non dovrebbe essere quella di introdurre nuovi e/o ulteriori vincoli – su base territoriale, soggettiva o altro – volti a limitare l'operatività delle nuove forme di servizi di mobilità urbana. Si dovrebbe al contrario perseguire una strada di "deregolazione dal basso" dei vincoli a carico degli operatori gravati da obblighi di servizio pubblico, in modo che essi abbiano la possibilità di rispondere in maniera adeguata ai cambiamenti imposti sia dalle nuove tecnologie sia da una domanda sempre più esigente. Al fine di creare un "*level playing field*" appare dunque decisamente più efficiente alleggerire la regolazione degli operatori esistenti, sviluppando le forme di servizio più innovative e benefiche per il consumatore.

Con riferimento al servizio taxi, infine è forte l'esigenza di un intervento nel mercato della fornitura di servizi di raccolta e smistamento della domanda del servizio taxi per evitare inutili strumentalizzazione dei soggetti già operanti nel settore a discapito dei nuovi entranti. Si tratta di mercati in cui al canale c.d. "tradizionale" (posteggi e colonnine) si affiancano il radiotaxi, i numeri unici comunali e le *app* che mettono direttamente in contatto l'utenza e i tassisti (come Mytaxi). L'ingresso di tali ultimi strumenti è tuttavia osteggiato da una *struttura* di mercato ormai obsoleta e legata a vecchi schemi corporativi. Si pensi alla forma cooperativa dei radiotaxi che, nel legare a vincoli di non concorrenza i tassisti aderenti, non permette lo sviluppo delle nuove forme di raccolta delle corse, a detrimento della possibilità per il consumatore di aver un più agevole accesso al servizio.

AEEGSI

(Cristiana Lauri, Maria Chiara Sole)

I Big Data sono oramai protagonisti di una vera e propria rivoluzione industriale che ha al centro le nuove tecnologie. Secondo recenti stime, i dati digitali stanno crescendo esponenzialmente ogni anno e possono essere di grande supporto per tutti i settori dell'economia, adducendo un notevole vantaggio competitivo, stimolando l'innovazione, aumentando la competitività con i conseguenti impatti sociali. Se nel settore privato l'utilizzo dei grandi quantitativi di dati per finalità di tipo commerciale è piuttosto intuitivo, notevole è il ruolo che l'utilizzo dei Big Data ha anche nel settore pubblico. In questo ambito rientrano gli aspetti legati alla sicurezza stradale, alla salute dei cittadini, alla salvaguardia dell'ambiente e all'utilizzo sostenibile delle risorse naturali. Il regolatore è oggi posto di fronte ad una nuova sfida che vede la necessità di coniugare l'innovazione, grazie all'utilizzo dei Big Data, con la tutela dei consumatori e degli utenti e, in definitiva, della collettività.

Tra i molteplici settori, l'utilizzo dei dati e delle informazioni relative ai consumi si è affermato come fattore essenziale per il buon funzionamento del mercato energetico. Solo in apparenza neutrale, lo strumento dei dati può rivelarsi un'arma potente, suscettibile di alterare i rapporti di forza tradizionalmente delineatisi tra i molteplici soggetti che in quel mercato si confrontano: per le imprese la disponibilità dei dati funge da stimolo concorrenziale; per i consumatori è un mezzo essenziale al fine di operare scelte consapevoli e aderenti ai propri bisogni. In questo scenario, l'Autorità per il gas, l'energia elettrica e il sistema idrico è protagonista nel delicato passaggio ad un mercato energetico tecnologicamente avanzato, attraverso un'attività regolatoria sempre più intensa ed in linea con l'inaugurazione di un nuovo corso orientato all'efficienza energetica.

I dati e le informazioni sui consumi energetici nel mercato *retail*

(Cristiana Lauri)

SOMMARIO: 1. GLI INTERVENTI REGOLATORI SUI SISTEMI DI *SMART METERING*. – 2. LA GESTIONE DEI DATI PER LO SVILUPPO COMPETITIVO DEL MERCATO. DISINTERMEDIAZIONE E SOGGETTI COINVOLTI. – 3. IL VALORE DEI DATI E DELLE INFORMAZIONI PER IL CONSUMATORE ENERGETICO NEL PARADIGMA DELLA *SOCIAL ECONOMY.*

1. GLI INTERVENTI REGOLATORI SUI SISTEMI DI *SMART METERING*

L'attuale stagione del settore energetico si mostra caratterizzata da interessi apparentemente contrapposti: da un lato lo sviluppo dal punto di vista economico e il consolidamento di un mercato sempre più concorrenziale; dall'altro la crescente attenzione alle ricadute sull'ambiente che l'utilizzo massiccio delle risorse energetiche impone[175]. Il *trait d'union*

[175] In dottrina v. F. de Leonardis, "*Risparmio energetico, efficienza energetica e amministrazioni: il Piano di azione nazionale per l'efficienza energetica nell'ambito della Programmazione energetica nazionale*", in Annuario di diritto dell'energia, Bologna, 2016, il quale individua tutela dell'ambiente e sviluppo economico come gli interessi più rilevanti in tema di efficienza energetica e li definisce

tra i due profili sembra potersi in larga parte ravvisare nell'utilizzo delle tecnologie disponibili, le quali permettono di coniugare i due aspetti attraverso l'introduzione sul mercato di soluzioni innovative[176]. Tra queste, di particolare rilievo anche in ragione dell'azione regolatoria a ciò dedicata negli ultimi mesi, vi è la possibilità di rilevare e utilizzare i dati e le informazioni relativi al consumo dell'energia.

Lo sfondo normativo del quadro delineato, come noto, è il d.lgs. n. 102/2014, che ha recepito nell'ordinamento italiano la direttiva sull'efficienza energetica 2012/27/UE. Negli ultimi due rapporti Consumer's Forum sono stati indagati due filoni di riforma promananti da tale novella normativa: il primo che già definimmo come "sostanziale", consistente nel superamento della struttura tariffaria progressiva rispetto ai consumi energetici, delle componenti di rete e degli oneri generali di sistema[177]; il secondo, "formale", la c.d. "Bolletta 2.0"[178].

Il presente contributo rappresenta lo sviluppo naturale di quelle premesse ed intende focalizzarsi sull'analisi degli "strumenti abilitanti" tali innovazioni e sulla contigua messa a disposizione dei dati sui prelievi di energia e di potenza ai consumatori domestici serviti in bassa tensione, riallacciandosi al tema generale della X edizione del Rapporto: la centralità del "dato" e la rilevanza della veridicità dello stesso.

In un contesto concorrenziale in cui la domanda diviene dinamica e l'offerta ritagliata sui bisogni dei clienti finali, la conoscenza dei consumi, attraverso i dati, diventa infatti imprescindibile. Anche l'introduzione degli *smart metering* si inserisce, dunque nella fondamentale transizione del mercato energetico verso agli ambiziosi obiettivi di efficienza energetica posti dalle politiche più recenti in ambito sovranazionale e recepite nell'ordinamento interno[179].

L'Italia è un esempio virtuoso nell'implementazione dei sistemi di *smart metering*[180], i quali hanno rivelato da subito significativi vantaggi per le imprese e per i consumatori[181]. La prima fase di misuratori elettronici, i cc.dd. *smart mete-*

---

come "*terribile coppia degli interessi in gioco*".

[176] Nel considerando 1 della Direttiva 2012/27/UE del Parlamento europeo e del Consiglio del 25 ottobre 2012 sull'efficienza energetica, che modifica le direttive 2009/125/CE e 2010/30/UE e abroga le direttive 2004/8/CE e 2006/32/CE, si legge che "*L'Unione si trova di fronte a sfide senza precedenti de terminate da una maggiore dipendenza dalle importa zioni di energia, dalla scarsità di risorse energetiche, nonché dalla necessità di limitare i cambiamenti climatici e di superare la crisi economica. L'efficienza energetica costituisce un valido strumento per affrontare tali sfide. Essa migliora la sicurezza di approvvigionamento dell'Unione, riducendo il consumo di energia primaria e diminuendo le importazioni di energia. Essa contribuisce a ridurre le emissioni di gas serra in modo efficiente in termini di costi e quindi a ridurre i cambiamenti climatici. Il passaggio a un'economia più efficiente sotto il profilo energetico dovrebbe inoltre accelerare la diffusione di soluzioni tecnologiche innovative e migliorare la competitività dell'industria dell'Unione, rilanciando la crescita economica e la creazione di posti di lavoro di qualità elevata in diversi settori connessi con l'efficienza energetica*".

[177] Vd. A. Affinito, "*Superamento delle tutele di prezzo e collective switching: la tutela simile*", in Consumerism 2016, Nono Rapporto annuale, Dalla *sharing* alla *social economy*.

[178] Vd. C. Lauri, *"Bolletta 2.0: trasparenza, semplificazione e partecipazione"*, In Consumerism 2015, Ottavo Rapporto annuale, Il Consumatore dell'era della condivisione.

[179] A livello internazionale v. Risoluzioni dell'Assemblea delle Nazioni Unite A/Res/69/315 del 1 settembre 2015; A/res/70/1 del 25 settembre 2015, da cui emerge tra i nuovi obiettivi di sviluppo sostenibile da realizzare entro il 2030 garantire a tutti l'accesso a un'energia affidabile, sostenibile, moderna e a prezzi accessibili. Per quanto riguarda il quadro europeo v. da ultimo la Direttiva 2012/27/UE e il d.lgs. che l'ha recepita, 102/2014.toPer quanil'itivi non replicabi moderna e a prezzi accessibilia realizzare entro il 2030 garantire a tuttil'itivi non replicabi.

[180] L'Italia è stato uno dei primi Paesi europei a dotarsi di strumenti di misura elettronica teleletti e telegestiti per la misura dell'energia elettrica prelevata dalla rete in bassa tensione e, nel caso di clienti con proprio impianto di produzione, per la misura dell'energia prodotta e immessa in rete. Nel sito dell'AEEGSI si legge che "L'Italia è stato il primo paese europeo a introdurre su larga scala gli *smart meter* elettrici per i clienti finali in bassa tensione ed è tuttora il primo paese al mondo per numero di *smart meter* di energia elettrica in servizio (oltre 35 milioni). Secondo un recente report della Commissione europea, il sistema italiano di *smart metering,* con sostituzione dei contatori tradizionali dal 2001, è stato il più efficiente in Europa". Cfr. Comunicazione della Commissione, COM (2014) 356 final, 17 aprile 2014, *"Relazione della Commissione. Analisi comparativa dell'introduzione dei sistemi di misurazione intelligenti nell'UE-27 in particolare nel settore dell'elettricità".*

[181] La telegestione dei misuratori di energia elettrica in bassa tensione ha consentito alcuni benefici ai clienti finali di energia elettrica, come la riduzione dei periodi di consumo fatturati in acconto, la possibilità di effettuare misure di chiusura del periodo contrattuale in caso di cambio del fornitore e l'introduzione di nuovi servizi come il "servizio minimo" assicurato per un certo periodo di tempo prima del distacco in caso di morosità.

ring 1G, fu avviata con carattere spontaneo[182], che divenne successivamente obbligatorio[183]. Il passaggio ad un mercato energetico estremamente dipendente dalla rilevazione e dalla messa a disposizione dei dati di consumo è proseguito con il piano di sostituzione massiva dei misuratori con quelli di nuova generazione, i cc.dd. *smart metering* o 2G[184].

L'attuale stagione dei sistemi di misurazione intelligenti di energia elettrica in bassa tensione di seconda generazione trova il suo referente normativo nell'art. 9, comma 3, del d.lgs. n. 102/2014, in cui risultano enfatizzati tre elementi: precisione dei dati; sicurezza nella loro gestione; considerazione dell'energia eventualmente prodotta dal cliente[185].

Nel *"Quadro strategico per il quadriennio 2015-2018",* punto 1, recante *"Linee strategiche della regolazione nei settori dell'energia elettrica e del gas e relativi obiettivi strategici"*, punto 1.4 "*Più concorrenza nei mercati* retail*, anche grazie a una domanda più consapevole ed attiva"*, l'Autorità affronta le tematiche principali del quadriennio richiamando i due fondamentali temi della bolletta 2.0 e della riforma delle tutele di prezzo. A questi si aggiungono tra le priorità strategiche per il 2016 (obiettivo strategico OS.7) tre elementi di novità: l'accesso ai dati di consumo; la definizione dei requisiti funzionali dei misuratori di energia elettrica in bassa tensione di seconda generazione ("misuratori 2G"); la fatturazione sulla base di consumi effettivi o delle autoletture.

L'Autorità riconosce che *"*l'accesso non discriminatorio ai dati e alle informazioni sui consumi di energia e il parallelo sviluppo degli smart meters, diventano snodi centrali dei mercati al dettaglio competitivi. Per i consumatori l'accesso a informazioni dettagliate sui propri prelievi è un requisito indispensabile sia per una partecipazione più attiva e consapevole al mercato, sia per adeguare i propri comportamenti di consumo e scelte di investimento verso un uso più razionale ed efficiente dell'energia. Per i soggetti terzi (es. venditori, ESCO e aggregatori) un accesso non discriminatorio alle informazioni e ai dati di prelievo dei consumatori, senza il venir meno delle garanzie di tutela della *privacy* e sicurezza dei dati, è condizione indispensabile per sviluppo competitivo del mercato dei servizi per l'efficienza energetica e la gestione attiva della domanda"[186].

L'art. 9, comma 6, lett. b) del d.lgs. n. 102/2014, con cui è stata recepita nell'ordinamento nazionale la direttiva 2012/27/UE sull'efficienza energetica, prevede che l'Autorità per l'energia elettrica il gas ed il sistema idrico, con uno o più provvedimenti da adottare entro dodici mesi dalla data di entrata in vigore dello stesso decreto, individui le modalità

---

[182] In particolare, furono avviate in via sperimentale da alcune aziende tra il 2001 e il 2006.

[183] V. Deliberazione 292/2006. Tenere inoltre presente che dal 1 luglio 2007, con la liberalizzazione si separa la società di distribuzione, che svolge la misura, dalla società di vendita.

[184] V. l'approvazione del Piano dall'Autorità con la deliberazione 222/2017/R/eel.

[185] In particolare, l'art. 9 comma 3 del d.lgs. stabilisce che "*nella prospettiva di un progressivo miglioramento delle prestazioni dei sistemi di misurazione intelligenti e dei contatori intelligenti, introdotti conformemente alle direttive 2009/72/CE e 2009/73/CE, al fine di renderli sempre più aderenti alle esigenze del cliente finale, l'Autorità per l'energia elettrica, il gas ed il sistema idrico, con uno o più provvedimenti da adottare entro ventiquattro mesi dalla Data di entrata in vigore del presente decreto, tenuto conto dei relativi standard internazionali e delle raccomandazioni della Commissione europea, predispone le specifiche abilitanti dei sistemi di misurazione intelligenti, a cui le imprese distributrici in qualità di esercenti l'attività di misura sono tenuti ad uniformarsi, affinché: a) i sistemi di misurazione intelligenti forniscano ai clienti finali informazioni sulla fatturazione precise, basate sul consumo effettivo e sulle fasce temporali di utilizzo dell'energia. Gli obiettivi di efficienza energetica e i benefici per i clienti finali siano pienamente considerati nella definizione delle funzionalità minime dei contatori e degli obblighi imposti agli operatori di mercato; b) sia garantita la sicurezza dei contatori, la sicurezza nella comunicazione dei dati e la riservatezza dei dati misurati al momento della loro raccolta, conservazione, elaborazione e comunicazione, in conformità alla normativa vigente in materia di protezione dei dati. Ferme restando le responsabilità degli esercenti dell'attività di misura previste dalla normativa vigente, l'Autorità per l'energia elettrica, il gas e il sistema idrico assicura il trattamento dei dati storici di proprietà del cliente finale attraverso apposite strutture indipendenti rispetto agli operatori di mercato, ai distributori e ad ogni altro soggetto, anche cliente finale, con interessi specifici nel settore energetico o in potenziale conflitto di interessi, anche attraverso i propri azionisti, secondo criteri di efficienza e semplificazione c) nel caso dell'energia elettrica e su richiesta del cliente finale, i contatori di fornitura siano in grado di tenere conto anche dell'energia elettrica immessa nella rete direttamente dal cliente finale; d) nel caso in cui il cliente finale lo richieda, i dati del contatore di fornitura relativi all'immissione e al prelievo di energia elettrica siano messi a sua disposizione o, su sua richiesta formale, a disposizione di un soggetto terzo univocamente designato che agisce a suo nome, in un formato facilmente comprensibile che possa essere utilizzato per confrontare offerte comparabili; e) siano adeguatamente considerate le funzionalità necessarie ai fini di quanto previsto all'articolo 11 [domanda attiva]*".

[186] Cfr. *Quadro Strategico per il Quadriennio 2015-2018*, in www.autorita.energia.it.

con cui, se tecnicamente possibile ed economicamente giustificato, "*le imprese di distribuzione ovvero le società di vendita di energia elettrica e di gas naturale al dettaglio, nel caso in cui siano installati contatori, conformemente alle direttive 2009/72/CE e 2009/73/CE, provvedono affinché i clienti finali abbiano la possibilità di accedere agevolmente a informazioni complementari sui consumi storici che consentano loro di effettuare controlli autonomi dettagliati. Le informazioni complementari sui consumi storici comprendono almeno: 1) dati cumulativi relativi ad almeno i tre anni precedenti o al periodo trascorso dall'inizio del contratto di fornitura, se inferiore. I dati devono corrispondere agli intervalli per i quali sono state fornite informazioni sulla fatturazione; 2) dati dettagliati corrispondenti al tempo di utilizzazione per ciascun giorno, mese e anno. Tali dati sono resi disponibili al cliente finale via internet o mediante l'interfaccia del contatore per un periodo che include almeno i 24 mesi precedenti o per il periodo trascorso dall'inizio del contratto di fornitura, se inferiore.*" Ai fini dell'analisi delle modalità di messa a disposizione dei dati storici di consumo, occorre primariamente evidenziare come i suddetti dati storici siano per loro natura differenti e rispondano a finalità diverse. In particolare: i dati storici corrispondenti agli intervalli di fatturazione rispondono principalmente all'esigenza di aumentare le informazioni al cliente finale per poter effettuare delle scelte contrattuali consapevoli (ad esempio essere in grado di scegliere in modo più opportuno tra le diverse offerte nonché di controllare il proprio contratto e valutare la scelta coerente con i propri consumi); tali dati possono corrispondere a quelli utilizzati ai fini della fatturazione del cliente finale, ciò comportando l'eventuale inclusione di dati validati dall'impresa di distribuzione, in qualità di soggetto responsabile della misura; i dati storici corrispondenti al profilo temporale di consumo, invece, contribuiscono ad aumentare le informazioni al cliente finale per poter verificare il proprio comportamento di consumo *(energy footprint)* – eventualmente comprensivo di autoconsumo – al fine di poterlo modificare in modo da minimizzare il consumo medesimo a parità di servizio energetico finale (tramite servizi e audit energetici); a tale fine i suddetti dati devono avere una maggiore granularità temporale ed essere messi a disposizione del cliente finale in un tempo ravvicinato rispetto al momento in cui si verifica il consumo; in tale ambito, quindi, può essere valutato, anche ai fini della fattibilità tecnica ed economica degli interventi, se utilizzare dati messi a disposizione più velocemente al cliente finale attraverso dispositivi che garantiscano un riscontro immediato, seppure senza validazione.

Con il termine "*smart metering*" si intendono, dunque, i sistemi che consentono la telelettura e telegestione dei contatori di energia elettrica, gas e acqua. I vantaggi dei sistemi di *smart metering* sono numerosi: oltre alla riduzione di costi per le letture e per le operazioni di gestione del contratto (come ad esempio il cambio di fornitore, la disattivazione etc.) che possono essere effettuate in modo automatico a distanza, e con maggiore frequenza, senza un intervento in loco dell'operatore, essi consentono altri benefici, che dipendono dal settore in cui sono applicati. Innanzitutto, per tutti i settori con contatori individuali essi contribuiscono a garantire una migliore consapevolezza del cliente finale in relazione ai propri consumi e di conseguenza la promozione dell'efficienza energetica e dell'uso razionale delle risorse. Inoltre, per tutti i settori (energia elettrica, gas, idrico, teleriscaldamento) permettono una migliore gestione della rete e una migliore individuazione delle perdite tecniche e commerciali. Nel contesto dei settori liberalizzati rappresentano una facilitazione della concorrenza grazie alla possibilità di ottenere una lettura al di fuori del ciclo in occasione del cambio di fornitore.

Rispetto alla precedente generazione, i misuratori 2.0 permettono un aumento dell'efficienza di telelettura e telegestione e di "granularità" delle misure di energia rilevata in telelettura. Per quanto attiene alla fatturazione, rendono possibile fornire le misure disponibili ai venditori entro 24h[187]; consegnare in tempo reale i dati al cliente; inoltrare spontaneamente messaggi; produrre fatturazione in modo continuo e con maggior livello di precisione.

Dal punto di vista dell'offerta, il venditore può configurare alcuni aspetti del misuratore (definire fasce di prezzo giornaliere multiorarie e modificare i parametri contrattuali) ampliando le opportunità commerciali: offerte con nuove fasce

[187] In particolare i dati quartiorari validati prossimi al momento di consumo, sono messi a disposizione del venditore con frequenza giornaliera.

orarie più aderenti alle esigenze di ciascun utente finale.

Dal punto di vista del consumatore, vi è un maggior coinvolgimento: risulta possibile effettuare lo *switching,* sulla base di dati effettivi e disporre dei dati istantaneamente per la fattura di chiusura, con notevoli riduzione dei tempi e controllabilità dei dati anche a fini di eventuali controversie sulle quantificazioni.

Per quanto riguarda la possibilità di lanciare offerte prepagate risultano facilitate le comunicazioni tra il venditore e il cliente (visualizzazione dei kWh residui).

Alcuni vantaggi sono direttamente legati all'*energy footprint* (cioè alla determinazione del profilo energetico del consumatore). Sulla base dell'analisi di dati di misura sono possibili nuove proposte di servizio personalizzate volte ad accrescere la consapevolezza e a modificare le condizioni di uso. L'interesse può riguardare sia i clienti finali, sia altri attori come terze parti o *service provider*.

Vi è, infine, un maggiore controllo sulla rete e sulle eventuali variazioni.

Al fine di comprendere in che modo i sistemi di *smart metering* stiano operando, le indicazioni fornite dalla norma citata, meritano dunque di essere lette nel contesto dell'azione regolatoria svolta dall'AEEGSI.

Le caratteristiche e le funzionalità degli *smart metering* rendono infatti necessaria la predisposizione di regole specifiche finalizzare a massimizzare i benefici per l'intero sistema elettrico, derivanti dalla loro implementazione. È per questo che tale passaggio è governato con gradualità da parte del regolatore [188].

Nell'ambito dell'obiettivo strategico OS7 sono stati redatti una serie di delibere e di documenti *ad hoc*[189]. Con la deliberazione 412/2014/R/efr, l'Autorità ha avviato il procedimento per l'attuazione delle disposizioni del decreto legislativo 102/2014, di competenza dell'Autorità, diversi da quelli in materia di regolazione del settore del teleriscaldamento e teleraffrescamento. Nell'ambito del procedimento avviato con la deliberazione 412/2014/R/efr, l'Autorità ha pubblicato, nell'agosto 2015, il documento per la consultazione 416/2015/R/eel, del 6 agosto 2015, "*Sistemi di smart metering di seconda generazione per la misura di energia elettrica in bassa tensione"* corredata dagli allegati A, B, C[190]*,* nel quale ha presentato i propri orientamenti in tema di requisiti funzionali minimi a cui i misuratori 2G e i sistemi di *smart metering* 2G dovranno essere conformi a livello nazionale, a prescindere dall'ambito di distribuzione. A questo hanno fatto seguito altri documenti significativi: la delibera 87/2016/R/eel dell'8 marzo 2016*, "Specifiche funzionali abilitanti i misuratori intelligenti in bassa tensione e performance dei relativi sistemi di* smart metering *di seconda generazione (2G)*

[188] V. Deliberazione 229/2017/R/eel, con cui l'Autorità ha introdotto gradualità nell'implementazione dei nuovi sistemi di misura 2G, individuando la configurazione di *default* dei misuratori 2G per la loro messa in servizio. Con la recente deliberazione 248/2017/R/EEL l'Autorità ha inoltre declinato gli obblighi di rilevazione e messa a disposizione dei dati di misura 2G prevedendo, tra l'altro, un periodo transitorio durante il quale la messa a disposizione dei dati di misura relativi ai punti di prelievo con nuovi misuratori 2G avvenga secondo una duplice modalità. Nel dettaglio, è stato stabilito che i dati di misura continuino ad essere messi a disposizione secondo le procedure tradizionali ed in parallelo seguendo le nuove modalità individuate per i dati di misura 2G, rimandando a successivo provvedimento la definizione della durata del suddetto periodo transitorio al termine del quale ai suddetti punti di prelievo potrà essere applicato il trattamento orario.

[189] Alcuni documenti riguardano specificamente la fatturazione dei consumi: 738/2016/R/com del 6 dicembre 2016, recante "*Fatturazione e regole di rateizzazione: modifiche alla disciplina definita dalla deliberazione dell'Autorità*"*;* 463/2016/R/com; 100/2016/R/com del 10 marzo 2016, "*Disposizioni relative alla emissione della fattura di chiusura per cessazione della fornitura di energia elettrica o gas naturale*"*;* 610/2015/R/com dell' 11 dicembre 2015, "*Bolletta 2.0: quantificazione dello sconto per le bollette in formato elettronico dirette ai clienti serviti in regimi di tutela. Modifiche ed integrazioni alle deliberazioni dell'Autorità 501/2014*/R/*com e 200/2015*/R/*com*"; 216/2016/R/com del 5 maggio 2016 "*Fatturazione di periodo nel mercato retail, nel quadro di evoluzione e superamento dei regimi di tutela di prezzo";* 201/2015/R/com del 30 aprile 2015 "*Bolletta 2.0: guida alla lettura e modello della bolletta dei clienti serviti in regime di tutela*"; 61/2015/R/com del 19 febbraio 2015 "*Bolletta 2.0: Glossario e livello di aggregazione degli importi fatturati*".

[190] Il documento per la consultazione illustra gli orientamenti dell'Autorità in merito alla definizione delle specifiche funzionali dei contatori intelligenti di seconda generazione di energia elettrica in bassa tensione (*smart meter* 2G), che l'Autorità deve predisporre in attuazione di quanto previsto dall'articolo 9, comma 3, del d.lgs. n. 102/2014.

nel settore elettrico, ai sensi del Decreto legislativo 4 luglio 2014, n. 102"[191]*;* la delibera 646/2016/R/eel del 10 novembre 2016, *"Sistemi di smart metering di seconda generazione (2G): riconoscimento dei costi per la misura dell'energia elettrica in bassa tensione e disposizioni in materia di messa in servizio. Modifiche* al *TIME"*[192]*;* la delibera 229/2017/R/eel del 6 aprile 2017 "*Disposizioni in merito alla prima configurazione dei misuratori 2G per la loro messa in servizio e relativi obblighi informativi a vantaggio dei clienti finali"*[193]*;* il documento di consultazione 466/2017/R/eel, *"Sistemi di misura 2G: orientamenti relativi alle disposizioni in materia di applicazione del trattamento orario, aggregazione e configurazione"*[194]. Inoltre, nella prospettiva di estendere l'applicazione anche al settore del gas, è stata avviata la Consultazione 230/2017/R/gas, del 6 aprile 2017 "*Gestione dei dati di misura nell'ambito del sistema informativo integrato per il settore gas. Orientamenti"*[195]*. A*ccanto all'attività settoriale, in ragione della complessità tecnica della materia e delle implicazioni interdisciplinari che la caratterizzano, l'AEEGSI ha avviato una collaborazione con l'AGCom[196].

Dal 2014 l'AGCom ha avviato un'indagine conoscitiva concernente i servizi di comunicazione *Machine to Machine* (M2M), con lo scopo di: esaminare i fattori che influenzano lo sviluppo dei servizi M2M (nonché l›interazione tra gli operatori del mercato che cooperano nella fornitura dei servizi); valutare criticamente le previsioni di sviluppo e le modalità di utilizzo; individuare le eventuali barriere normative/regolamentari per lo sviluppo di servizi M2M (con particolare riferimento ai profili di numerazione e *roaming);* individuare le eventuali aree dove è utile sviluppare un coordinamento tra le diverse Istituzioni nazionali ed europee coinvolte nel M2M. L'indagine conoscitiva ha individuato i principali ambiti di un possibile intervento regolamentare, che riguardano: l'investimento nelle infrastrutture e nello sviluppo dei servizi; la regolamentazione della connettività; il servizio finale; i mercati verticali del M2M.

La tipologia e l'urgenza dell'intervento regolamentare sul punto dipenderà dal livello di diffusione dei servizi M2M che, al momento, mostrano apprezzabili valori di impiego e significative tendenze di sviluppo in particolare nei settori dell'energia e dei servizi idrici.

L'AEEGSI ha contribuito all'indagine con la memoria 457/2014/I/COM individuando i principali ambiti di un possibile intervento regolamentare, che riguardano: l'investimento nelle infrastrutture e nello sviluppo dei servizi; la regolamentazione della connettività; il servizio finale; i mercati verticali del M2M. L'indagine conoscitiva si è conclusa con la delibera 201/15/CONS.

---

[191] Con il documento, l'Autorità definisce le specifiche funzionali abilitanti i misuratori intelligenti in bassa tensione e performance dei relativi sistemi di *smart metering* di seconda generazione (2G) nel settore elettrico, ai sensi del d.lgs. 4 luglio 2014, n. 102.

[192] Il provvedimento definisce, per il triennio 2017-2019, il riconoscimento dei costi per la misura dell'energia elettrica in bassa tensione e altre disposizioni in materia di messa in servizio dei sistemi di *smart metering* di seconda generazione, prevedendo piani dettagliati per la sostituzione dei contatori elettronici di prima generazione e sottoporre all'Autorità (successivamente modificato per un errore materiale dalla 696/2016/R/eel).

[193] Il provvedimento definisce la configurazione di *default* dei misuratori di energia elettrica in bassa tensione di seconda generazione (misuratori 2G) per la loro messa in servizio, prima della messa a disposizione, da parte dei distributori ai venditori, degli strumenti informatici necessari per le singole configurazioni. Vengono altresì indicati specifici obblighi informativi nei confronti dei clienti finali.

[194] Il presente documento per la consultazione illustra gli orientamenti in merito all'applicazione del trattamento ai sensi del TIS ai punti di prelievo per i quali verrà installato un nuovo misuratore nell'ambito dei sistemi di misura 2G nonché in tema di processo di configurazione di tali sistemi da parte delle parti commerciali.

[195] Il documento per la consultazione descrive gli orientamenti in merito all'invio sperimentale dei dati di misura di tutti i punti di riconsegna al Sistema Informativo Integrato. Vi ha fatto seguito la Delibera 434/2017/R/gas, del 15 giugno 2017, *Disposizioni in merito alla gestione dei dati di misura nell'ambito del Sistema Informativo Integrato, con riferimento al settore gas.*

[196] La predisposizione delle specifiche funzionali dello *smart metering* elettrico di seconda generazione costituisce un elemento di interesse comune e di presente e futura collaborazione tra le due Autorità, considerato che le scelte assunte avranno impatto sulla messa a disposizione dei dati di misura, con effetti anche su soggetti esterni al perimetro del sistema elettrico nazionale ma interessati ai servizi a valore aggiunto.

Con il Protocollo del 7 settembre 2015 le autorità hanno avviato una collaborazione specifica volta all'approfondimento delle questioni regolamentari riguardanti i servizi di comunicazione *Machine to Machine* nell'ambito delle applicazioni verticali per i settori dell'energia elettrica, del gas e del servizio idrico integrato, tra cui in particolare, i servizi di *Smart Metering* e, limitatamente al settore elettrico, di *Smart Distribution System* (art. 1).

Con delibera n. 459/15/CONS del 28 luglio 2015, l'AGCOM ha, inoltre, istituito un Comitato permanente sul M2M in cui sono coinvolti i principali attori, sia pubblici che privati, con la finalità di assicurare un maggior coordinamento dell'intervento pubblico. L'azione del comitato si avvale anche di accordi bilaterali con le altre Autorità di settore e con altri enti coinvolti nello sviluppo dei servizi M2M, a seconda delle esigenze dei vari settori che di volta in volta vengono in rilievo[197].

AGCom ha, peraltro, fornito il proprio fondamentale contributo alla già citata consultazione 416/2015/R/eel dell'Autorità.

2. LA GESTIONE DEI DATI PER LO SVILUPPO COMPETITIVO DEL MERCATO. DISINTERMEDIAZIONE E SOGGETTI COINVOLTI

Al fine di comprendere l'impatto sul mercato, occorre domandarsi quali sono i profili che la gestione dei dati pone in evidenza nel settore dell'energia.

Come già messo in luce, infatti, i dati sono uno strumento neutro, suscettibile di differenti utilizzazioni. Nei mercati liberalizzati dell'energia elettrica e del gas, ogni anno una moltitudine di soggetti (più di 250 distributori e oltre 500 venditori) si scambia circa 100 milioni di flussi di dati, riguardanti poco meno di 60 milioni di consumatori[198].

Sembrano, dunque, emergere tre profili fondamentali: la primarietà del ruolo di chi li gestisce; l'individuazione dell'uso che il soggetto che li gestisce e di chi li utilizza interne farne; la piena consapevolezza degli effetti che l'utilizzo dei dati può assumere nella dinamica della domanda e dell'offerta nel mercato energetico.

Per cercare di porre un ordine tra numerosi di standard e linguaggi comunicativi diversi, gestire i flussi informativi fra i soggetti che partecipano ai mercati dell'energia elettrica e del gas sulla base delle regole fissare dall'AEEGSI, la Legge 13 agosto 2010, n. 129 successivamente integrata con la Legge 24 marzo 2012, n. 27 ha istituito presso l'Acquirente Unico (AU) il Sistema Informativo Integrato (SII)[199] per la gestione dei flussi informativi relativi ai mercati dell'energia elettrica

[197] Le tecnologie di comunicazione a banda stretta dedicate ai servizi di comunicazione M2M sono assai promettenti, in termini sia di efficienza (per riduzione dei costi) che di efficacia (per maggiore capacità di propagazione in ambienti chiusi anche sotterranei), rispetto ai servizi di telecomunicazione radiomobile di attuale generazione; tuttavia, tali tecnologie sono tuttora in fase di standardizzazione e allo stato non possono essere ritenute sufficientemente mature né assicurare adeguata copertura del territorio senza sperimentazione in campo di adeguata scala per testare le diverse condizioni operative in caso di applicazione allo *smart metering* nei diversi settori di interesse dell'Autorità, inclusi i servizi idrici e il teleriscaldamento/teleraffrescamento; a tale proposito, con la deliberazione 646/2015/R/eel, l'Autorità ha definito la regolazione incentivante di tipo *output-based* dei servizi di trasmissione, distribuzione e misura per il periodo regolatorio 2016-2023. In particolare, l'art. 135 del TIDE prevede che l'Autorità possa dare luogo a sperimentazioni, in aree urbane densamente popolate, di sistemi intelligenti di distribuzione (*smart distribution system*) con funzionalità innovative sulla rete di bassa tensione che consentano la gestione avanzata dei misuratori, in integrazione con tecnologie di comunicazione avanzate e con la sperimentazione di soluzioni di telegestione multiservizio.

[198] Dati disponibili sulla pagina web http://www.acquirenteunico.it/attivita/sistema-informativo.

[199] Istituito presso l'acquirente unico con la l. 13 agosto 2010, n. 129. Tutte le informazioni sul portale ufficiale: https://siiportale.acquirenteunico.it/home

e del gas naturale. Il SII è basato su una banca dati a livello nazionale dei punti di prelievo e dei dati identificativi dei clienti finali il cui fine è garantire la fluidità nello scambio dei dati e la loro qualità. Ecco, dunque, la novità: la banca dati del SII, il Registro Centrale Ufficiale (di seguito: RCU) [200] raccoglie, oltre alle informazioni sui punti di prelievo ed ai dati identificativi dei clienti finali, anche i dati sulle relative misure dei consumi di energia elettrica e di gas.

Tale *database* risulta dunque "terziarizzato" e cioè esulante dai soggetti in potenziale conflitto con gli interessi del cliente finale e dunque con un *audit* corretto. Il sistema, infatti, è terzo sia rispetto a venditori, che a distributori e clienti finali laddove coinvolti nelle fasi di mercato (laddove si facciano produttori) e per tale via risulta ispirato ad un principio di neutralità, pubblicità e indipendenza.[201]

I benefici dell'implementazione del sistema sono molteplici. Oggi, il SII rende ad esempio possibile che il cambio fornitore venga eseguito in sole 3 settimane, come richiesto dalla normativa comunitaria, rispetto ai tempi lunghi occorrenti in precedenza. Al contempo, è garantita la sicurezza dei dati e il rispetto della *privacy*[202], secondo una logica di contenimento dei costi.

Per il ruolo centrale che riveste e per i dati che gestisce, il SII è uno strumento in grado di svolgere nuove funzioni anche relativamente ad esigenze e settori diversi. Il vero perno di sviluppo del SII è la sua duplice funzionalità: la disponibilità dei dati contribuisce a migliorare sia le politiche commerciali degli operatori sia la capacità decisionale dei consumatori, rendendo così il mercato più dinamico ed efficiente[203].

In attuazione delle disposizioni normative relative alle misure, l'Autorità si è focalizzata sul settore elettrico prevedendo, con la deliberazione 65/2012/R/eel, la standardizzazione dei flussi operativi relativi alle misure elettriche scambiati tra gli operatori (imprese distributrici e utenti del dispacciamento), strutturati in modo tale da essere successivamente inclusi nel perimetro dell'attività del SII.

Sempre con riferimento al settore elettrico, in una seconda fase, con le deliberazioni 640/2014/R/eel e 402/2015/R/eel l'Autorità ha disposto l'avvio di una sperimentazione concernente la gestione dei dati di misura nell'ambito del SII, prevedendo la contestuale messa a disposizione al Sistema dei dati di misura da parte delle imprese distributrici in relazione ai punti di prelievo rispettivamente con trattamento orario e con trattamento non orario. Relativamente ai punti di prelievo con trattamento orario, a seguito dei positivi riscontri della fase di sperimentazione, le modalità operative sono divenute standard con la deliberazione 358/2016/R/eel, che ha assegnato al SII anche l'attività di aggregazione delle misure dei prelievi ai fini del *settlement*, con riferimento ai punti di prelievo trattati orari.

Avviata verso la piena conclusione la fase sperimentale per il settore elettrico, l'Autorità ha ritenuto che potessero esserci le condizioni per aprire una fase sperimentale di invio parallelo al SII dei dati di misura anche per il settore gas[204].

---

[200] Con riferimento al settore elettrico, a decorrere dal mese di luglio 2013, il SII è diventato il canale ufficiale per la messa a disposizione agli utenti del dispacciamento di alcuni dati rilevanti ai fini del *settlement* (anagrafica ex-TIS, coefficienti di ripartizione dei prelievi o CRPU, dati di PRA e delta PRA). Attualmente sono in via di implementazione il processo di *pre-check* (ovvero l'attività di verifica della corrispondenza tra il codice POD di un punto di prelievo e i dati identificativi del cliente finale titolare di tale punto) e di voltura contrattuale.

[201] Secondo quanto stabilito dall'allegato A alla deliberazione ARG/com 201/10.

[202] Si vedano Il Codice in materia di dati personali (d.lgs. n. 196/2003) e il Disciplinare tecnico in materia di misure minime di sicurezza, per il trattamento dei dati con o senza l'ausilio di strumenti elettronici. Cfr. inoltre il Provvedimento del Garante Privacy del 27 novembre 2008 in materia di misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema dell'Allegato A alla delibera ARG/com 201/10, riguardante criteri generali, modello di funzionamento e modello organizzativo del SII. I dati personali dei clienti finali scambiati tra gli Utenti ed il Gestore sono necessari e sono utilizzati esclusivamente ai fini dell'esecuzione dei Processi del SII, in conformità alla regolazione dei Processi medesimi da parte dell'Autorità per l'energia elettrica e il gas e secondo le modalità previste nelle regole e nelle specifiche tecniche pubblicate dal Gestore.

[203] Cfr. i dati disponibili su acquirenteunico.it

[204] Vd. Documento per la Consultazione 230/2017/R/gas, "*Gestione dei dati di misura nell'ambito del sistema informativo integrato per il settore gas*".

Le curve di misura giornaliere validate vengono messe a disposizione dalle imprese distributrici al SII e dal SII agli utenti del dispacciamento quotidianamente ai sensi della delibera 248/2017/R/eel. Inoltre, i dati di misura vengono messi mensilmente a disposizione del SII. Tuttavia, la struttura dei dati oggetto di aggregazione (curve orarie giornaliere e non più mensili) determina la necessità di continui adeguamenti ai processi (*software*) e ai sistemi informativi (*hardware*) del SII, ai fini dell'aggregazione, anche in ragione del volume di dati previsto e della necessaria capacità di calcolo.

Gli strumenti informatici predisposti secondo il programma della delibera 87/2016/R/eel devono garantire la piena interoperabilità con il SII, al fine di sfruttare i benefici derivanti dalla centralizzazione dei processi.

Un'ulteriore riflessione deve essere effettuata in relazione all'opportunità di estendere il corredo informativo contenuto nel SII con i dati gestiti nell'ambito del *processo di configurazione* il quale prevede che ciascun venditore (vale a dire la parte commerciale associata al punto di prelievo del cliente finale) potrà gestire le proprie operazioni di configurazione con riferimento alle informazioni di propria esclusiva competenza e che costituirà l'interfaccia con le imprese distributrici. L'estensione a tali dati potrebbe consentire ai soggetti di consultare, anche massivamente, la correttezza dei dati caricati e/o aggiornati secondo le modalità già vigenti. Peraltro, la disponibilità nel SII di informazioni attinenti la configurazione, quali ad esempio le fasce di prezzo, potrebbe essere funzionale a migliorare e innovare diverse attività connesse al monitoraggio del mercato *retail*, anche con l'obiettivo di sviluppare l'abilitazione di nuovi servizi e/o strumenti atti a rafforzare la capacitazione del cliente finale.

La delibera 87/2016/R/eel chiarisce quali sono le informazioni da valorizzare. Il primo gruppo individuato comprende: a) le fasce di prezzo multiorarie definite nell'ambito del contratto di fornitura con il cliente finale; b) le informazioni contrattuali cosiddette minime (Codice cliente, Gruppo PESSE, Potenza contrattualmente impegnata); c) altre informazioni contrattuali, inerenti all'avvio del contratto o alla sua esecuzione (POD, nome del venditore; numero telefonico di contatto del venditore; data di inizio del contratto con il venditore; motivo di intervento sul limitatore; giorno del mese in cui ha inizio il periodo di *freezing*; messaggi al cliente). La potenzialità degli *smart metering* è, tuttavia, ancora in fase di studio e sarà soggetta a ulteriori evoluzioni sia circa le informazioni da mettere a disposizione, sia, soprattutto per quanto riguarda finalità ulteriori di cui l'azione regolatoria ancora non ha tenuto conto[205].

Un ultimo profilo riguarda la responsabilità di configurazione delle informazioni a venditori e imprese. Nel dettaglio, si ritiene che la configurazione sul misuratore 2G delle informazioni relative al Codice POD e al Gruppo PESSE debba essere gestita direttamente dall'impresa distributrice in quanto il primo è definito dall'impresa distributrice stessa e il secondo è programmato su input di Terna. Analoga considerazione, con le precisazioni di seguito riportate, vale per i dati relativi alla gestione del dato di potenza contrattualmente impegnata. Tutte le altre informazioni, meramente connesse al rapporto contrattuale con il cliente finale, verranno invece gestite dal venditore.

3. IL VALORE DEI DATI E DELLE INFORMAZIONI PER IL CONSUMATORE ENERGETICO NEL PARADIGMA DELLA *SOCIAL ECONOMY*

La ricostruzione sinora svolta ha illustrato gli strumenti attraverso cui l'azione regolatoria – con particolare riferimento all'elettricità – grazie alla massimizzazione della disponibilità dei dati relativi al mercato di riferimento, riesce a fungere da impulso verso l'innovazione per l'intero settore.

Come evidenziato, consumatori e imprese, tradizionalmente portatori di interessi a tratti opposti, hanno oggi a dispo-

[205] La deliberazione 289/2017/R/eel ha previsto che siano valutate funzionalità ulteriori, in quanto necessarie alla compiuta realizzazione di tutto il potenziale di benefici estraibile dalla nuova generazione di *smart meter*. Tra queste vi rientrano quelle relative alla gestione di parametri abilitanti formule contrattuali prepagate.

sizione un terreno comune e neutrale rappresentato dalla disponibilità di dati e di informazioni, che coincide con il *leitmotiv* della rivoluzione *digitale*[206]– o, come definita nel nostro lavoro, *social* –.

Sebbene per una piena cognizione dei vantaggi occorrerà attendere che le iniziative intraprese dalle Autorità vadano a regime, alcuni segnali positivi sono già evidenti.

Più immediato è individuare luci e ombre dal lato dell'impresa. Questa, infatti, è per sua natura in possesso delle specializzazioni tecniche e professionali per comprendere e valorizzare (nonché monetizzare) lo strumento dello *smart metering*[207] e della gestione dei dati. Il mercato basato sulle tecnologie digitali, infatti, nasce con carattere fortemente concorrenziale e della concorrenza per l'innovazione si nutre.

Alcune questioni specifiche restano tuttavia aperte e saranno oggetto degli interventi regolatori di un futuro ormai prossimo. Innanzitutto, resta pendente la questione relativa all'intercambiabilità tra imprese distributrici dei sistemi di *smart metering* 2G, in vista del riassetto dell'attività di distribuzione che dovrebbe intervenire entro il 2030, per effetto delle disposizioni di cui all'articolo 9, comma 2, del decreto legislativo 79/1999 (che impone uno standard unificato a livello nazionale).

Vi sono poi i molteplici profili legati alla tutela della *privacy* e agli strumenti in capo al Garante[208], a cui si lega il tema della tutela delle situazioni soggettive dei consumatori che fornendo i propri dati alle imprese integrate del mercato libero dell'energia, diventano vulnerabili ad attività di *marketing* – potenzialmente suscettibili di tradursi in comportamento anticoncorrenziale –[209].

Un altro tema in via di implementazione è, inoltre, la diffusione di sistemi di domotica, i quali ampliano la possibilità per i clienti in prelievo di offrire risorse di bilanciamento, contribuendo alla diminuzione dei costi e ampliando il ruolo del consumatore attraverso una migliore qualità del servizio. I nuovi contatori si integrano nel mondo IoT (*Internet of Things*) e nei prossimi anni permetteranno interazioni con altri dispositivi grazie a flussi bidirezionali di energia. Pertanto il protocollo tra AGCom e AEEGSI, già siglato, è solo il primo passo di una collaborazione che senz'altro continuerà sui temi degli impatti intersettoriali delle applicazioni IoT e 5G.

In generale risulterà prezioso su scala europea uno scambio plurilaterale delle *best practices*, in cui il sistema italiano, di cui l'AEEGSI è protagonista assoluta, può fornire un valido esempio nei confronti di altri ordinamenti[210].

Se per le imprese il valore dei dati è chiaro, percorso non del tutto speculare è tuttavia quello del consumatore, non sempre (o non ancora) sufficientemente consapevole delle possibilità di mercato e dei vantaggi in termini sia di risparmio che di efficienza derivanti dall'applicazione dei processi digitali al mercato energetico.

A chiusura del cerchio, riemerge, dunque, il tema di fondo del Nostro Rapporto: il ruolo del consumatore. In particolare, riprendendo un concetto già noto, la chiave di volta della messa a regime della rivoluzione *social* all'interno del

---

[206] Il passaggio al digitale è declinabile su larga scala ed estensibile alla quasi totalità dei settori dal punto di vista giuridico. Importanti indicazioni, soprattutto con attinenza ai temi oggetto di questa indagine, sono forniti dai documenti elaborati in sede europea. Si veda sul punto la Comunicazione della Commissione del 6 maggio 2015, *Strategia per il mercato unico digitale in Europa*, COM (2015) 192 final.

[207] Si ricorda che in una prima fase l'introduzione degli *smart metering* 1G è avvenuta ad opera di alcune imprese in via sperimentale.

[208] Per un'analisi dei quali, in generale, si rinvia al relativo contributo in Questo Rapporto.

[209] Sul punto v. le istruttorie AGCM A511, A512, A513 volte a verificare le condotte anticoncorrenziali nel mercato della vendita di energia elettrica, in violazione dell'art. 102 TFUE. In particolare con riguardo a quelle strategie finalizzate nella prospettiva del definitivo superamento del servizio di maggior tutela, a spostare al libero mercato la base clienti servita da alcune aziende in maggior tutela, tramite lo sfruttamento commerciale delle informazioni relative all'anagrafica e ai dati di fatturazione dei clienti serviti in maggior tutela tali da costituire vantaggi competitivi non replicabili da altri soggetti sul mercato.

[210] Cfr. Comunicazione della Commissione europea, cit.

mercato energetico è rappresentata dall'*empowerment* del consumatore[211].

Sembra, infine, potersi affermare che l'implementazione degli *smart metering,* in futuro, inciderà su tre fronti fondamentali: accrescere la consapevolezza dei consumi in tempo reale, nelle case o su applicazione *smartphone*; aumentare il livello di sicurezza (ad esempio fornendo allarme per interruzione del servizio o per superamento dei limiti di potenza); pianificare i consumi e coordinare dispositivi al fine di limitare e razionalizzare i costi di utilizzo.

In generale, tuttavia, permangono criticità di fondo cui l'azione regolatoria dovrà ancora dedicarsi. L'analisi della struttura dell'offerta e delle dinamiche concorrenziali nell'ambito dei mercati *retail* evidenzia condizioni concorrenziali ancora disomogenee tra tipologie di clienti, con deficit maggiori nel segmento dei clienti domestici. Inoltre, pur a fronte di segnali di miglioramento di alcuni indicatori, quali ad esempio le tempistiche di messa a disposizione dei dati di misura al momento dello *switching* o il numero delle doppie fatturazioni, persistono ancora elementi di preoccupazione circa il funzionamento del mercato[212].

In questo scenario, la regolazione dei mercati *retail* non potrà fare a meno di valorizzare l'evoluzione in atto legata ai profondi cambiamenti trainati dallo sviluppo tecnologico promosso dalle politiche di decarbonizzazione del sistema energetico europeo e nazionale (contatori e reti intelligenti, elettrotecnologie, domotica).

Un ulteriore elemento da tenere presente è l'emersione della nuova figura del consumatore-piccolo produttore di energia elettrica, in grado di immettere in rete quanto prodotto in eccesso rispetto alle proprie esigenze di consumo (*prosumer*). La capacitazione del consumatore assume quindi una dimensione ulteriore, legata alla necessità di migliorare la sua conoscenza, capacità di controllo, razionalizzazione ed efficientamento dei propri consumi e, con essi, della propria spesa energetica.

L'evoluzione tecnologica favorisce al contempo lo sviluppo dell'offerta di nuovi servizi per il risparmio, l'efficienza energetica e la gestione attiva dei consumi (*demand response*). Nel mercato così delineato non si affacceranno solo soggetti terzi, come le *energy service companies*, gli aggregatori di domanda e operatori del settore IT, ma anche i tradizionali venditori di energia al dettaglio che intenderanno diversificarsi con offerte congiunte di energia e servizi energetici per i propri clienti per conquistare nuove quote del mercato.

Il tema della disintermediazione è un nodo centrale del mercato energetico, ormai letto perlopiù come un profilo da potenziare al fine di abbattere alcuni costi finali gravanti sui consumatori. In tal senso, nuove possibilità si potrebbero prefigurare utilizzando la tecnologia *BlockChain*[213] (la quale in ragione delle ricadute di sistema che potrebbe generare, dovrà essere opportunamente ponderata, essendo, ad esempio ipoteticamente in grado di eliminare l'intermediazione di alcuni soggetti, non da ultimo l'Acquirente Unico e il SII, così come i soggetti che si occupano di distribuzione e misura).

Ritornando, infine, al binomio cui si faceva riferimento in apertura, assumendo il punto di vista economico, si deve aver riguardo alla commerciabilità dell'energia come bene di consumo[214]. Su questo fronte si apre la questione dei costi dell'energia come elemento da tenere in considerazione in ragione dell'impatto sulle famiglie – dove la crescente aggressione dei redditi determinata dalle voci dei consumi, conduce talora a situazioni di c.d. povertà energetica[215] – e

---

[211] In dottrina v. N. Rangone, *Empowerment cognitivo a supporto dell'efficienza energetica*, in Annuario di diritto dell'energia 2016, Bologna, 2016, 331 ss.

[212] Si fa riferimento, ad esempio, all'elevata e crescente percentuale dei cambi di fornitore iniziati ma non completati, relativi al settore del gas naturale: in media nazionale nel 2013 quasi il 12% dei cambiamenti di fornitore avviati non è andato a buon fine.

[213] Derivante dalla criptografia. È la stessa alla base della moneta elettronica.

[214] Molteplici pronunce della giurisprudenza comunitaria definiscono l'energia come "merce". In dottrina cfr. A. Colavecchio, *La liberalizzazione del settore elettrico nel quadro del diritto comunitario*, Bari, 2000, 111 ss.

[215] Il fenomeno della povertà energetica, già approfondito dagli studi nel Regno Unito in ragione dell'aumento della casistica, sta attirando attenzione crescente anche in altri paesi. Sul punto è significativa l'istituzione di un osservatorio sulla povertà

sulle imprese, dove potrebbe spingere a ricercare condizioni di prezzo più favorevoli anche in scenari nazionali diversi, con evidenti ricadute di sistema.

Anche a questo genere di problematiche supplisce oggi l'introduzione di strumenti tecnologici, con effetti ancora tutti da studiare.

L'incontro di tali interessi è, infine, foriero di un'ulteriore ricaduta: la creazione di un mercato nuovo, che si affianca a quello tradizionale della fornitura di energia e la cui caratteristica fondamentale si sostanzia in una serie di soluzioni per i clienti finali destinati a rimodulare la domanda di energia.

Due sono le sue leve: in primo luogo il *risparmio energetico*, laddove a tecnologie invariate, si promuova un uso del prodotto più razionale; in secondo luogo l'*efficienza energetica,* laddove si investa in tecnologie differenti e innovative che permettano ai clienti finali un contenimento dei consumi a parità di domanda[216].

Un mercato energetico "su misura" del consumatore, in grado di offrire servizi personalizzabili ad una platea di consumatori sempre più variegata, specchio di quella "società liquida"[217] portatrice di bisogni estremamente mutevoli.

Ecco, dunque, che sorgono esigenze regolatorie nuove, che l'Autorità si trova a dover mettere in campo sui due fronti necessari: dal lato dei consumatori, agevolando gli strumenti di capacitazione afferenti all'efficienza energetica; dal lato delle imprese, garantendo quell'accresciuto bisogno di vigilanza e monitoraggio nel delicato percorso di ampliamento dell'offerta in segmenti di mercato contigui e variegati.

energetica, http://fuelpoverty.eu/2017/04/12/announcing-the-new-european-energy-poverty-observatory/.

[216] La creazione del mercato descritto, viene definita "cata-energia, ovvero quella contro-energia, sorgente in situ presso il cliente finale, che consente di evitare corrispondenti acquisti o produzioni di energia nel mercato delle forniture come siamo abituati a conoscerlo dalla liberalizzazione in poi", così il presidente dell'AEEGSI G. Bortoni, *Il ruolo della regolazione nel mercato dell'efficienza energetica*, in Annuario di diritto dell'energia 2016, Bologna, 2016, 363.

[217] L'espressione, come noto, è da ricondurre agli studi sociologici di Z. Bauman.

I Big Data nel settore delle risorse idriche

(Maria Chiara Sole)

SOMMARIO: 1. I BIG DATA: UNA RAPIDA EVOLUZIONE. – 2. BIG DATA E SETTORE PUBBLICO: LA DISINTERMEDIAZIONE NELLA GESTIONE DEI BIG DATA DEI SERVIZI IDRICI. – 3. LA TUTELA DELL'UTENTE FINALE NEL SETTORE IDRICO DA PARTE DELL'AUTORITÀ. – 4. CRITICITÀ E MARGINI DI MIGLIORAMENTO.

1. I BIG DATA: UNA RAPIDA EVOLUZIONE

Stando alle più recenti definizioni, con il termine Big Data si fa riferimento, *in primis*, ai dati che superano i limiti dei *database* tradizionali (ossia maggiori ai 10 terabyte). Tuttavia, rientrano in questa definizione anche gli strumenti tecnologici finalizzati alla gestione di tale quantità di dati, che ne rendono possibile non solo la raccolta, ma anche l'elaborazione e l'analisi. Nel corso degli ultimi due anni il flusso di informazioni ha superato l'ordine dei Zettabyte (ossia 10^{21} byte) e secondo recenti stime, i dati digitali stanno crescendo esponenzialmente ogni anno[218]: si prevede che entro il 2020 ci saranno più di 16 Zettabyte di dati utili (16 Trilioni di Gigabyte). Le aziende, infatti, oramai catturano incessantemente trilioni di byte di informazioni sui propri clienti, fornitori e sul loro comportamento, attraverso numerosi dispositivi tra i quali vi sono, tra gli altri, i telefoni cellulari, i contatori e i sensori.

I Big Data rientrano quindi a pieno titolo in quella che può considerarsi la nuova rivoluzione industriale, che ha al centro le nuove tecnologie digitali. Secondo un recente rapporto di McKinsey[219] (2016), tale rivoluzione seguirà quattro linee di sviluppo: la raccolta di dati (in questo ambito rientrano i Big Data, gli open data, l'*Internet of Things* ecc.); i processi di analisi di grandi volumi di dati per estrarre informazioni; l'interazione uomo-macchina mediante le realtà virtuali o aumentate ed, infine, la conversione nel mondo fisico di idee virtuali (attraverso la manifattura additiva, la robotica avanzata e lo stoccaggio di energia).

Secondo lo studio dell' International Institute for Analytics[220], utilizzando la definizione odierna di Big Data, il 71% delle aziende intervistate ha Big Data da gestire ma solo una piccola percentuale di esse è riuscita ad analizzarli. Gli strumenti di gestione dei dati convenzionali non sono infatti ancora sufficientemente sviluppati e, in molti casi, finiscono per fallire quando è necessario estrarre, integrare ed analizzare i grandi set di dati[221]. Qualora incrociati e collegati tra loro, invece, potrebbero potenzialmente portare a dei risultati incredibili ed essere di supporto in tutti i settori della nostra economia. Ad oggi, quando si parla di Big Data è facile pensare alle campagne *marketing* ritagliate *ad hoc* sui consumatori che vengono letteralmente bombardati ogni giorno dalle offerte più disparate, sia attraverso una profilazione degli utenti generica (sesso, età, status sociale…) sia attraverso una invece più specifica, definita in base alle "tracce" lasciate dai consumatori stessi (sui *social*, con le ricerche Google e con la propria geolocalizzazione). È chiaro, quindi, che oggigiorno i dati sono un bene che può creare un notevole vantaggio competitivo e stimolare l'innovazione, aumentare la competitività e generare impatti sociali. Tuttavia, le aziende che intendono affidarsi alle soluzioni basate

[218] Forrester, *Big Data, Big promises, Big growth*, 2016.

[219] McKinsey, *Industry 4.0 Global Expert Survey*, 2015.

[220] International Institute for Analytics, *Advanced Analytics & Big Data Adoption Report*, 2016.

[221] A titolo esemplificativo, un importante centro commerciale statunitense gestisce più di 1 milione di transazioni clienti ogni ora, che viene importato in un *database* che si stima contenga una quantità di dati che equivale a 167 volte le informazioni contenute in tutti i libri della Biblioteca del Congresso USA.

su dati affrontano sfide che vanno ben oltre la tecnologia, perché decidere di utilizzare i Big Data richiede cambiamenti nell'orientamento, nella strategia e nei processi aziendali. Accanto alle potenzialità dei Big Data in ambito privato, che sono di facile intuizione, non si possono tralasciare quelle che investono il settore pubblico. In questo ambito, infatti, i Big Data possono essere strumenti molto utili per le decisioni di *policy*. Tale argomento, con un particolare focus sulla risorsa idrica, è oggetto del seguente paragrafo.

2. BIG DATA E SETTORE PUBBLICO: LA DISINTERMEDIAZIONE NELLA GESTIONE DEI BIG DATA DEI SERVIZI IDRICI

Le *app* di comunicazione sociaI Big Data possono oramai considerarsi un bene primario per tutti i settori, organizzazioni, paesi e regioni. Le attività economiche e sociali sono da sempre influenzate dai dati. Ma oggi l'aumento del loro volume, velocità e varietà segna un passaggio paradigmatico verso un modello socioeconomico basato su di essi.

In quest'ottica nel settore pubblico i Big Data rappresentano un grande supporto, così come evidenziato dalla Commissione Europea, che si è augurata che si possa presto realizzare "una società elettronica inclusiva, nella quale i cittadini e le imprese abbiano le competenze necessarie e possano usufruire di servizi elettronici interconnessi e plurilingue che spazino dalla pubblica amministrazione alla giustizia, dalla sanità all'energia e ai trasporti"[222].

Basti pensare all'uso che se ne può fare per gestire aspetti legati alla sicurezza stradale, alla salvaguardia dell'ambiente e alla salute dei cittadini[223]. Proprio in riferimento alla salvaguardia dell'ambiente, data la centralità che il tema ha assunto negli ultimi anni, in più occasioni è stato sottolineato come l'accesso tempestivo a dati ambientali può essere di grande aiuto nella definizione delle politiche ambientali sostenibili locali e regionali.

Tuttavia, va da sé che la gestione di questi dati non è esente da problematiche, le quali riguardano in particolar modo la sicurezza degli stessi. Abbiamo visto che nel settore privato "i Big Data rappresentano un notevole patrimonio informativo e l'utilizzo di queste informazioni comporta specifici rischi per la tutela della riservatezza delle persone, tenuto conto anche del fatto che, grazie alle nuove tecnologie e alle tecniche di analisi, elaborazione ed interconnessione dei dati, in molti casi risulta possibile "re-identificare" un individuo attraverso informazioni apparentemente anonime. La potenzialità dei Big Data, anche rispetto a dati anonimi o aggregati, può tradursi in profilazioni sempre più puntuali ed analitiche, con il rischio di nuove forme di discriminazione per le persone e, più in generale, in possibili restrizioni delle libertà".[224] In ambito pubblico questo discorso è, però, solo marginalmente valido; tuttavia, il problema della sicurezza, anche se si manifesta in maniera diversa, comunque rimane: basti pensare a come la discriminazione nella scelta dei dati può portare a diverse decisioni di *policy* che hanno ricadute sull'intera collettività.

In questo contesto, anche la risorsa idrica può essere oggetto di analisi nell'ottica della raccolta dei Big Data. Occorre, in primo luogo, sottolineare che l'acqua è stata a lungo considerata libera, accessibile a chiunque ne avesse bisogno; analogamente, l'immissione in natura delle acque di scarico è stata tradizionalmente ritenuta un'ovvia necessità e, quindi, un diritto del consumatore. La crescita dei consumi, a determinare la quale ha contribuito probabilmente la

[222] Cfr. la Comunicazione della Commissione del 6 maggio 205, Strategia per il mercato unico digitale in Europa, COM (2015) 192 Final.

[223] Al riguardo è interessante riportare l'esempio di un progetto portato avanti da Google nel 2008 (*The Flu Trends*) che, analizzando i gruppi dei termini di ricerca digitati dagli utenti sul proprio motore, era riuscito a prevedere l'avanzamento dei focolai di influenza nei territori degli USA più velocemente di come lo stesso ministero della salute non fosse riuscito a fare utilizzando i record di ammissione ospedaliera delle strutture sanitare pubbliche e private.

224 AGCom, Comunicato stampa IC53 - Avviata indagine conoscitiva sui Big Data, 1 giugno 2017.

gratuità della risorsa, ha tuttavia messo in evidenza il problema della scarsità. Oggi anche la risorsa idrica necessita di una sistema di gestione integrato – relativamente alle attività di produzione e distribuzione dell'acqua potabile, le fognature e la depurazione delle acque reflue – per la definizione di un nuovo assetto gestionale che sia socialmente, economicamente ed ambientalmente sostenibile.

L'utilizzo congiunto delle tecnologie digitali può, quindi, portare ad una gestione più sostenibile della risorsa idrica. Tuttavia, va sottolineato che l'innovazione della gestione delle risorse e dei servizi idrici non passa solo attraverso il progresso tecnologico, ma deriva anche dall'innovazione dei mercati di riferimento e delle regole. Diventa, quindi, fondamentale la forte collaborazione tra competenze diverse, tra fornitori di tecnologie, ricerca, utilizzatori finali e soggetti politici. La sfida richiede una soluzione collaborativa tra settore pubblico e privato, con un nuovo approccio e soluzioni organizzative, economiche, tecnologiche per la condivisione dei dati a cui devono partecipare tutte le fonti: fornitori di dati di risorsa energetica e idrica, tra cui i principali produttori, i consumatori, gli operatori di sistemi di trasmissione (TSO) e gli operatori di sistemi di distribuzione (DSO), autorità locali, agenzie nazionali. Al riguardo è interessante citare il Protocollo generale di intesa tra l'Autorità per le garanzie nelle comunicazioni (AGCom) e l'Autorità per l'energia elettrica, il gas e il sistema idrico (d'ora in poi AEEGSI o Autorità). L'accordo, da quanto si evince da una nota AGCom, "rientra nelle iniziative di collaborazione tra autorità indipendenti ed è finalizzato a promuovere sinergie e complementarità in materia gestionale e tecnico-scientifica". Una cornice che, riconosciuta la sempre maggiore importanza dell'ICT e delle applicazioni digitali per il settore energetico, promuoverà "iniziative congiunte di natura specifica, come ad esempio il protocollo di gestione in comune di alcuni servizi e lo scambio di personale, il progetto M2M *Machine to Machine, già avviato, il ruolo delle utilities* energetiche e idriche nei progetti di sviluppo delle infrastrutture di comunicazioni elettroniche, le analisi e il confronto dei diversi modelli di regolamentazione dei servizi".

3. LA TUTELA DELL'UTENTE FINALE NEL SETTORE IDRICO DA PARTE DELL'AUTORITÀ

L'utente finale è, quindi, al centro di questo nuovo sistema e vi partecipa sia attivamente, rendendo disponibili dati collegati al suo comportamento, sia passivamente, in quanto destinatario di scelte aziendali e politiche stabilite sulla base dell'analisi che di tali dati viene fatta.

In questa prospettiva, il rilievo giuridico che assumono i Big Data si manifesta in una duplice forma: dal punto di vista del privato, la disciplina a tutela della concorrenza e del consumatore si configura nel trattamento dei dati personali nel rispetto della normativa della *privacy*, dal punto di vista pubblico, non si possono sottovalutare gli effetti indesiderati che potrebbe generare l'utilizzo di algoritmi e tecnologie che elaborano i Big Data per prendere delle decisioni, dando luogo a discriminazioni, seppur l'intento sia diametralmente opposto. Ecco perché in questo secondo caso l'utente deve essere tutelato attraverso una corretta regolamentazione che stabilisca delle regole precise lasciando però anche spazio all'innovazione. Servono, quindi, regole, e il delicato ruolo di chi le dovrà scrivere è stato sintetizzato da Roberto Malaman, direttore Advocacy e Utenti dell'AEEGSI: "il regolatore deve riuscire a guardare avanti senza frenare il cambiamento".

Secondo un recente studio dell'OCSE, i Big Data possono migliorare enormemente i processi decisionali e, in particolare, la decisione pubblica. Infatti, in un contesto sempre più globalizzato e digitalizzato, i dati sono motore di crescita e di benessere e, in particolare, diventano uno dei migliori strumenti di governo a disposizione dell'autorità pubblica. Non a caso negli ultimi anni si è diffuso il concetto di *data driven innovation,* con il quale ci si riferisce esattamente alla dinamica che mette i dati al centro delle decisioni, anche di carattere pubblico. In altre parole, i governi e le amministrazioni elaborano i Big Data con i nuovi strumenti di analisi al fine di creare un fondamento conoscitivo completo su cui

basare le proprie decisioni. Decisioni pubbliche che, se prese con una base conoscitiva esaustiva e non discriminatoria – evitando, quindi, il rischio di automatizzare i processi decisionali – potrebbero favorire sostanzialmente la crescita economica e migliorare il benessere dei cittadini.

In questa nuova realtà, ognuno deve fare la propria parte e diventa fondamentale saper coniugare esigenze di apertura del patrimonio informativo e la necessità di garantire un'adeguata tutela al cittadino. A tal fine, occorre prestare attenzione ad ogni *step* della fase decisionale, a partire dagli interventi legislativi e regolatori a quelli amministrativi. Bisogna, inoltre, trattare separatamente i concetti di dati, informazioni e conoscenze e conseguentemente anche il momento della raccolta dei dati da quello dell'estrazione di informazioni dagli stessi e, ancora, quest'ultimo da quello della formazione della conoscenza che porta alla decisione. La regolamentazione dei Big Data è, pertanto, cruciale perché il fenomeno produce effetti sulla società, sulla politica, sull'economia, e saranno effetti positivi o negativi anche in ragione delle scelte regolatorie che si compiono.

Il tema della regolazione dei Big Data non è stato ancora indagato pienamente dalla dottrina, ma resta determinante anche per rendere lo strumento tecnologico più democratico possibile. Per comprendere come disciplinarlo, è necessario partire dall'oggetto della regolazione e differenziarla rispetto all'uso che se ne fa o rispetto a chi utilizza i Big Data.

In questo contesto si inserisce pertanto il ruolo dell'Autorità, che recentemente è stata fortemente incentivata alla tutela dell'utenza nel settore idrico, a partire dalla definizione di standard vincolanti in tema di qualità contrattuale del Sistema Informativo Integrato (SII). I provvedimenti finalizzati alla garanzia di qualità del SII hanno riguardato standard generali e specifici, vincolanti ed omogenei sul territorio nazionale per le diverse fasi del rapporto contrattuale, nonché le modalità di registrazione, di comunicazione e di verifica dei dati relativi alle prestazioni fornite dai gestori su richiesta degli utenti.

Ancora, nell'ambito delle funzioni di regolazione e controllo attribuite all'Autorità, con la determina 16 febbraio 2016, 1/2016 – DSID, recante *Definizione delle procedure di raccolta dati ai fini dell'Indagine conoscitiva sull'efficienza del servizio idrico integrato e della relativa regolazione*, è stata avviata la seconda edizione della raccolta dati sull'efficienza e sulla qualità del SII. Come si legge dall'ultima Relazione annuale dell'AEEGSI, in questa seconda edizione di raccolta dati, l'Autorità ha condotto diversi approfondimenti con rappresentanti dell'UE, dell'Istat, di Unioncamere e delle associazioni di categoria "con l'obiettivo di individuare in modo condiviso a livello euro-unitario e nazionale le grandezze da acquisire per la costruzione di indicatori e variabili rappresentativi dei fenomeni inerenti al SII, al fine di semplificare e ottimizzare i flussi e gli adempimenti informativi da parte dei gestori e degli enti di governo dell'ambito".

Il patrimonio informativo del SII nei prossimi anni aumenterà nella numerosità e nella granularità dei dati trattati: si passerà da circa 500 milioni a oltre 7.000 miliardi di dati di misura all'anno. Tale patrimonio dà la possibilità anche ad un soggetto pubblico di fare innovazione[225].

4. CRITICITÀ E MARGINI DI MIGLIORAMENTO

Alla luce di quanto esposto, si evince che i Big Data sono capaci di modificare profondamente i processi decisionali, pubblici e privati, in quanto capaci di fornire conoscenze approfondite e punti di vista originali sui fenomeni scientifici, sociali, economici e culturali in atto; sono capaci di incentivare la produttività delle imprese e di interi settori economici creando nuove competenze, nuovi spazi di mercato e un nuovo modo di prendere le decisioni pubbliche.

[225] Rapporto I-COM, *Reti e servizi di nuova generazione*, 2016.

Ma la centralità del dato potrebbe anche mettere al centro la persona, in maniera del tutto inedita. Se infatti l'individuo è una delle maggiori fonti di produzione di Big Data, in futuro potrebbe cambiare il rapporto tra la persona e i propri dati: il singolo potrebbe avere un ruolo centrale nella loro gestione mai avuto precedentemente; potrebbe utilizzare i dati, da solo o in forme collettive, in modo tale da valorizzare le sue prerogative.

Il fenomeno dei Big Data, però, non ha solo delle intrinseche potenzialità, ma anche dei limiti che, se non affrontati nel modo giusto, potrebbero dare luogo a effetti negativi per la collettività.

Tra questi vi è la pervasività dello strumento, che produce, innanzitutto, effetti negativi sulla *privacy* degli individui. Come già evidenziato, infatti, l'utilizzo dei Big Data per le strategie di *marketing* aziendale o per la sorveglianza, sollevano numerosi rischi per la *privacy* legati alla questione del *profiling* e ne potenziano enormemente gli effetti.

Il secondo grande limite dei Big Data coinvolge direttamente coloro che li utilizzano: alcuni studiosi, infatti, hanno parlato del rischio di una vera e propria "dittatura dei dati". Possederne una quantità enorme e avere tutte le capacità tecniche e culturali per raccoglierne ancora in merito a tutti i fenomeni esistenti, umani e naturali, potrebbe favorire un sistema in cui paradossalmente i dati non sono più uno strumento a supporto della decisione, ma diventano essi stessi "fautori" delle decisioni, rischiando di appiattire le decisioni su logiche troppo quantitative e di renderle, anziché più complete e adeguate ai problemi e alle situazioni che è necessario affrontare, fortemente parziali, incomplete e discriminatorie. Non bisogna, quindi, dimenticarsi che al centro delle decisioni devono rimanere le persone e i loro comportamenti. Per quanto le dinamiche sociali siano oggetto di "datizzazione", infatti, non saranno mai pienamente interpretabili dai dati.

Se, quindi, è necessario stare al passo con i tempi e sfruttare al meglio le nuove potenzialità emerse dai Big Data e dalle nuove tecnologie che li rendono fruibili ed utilizzabili, non bisogna comunque abbassare il grado di attenzione sulle conseguenze che tale strumento potrebbe avere se non sufficientemente sorvegliato. Al regolatore è, quindi, lasciato il compito di trovare il giusto equilibrio tra innovazione e tutela degli utenti e, in definitiva, della collettività.

AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI

(Valentina Angelini, Francesca Pellicanò, Rosaria Petti)

L'ecosistema digitale tra *fake news*, *hate speech* e *cyberbullismo*: l'intervento dell'Autorità per le garanzie nelle comunicazioni

In un'economia sempre più data driven*, i dati divengono una risorsa strategica per le attività delle piattaforme digitali e lo sviluppo dei servizi. Il valore economico di questi determina, tuttavia, problematiche di ordine competitivo nell'accesso diretto alle informazioni e di tutele individuali e collettive. Ci si riferisce alla crescente rilevanza di usi distorti della rete, che comportano nuove fattispecie giuridicamente rilevanti e impongono necessità di strumenti di tutela adeguati:* cyberbullismo*, incitazione al terrorismo,* hate speech *e* fake news.

Le implicazioni di un tale ecosistema hanno un impatto non marginale sul pluralismo e sulla libertà di informazione, le cui conseguenze rilevanti incidono significativamente sul diritto degli utenti a ricevere un'informazione obiettiva, completa, corretta e imparziale.

Soggetto istituzionalmente preposto dalla sua legge istitutiva alla garanzia dell'affidabilità e imparzialità dell'informazione, alla tutela del pluralismo informativo, è l'Autorità per le garanzie nelle comunicazioni, chiamata a indagare, con sempre maggior attenzione, il fenomeno della disinformazione online*. In termini pratici, però, la risoluzione del problema appare ancora lontana. Del resto, la transnazionalità del fenomeno richiede un approccio sovranazionale in grado di superare, per quanto possibile, l'attuale frammentazione dei regimi giuridici applicabili alle diverse tipologie di piattaforme che distribuiscono contenuti editoriali e audiovisivi.*

I temi di interesse. Le questioni all'attenzione del regolatore

SOMMARIO: 1. I BIG DATA E I NUOVI BISOGNI DI PROTEZIONE DEL CITTADINO DIGITALE: STATO DELL'ARTE E QUESTIONI APERTE. – 2. I FENOMENI DEVIANTI DEL *WEB*: LA RESPONSABILITÀ DELLE PIATTAFORME E I POTERI DI INTERVENTO DEL REGOLATORE. – 3. L'INFORMAZIONE *ONLINE* E IL VALORE DEI DATI. – 4. I PRINCIPI FONDAMENTALI APPLICATI ALL'INFORMAZIONE *ONLINE* E L'INQUADRAMENTO DEL FENOMENO *FAKE NEWS*.

1. I BIG DATA E I NUOVI BISOGNI DI PROTEZIONE DEL CITTADINO DIGITALE: STATO DELL'ARTE E QUESTIONI APERTE

(Valentina Angelini)

Oggigiorno l'innovazione corre alla velocità della luce, generando nuove economie. I nuovi mercati digitali, figli di moderni ed inediti modelli di consumo, seguono questo divenire e, come evidenziato nel Rapporto dello scorso anno[226], si consolidano con il passare del tempo (e, aggiungerei, mutano), affiancandosi, di fatto, ai mercati tradizionalmente intesi.

[226] In particolare, si veda F. Bassan, M. Rabitti, *Introduzione. Dalla sharing, alla social verso la shadoweconomy*, in *Consumerism 2016 Nono Rapporto annuale*, Consumers' Forum e Università degli Studi di Roma Tre, 2016, 8-11.

Dall'economia della condivisione, passando per la *social economy*, siamo giunti all'era della *data economy*.

I dati sono l'anello di congiunzione fra questi sistemi: il consumatore di oggi condivide, ma non solo; nasce e cresce il suo bisogno di entrare in connessione con altri utenti, sempre ed ovunque.

Tuttavia, nel linguaggio di oggi, bisogna rilevare che i termini come "condivisione" o "connessione" sono sempre più legati all'azione di registrare i propri dati.

Qualche decennio fa, prima che dilagasse prepotentemente la febbre digitale, la registrazione avveniva per lo più tramite la scrittura e serviva a ricomprendere solo una piccola parte delle interazioni sociali, essendo per lo più legata ad effetti formali, connessi, ad esempio, a norme o contratti. Allora le relazioni *inter homines* non trovavano spazio in questo scenario, così come le loro conversazioni, che sfuggivano ai lacci della "rete" di quel tempo essendo perlopiù frutto di incontri *vis-à-vis*[227].

Oggi lo scenario si è capovolto.

Le relazioni fra persone sono, soprattutto, il risultato di contatti digitali in cui nulla può sfuggire: i dati che lasciamo tramite i vari strumenti digitali che abbiamo a disposizione ci consentono, infatti, di lasciare infinite tracce di noi, dei nostri gusti, che rimangono così intrappolate nella memoria della rete.

Occorre, inoltre, evidenziare che, spesso, il consumatore *social* non paga materialmente un prezzo per fruire di certi servizi di reti sociali (i.e., basti pensare a Facebook) e per tale motivo, nella maggior parte dei casi, percepisce detta fruizione come gratuita anche se in realtà così non è.

Il corrispettivo che egli versa alle imprese, infatti, ha un prezzo molto alto e risiede nella cessione dei propri dati (una grande quantità di dati!).

Sulla base del quadro pocanzi delineato, emerge chiaramente come il tema connesso al grande volume di dati detenuto oggi dalle aziende – cc.dd. Big Data –, e conseguentemente del loro valore, sia di fondamentale importanza sia con riguardo al tempo che stiamo vivendo che al futuro che verrà.

Affinché si possano valutare ed analizzare le problematiche che la gestione dei Big Data può comportare ai tempi della *data economy* – sia sotto il profilo consumeristico che sotto quello regolatorio – è necessario però fare un passo indietro, guardando a quei fattori prodromici all'avvento del fenomeno in analisi.

Il *web*, fin dalla sua nascita, ha infatti rappresentato il mezzo tramite il quale i suoi fruitori potevano scambiarsi informazioni di ogni tipo, senza che vi fosse una qualche barriera d'accesso ad ostacolarne l'utilizzo.

Internet, in qualità di libera piazza di scambio globale delle informazioni, ha quindi modificato il modo di comunicare delle persone che, navigando, hanno scoperto la possibilità di entrare in contatto con una molteplicità di oggetti immateriali creati dall'uomo (i cc.dd. "artefatti", fra cui possiamo annoverare, ad esempio, i documenti complessi)[228].

Tuttavia, a seguito della costante evoluzione della rete a cui si è assistito negli ultimi anni, è cambiato l'oggetto su cui Internet si fonda: nel corso del tempo, infatti, si è passati da "una rete di documenti" ad una "rete di dati"[229], i quali, se messi in connessione fra loro, consentono di scovare altri dati ad essi correlati.

Volendo provare a dare una definizione del fenomeno in oggetto, possiamo dire che Big Data è il termine usato per descrivere "una raccolta di dati così estesa in termini di volume, velocità e varietà da richiedere tecnologie e metodi

---

[227] In questo senso v. A. Pilati, *Rivoluzione digitale e disordine politico*, Milano, 2016, 15.

[228] Cfr. G. Rizzo, F. Morando, J.C. De Martin, Open Data*: la piattaforma di dati aperti per il Linked Data*, in *Informatica e diritto*, Napoli, 2011, fasc. nn. 1-2, 493.

[229] Cfr. T. Agnoloni, M.-T. Sagri, D. Tiscornia, Open Data*: nuova frontiera della libertà informatica?*, in *Informatica e diritto*, Napoli, 2009, fasc. n. 2, 9.

analitici specifici per l'estrazione di valore"[230].

Guardando alle peculiarità di quello che è stato definito il giacimento petrolifero del Terzo Millennio[231], possiamo rilevare che la comunità scientifica è pressoché unanime nel ritenere che i Big Data si caratterizzino per la presenza delle quattro (o cinque) "V" [232]:

- *volume*: definita la caratteristica più importante, è stato osservato come i recenti sviluppi nella capacità di raccolta, nella memorizzazione e nell'analisi dei dati abbiano prodotto un incremento esponenziale del volume di dati che possono essere raccolti e analizzati[233].

- *varietà*: è connessa alla molteplicità di fonti da cui possono derivare i dati (testo, dati *web*, *tweets*, dati sensori, audio, video, flussi di *click*, ecc.) nonché alla complessità delle diverse tipologie di dati a disposizione delle imprese (strutturati, semistrutturati, non strutturati)[234];

- *velocità*: si riferisce alla velocità di cambiamento/aggiornamento dei dati (è stato osservato che soprattutto nei mercati dinamici i nuovi dati potrebbero renderne obsoleti altri, precedenti ad essi)[235];

- *veracità*: si riferisce alla veridicità dei dati, cioè alla loro capacità di essere precisi[236];

- *valore*: corrisponde al valore monetario che un'azienda può trarre dall'analisi di grandi quantitativi di dati[237].

Il meccanismo mediante il quale le imprese utilizzano i dati immessi dagli utenti per ricavarne informazioni utili per il proprio *business* è un processo di analisi del *web* articolato nelle fasi che seguono: 1) raccolta dei dati di base degli utenti, al fine di ottenere il maggior numero possibile di dati; 2) la trasformazione dei dati in informazioni misurabili; 3) lo sviluppo di indicatori chiave (c.d. *Key Performance Indicator*); 4) la formulazione di una strategia aziendale sulla base dei dati raccolti[238].

Da ciò consegue che, potenzialmente, l'impatto economico e sociale che l'analisi di questa grande vastità di dati può produrre è tale da essere ritenuto, da autorevole dottrina, enorme ed incommensurabile[239].

---

[230] In questo senso, cfr. A. De Mauro, M. e Greco, M. Grimaldi, *A Formal definition of Big Data based on its essential Features*, in *Library Review*, Vol. 65, n. 3, 2016, 122 ss.

[231] Espressione ascrivibile a M. Bogni, A. Defant, *Big Data: diritti IP e problemi della privacy*, in *Il diritto industriale*, 2015, fasc. n. 2, 117.

[232] In questo senso, cfr. F. Di Porto, *La rivoluzione Big Data. Un'introduzione*, in *Concorrenza e Mercato*, 2016, Vol. 23, nota 3. Per quanto concerne i contributi sul tema dei *Big Data*, si veda, *ex multis*, M.D. Assuncao, R.N., Calheiros, S. Bianchi M.A.S. Netto, R. Buyya *Big Data computing and clouds: Trends and future directions*, in *Journal of Parallel and Distributed Computing*, 2015, 3-15 e 79-80; J. Hurwitz, M. Kaufman, A. Bowles, *Cognitive Computing and Big Data Analytics*, Wiley, Indianapolis, 2015, 56-57; M.S. Gal, D.L. Rubinfeld, *Access Barriers to Big Data*, in *Arizona L. Review*, 2017, Vol. 59, fasc. n. 2, 340 ss.

[233] In questo senso, M.S. Gal, D.L. Rubinfeld. *Op. cit.,* 346.

[234] M. Schroeck, R. Shockley , J. Smart, D., Romero-Morales, P. Tufano, *Analytics: The real world use of Big Data*, IBM Institute for Business Value and Saïd Business School at the University of Oxford, 2012, 4, disponibile al seguente indirizzo: *http://www.bdvc.nl/images/Rapporten/GBE03519USEN.PDF.*

[235] Ancora M.S. Gal, D.L. Rubinfeld*, Op. cit.,* 347.

[236] M. Schroeck, R. Shockley , J. Smart, D., Romero-Morales, P. Tufano *Op. cit.*, 4.

[237] Così M.D. Assuncao, R.N., Calheiros, S. Bianchi M.A.S. Netto, R. Buyya., *Op. cit.,* 5.

[238] Cfr. G.A.M. Bellomo, *"There ain't no such thing as a free lunch". Una riflessione sui meccanismi di mercato dell'economia digitale e sull'effettività delle tutele esistenti*, in *Concorrenza e Mercato*, 2016, Vol. 23, 207-208.

[239] In questo senso, v. F. Di Porto, *Op. cit.*, p. 6. Analogamente v. A. Pilati, *Op. cit.*, 28, il quale ricorda che solo nel 2015 i dati prodotti siamo stati pari a tutti quelli generati dal debutto della scrittura fino al 2014 e che la stima prevista per gli oggetti interconnessi nel 2020 è di circa 200 miliardi.

In particolare "i Big Data costituiscono un importante asset sia per le imprese sia per i governi che ne fanno uso. Le imprese li utilizzano per migliorare i loro prodotti sempre più orientati alle esigenze del singolo consumatore e per l'innovazione. Mentre i governi li utilizzano per rendere più efficienti l'erogazione dei servizi pubblici e migliorare le proprie politiche socio economiche come ad esempio il settore sanitario"[240].

Il profilo dei detentori di queste grandi quantità di dati è, infatti, riconducibile a operatori pubblici e privati che raccolgono una notevole quantità di contenuti nell'ambito delle loro attività istituzionali ed economiche e che operano sfruttando un modello di *business* "a due versanti" (c.d. *two-sided networks*)[241].

In particolare, guardando al lato delle aziende e non dalla P.A., spesse volte queste sono aziende *ex* monopoliste e/o fornitrici di servizi Internet (c.d. *Over The Top*)[242].

Ma quali vantaggi comporta l'utilizzo dei Big Data?

In primo luogo, questi grandi volumi di dati conferiscono alle imprese che li detengono un vantaggio competitivo – che cresce al crescere della quantità di dati disponibili e della loro qualità – poiché consente loro di offrire ai consumatori servizi e prodotti migliori, modellati sui loro effettivi bisogni[243]. Ne consegue che le imprese utilizzatrici riescono ora a raggiungere più facilmente sia i propri consumatori che gli acquirenti potenziali mediante contenuti mirati sulla base delle loro preferenze espresse. Parimenti, il propagarsi del fenomeno in esame ha permesso loro anche di monetizzare i servizi offerti online tramite pubblicità mirate[244].

In secondo luogo, l'utilizzo dei Big Data consente ai consumatori – tramite i *social network*, le *app* di *rating*, le piattaforme di intermediazione, ecc. – di ridurre i costi di ricerca di informazioni e di comparazione di prodotti e servizi[245].

In terzo luogo, grazie all'impiego di una vastità di dati, i consumatori possono fruire di informazioni a basso costo in quanto i Big Data sono un fenomeno caratterizzato dalla non rivalità (l'analisi di un certo volume di dati da parte di un'impresa non implica l'impossibilità per un'altra di fare altrettanto, essendo la loro elaborazione illimitatamente ripetibile) e dall'ubiquità (i Big Data, infatti, sono ovunque e possono essere conservati in infiniti luoghi)[246].

Accanto ai vantaggi derivanti dall'utilizzo – o riutilizzo – dei Big Data, si devono tuttavia registrare degli aspetti negativi.

In primo luogo, giova osservare che la gestione di tali dati è una prerogativa circoscritta a poche grandi aziende operanti, soprattutto, attraverso Internet (fra queste possiamo annoverare Google, Facebook, Amazon, Linkedin ed Ebay). Il potere che può derivare dal controllo dei Big Data, detenuto da questa rosa di imprese, potrebbe infatti generare, in prospettiva, sia la detenzione di una posizione dominante nei mercati in cui essi operano che delle ricadute sociali (c.d. controllo sociale)[247]. La capacità di raccolta di tali aziende è tale da coprire quasi tutto il traffico *web* e da determinare

---

[240] Così, testualmente, G. Ghidini, *Big Data fra potere di mercato e potere di orientamento informativo e di opinione*, Relazione svolta in occasione del Convegno "*Big Data e concorrenza*," organizzato a Roma presso l'Università Luiss Guido Carli, con il patrocinio dell'Autorità Garante della Concorrenza e del Mercato, in Data 9 novembre 2016, reperibile sul sito *www.agcm.it,* 2.

[241] A tal proposito si rimanda alle riflessioni di cui al paragrafo 1, Parte I, del presente contributo. Analogamente cfr. G.A.M. Bellomo, *Op. cit.,* 211. In particolare, l'Autrice ricorda come detti modelli di *business* non siano un fenomeno economico recente, anche se lo sviluppo della tecnologia IT ha creato spazio per nuove opportunità economiche, facendo convergere *online* due ambiti distinti di clienti-utilizzatori.

[242] Così G. Crea, *Open (Big) Data, tra implicazioni di potere e prospettive di evoluzione cognitiva della specie*, in *Diritto ed economia dei mezzi di comunicazione*, 2015/2016, n. 1, 57 ss.

[243] Giova evidenziare però, che ciò non sempre si traduce in altrettanti benefici per i consumatori, come si vedrà nel proseguo dell'analisi.

[244] Cfr. F. Di Porto, *Op. cit.*, p. 6. Analogamente v. anche Bellomo G.A.M., *Op. cit.,* 209.

[245] F. Di Porto *Big Data e regolazione a tutela dei consumatori. La* disclosure regulation, Contributo fornito in occasione del Convegno "*Big Data e concorrenza*," organizzato a Roma presso l'Università Luiss Guido Carli, con il patrocinio dell'Autorità Garante della Concorrenza e del Mercato, in Data 9 novembre 2016, reperibile sul sito *www.agcm.it,* 8.

[246] Come evidenziato nell'articolo di F. Di Porto., *Op. cit.*, 8 e *passim.*

[247] Cfr. G. Crea, *Op. cit.*, 73.

una posizione definita in dottrina di "sesto potere"[248].

In secondo luogo, spesso i cittadini digitali non sono pienamente consapevoli delle ricadute che l'immissione dei propri dati in rete – soprattutto quelli personali – può provocare, dell'importanza stessa dei dati ceduti, dell'uso che ne verrà fatto[249].

Si viene a creare, quindi, un rapporto fra il consumatore ed il professionista caratterizzato da una asimmetria derivante da un sovraccarico di fonti informative a discapito degli utenti, i quali spesso, guidati da una sorta di automatismo, si trovano ad autorizzare il trattamento dei propri dati personali senza essere pianamente consapevoli dell'utilizzo che ne faranno in realtà le piattaforme alle quali accedono.

Infine, grazie all'impiego dei Big Data i consumatori (reali e potenziali) vengono profilati dalle aziende. Se questo comporta, come già detto in precedenza, un vantaggio competitivo per le imprese, non sempre porta dei benefici per i consumatori.

La capacità delle aziende di conoscere, tramite i dati, l'attitudine al consumo del singolo, le sue preferenze e la sua disponibilità a pagare per un dato bene può provocare come effetto la differenziazione dei prezzi a prescindere dai costi effettivi di un determinato bene o servizio[250].

Concludendo, quindi, emerge come l'utilizzo di grandi volumi di dati dia luogo a luci ed ombre che necessitano dell'attenzione delle Autorità competenti – sia di garanzia che di regolazione – per contemperare gli interessi dei soggetti coinvolti (sia consumatori che professionisti) operanti nei nuovi mercati digitali[251].

2. I FENOMENI DEVIANTI DEL WEB: LA RESPONSABILITÀ DELLE PIATTAFORME E I POTERI DI INTERVENTO DEL REGOLATORE

(Francesca Pellicanò[252]).

L'anno che volge ormai al termine è stato in larga parte scenario di un intenso dibattito mediatico e istituzionale nei confronti della responsabilità delle piattaforme *online* in relazione alla proliferazione di quelli che possono essere considerati i fenomeni devianti del *web*: *fake news*, *hate speech*, incitazione al terrorismo, *cyberbullismo*. Fenomeni la cui propagazione è incontrollabile, velocissima e virale, con ripercussioni anche gravi, non essendo, invece, altrettanto rapido ed incisivo lo sviluppo degli strumenti legali per fronteggiarli. La diffusione di contenuti illegali *online* mina, infatti, la fiducia di cittadini e imprese nell'ambiente digitale e danneggia lo sviluppo economico dello stesso ecosistema delle piattaforme e del Mercato unico digitale europeo.

Il *corpus* normativo tradizionale non si presta completamente ad essere integramente trasfuso e adattato alle nuove esigenze della società, soprattutto per l'ontologico limite dei confini nazionali: manca un quadro normativo comune, trasversale e transnazionale, come è, invece, per sua stessa natura, la rete internet. Si pone quindi, pressante, l'esigenza di dotarsi di strumenti che consentano un intervento efficace e sufficientemente celere.

---

[248] Così Z. Bauman, D. Lyon, *Sesto potere. La sorveglianza nella modernità liquida*, Laterza, Roma, 2014.

[249] In questo senso si veda G.A.M. Bellomo, *Op. cit.,* 207-209 ed in particolare le note 3 e 10, cui si rinvia per ulteriori approfondimenti sul punto.

[250] Cfr. F. Di Porto., *Op. cit.*, 10.

[251] A tal proposito, con una particolare attenzione al ruolo svolto sul tema in oggetto dall'Autorità per le Garanzie nelle Comunicazioni, si rinvia alla Parte III, paragrafo 1, del presente Lavoro.

[252] Le opinioni espresse sono personali e non impegnano in alcun modo, né rappresentano necessariamente, quelle dell'Autorità per le garanzie nelle comunicazioni.

Soluzioni uniformi a livello mondiale non sono di certo praticabili, e probabilmente neanche auspicabili, tuttavia ciò non significa che le istituzioni, a livello internazionale e locale, non si siano dimostrate sensibili e proattive sul punto. Da più parti e a più livelli si è sentita l'esigenza di lanciare iniziative[253], convegni[254], consultazioni pubbliche[255], momenti di riflessione collettiva[256] sulla portata dei fenomeni.

Non manca chi sia andato oltre, proponendo o portando avanti iniziative legislative che, nel comprensibile tentativo di arginare gli effetti negativi di questi fenomeni, offrono tuttavia soluzioni spesso troppo oppressive, aggiungendo ulteriore carico al già gravoso lavoro delle autorità giudiziarie. E, al di là di difetti e aspetti negativi specifici, queste proposte soffrono comunque, tutte, il limite dell'applicazione nazionale, non ponendo rimedio se non parzialmente e localmente.

Tra quelli che sopra si sono definiti come i fenomeni devianti del *web*, particolare rilevanza ha assunto nel corso del 2016 e del 2017 la diffusione delle *fake news*: il tema della diffusione della disinformazione *online* e della diffusione e condivisione di notizie false, provenienti da una fonte non professionale, è attualmente al centro di un dibattito che coinvolge non solo l'opinione pubblica, ma anche centri di ricerca e istituzioni a livello internazionale.

Pur non trattandosi di certo di un tema nuovo (basti pensare, per un esempio noto e di grande impatto, alla reazione di panico del pubblico radiofonico allo sceneggiato in cui Orson Welles leggeva il romanzo "*La Guerra dei mondi*"[257]), il tradursi della circolazione di notizie false in Internet, la condivisione e circolazione indiscriminata sui *social media*, hanno comportato una capillare propagazione del fenomeno, attribuendogli una rilevanza prima inedita, soprattutto alla luce della campagna elettorale per le ultime elezioni presidenziali americane[258]. Non sorprende, dunque, che la "parola dell'anno 2016" secondo il Dizionario di Oxford sia "*post-truth*"[259]. E per il 2017 la tendenza non è affatto invertita. Infatti, se l'Università di Stanford ha pubblicato uno studio incentrato sul fenomeno e il suo possibile impatto sull'esito delle elezioni americane dell'autunno 2016[260], la Commissione europea, per voce del vice-Presidente Andrus Ansip, ha annunciato nel gennaio 2017[261] di voler affrontare il tema, auspicando una maggiore responsabilizzazione delle piattaforme *online* attraverso forme di autoregolamentazione e il potenziamento di iniziative di *media literacy.* A fine agosto 2017, poi, il Commissario europeo per il digitale Mariya Gabriel ha annunciato entro la fine dell'anno una consultazione pubblica e la formazione di una *task force* di esperti sul tema, come misura per contra-

---

[253] Da molti anni la lotta al cosiddetto "*hate speech*", ovvero l'incitazione all'odio propagata attraverso la rete internet, costituisce uno degli obiettivi del Consiglio d'Europa, promotore di studi e iniziative al riguardo, riassunti al seguente *link*: https://www.coe.int/en/web/freedom-expression/hate-speech

[254] Tra le numerose iniziative dell'ultimo anno, si menziona il *Safer Internet Day*, promosso annualmente dalla Commissione europea per promuovere la riflessione e la sensibilizzazione sui temi della tutela dei minori *online*, bullismo e *cyberbullismo*, al fine di promuovere un uso più sicuro e responsabile del *web* e delle nuove tecnologie tra i bambini e i giovani di tutto il mondo, nell'ambito del quale, a febbraio 2017, l'AGCom ha organizzato un convegno presso la Camera dei Deputati https://www.agcom.it/safer-internet-day

[255] Ad esempio, la Commissione Cultura, Media e Sport del Parlamento UK ha lanciato nella primavera del 2017 un'*inquiry online* per acquisire una maggiore consapevolezza della portata della circolazione di *fake news* http://www.parliament.uk/business/committees/committees-a-z/commons-select/culture-media-and-sport-committee/news-parliament-2015/fake-news-launch-16-17/

[256] L'impatto delle *fake news* è stato discusso, unitamente ad altri aspetti dell'impatto dell'era digitale sull'informazione, durante la riunione plenaria dell'EPRA, la piattaforma europea dei regolatori dell'audiovisivo, nel maggio 2017. https://epra3-production.s3.amazonaws.com/attachments/files/3059/original/PS1_news_in_digital_age_final.pdf?1493971279

[257] https://it.wikipedia.org/wiki/War_of_the_Worlds_(programma_radiofonico)

[258] https://www.theguardian.com/us-news/2017/jan/11/trump-attacks-cnn-buzzfeed-at-press-conference.

[259] Si veda il seguente link https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016 in cui "*post-truth*" viene definito "*an adjective defined as 'relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief'.*"

[260] H. Allcott, M. Gentzkow *Social Media and Fake News in the 2016 Election*, disponibile sul sito della Stanford University al *link*: https://web.stanford.edu/~gentzkow/research/fakenews.pdf

[261] Tra i numerosi articoli che hanno riportato la notizia, si veda esemplificativamente https://www.neweurope.eu/article/eu-take-combating-fake-news/

stare un fenomeno in ascesa sulle piattaforme *social*, Facebook *in primis*, che rischia di diventare senza controllo[262]. L'obiettivo è, per stessa ammissione della Gabriel, creare un approccio comune europeo, armonizzando le iniziative formatesi a livello nazionale da più parti e profondamente divergenti tra loro.

Il problema principale nel fronteggiare questi fenomeni devianti del *web* consiste nella effettiva disponibilità di strumenti regolatori con cui fronteggiarli. Questi fenomeni, sebbene siano così variegati e afferiscano a numerosi aspetti della vita sociale (la *privacy*, la tutela dei minori, il bullismo, l'affidabilità dell'informazione, la fiducia nei media, la libertà di espressione, l'incitamento al terrorismo svolto *online*, sono solo alcuni degli aspetti su cui incidono), tuttavia mostrano un oggettivo tratto comune: costituiscono, tutti, un abuso e uso distorto delle rete internet, posto in essere prevalentemente mediante la diffusione e la condivisione dei contenuti sulle piattaforme *online* e i *social media*. Soggetti che, tradizionalmente, sfuggono in gran parte alle maglie dell'intervento legislativo e regolamentare: difficile è la loro qualificazione in categorie giuridiche univoche, quali ad esempio quella che più gli si avvicina, quella dei prestatori di servizi della società dell'informazione, di cui alla direttiva del Parlamento europeo e del Consiglio 2000/31/CE sul commercio elettronico, recepita in Italia dal decreto legislativo n. 70/2003.

Le diverse tipologie di attività dei fornitori di servizi intermediari della società dell'informazione, ovvero *mere conduit*, *caching* e *hosting*, non sono del tutto sovrapponibili ai *social network* e alle piattaforme *online*.

Per i prestatori di servizi della società dell'informazione, la direttiva e il relativo decreto legislativo di recepimento in Italia riconoscono peraltro un generale regime di assenza di responsabilità, prevedendo delle condizioni al verificarsi delle quali essi non sono responsabili del contenuto delle informazioni trasmesse o memorizzate; tuttavia, può loro essere richiesto dall'autorità giudiziaria o amministrativa competente di "*agire prontamente*", nell'ambito dei mezzi tecnici di cui dispongono, per "*impedire l'accesso*" ai contenuti in violazione della legge. È su tale base giuridica che occorre incentrare l'azione definitoria di strumenti e buone prassi che consentano di intervenire per la cessazione della violazione *online* e, ove possibile, il ripristino della situazione preesistente. Il considerando 40 della Direttiva prevede che le disposizioni di questa possano "*costituire la base adeguata per elaborare sistemi rapidi e affidabili idonei a rimuovere le informazioni illecite e disabilitare l'accesso alle medesime*". La Commissione europea ha più volte espresso la sua volontà di non procedere a modificare il regime di cui alla direttiva sul commercio elettronico, affermando di prediligere approcci normativi più strategici, che rispondano direttamente alle sfide e che siano al contempo flessibili e "*future-proof*". In tale cornice si pongono e devono essere lette le recenti comunicazioni della Commissione europea sul tema: il documento COM (2016) 288 del 25 maggio 2016 (cui ci si riferisce di seguito anche come "Comunicazione sulle piattaforme *online*" e la recentissima COM(2017) 555 del 28 settembre 2017 (di seguito anche Comunicazione sulla lotta ai contenuti illegali *online*).

La Comunicazione sulle piattaforme *online* riferisce sugli aspetti principali individuati nella valutazione delle piattaforme *online* e presenta nel contempo la posizione della Commissione sia sulle opportunità di innovazione che sulle sfide normative che ne derivano. Nella Comunicazione si evidenzia la necessità di individuare un quadro normativo equilibrato per le piattaforme *online* del mercato unico digitale, che contribuisca alla promozione di uno sviluppo sostenibile e che, soprattutto, rappresenti un quadro normativo comune, al fine di non ingenerare incertezze negli operatori del settore ed evitare fenomeni di *home shopping*; stabilendosi in Paesi dove è più conveniente e negando così quest'occasione di sviluppo al mercato europeo. È, dunque, necessario offrire la garanzia effettiva di un *level playing field* mediante la certa applicazione delle rilevanti norme UE in materia, ad esempio, di concorrenza, tutela dei consumatori, protezione dei dati personali.

La Commissione dichiara di ritenere strategico l'utilizzo di approcci di auto-regolamentazione e co-regolamentazione basati su principi di riferimento, con l'aiuto dei quali conseguire il giusto equilibrio tra le esigenze di prevedibilità,

[262] Per un commento al riguardo, si veda l'intervista al Commissario dell'AGCOM Antnio Martusciello sul Corriere delle comunicazioni http://www.corrierecomunicazioni.it/digital/48617_martusciello-agcom-fake-news-piu-responsabilita-per-facebook--co-ecco-come.htm

flessibilità ed efficienza e la necessità di sviluppare soluzioni efficacemente applicabili nel lungo periodo.

Al fine dell'ottenimento di tali condizioni, si prevede la necessità di semplificare, modernizzare e snellire la regolamentazione esistente e di assoggettare ad essa, per quanto applicabile, le piattaforme *online*. Ciò va comunque raccordato con il regime di responsabilità degli intermediari di cui alla direttiva sul commercio elettronico, i cui principi in materia sono sopra illustrati. Uno degli obiettivi dichiarati è proprio l'introduzione e il monitoraggio di procedure di *notice and action* per garantire la coerenza e l'efficacia del regime di responsabilità degli intermediari, mentre, sul versante della domanda, assurgono a temi centrali la promozione della fiducia dei consumatori, la trasparenza nell'utilizzo dei dati, la garanzia dell'imparzialità, la salvaguardia dell'innovazione.

Se con la Comunicazione del 2016 la Commissione iniziava una riflessione sulla rilevanza sociale, economica e di mercato delle piattaforme, ponendo le basi per iniziative strategiche armonizzate a livello europeo, nel 2017 va oltre, incentrando la Comunicazione del 28 settembre u.s. sulla lotta ai contenuti illegali *online*, affrontando dunque una specifica declinazione del fenomeno delle piattaforme. La Commissione dichiara, infatti, che le diverse fattispecie di illeciti che si verificano su internet, dalla pedopornografia all'incitamento al terrorismo, dalle pratiche commerciali scorrette alle violazioni dei diritti di proprietà intellettuale, sono ovviamente molto diverse tra loro, come diversi sono gli interventi legislativi che, a livello europeo e nazionale, regolano questi fenomeni.

Tuttavia, queste violazioni sono accomunate dall'ambiente in cui si verificano e vengono diffuse, ovvero l'ecosistema delle piattaforme. Il quadro comune di riferimento, pertanto, è rappresentato dalla già citata Direttiva *e-commerce*, mentre gli strumenti di intervento e cessazione della condotta rientrano tutti, con le specifiche differenze settoriali, nella stessa tipologia di rimozione. La Comunicazione delinea, dunque, strumenti flessibili che possano adeguarsi alle diverse necessità, prevedendo meccanismi efficaci uniformi, facili da utilizzare per facilitare l'invio e la valutazione di segnalazioni sufficientemente precise in modo da garantire un celere, ma ponderato, intervento mirato, che contempli altresì la possibilità di prevenire, con misure tecniche e sanzioni nei confronti dei reiterati trasgressori, che il contenuto rimosso ricompaia nuovamente sulla piattaforma.

3. L'INFORMAZIONE *ONLINE* E IL VALORE DEI DATI

(Rosaria Petti)

È evidente come in un'economia sempre più *data driven* il valore economico dei dati determini problematiche di ordine competitivo nell'acquisizione diretta delle informazioni e di tutele individuali e collettive.

Sotto il primo aspetto la disponibilità quasi esclusiva dei dati può determinare conseguenze rilevanti in termini di accesso al mercato, aumentando le barriere all'ingresso nei confronti di nuovi entranti. Il potere di mercato detenuto dalle piattaforme digitali può infatti creare un significativo pregiudizio alla concorrenza e alla trasparenza del mercato attraverso comportamenti escludenti a danno dei concorrenti o innalzando le barriere d'ingresso. I dati raccolti, che consentono di offrire servizi più personalizzati agli utenti, rendono di fatto meno contendibile la posizione di mercato raggiunta dalla piattaforma.

E se questo è vero per i servizi digitali in generale, altrettanto si verifica con riguardo ai servizi di informazione. Proprio la disponibilità e l'accesso all'ampia mole di dati detenuta dalle piattaforme digitali, in quanto *driver* rilevante nell'economia dell'informazione *online*, ostacola l'accesso al mercato digitale di soggetti economici tradizionalmente operanti nei settori analogici.

Nel settore dell'informazione, l'intermediazione offerta dalle piattaforme e la detenzione esclusiva dei dati raccolti

contribuisce ad annichilire un settore già in declino, riducendo la principale fonte di finanziamento, ossia raccolta pubblicitaria.

La riaggregazione di contenuti è il più delle volte gratuita e viene remunerata dalla pubblicità legata all'*audience* del sito, il che significa che tali servizi competono direttamente con gli stessi editori per l'acquisizione di quote pubblicitarie, senza però sopportare i costi di produzione delle notizie.

La diffusione di nuove tecniche di commercializzazione ispirate alla logica *data driven* anche per gli spazi pubblicitari consente infatti di modificare la struttura tradizionale della raccolta pubblicitaria che, introducendo un'ulteriore intermediazione delle piattaforme, inevitabilmente penalizza i produttori di contenuti editoriali, a cui sarà retrocessa una quota minore di ricavi generati dai loro contenuti. Un processo che in ultima istanza rischia di danneggiare in modo durevole la qualità dell'informazione, implicando inevitabilmente una contrazione degli investimenti in informazione primaria.

Tali riflessioni consentono di introdurre anche il secondo aspetto, quello relativo alle tutele. Invero, se l'accesso e la conseguente disponibilità dei dati diviene *asset* strategico e indispensabile per competere nell'economia dell'informazione digitale, è chiaro che concentrare tale "ricchezza" in capo a taluni operatori rischia di renderli capaci di orientare l'opinione pubblica attraverso una accurata selezione dei contenuti.

Certo l'intermediazione offerta dalle piattaforme (per la cui trattazione si rinvia al precedente paragrafo) può operare in modo neutrale, come risposta al fallimento di mercato dovuto all'asimmetria informativa che caratterizza i due versanti; ma essa può anche agire in modo "interessato", manipolando le informazioni in proprio possesso e oscurando alcuni risultati di ricerca.[263] Il benessere del consumatore può essere, quindi, compromesso quando l'opacità dei risultati di ricerca non consente a questi di migliorare il risultato informativo atteso, con la conseguenza che saranno mostrati all'utente solo contenuti filtrati sulla base delle scelte compiute in precedenza secondo un sistema di corrispondenza (c.d. *machine system*). Tale processo, infatti, si manifesta come il risultato dell'applicazione dell'algoritmo alla base della *news feed*. Questo è in grado di ordinare e presentare i contenuti da mostrare agli utenti in ragione di caratteristiche quali la prossimità dei contenuti rispetto ai *post* valorizzati dagli amici, l'*engagement* ottenuto da questi in termini di *like*, *reactions*, condivisioni e commenti. Ciò a discapito di criteri come credibilità, qualità giornalistica, rilevanza in termini di *public interest* del contenuto, che divengono elementi trascurati nella valutazione della *news feed* offerta dai *social network*.[264]

4. I PRINCIPI FONDAMENTALI APPLICATI ALL'INFORMAZIONE *ONLINE* E L'INQUADRAMENTO DEL FENOMENO *FAKE NEWS*

(Rosaria Petti)

Le implicazioni di un questo ecosistema informativo hanno un impatto non marginale sul pluralismo e sulla libertà di informazione, le cui conseguenze rilevanti incidono significativamente sul diritto degli utenti a ricevere un'informazione obiettiva, completa, corretta e imparziale.

Come noto, la garanzia del pluralismo costituisce una delle *mission* fondamentali dell'Autorità e proprio i principi sanciti a tutela di questo e le competenze espressamente previste dalla legge istitutiva (legge 249 del 1997) l'hanno chiamata

[263] Per una trattazione più approfondita sul tema si rinvia a G. Colangelo, *Big Data, piattaforme digitali e antitrust*, in *Mercato Concorrenza Regole*, 2016, 3, 425.

[264] P. Napoli (2015), *Social Media and the Public Interest: Governance of News Platforms in the Realm of Individual and Algorithmic Gatekeepers*, Media + the Public Interest Initiative Working Paper, Rutger School of Communication and Information.

a indagare, con sempre maggior attenzione, il fenomeno della disinformazione *online*.

Sul tema, l'Autorità è recentemente intervenuta al dibattito svoltosi lo scorso 9 febbraio alla Camera dei Deputati durante il quale ha stimolato il dialogo tra gli *stakeholders*, mentre lo scorso anno ha avviato, con delibera n. 309/16/CONS, un'indagine conoscitiva – ancora in corso – sulle piattaforme digitali e il sistema dell'informazione, al fine, tra l'altro, di approfondire il tema delle *fake news*. Lo scopo è quello di indagare la relazione tra il sistema dell'informazione e la diffusione di notizie per il tramite dei nuovi intermediari digitali, con particolare riferimento all'impatto che essi esercitano sull'apparato di divulgazione, sul funzionamento dei meccanismi adottati dalle piattaforme digitali, nonché le caratteristiche della domanda di informazione *online*, mettendo in luce le eventuali criticità sotto il profilo del pluralismo informativo.

Sui Big Data, invece, l'Autorità ha recentemente avviato, con delibera n. 217/17/CONS, un'indagine conoscitiva congiunta con l'Autorità garante per la concorrenza e il mercato e l'Autorità garante per la protezione dei dati personali. L'approccio multidisciplinare, che lo studio si prefigge, intende analizzare l'impatto sulla concorrenza, sulla tutela dei consumatori e sulla protezione dei dati personali, sul vantaggio competitivo generato dalla disponibilità di dati in via esclusiva, sul futuro sviluppo delle comunicazioni elettroniche e del settore audiovisivo, anche ai fini di valutare l'impatto sul pluralismo e sulle garanzie nelle nuove comunicazioni, tenuto conto dell'interesse pubblico all'accesso ad alcune tipologie di dati per finalità sociali.[265]

Si tratta di una questione di rilievo se si considera l'offerta informativa esistente, sempre più veicolata tramite social media e motori di ricerca. In particolare, si pensi ai sistemi di *in-app browsing* e di *Instant Articles* di Facebook, nonché al formato AMP (*Accelerated Mobile Pages*) di Google. Un tale assetto determina rilevanti effetti in termini di *secondary gate-keeping*.

Del resto, l'informazione *online* si presenta come un fenomeno complesso che richiede di transitare da una situazione di relativa scarsità a una situazione di "surplus" di informazione per l'utente.[266] Non a caso, proprio l'abbondanza di informazioni che circolano *online* ha generato la necessità di utilizzare piattaforme di orientamento nella navigazione (motori di ricerca), sistemi di aggregazione dei contenuti (portali) e strumenti di condivisione delle opinioni (*social network*).

Tenendo conto della maggiore disponibilità di fonti informative, professionali e non, il fenomeno delle *fake news* sulle piattaforme va affrontato considerando le specifiche modalità di organizzazione, posizionamento e personalizzazione dei contenuti editoriali mediante l'impiego di algoritmi e sistemi automatizzati. Tale sistema, infatti, è in grado di incidere sull'effettiva capacità di dare voce a tutte le opinioni e punti di vista che caratterizzano il dibattito pubblico sui temi di attualità.

Un contesto in cui si accresce un fenomeno di autoconvincimento dell'utente attraverso la creazione del fenomeno delle cc.dd. "*echo chambers*". In queste stanze virtuali, agli utenti sono presentate in maniera amplificata soltanto le notizie che già riflettono le opinioni e preferenze politiche che si presumono favorite in base alle notizie scelte in precedenza o ad altri parametri di personalizzazione[267].

Si realizza in tal modo l'omofilia delle reti comunicative, intesa come appartenenza al gruppo, in cui appunto gli utenti tendono ad aggregarsi in ragione della polarizzazione verso un dato argomento, condividendo modelli di consumo informativo e una struttura sociale simile e dando luogo appunto alle camere dell'eco.[268]

---

[265] Le finalità riportate sono espressamente indicate nella delibera di avvio al punto 15.

[266] In questi termini, il Commissario AGCom Antonio Martusciello, in un intervento alla LUISS Guido Carli, in occasione del Master di II livello in Diritto della Concorrenza e dell'Innovazione, ed. 2015/2016.

[267] Cfr. W. Quattrociocchi, A. Vicini, *Misinformation guida alla società dell'informazione e della credulità*, , Milano, 2016.

[268] In questi termini, il Commissario AGCom Antonio Martusciello, intervenuto alla IX edizione del Premio Internazionale

È evidente la relazione tra questo fenomeno e gli algoritmi utilizzati dalle piattaforme. Se questi restituiscono pagine che favoriscono argomenti e persone simili a quelle che sono state in passato apprezzate agli utenti, attraverso un filtraggio dei contenuti, di fatto formano delle bolle informative intorno a ciascun lettore virtuale, grazie alle quali egli vede e legge prevalentemente contenuti che somigliano a ciò che ha già gradito[269].

Certo anche nell'informazione analogica il cittadino è chiamato costantemente a operare una scelta, ispirando la propria selezione a talune fonti, preferendo alcune testate su altre. Ma va sottolineato che per il versante *digital*, l'intermediazione si presta a un duplice scopo: da un lato l'interesse meramente commerciale di coloro che intendono attirare traffico sulle proprie pagine; dall'altro l'interesse politico con lo scopo di condizionare l'opinione pubblica.

Va poi ulteriormente considerato che, nella scelta della propria dieta informativa, l'utente-cittadino non sempre è orientato dalla professionalità delle fonti. Un concetto questo che appare comunque datato e inadatto alle nuove forme d'informazione. La principale distinzione, infatti, va ricondotta alla definizione di prodotto editoriale, come contenuto nella legge n. 62 del 2001, recante "Nuove norme sull'editoria e sui prodotti editoriali". In base a essa, la distinzione, anche per le testate *online*, è connessa all'obbligo di registrazione presso il Tribunale territorialmente competente. A ciò si aggiunge la previsione di cui all'art. 7, comma 3, del d.lgs. n. 70 del 2003, il quale ha sancito che la registrazione della testata editoriale telematica è obbligatoria esclusivamente per le attività per le quali i prestatori del servizio intendano avvalersi delle provvidenze economiche previste dalla richiamata legge n. 62 del 2001.

Ulteriore considerazione riguarda la tipologia di notizie. Queste se divulgate da fonti informative non professionali chiaramente non risultano neanche assoggettabili alle regole sulla responsabilità editoriale e, quindi, ai canoni di correttezza e professionalità giornalistica. In tal contesto, appare ancor più evidente come il *framework* normativo sia certamente inattuale, prestando il fianco a possibili strumentalizzazioni, soprattutto in occasione di appuntamenti elettorali. Il risultato è che il dibattito su temi di attualità, da un lato, può essere sfruttato per finalità strettamente commerciali, ispirate dagli introiti derivanti dai *click*; dall'altro, utilizzato per finalità politiche, approfittando della tendenza alla polarizzazione politica insita nella stessa struttura di funzionamento (*algorithm-based*) delle piattaforme di *social networking*. Ne consegue che l'ecosistema informativo rischia di determinare, attraverso notizie false amplificate dalla viralità dei *social*, uno stato di continua e pericolosa propaganda.

Policy regolatoria dell'Autorità per le garanzie nelle comunicazioni e soluzioni prospettiche

del Giornalismo dedicato a Biagio Agnes. Il Commissario ha spiegato che l'informazione si fonda su circuiti di interesse e autoreferenzialità, sviluppando l'omofilia della nuova struttura divulgativa, in cui le notizie hanno lo scopo di assecondare gusti e preferenze del lettore digitale.

[269] E. Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin Group, 2011.

SOMMARIO: 1. IL RUOLO DELL'AGCOM NELLA LOTTA ALLE PRINCIPALI PROBLEMATICHE LEGATE ALL'UTILIZZO DEI BIG DATA. – 2. L'EVOLUZIONE NORMATIVA IN CORSO E LA NECESSITÀ DI STRUMENTI FLESSIBILI. POSSIBILI SCENARI DI INTERVENTO DEL REGOLATORE. – 3. POTESTÀ DI INTERVENTO DI AGCOM NEL CONTRASTO ALLA DIFFUSIONE DI *FAKE NEWS* E DISINFORMAZIONE *ONLINE*.

1. L RUOLO DELL'AGCOM NELLA LOTTA ALLE PRINCIPALI PROBLEMATICHE LEGATE ALL'UTILIZZO DEI BIG DATA

(Valentina Angelini)

Alla luce di quanto esposto nei paragrafi che precedono[270], possiamo affermare che le relazioni fra gli utenti-consumatori sono al centro della nuova economia che si è venuta a creare in questi ultimi anni, in cui, grazie all'uso di piattaforme, è possibile far incontrare chi richiede un determinato bene o servizio con chi è in grado di fornirlo.

Tuttavia, si sta assistendo ad un cambio di prospettiva: se in una prima fase – quella relativa all'economia della condivisione – la figura del consumatore cessava di avere un ruolo passivo ma diventava un soggetto attivo del mercato in quanto *prosumer*[271] in grado, da un lato, di creare valore, di monetizzare il suo tempo, le sue capacità e le sue risorse e, dall'altro, di utilizzare i vari beni e servizi messi a sua disposizione dal sistema economico, nella fase che stiamo vivendo – quella della *data economy* – il consumatore diviene preda, oggetto, del mercato, poiché le aziende riescono, mediante strumenti complessi come gli algoritmi, a trasformare ogni utente in una fonte inesauribile di informazioni[272].

Muovendo da queste considerazioni inziali, nonché dall'analisi fatta in precedenza sui vantaggi e sugli svantaggi derivanti – sia per le imprese che per i consumatori – dall'utilizzo di una grande quantità di dati[273], emerge come sia fondamentale il ruolo svolto dalle Autorità nel tempo in cui stiamo vivendo e, in particolare, dall'Autorità per le Garanzie delle Comunicazioni.

A ben vedere, nel corso di questi anni, l'Autorità ha già avviato alcune Indagini Conoscitive per monitorare i cambiamenti derivanti dall'avvento di questi nuovi mercati.

In particolare, giova ricordare: la delibera 357/15/CONS concernente l'indagine conoscitiva sullo sviluppo delle piattaforme digitali e dei servizi di comunicazione[274]; la delibera 165/16/CONS riguardante l'indagine conoscitiva sui cosiddetti "*consumer communications services*"[275]; la delibera 309/16/CONS, relativa all'indagine conoscitiva sulle piattaforme digitali e il sistema dell'informazione, tutt'ora in corso[276].

---

[270] In particolare, si veda Parte II, paragrafo 1, del Capitolo in esame.

[271] Com'è noto, questo termine è stato coniato da Toffler (cfr. A. Toffler, *The third wave*, Bantam, 1980, 11 e *passim*) ed è una crasi dei termini *producer* e *consumer*. Per un approfondimento sull'evoluzione della figura del consumatore dal punto di vista sociologico, cfr., G. Ritzer, P. Dean, N. Jurgenson, *The Coming of Age of the Prosumer*, in *American Behavioral Scientist*, 2012, Vol. 56, fasc. n. 4, 379-398.

[272] Cfr. A. Pilati, *Op. cit.*, 78.

[273] Ancora una volta, v. Parte II, paragrafo 1, del Capitolo in esame.

[274] La quale, partendo da una disamina economica della natura multi-versante delle piattaforme digitali per la diffusione di servizi ad elevato valore aggiunto su Internet, voleva esplorare gli eventuali interventi regolamentari utili alla promozione di una concorrenza sostenibile, allo sviluppo dei servizi digitali e alla tutela dei consumatori.

[275] Per un'analisi su detta indagine si rinvia al Rapporto dello scorso anno, ed in particolare a V. Angelini, *Le* app *di comunicazione sociale. Mutamenti del mercato e nuovi bisogni di protezione del consumatore nella prospettiva digitale*, n *Consumerism 2016 Nono Rapporto annuale*, Consumers' Forum e Università degli Studi di Roma Tre, 2016, 24 ss.

[276] Come si legge nella delibera in analisi, detta indagine è "*volta ad investigare la relazione tra il sistema dell'informazione e la diffusione dei nuovi intermediari digitali, analizzando la struttura delle piattaforme digitali, con particolare riferimento all'impatto che esse esercitano sul sistema informativo; il funzionamento dei meccanismi adottati dalle piattaforme digitali nel diffondere informazione; nonché le caratteristiche della*

Tuttavia, l'azione più rilevante con riguardo al tema specifico della grande vastità di dati portata avanti dall'Autorità è rinvenibile nella richiamata indagine dello scorso maggio, in corso, riguardante proprio i Big Data (cfr. delibera 217/17/CONS). Tale indagine è svolta congiuntamente con l'Autorità Garante della Concorrenza e del Mercato e con il Garante per la protezione dei dati personali, a conferma che il tema in oggetto meriti un'ampia analisi, necessitando, seppur ognuna nell'ambito delle proprie competenze, di uno sguardo aperto e trasversale da parte delle Autorità.

In particolare, in sede di avvio dell'indagine in esame, si è evidenziato come "i settori di competenza dell'Autorità per le garanzie nelle comunicazioni sono profondamente interessati al fenomeno dei Big Data, in quanto le comunicazioni fisse e mobili, i servizi media e dell'audiovisivo e i servizi postali (o diffusi tramite la rete postale) sono caratterizzati da: un'ampia quantità di consumatori (servizi universali e ad elevato tasso di domanda); il consumo dei servizi attraverso reti digitali correlate e interconnesse alla piattaforma IP attraverso l'uso in modalità continuativa (abbonamento, contratti di medio termine, TV lineare, risparmio postale) o attraverso scelte specifiche di acquisto (video *on demand*, servizi di comunicazione mobile a richiesta). Le caratteristiche intrinseche ai settori rientranti nella sfera istituzionale dell'Autorità per le garanzie nelle comunicazioni rendono di fondamentale importanza interrogarsi sugli effetti del fenomeno dei Big Data e sui possibili strumenti di tutela dei consumatori finali nei mercati di competenza".

In attesa di conoscere gli esiti di questa indagine, e alla luce del fatto che la gestione dei Big Data è affidata ad una platea circoscritta di grandi aziende operanti, soprattutto, attraverso Internet, si potrebbe pensare di affiancare i necessari interventi regolamentari anche a delle efficaci forme di auto-regolamentazione.

Concludendo, quindi, possiamo affermare che all'avvento di questi nuovi mercati in continua evoluzione genera come effetto che le Autorità Amministrative Indipendenti debbano affrontare delle sfide continue per stare al passo con detti mutamenti.

Ma non solo.

Si richiede anche che lavorino di concerto l'una con l'altra affinché si possa produrre il miglior risultato, in termini di tutele, per i soggetti che operano nell'ecosistema digitale.

Lo stesso Presidente Cardani ha recentemente affermato come "sia necessario un approccio multidisciplinare ai Big Data, sia a livello nazionale che internazionale, capace di racchiudere in un unico intervento complessivo e coordinato le tutele di fondamentali diritti individuali e collettivi in materia di *privacy*, concorrenza, e di tutela degli utenti". Secondo lui, infatti, il trattamento dei Big Data, pur rappresentando un notevole patrimonio informativo, "comporta specifici rischi per la tutela della riservatezza delle persone, tenuto conto anche del fatto che, grazie alle nuove tecnologie e alle tecniche di analisi, elaborazione ed interconnessione dei dati, risulta in molti casi possibile re-identificare un individuo attraverso informazioni apparentemente anonime"[277].

La vicenda della rete, quindi, come già osservato illustre ed attenta dottrina, obbliga ad un ripensamento di categorie che sembravano consolidate e ad una elaborazione di principi nuovi, poiché "le trasformazioni determinate dalla tecnologia possono essere comprese, e governate, solo se si è capaci di mettere a punto strumenti «prospettici»"[278].

2. L'EVOLUZIONE NORMATIVA IN CORSO E LA NECESSITÀ DI STRUMENTI FLESSIBILI. POSSIBILI SCENARI DI INTERVENTO DEL REGOLATORE

(Francesca Pellicanò)

---

domanda di informazione online, mettendo in luce le eventuali criticità sotto il profilo del pluralismo informativo".

[277] A tal proposito si rinvia alle ulteriori riflessioni del Presidente Cardani, intervenuto lo scorso 30 giugno alla *FSR Communications & Media Annual Conference*, presso la *Florence School of Regulation*, disponibili al seguente *link*: https://www.agcom.it/documents/10179/7834943/Comunicato+stampa+30-06-2017/9ac8d843-3941-4e4d-9cf3 35a0bad10440?version=1.0.

[278] Cfr. S. Rodotà , *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma, 2014, 23 e *passim*.

A livello europeo, in attesa degli sviluppi che deriveranno dalle attese (e sopra menzionate) iniziative annunciate dal Commissario Mariya Gabriel per i prossimi mesi in tema di *fake news*, che forniranno auspicabilmente linee guida armonizzate, il dibattito intanto prosegue, delineando fondamentalmente due diversi approcci. Da una parte, chi propone di lasciare la risoluzione all'autoregolamentazione, attraverso rimedi proposti dai gestori delle piattaforme *online*, dall'altro i fautori di un intervento legislativo e/o regolamentare che imponga normativamente strumenti e sanzioni. Alcuni esempi sono già attuati con riferimento sia all'uno che all'altro approccio. Sotto il profilo dell'autoregolamentazione, ad esempio, si segnala la *policy* di Facebook, che ha testato negli USA un *tool* che consente, attraverso un sistema di *tagging*, la possibilità per gli utenti che si imbattono in una notizia falsa condivisa sulla piattaforma di segnalarlo. I contenuti così segnalati vengono elaborati dall'algoritmo come poco affidabili e il risalto concesso a questi nella bacheca degli utenti sarà ridimensionato, in attesa che una società indipendente di *fact checking*, certificata ai sensi del IFCN Code[279] verifichi la fondatezza o meno della notizia. Infine, siti di *spam* che creano reiteratamente *fake news* per incentivare le *revenues* pubblicitarie o che le presentano in modo da incoraggiare il *click baiting* si vedranno ridurre gli investimenti pubblicitari e la visibilità.

Dal punto di vista degli interventi legislativi, invece, un esempio eloquente è rappresentato dalla Germania, dove da più parti politiche è stato auspicato un intervento legislativo per introdurre sanzioni nei confronti delle piattaforme *online* che non rimuovano contenuti in violazione del quadro normativo, la "*Legge per il miglioramento dell'applicazione del diritto nei social network (legge NetzDG)*", che prevede l'introduzione di norme giuridiche di conformità per i *social network*. *Ratio* della legge è sollecitare i *social network* (categoria prima ancora non definita a livello normativo) ad un trattamento più rapido ed efficace dei reclami relativi a reati generati dall'odio e ad altri contenuti penalmente punibili e ciò al fine di pervenire alla tempestiva cancellazione dei contenuti illeciti. La norma tedesca circoscrive l'ambito soggettivo ai soli *social network* che abbiano il potere di influenzare l'opinione pubblica, introducendo una soglia *de minimis* di utenti attivi ed escludendo dalla definizione le piattaforme giornalistiche. Sul piano dell'*enforcement*, si evidenzia il presidio sanzionatorio (fino a 5 milioni di euro) che indubbiamente andrà a svolgere un'efficace azione disincentivante rispetto alla violazione degli obblighi introdotti.

L'iniziativa del legislatore tedesco costituisce il primo tentativo di intervento così configurato in Europa è parte dal condivisibile assunto che lasciare che la responsabilità di un intervento sia assunta sulla base di spontanee e volontarie iniziative da parte degli *stakeholder* costituisca una misura insufficiente, tuttavia si ritiene che un approccio eterodiretto, imposto dall'alto, privi l'intervento della celerità e dell'efficacia derivanti da un modello di regolazione più inclusivo, che preveda nella creazione del set minimo di regole anche il coinvolgimento degli operatori stessi. Inoltre, è opinione di chi scrive che l'imposizione di sanzioni pecuniarie dovrebbe essere un'*extrema ratio* in tali casi, premendo assai maggiormente per una fattiva collaborazione con i gestori delle piattaforme che possono, loro soli, garantire una pronta ed efficace azione di rimozione "chirurgica" del contenuto che viola la legge.

Un diverso approccio di un legislatore nazionale è quello francese: la *Loi pour une République numérique* del 2016 impone agli operatori di piattaforme *online* obblighi di informazione corretta, chiara e trasparente (ivi incluse modalità di funzionamento degli algoritmi) affidando alle autorità amministrative competenti, per i rispettivi profili (tra cui il CSA, ovvero il regolatore nazionale in tema di audiovisivo) il compito di monitorare la qualità delle informazioni fornite e, se del caso, di rendere note le infrazioni commesse dalle piattaforme. Inoltre, una recente iniziativa sempre francese è rappresentata dall'intesa raggiunta tra Facebook e alcune tra le più note testate giornalistiche francesi[280], in base al quale sarà elaborato un sistema messo a disposizione degli utenti del *social* che permetterà, grazie a una

[279] Ci si riferisce al codice di principi promosso da IFCN, International Fact Checking Network, i cui sottoscriventi garantiscono un impegno di *fact-checking* improntato a requisiti di imparzialità, trasparenza e completezza dell'informazione http://www.poynter.org/fact-checkers-code-of-principles/.

[280] Ci si riferisce a Le Monde, France-Press, Bfm-Tv, France Televisions, France Medias Monde, L'Express, Liberation e 20 Minutes. I *link* segnalati finiscono raccolti in un portale cui hanno accesso i *media partner*, che possono verificare le informazioni. Se almeno due redazioni stabiliscono che il contenuto è falso, la notizia apparirà agli utenti con un simbolo rosso, menzionando che i *fact-checker* ne contestano la veridicità.

nuova categoria di segnalazione, di rilevare una notizia sospettata di essere falsa. Il regolatore nazionale, l'Autorità per le garanzie nelle comunicazioni, per voce del suo Presidente Cardani, ha esplicitamente affermato, alla presentazione dell'ultima relazione annuale lo scorso luglio, di propendere per un intervento legislativo, che assegni ad AGCom chiari poteri regolamentari per consentirle un effettivo esercizio di tutela nei confronti delle *fake news* [281].

In attesa di eventuali interventi del legislatore nazionale o comunitario, e concordando con quanto espresso dal Presidente AGCom sulla necessità di un chiaro e univoco quadro normativo e regolamentare, è opinione di chi scrive che, nel mentre, sia comunque proficuo incoraggiare un dialogo tra gli attori coinvolti: gestori delle piattaforme, federazioni rappresentative di agenzie o testate nazionali, servizi di media audiovisivi, rappresentanze degli utenti.

Infatti, per stessa ammissione della Commissione europea, spesso l'auto-regolamentazione e la co-regolamentazione possono conseguire i risultati migliori al fine di favorire lo sviluppo di ecosistemi di piattaforme forti e possono consolidare o andare ad integrare la normativa esistente che già disciplina determinate attività delle piattaforme *online*. In attesa di sviluppi normativi *ad hoc* relativamente alle *fake news*, si evidenzia come altre iniziative legislative in corso abbiano già in ogni caso afferenza e rilevanza per i temi che qui ci impegnano.

È il caso del contenuto della proposta di revisione della Direttiva 2010/13/UE sui servizi di media audiovisivi, che prevede, tra l'altro, l'estensione dell'ambito di applicazione della Direttiva anche alle piattaforme di *video-sharing*, chiamate a garantire un rafforzamento della tutela dei minori *online* e a collaborare nell'ambito della *Alliance for a better protection of minors online*[282], al fine di elaborare un codice di condotta per questo settore. Grande è quindi l'impulso dato dalla proposta della Commissione[283] all'auto- e co-regolamentazione: con l'articolo 28-*bis*, relativo alle disposizioni applicabili ai servizi di piattaforma per la condivisione di video, si prevede che, fatti salvi gli artt. 14 e 15 della direttiva sul commercio elettronico, gli Stati membri garantiscono che i fornitori delle piattaforme per la condivisione di video adottino misure adeguate – in base al contenuto in questione, al danno che può causare, alle caratteristiche della categoria di persone da tutelare nonché dai diritti e dagli interessi legittimi coinvolti – per tutelare i minori da contenuti che potrebbero nuocere allo sviluppo fisico, mentale o morale, nonché tutelare tutti i cittadini da contenuti che istighino alla violenza o all'odio. Siffatte misure consistono nel definire e applicare nei termini e nelle condizioni dei fornitori di piattaforme per la condivisione di video i concetti di istigazione alla violenza o all'odio e di contenuto che potrebbe nuocere allo sviluppo fisico, mentale o morale dei minori; istituire e applicare meccanismi affinché gli utenti delle piattaforme per la condivisione di video possano segnalare o indicare al fornitore di piattaforme per la condivisione di video interessato il contenuto conservato sulla sua piattaforma, unitamente a sistemi per verificare l'età degli utenti, per valutare i contenuti; per introdurre sistemi di controllo parentale. Inoltre,

---

[281] Il Presidente dell'AGCom ha motivato tale decisione in ragione della "preoccupazione per l'eccessivo potere delle piattaforme *online*. Ci si chiede, infatti, come sia possibile fidarsi della promessa dei colossi del *web* di sviluppare algoritmi finalizzati a rimuovere le informazioni false e virali se questi stessi colossi sono anche i principali "utilizzatori" gratuiti dell'informazione attraverso i motori di ricerca e la gestione degli algoritmi che determinano la gerarchia delle preferenze. Inoltre, sembra legittimo dubitare che, in assenza di un controllo esterno e terzo, questi operatori siano disponibili a sacrificare i ricchi introiti pubblicitari a favore di costi (tra l'altro indiretti perché danneggerebbero in via diretta gli inserzionisti) per il contenimento dei danni in reputazione. È vero che le soluzioni di controllo ed *enforcement* sono estremamente difficili da attuare, soprattutto perché dovrebbero essere condivise a livello globale, ma è altresì auspicabile che, anche laddove si optasse per soluzioni di autoregolamentazione, queste partano dal basso e consentano la partecipazione dei veri danneggiati dalle notizie false e virali o dalla diffamazione: innanzitutto i consumatori fuorviati e i singoli individui lesi, in secondo luogo l'informazione plurale, garantista e di qualità difesa dalla nostra Carta Costituzionale". Estratto dalla presentazione del Presidente dell'Autorità per le garanzie nelle comunicazioni della Relazione annuale 2017 sull'attività svolta e sui programmi di lavoro, disponibile al *link*: https://www.agcom.it/documents/10179/3058729/Presentazione+del+Presidente+dell%27Autorit%C3%A0.pdf/c117b512-2e21-402f-bdfb-b09e7469bf21

[282] Si veda più diffusamente al seguente *link*: https://ec.europa.eu/digital-single-market/en/news/commission-broker-new-alliance-better-protect-minors-online

[283] Si precisa che l'*iter* legislativo della modifica della Direttiva SMAV è ancora in corso, e che numerosi emendamenti sono stati presentati dal Parlamento europeo e dal Consiglio, che sono attualmente impegnati in trilogo per la prosecuzione dei lavori e il conseguimento di un testo condiviso.

ai fini dell'attuazione di tali misure, gli Stati membri promuovono la co-regolamentazione e si dotano dei meccanismi necessari per valutare l'adeguatezza delle misure di cui ai paragrafi citati, adottate dai fornitori di piattaforme per la condivisione di video, con la garanzia che siano disponibili meccanismi di reclamo e ricorso per la risoluzione delle controversie fra utenti e fornitori di piattaforme per la condivisione di video relativi all'applicazione delle opportune misure.

Un ulteriore tassello è rappresentato da un'altra proposta della Commissione europea, "*Proposta di direttiva del Parlamento europeo e del Consiglio sul diritto d'autore nel mercato unico digitale*" COM (2016) 593 final, il cui articolo 13 si riferisce all'utilizzo di contenuti protetti dal diritto d'autore da parte dei fornitori di servizi della società dell'informazione che conservano e danno accesso al pubblico alle opere o altri contenuti protetti dal *copyright* caricati dai propri utilizzatori. Il comma 1 dell'articolo 13 prevede, in primo luogo, che le piattaforme di condivisione – definite come "[i]*nformation society service providers that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users*" – adottino, in collaborazione con i titolari dei diritti, misure appropriate e proporzionate come, ad esempio, tecnologie volte all'individuazione automatica dei contenuti identificati precedentemente dai titolari stessi. Tale previsione è finalizzata a garantire il corretto funzionamento di accordi di licenza conclusi tra le piattaforme e i titolari dei diritti stabilendo, inoltre, che i fornitori di servizi così definiti diano ai titolari dei diritti adeguate informazioni sul funzionamento e l'implementazione delle tecnologie sopracitate. Ancor più rilevante, a giudizio di chi scrive, il considerando 38 della proposta di direttiva, il quale specifica che, qualora le piattaforme di condivisione dei contenuti, al di là della mera fornitura di attrezzature fisiche, eseguano un atto di comunicazione al pubblico, sono obbligate a concludere accordi di licenza con i titolari dei diritti, a meno che non siano esenti da responsabilità ai sensi dell'art. 14 della direttiva sul commercio elettronico. Preme evidenziare che la proposta di direttiva, pur facendo riferimento, nel suo articolo 13, esclusivamente a soggetti "*that store and provide to the public access to large amounts of works or other subject-matter uploaded by their users*" – tiene a sottolineare, nel considerando in commento, l'importanza di verificare se il fornitore di servizi svolga o meno un ruolo attivo "*including by optimising the presentation of the uploaded works or subject-matter or promoting them, irrespective of the nature of the means used therefor*". Ancora, il medesimo considerando aggiunge che, allo scopo di garantire il funzionamento di qualsiasi accordo di licenza, i fornitori di servizi hanno l'obbligo di adottare tecnologie efficaci, anche nel caso in cui siano esenti da responsabilità ai sensi dell'art. 14 della direttiva sul commercio elettronico.

Un'ulteriore conferma della progressiva maggior focalizzazione sui *provider* e l'attività in concreto da questi esercitata da parte del legislatore europeo, che può altresì valere quale appiglio normativo[284] per fornire strumenti di intervento al regolatore.

Occorre, tuttavia, specificare, in conclusione, come i soli strumenti di *enforcement* non siano certamente idonei, da soli, a fronteggiare il problema delle *fake news* e in generale degli abusi sul (e del) *web*: occorre, infatti, un cambiamento culturale, che può essere perseguito con un forte investimento nella *media* e *digital literacy* (alfabetizzazione mediatica e digitale), fornendo ai cittadini/utenti gli strumenti per informarsi, riflettere sui contenuti e analizzarli criticamente, potendo, quindi, formare compiutamente e correttamente la propria opinione.

3. POTESTÀ DI INTERVENTO DI AGCOM NEL CONTRASTO ALLA DIFFUSIONE DI *FAKE NEWS* E DISINFORMAZIONE *ONLINE*

(Rosaria Petti)

L'Autorità per le garanzie nelle comunicazioni è, come noto, soggetto istituzionalmente preposto dalla sua legge

[284] Con le dovute cautele del caso, essendo anche in tal caso, come per la direttiva SMAV, ancora in corso l'*iter* legislativo che porterà all'adozione definitiva del testo, che non sarà sicuramente esente da modifiche.

istitutiva alla garanzia dell'affidabilità e imparzialità dell'informazione, alla tutela del pluralismo informativo, anche nel suo significato di parità delle condizioni di accesso ai mezzi di informazione (*par condicio*) per le formazioni politiche che competono nell'arena pubblica, su tutti i mezzi di comunicazione, comprese le piattaforme digitali.[285] Come risaputo, l'art. 3 del TUSMAR, impone una serie di prescrizioni stabilendo, tra i principi fondamentali del sistema dei servizi di media audiovisivi, l'obiettività, completezza, lealtà e imparzialità dell'informazione.

Sebbene, quindi, la tutela del pluralismo sia frutto di un principio di portata generale, i poteri di intervento dell'Autorità sono destinati a variare in virtù delle discipline positive settoriali a seconda del destinatario della misura (testate *online*, fornitori di SMAV, intermediari che forniscono servizi di *social network* o motori di ricerca, ecc.). L'art. 7 del TUSMAR, ad esempio, prevede per l'attività di informazione una serie di previsioni dettate però nell'ambito dell'informazione radiotelevisiva, la quale deve garantire "*la presentazione veritiera dei fatti e degli avvenimenti, in modo tale da favorire la libera formazione delle opinioni*". Il principio, espressamente coniato per fornitori di media audiovisivi e radiofonici ed essenzialmente per gli editori, richiede, per una sua estensione, di ispirarsi a nozioni giuridiche funzionali piuttosto che a interpretazioni letterali. In tal senso, ad esempio, con riferimento alla stampa, si potrebbe prescindere dalla piattaforma tecnologica distributiva dei contenuti editoriali aventi natura di notizie, articoli o programmi di informazione.

In ragione di tali considerazioni il percorso regolamentare intrapreso dall'Autorità per circoscrivere il fenomeno della disinformazione *online* si preannuncia impervio. Sicuramente un primo passo è rappresentato dall'attività di studio realizzata nell'ambito della richiamata indagine conoscitiva avviata con delibera 309/16/CONS, i cui esiti saranno presumibilmente pubblicati nell'anno in corso.

In termini pratici, però, la risoluzione del problema appare ancora lontana. Se, infatti, con riguardo ai mezzi di informazione tradizionale la declinazione dei principi in materia di pluralismo è ben tracciata, per quelli digitali non può rilevarsi altrettanto. Certo un'apertura si è manifestata già con gli interventi legislativi del 2012 che hanno ampliato anche all'*online* l'ambito di applicazione di alcuni strumenti regolatori. Al riguardo, si pensi all'inserimento nel Sistema Integrato delle Comunicazioni anche dei ricavi derivanti da "*pubblicità on line e sulle diverse piattaforme*", oppure all'estensione dell'obbligo di iscrizione al Registro degli Operatori della Comunicazione alle concessionarie di pubblicità "*sul web e altre piattaforme digitali fisse o mobili*". Tali interventi sembrano mostrare l'intento, a livello legislativo, di rafforzare i poteri dell'Autorità anche con riguardo al settore *online*.

In tale ottica poi, l'AGCom, l'AGCM e il Garante Privacy nella richiamata Indagine congiunta si prefiggono di esaminare le modalità di approvvigionamento e diffusione delle notizie, sempre più spesso collegate a intermediari digitali, quali *social network* e motori di ricerca. Come si è potuto evidenziare nei paragrafi precedenti, questi soggetti utilizzano i dati personali come *asset* strategico secondo la logica dei mercati multiversante e attraverso forme di profilazione e definizione di algoritmi che possono incidere sia sul mantenimento della *net neutrality* tra operatori di rete e fornitori di contenuti, sia sulla pluralità della rappresentazione di fatti e opinioni presso l'utente alimentando camere di risonanza e false percezioni di determinati fenomeni.

L'Indagine si presenta certamente come strumento di dialogo e scambio di *best practice* tra i principali attori del sistema. L'obiettivo resta quello di conciliare il *trade-off* tra il valore commerciale dell'informazione e il rispetto di diritti individuali e collettivi fondamentali quali la *privacy*, la tutela della concorrenza e le garanzie del pluralismo informativo.

Più diffusamente il tema della disinformazione ha aperto un dibattito anche sul fronte legislativo. Notevoli, però, sono

[285] Sul tema delle *fake news* e in particolare sull'intervento dell'Autorità si rinvia alle riflessioni del Presidente Cardani, intervenuto, lo scorso 5 maggio, al convegno su *Fake news e allarme sociale: responsabilità, non censura*, organizzato a Milano dall'Osservatorio "Giordano Dell'Amore" sui rapporti tra diritto ed economia. In quella sede il Prof. Cardani, nel qualificare AGCom come soggetto istituzionalmente preposto dal quadro costituzionale e legislativo alla garanzia del pluralismo informativo su tutti i mezzi di informazione, ha rilevato che frammentarietà delle discipline settoriali applicabili nei confronti di diverse categorie di soggetti che concorrono al fenomeno delle *fake news*, condiziona la scelta dei rimedi da parte del regolatore.

state le polemiche che hanno investito il disegno di legge recentemente presentato al Senato[286] che intende introdurre un sistema essenzialmente penalistico prevedendo sanzioni pecuniarie, o finanche detentive se le notizie false diventano mezzo per campagne di odio o minano i processi democratici. Il d.d.l. prevede altresì una costante attività di monitoraggio in capo ai gestori delle piattaforme informatiche sui contenuti da queste diffusi. Attività che però sembra difficilmente coordinarsi con la direttiva *e-commerce* del 2000 e con il relativo decreto di recepimento a livello nazionale (d.lgs. 70/2003) che, come noto, escludono a carico di questi un obbligo generale di sorveglianza. Ulteriori critiche sono state sollevate nei confronti del d.d.l. per la previsione che affiderebbe a soggetti essenzialmente privati il controllo sui contenuti diffusi in Rete.

In attesa del perfezionamento dell'*iter* legislativo, resta però di fondamentale rilevanza il ruolo che Governo e Parlamento, nell'esercizio delle rispettive funzioni, rivestiranno nel processo europeo di riforma della direttiva SMAV, su cui si veda più diffusamente il paragrafo precedente. La transnazionalità del fenomeno richiede, infatti, un approccio sovranazionale in grado di superare, per quanto possibile, l'attuale frammentazione dei regimi giuridici applicabili alle diverse tipologie di piattaforme che distribuiscono contenuti editoriali e audiovisivi.

BANCA D'ITALIA

(Antonio Affinito, Giorgia Biferali, Vincenzo Floccari)

[286] Si tratta del disegno di legge n. 2688, recante "Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul *web* e incentivare l'alfabetizzazione mediatica". Le previsioni prevedono l'introduzione nel codice penale dell'art. 656-*bis* con il quale è fissata un'ammenda per coloro che pubblicano o diffondono false notizie. In caso, invece, di procurato allarme o di danni a interessi e ordine pubblico, la proposta prevede, con l'inserimento nel codice penale dell'art. 265-*bis* e dell'art. 256-*ter*, oltre all'ammenda, anche una sanzione che sconfina in pene detentive.

I Big Data nel settore bancario: tra opportunità e rischi per i consumatori

(Antonio Affinito, Vincenzo Floccari)

Il settore bancario, come tutti i comparti produttivi, negli ultimi anni ha subito le conseguenze dello sviluppo tecnologico. Ingenti quantità di dati, ogni giorno, vengono conservate e analizzate dalle banche e da altri soggetti che, pur non essendo autorizzate all'esercizio dell'attività bancaria, sfruttano il loro Know how *per fornire nuovi prodotti e servizi. Si tratta di un fenomeno complesso, che necessariamente non può essere confinato all'interno dei confini nazionali. Le autorità di vigilanza, la Banca d'Italia, la Bce, l'Eba, l'Esma, sono davanti a una sfida epocale: l'unione tra finanza e tecnologia genera una nuova forma di globalizzazione caratterizzata dalla scomparsa dei mercati nazionali.*

Per l'industria dei servizi bancari il futuro è di fatto già segnato e non investire nelle nuove tecnologie e nel Big Data analytics *e* management *significa sparire senza nemmeno lasciare traccia. Ma se questa è la situazione per le banche, anche i regolatori sono chiamati ad uno sforzo: trovare un punto di equilibrio tra rischi e benefici; garantire protezione ai consumatori e al mercato senza contrastare l'innovazione e la competitività.*

SOMMARIO: 1. INTRODUZIONE. – 2. LA DESCRIZIONE DEL FENOMENO: I BIG DATA. – 3. RISCHI E OPPORTUNITÀ DERIVANTI DALL'UTILIZZO DEI BIG DATA NEL SETTORE BANCARIO. – 4. LA LEGISLAZIONE ATTUALE E L'AZIONE DELLE AUTORITÀ. – 4.1. L'ATTIVITÀ DI VIGILANZA BANCARIA E LE FINTECH: UNA QUESTIONE APERTA.

1. INTRODUZIONE

La rivoluzione digitale, iniziata circa 25 anni fa con la creazione del primo sito *web*, ha modificato radicalmente la vita delle persone e il loro modo di comunicare, incidendo, in modo diverso, su tutti i comparti produttivi.

Il settore bancario non poteva essere esente da questa trasformazione. Anche se l'utilizzo della tecnologia non può essere considerato una novità per tale comparto[287], lo sviluppo tecnologico che l'umanità sta sperimentando nell'ultimo decennio rappresenta, senza alcun dubbio, un elemento di forte discontinuità tale da meritare un serio approfondimento.

Il citato sviluppo pare essere supportato da tre fattori principali. Il primo di questi deve essere individuato nell'enorme disponibilità di dati e informazioni oggi disponibili grazie anche all'utilizzo dei cc.dd. *social network* come Facebook, Instagram, ecc.

Il secondo fattore, invece, è rappresentato dalla circostanza che lo sviluppo della rete internet consente oggi a chiunque di trasmettere enormi quantità di dati, in modo più o meno sicuro, ma senza l'utilizzo di particolari e costose reti.

Il terzo ed ultimo fattore, infine, deve essere individuato nello sviluppo di nuovi *software* e *hardware* sempre più po-

[287] Gli studi effettuati da Banca d'Italia, relativi agli anni tra il 1989 e il 2000, avevano già rilevato che gli investimenti in capitale tecnologico hanno consentito un aumento della produttività del sistema bancario compreso tra l'1,3 e l'1,8 per cento all'anno.

tenti ed economici, il quale ha consentito il vertiginoso calo del costo dell'elaborazione automatica dei dati.

Tali fattori non potevano non incidere in maniera significativa anche sul sistema bancario, in considerazione del fatto che mentre in precedenza gli investimenti tecnologici, richiedendo grandi stanziamenti di capitale, contribuivano a mantenere elevate le barriere all'ingresso nel mercato, le nuove tecnologie, per i motivi sopra descritti, consentono a imprese, anche piccole, ma innovatrici, di offrire servizi fino a pochi anni fa di esclusivo appannaggio del sistema bancario[288].

Queste nuove imprese, note come FinTech, sfruttando le potenzialità della rete internet e dei dati da essa messi a disposizione, offrono servizi di pagamento, di investimento, di consulenza e di finanziamento ad alta intensità tecnologica ed a prezzi competitivi.

Lo sviluppo di tali nuove realtà è ancora in essere, soprattutto in Italia, e a chi scrive pare ancora azzardato tentare di valutare quanto la concorrenza di queste nuove realtà imprenditoriali possa sottrarre quote di mercato, nonché margini di profitto, alle banche tradizionali.

Tuttavia, ciò che pare certo già ora è che la stessa esistenza delle imprese FinTech, rappresenta un forte stimolo all'innovazione per l'industria bancaria, chiamata oggi ad utilizzare appieno il patrimonio informativo potenzialmente disponibile, elaborandolo nel tentativo di creare nuovi prodotti o nuovi canali distributivi, così come in realtà le grandi realtà digitali già stanno facendo.

Pare opportuno segnalare, infatti, che lo sviluppo delle tecnologie sta comportando, da un lato, la creazione di start-up che operano nel sistema finanziario tramite l'utilizzo e lo sfruttamento di nuove tecniche, ma, dall'altro lato, sta causando l'ingresso in tale settore di grandi *player* mondiali quali Amazon, Alibaba, Facebook, Google, Yahoo, Apple ecc., che, sempre nel tentativo di aumentare i margini di profitto, cercano di utilizzare appieno, mediante le innovative tecnologie di cui dispongono, le ingenti informazioni accumulate nello svolgimento dell'attività d'impresa caratterizzante il loro *core business*, per offrire servizi finanziari a condizioni migliori rispetto a quelle praticate dalle imprese istituzionalmente dedicate a tali attività.

Non è, pertanto, un caso che negli ultimi anni si è assistito all'ingresso nel mercato dei pagamenti di Alibaba, colosso del *e-commerce* cinese, che ha attivato un proprio circuito di pagamento, Alipay, raggiungendo in pochissimo tempo la quota di 400 milioni di clienti[289].

La stessa Amazon, già dal 2011, ha creato Amazon lending, una piattaforma di erogazione di prestiti alle piccole e medie imprese presenti, in qualità di rivenditori, sulla piattaforma.

Amazon eroga, così, prestiti a breve termine (durata massima 12 mesi) per importi che vanno da un minimo di 1.000 dollari a un massimo di 750 mila, con tassi di interesse che spaziano dal 6% al 17%.

Nonostante i tassi non particolarmente contenuti, il colosso di Seattle ha annunciato di aver toccato i 3 miliardi di dollari concessi in prestito dalla data di fondazione, di cui 1 miliardo solo nell'ultimo anno a più di 20.000 clienti con sede in Usa, Gran Bretagna e Giappone.

Si tratta di un meccanismo ad invito in forza del quale è Amazon a selezionare le imprese cui concedere i finanziamenti, in base ad algoritmi interni che analizzano la popolarità dei prodotti di un venditore, la frequenza con cui si esauriscono le scorte e i cicli d'inventario.

---

[288] Per un approfondimento, L. Casolaro e G. Gobbi, 2007 "*Information Technology and Productivity Changes in the Banking Industry*", Economic Notes, Vol. 36.

[289] C. Scozzari, su *https://it.businessinsider.com/fintech-la-guerra-alle-banche-tradizionali-parte-dalla-cina-con-alibaba-tencent-e-baidu/*

Ciò che colpisce è che per tale attività Amazon utilizza dati e informazioni relativi a più di 2 milioni di commercianti per identificare quelli che ritiene meritevoli di credito.

Un'attività simile, inoltre, è già posta in essere da Paypal che ha annunciato nel mese di maggio di quest'anno di aver rilasciato più di 3 miliardi di dollari in prestiti a più di 115.000 imprese in tutto il mondo attraverso il programma PayPal Working Capital lanciato nel 2013. Anche in questo caso, la società americana seleziona i propri clienti elaborando i dati ottenuti fornendo servizi di pagamento[290].

È del tutto evidente, dunque, come l'elaborazione di quelli che vengono definiti Big Data sia oggi un fenomeno di rilevanza mondiale rispetto al quale le Autorità di vigilanza non possono mostrarsi indifferenti.

Con specifico riferimento, invece, al mercato italiano occorre segnalare che l'ultimo rapporto annuale sul *Digital Economy and Society Index* (in breve "DESI") pubblicato dalla Commissione Europea colloca l'Italia al venticinquesimo posto su ventotto paesi europei per grado di digitalizzazione complessivo. Con specifico riferimento all'utilizzo di servizi di *e-banking*, il rapporto segnala che solo il 42% degli italiani ne usufruisce, contro una media di fruitori europei pari al 59%[291].

Sul fronte del capitale umano è dato riscontrare, in particolare, l'assenza di competenze digitali elementari: ancora pochi sono gli specialisti Ict e i laureati nelle discipline scientifiche[292.]

In tale contesto, dunque, è possibile rilevare che in Italia mentre la digitalizzazione nei servizi bancari per la famiglia è più sviluppata dei servizi *online* per le imprese, la concorrenza dei grandi *player* mondiali come Google, Amazon ecc. riguarda attualmente solo i servizi di pagamento, essendo lo sfruttamento dei Big Data molto limitato.

Ciò nonostante, in considerazione del fatto che l'utilizzo delle nuove tecnologie consente una diminuzione dei costi, soprattutto nel settore della distribuzione, nonché la possibilità di migliorare la qualità dell'offerta, anche alla luce degli investimenti pubblici e privati programmati nella c.d. banda larga, il divario italiano con il resto d'Europa pare destinato a ridursi nei prossimi anni.

Ciò chiarito in via generale, appare ora opportuno fornire una definizione del fenomeno e, poi, valutare quale siano i vantaggi e quali le criticità rinvenibili nell'utilizzo dei Big Data da parte delle imprese che esercitano attività bancaria e finanziaria. sCiò al fine di valutare, per un verso, l'adeguatezza della normativa attuale e, per altro verso, l'atteggiamento che l'Autorità di vigilanza è chiamata ad assumere.

2. LA DESCRIZIONE DEL FENOMENO: I BIG DATA

Con il termine Big Data si fa riferimento, almeno in ambito bancario, al fenomeno per cui elevati volumi di dati[293], prodotti da un'infinita serie di fonti, vengono elaborati ad alta velocità, spesso in tempo reale, tramite l'utilizzo di strumenti IT come potenti processori, *software* e algoritmi[294].

---

[290] S. Soper, S.Wang, *Amazon's Lending Business for Online Merchants Gains Momentum,* su *https://www.bloomberg.com/news/articles/2017-06-08/amazon-s-lending-business-for-online-merchants-gains-momentum.*

[291] Tale dato colloca il nostro paese al 23 posto in Europa per utilizzo dei servizi di *e-banking*.

[292] Tutti dati sono disponibili su *c.europa.eu/newsroom/document.cfm?doc_id=43020*

[293] A seconda della loro complessità, i dati possono essere strutturati, semi-strutturati o non strutturati.

[294] Definizione tratta da *Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions* a cura di EBA, EIOPA, and ESMA, pubblicata il 19 dicembre 2016 e reperibile su *https://www.esma.europa.eu/press-news/consultations/joint-committee-discussion-paper-use-Big-Data-financial-institutions*. In tale documento, si legge che "*The European Commission Communication on Data Driven Economy used the term "Big Data" to refer to situations where high volumes of different types of Data produced with high velocity from a high number of various types of sources are processed, often in real time, by IT tools (powerful processors, software and algorithms*)".

Le fonti da cui le banche estrapolano tali dati possono essere sia interne[295], come ad esempio i dati relativi ai pagamenti effettuati dai clienti, i *database* dei reclami presentati, le informazioni fornite dai clienti all'atto della registrazione, sia esterne, come notizie, *social media*, dati forniti da altri settori finanziari.

È il caso di evidenziare, inoltre, che proprio tali ultime fonti, che sono in rapida crescita grazie all'utilizzo da parte degli individui dei *social network*[296], richiedono un' attenta valutazione in ordine sia alle modalità di protezione dei dati sia alla stessa legittimità del loro utilizzo[297].

Il settore bancario al momento utilizza i Big Data nell'ambito dei servizi ai consumatori sia per fornire prodotti contabili, sia per valutare il merito creditizio dei consumatori.

Grande rilevanza, inoltre, assumono i Big Data nell'ambito dell'attività di *marketing*[298], allo scopo di valutare possibili segmentazioni di mercato, l'idoneità dei prezzi dei servizi forniti, nonché per valutare la possibilità di creare nuovi prodotti o fornire servizi complementari. Nell'ambito dei servizi di investimento, le relative decisioni sono già prese attraverso l'utilizzo di algoritmi che analizzano grandi volumi di dati a elevata velocità, allo scopo di indirizzare le strategie di investimento verso un aumento dei profitti cercando di minimizzare i rischi[299].

In ultimo, l'attività di elaborazione dei dati e la connessa profilazione dei consumatori, fornisce un forte ausilio alle strutture, all'interno del settore creditizio, che si occupano di sicurezza e prevenzione frodi.

È del tutto evidente, dunque, l'enorme valore dei Big Data in ambito finanziario, il quale, come è stato correttamente evidenziato, è troppo grande per essere ignorato[300].

Elencate, a grandi linee, le attività in cui gli operatori bancari utilizzano ed elaborano i Big Data, occorre ora valutarne le utilità e le possibili criticità che da ciò ne possono derivare, sia per i consumatori sia per le imprese esercenti attività bancaria.

3. RISCHI E OPPORTUNITÀ DERIVANTI DALL'UTILIZZO DEI BIG DATA NEL SETTORE BANCARIO

[295] Sono tali ad esempio gli id o dettagli di contatto forniti dai clienti, la cronologia di navigazione sul sito, i dati professionali, gli interessi personali, i dati finanziari e di pagamento, le informazioni nelle negoziazioni effettuate con carte di credito, i dati raccolti per valutazioni di idoneità o per valutazioni del merito di credito.

[296] Così come affermato nel *Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions*, in cui si legge che "*At the same time, it is important to stress that Data sources are expanding exponentially and certain institutions appear to already have access to an increasing set of sources. Data obtained through the internet of things, sensors, etc. will be more and more used*"

[297] Con specifico riferimento a tali fonti esterne, inoltre, sussistono anche rischi di inesattezza se non falsità delle informazioni estratte.

[298] Un *trend* crescente tra le istituzioni finanziarie, infatti, è quello di utilizzare la profilazione della clientela tramite i Big Data, per fare offerte mirate e personalizzare i prodotti e i servizi.

[299] Nel Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions, si legge, così che "*for example, investment strategies based on Big Data analytics can incorporate market changes continuously, to provide real-time, personalised services and feedback to consumers, reflecting relevant market developments and thus more tailored to consumers' needs - Artificial Intelligence (AI) technology started to being applied by certain asset managers, with advanced machine learning turning Big Data into algorithmic trades and strategies, Digitizing Intelligence: AI, Robots and the Future of Finance, 3 March 2016. KPMG AIMA MFA Global Hedge Fund Survey (Transformative change - How innovation and technology are shaping an industry, 2016) indicate that a significant number of hedge fund managers (58% of those interviewed) consider that artificial intelligence/machine learning will have a "medium to high" impact on the sector over the next five years; 32% of managers reported they are already using predictive analytics to uncover new trends and identify new opportunities*".

[300] In tal modo è stato definito da P. Simon, in *Too Big to ignore. The Business Case for Big Data*, Wiley, March 18, 2013.

Con riferimento a tali ultimi soggetti, appare evidente che l'elaborazione dei dati può incidere sulla qualità dei processi e dei servizi offerti, producendo un aumento dei ricavi[301] o comunque un inferiore livello dei costi[302].

Dal punto di vista della qualità del merito creditizio, inoltre, tramite l'analisi dei dati, le banche potrebbero valutare il merito di chi chiede un finanziamento in modo più preciso e raffinato, prevenendo e/o diminuendo il rischio di insolvenze.

Anche i consumatori potrebbero trovare benefici dall'utilizzo dei Big Data, soprattutto grazie alla possibilità per quest'ultimi di ottenere prodotti e servizi personalizzati.

Le banche, infatti, tramite l'elaborazione delle informazioni di cui dispongono, potrebbero essere in grado di attuare più efficaci processi di *governance* dei prodotti, per definire mercati più conformi ai bisogni dei consumatori, offrendo determinati prodotti solo a coloro che mostrano interesse alle finalità e alle caratteristiche di quel determinato servizio[303].

Una maggiore elaborazione delle informazioni, inoltre, potrebbe facilitare la fornitura di servizi di consulenza più precisi, in modo tale che vi sia maggiore corrispondenza tra il profilo del cliente e gli investimenti consigliati[304].

La stessa corretta valutazione del merito di credito, poi, potrebbe essere in grado di far ottenere al consumatore meritevole condizioni contrattuali più favorevoli rispetto a quelle praticate dall'impresa bancaria alla massa indifferenziata.

Parimenti, l'ottimizzazione dei processi, comportando una riduzione dei costi a carico della banca, potrebbe produrre un proporzionale calo del prezzo pagato dal consumatore[305]. L'utilizzo dei Big Data, inoltre, pare essere in grado di facilitare la gestione finanziaria personale dei consumatori, aumentando la consapevolezza di questi in relazione ai loro comportamenti, alla propria propensione alla spesa, nonché alla propria situazione finanziaria.

Tramite le applicazioni basate sui Big Data, dunque, le banche potrebbero fornire in tempo reale informazioni per aiutare i consumatori a prendere decisioni più informate sulle proprie spese nonché sugli investimenti.

L'utilizzo delle informazioni in possesso delle banche, ancora, potrebbe aumentare il livello di interazione tra imprese bancarie e consumatori, valorizzando il coinvolgimento di quest'ultimi nella progettazione di migliori prodotti e servizi bancari[306].

Da un punto di vista generale, inoltre, elaborando i Big Data, le istituzioni bancarie possono meglio analizzare i mercati

---

[301] Le banche, così, potrebbero aumentare i loro ricavi vendendo i dati che posseggono ad altre parti interessate.

[302] L'utilizzo di Big Data, infatti, potrebbe ridurre i costi operativi delle imprese nel settore della produzione, del *marketing*, della gestione reclami, nonché della distribuzione. Al riguardo si segnala, infatti, che anche se tali nuovi tecnologie necessitano di un cospicuo investimento iniziale, una volta raggiunto lo sviluppo del sistema, finanziariamente le banche possono trarre vantaggio da economie di scala attraverso una potenziale clientela più ampia. Inoltre, anche se alcuni dati potrebbero diventare obsoleti, altri tipi di dati potrebbero essere utilizzati e riutilizzati più volte, offrendo l' opportunità alle imprese di sviluppare nuovi servizi o attività.

[303] Si tenga presente che la stessa MIFID II agli artt. 16- 24 richiede agli istituti finanziari di sviluppare prodotti che rispondano all' esigenze di un mercato target identificato dei consumatori finali. Sullo stesso punto paiono conformi anche le line guida dell' EBA "*on product oversight and governance*" e la Joint Position of the European Supervisory Authorities on Manufacturers' Product Oversight & Governance del 2013.

[304] Le istituzioni finanziarie, inoltre, potrebbero assicurare servizi di consulenza o di gestione del portafoglio sempre adeguati nel tempo, potendo tenere in considerazione in ogni momento, e senza costi aggiuntivi, i cambiamenti di mercato o del profilo dei consumatori senza significativo costi aggiuntivi.

[305] Al riguardo si segnala che le associazioni dei consumatori hanno espresso dubbi al riguardo. Sul tema l'EBA nel *Report on innovative uses of consumer Data by financial institutions* del giugno 2017 segnala che tali associazioni "*expressed doubts that reductions in costs achieved by financial institutions would be passed on to consumers*".

[306] Cfr. *Big Data*, Time *for a lean approach in financial services*, Deloitte, reperibile all'indirizzo *https://www2.deloitte.com/it/it.html*. Pare evidente, infatti, l'utilità dell'interazione dei consumatori con i propri fornitori, che potrebbero tempestivamente adattare i loro prodotti ai *feedback* ricevuti dai primi.

a sostegno delle decisioni di investimento nei mercati finanziari.

La grande massa di dati di cui le banche dispongono, potendo essere utilizzata per la condivisione istantanea delle informazioni in tutto il mercato finanziario, è in grado anche di aumentare la trasparenza all'interno delle istituzioni, fornendo ai *decision maker* una visione migliore e promuovendo un mercato più efficiente.

Ma oltre che incidere sull'efficienza, i Big Data, se adeguatamente sfruttati dalle banche, possono anche far aumentare la sicurezza delle transazioni e del mercato dei servizi di pagamento.

Tali istituzioni finanziarie, infatti, possono utilizzare l'analisi dei Big Data per individuare potenziali attività commerciali illegali e individuare frodi o abusi di mercato.

Utilizzando i dati relativi alle transazioni con carta di credito[307], ad esempio, le imprese che esercitano l'attività bancaria potrebbero identificare le possibili transazioni sottoposte al rischio frode, prevenendo danni ai consumatori, nonché diminuendo le perdite che le stesse banche avrebbero sostenuto[308].

A fronte di tali benefici, tuttavia, occorre segnalare che, per alcuni consumatori, l'elaborazione di grandi volumi di dati da parte delle banche potrebbe comportare elevate criticità.

Se è vero, infatti, che un attenta valutazione potrebbe recare benefici ai consumatori particolarmente meritevoli, la stessa potrebbe causare, per i consumatori indesiderati, una maggiore limitazione all'accesso al mercato del credito[309].

La stessa modalità di determinazione dei prezzi, basata sulle particolari caratteristiche del singolo consumatore e sui propri comportamenti, potrebbe violare il generale obbligo di equità e di non discriminazione posto a carico delle istituzioni finanziarie[310]. Ciò sarebbe più evidente nelle ipotesi in cui i dati elaborati per individuare le caratteristiche dei singoli consumatori siano fallaci o per la non affidabilità della fonte o per il differente livello di utilizzo delle nuove tecnologie da parte dei soggetti citati, o, infine, per il rifiuto da parte del consumatore a condividere le proprie informazioni personali con gli istituti bancari[311].

La distribuzione di servizi e prodotti estremamente personalizzati, inoltre, potrebbe rendere difficile la comparabilità, rendendo sempre più complicato per i consumatori confrontare un'offerta con un'altra, con un impatto distorsivo sulla concorrenza all'interno del settore bancario.

La stessa influenza, inoltre, potrebbe avere un'eccessiva profilazione del consumatore che, nell'ipotesi in cui i dati non fossero liberamente trasferibili, potrebbe causare una riduzione della sua possibilità di cambiare fornitore.

Un trattamento eccessivo di Big Data, per di più, potrebbe sottoporre i consumatori a un *marketing* aggressivo, con maggiori rischi di subire pratiche di *cross-selling*[312] .

Le banche, infatti, possono utilizzare i Big Data per monitorare e prevedere le necessità e le preferenze dei consumatori verso alcuni prodotti e servizi, al fine di offrire sconti mirati e servizi aggiuntivi.

---

[307] Combinandoli con altre banche dati esterne (ad esempio i dati forniti dalle pubbliche autorità, i modelli di spesa, le pregresse attività in internet e sui social media, le informazioni sulla geolocalizzazione).

[308] Si veda anche l'art. 94 della PSD2 che invita gli Stati membri a consentire l'elaborazione dei dati da parte dei prestatori di servizi di pagamento, quando necessario per la salvaguardia la prevenzione, la ricerca e l'individuazione di frodi di pagamento.

[309] Rischio rilevato anche dal FSUG Paper *on Assessment of current and future impact of Big Data on Financial Services*, June 2016.

[310] Rischio paventato in the *European Parliament Report New Trends and Key Challenges in the Area of Consumer Protection or the Report from Office of Fair Trading, Personalised Pricing: Increasing Transparency to Improve Trust in the Market*, May 2013.

[311] Si pensi all'ipotesi in cui due consumatori richiedano un finanziamento alla stessa banca, avendo in realtà lo stesso merito creditizio, ma un differente livello di profilazione. La banca, in questo caso, è in grado di elaborare i dati solo di uno dei due, perché l'altro non utilizza *social media* o non è registrato o profilato in nessuna piattaforma. In tale circostanza, l'operatore bancario tenderà a proporre condizioni migliori al soggetto profilato, quindi conosciuto.

[312] Con tale espressione, ci si riferisce ad una strategia di vendita di un prodotto o servizio in più rispetto a quanto richiesto dal cliente, dopo aver consolidato e confermato la vendita del primo.

Parimenti, nel tentativo di creare sinergie offrendo ai partner commerciali dati personali dei propri clienti, le banche potrebbero sottoporre i consumatori al rischio di scontrarsi con un'imprevista ed eccessiva quantità di pubblicità non richiesta[313].

A ciò si aggiunga che uno dei pericoli maggiori conseguenti al trattamento di grandi quantità di informazioni da parte dell'imprese bancarie attiene all'asimmetria informativa da declinare a totale svantaggio dei consumatori.

Ma forse, il rischio maggiore, a parere di chi scrive, è legato ai possibili difetti di funzionamento degli strumenti che analizzano e elaborano i Big Data.

L'attività di acquisizione, conservazione ed elaborazione di tali informazioni, infatti, si caratterizza per essere potenzialmente sottoposta al rischio di errore in ogni sua fase.

Si pensi all'ipotesi di un algoritmo difettoso o di una notizia errata o palesemente falsa, c.d. *fake news*, acquisita tuttavia come vera. In tali circostanze, le decisioni prese in base a tali informazioni potrebbero manifestarsi come palesemente errate, perché minate nei presupposti. Ciò potrebbe rilevarsi ancora più dannoso nelle ipotesi in cui né i consumatori[314] né le banche siano in grado di rilevare l'errore o comunque la fallacità del dato.

In tali circostanze, il rischio di danni diretti per i consumatori e l'aumento dei costi per le banche, anche in termini di reputazione, inoltre, è direttamente proporzionato al livello di concentrazione e centralizzazione dei fornitori di dati o di *storage* o *analytics providers*.

Particolari rischi, inoltre, possono rilevarsi nell'ipotesi di *cyber* attacco. Anche se le banche dovrebbero disporre di sistemi e meccanismi di controllo adeguati, non è infatti possibile escludere la possibilità di perdita o manomissione dei dati a seguito di attività fraudolente, con possibili danni per i consumatori.

4. LA LEGISLAZIONE ATTUALE E L'AZIONE DELLE AUTORITÀ

Dopo aver indicato le opportunità e soprattutto le criticità che il trattamento dei Big Data da parte delle banche può comportare, pare necessario a questo punto verificare se i rischi sopra esposti possano comunque essere controllati dalla normativa oggi in vigore.

Al riguardo deve necessariamente farsi riferimento alla disciplina adottata dal legislatore dell'Unione, in considerazione del fatto che la materia impone una regolamentazione che travalichi i confini di ciascun stato membro.

Sul tema, l'analisi non può non partire dal regolamento EU 2016/679 in materia di Protezione dei Dati Personali, c.d. GDPR[315].

Tale testo normativo, che entrerà in vigore il 25 maggio 2018 è, a parere di chi scrive, particolarmente utile nel prevenire o risolvere molti dei rischi che in precedenza sono stati individuati.

È indubbio che le norme dettate dal GDPR siano direttamente applicabili anche alle attività di tenuta e elaborazione dei Big Data da parte delle banche, atteso che l'articolo 29 *data protection working party*, precisa che i principi di pro-

[313] Nel Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions, si legge che "*These practices should in any event be considered against some of the more general Data protection and consumer protection requirements mentioned above*".

[314] I consumatori potrebbero, ad esempio, non essere consapevoli del fatto che i dati personali vengono utilizzati per finalità diverse rispetto a quelle per cui sono stati forniti.

[315] *Regulation (EU)* 2016/679 *of the European Parliament and of the Council of* 27 *April* 2016 *on the protection of natural persons with regard to the processing of personal Data and on the free movement of such Data, and repealing Directive* 95/46/EC

tezione ivi previsti si applicheranno a qualsiasi informazione relativa a persona fisica identificabile, a prescindere dal fatto che tale informazione sia resa disponibile al pubblico o meno[316].

Come appena evidenziato, quindi, il semplice fatto che tali dati siano stati resi pubblici e disponibili non comporta un'esenzione dalla disciplina detta in materia di protezione dei dati personali.

Facendo applicazione dei principi dettati dal regolamento del 27 aprile 2016, è possibile, se non escludere, quanto meno limitare i rischi riguardanti le asimmetrie informative.

Il legislatore dell'Unione, infatti, richiede, in primo luogo, che il trattamento dei dati personali sia trasparente[317].

Ciò si traduce nel diritto di ciascuno di essere informato, in modo chiaro, sui fini per cui i suoi dati vengono raccolti e trattati, sulla possibilità che gli stessi possano essere condivisi con terzi, nonché sull'eventualità che la banca raccolga dati provenienti da altre fonti[318].

Tale disponibilità dei dati a favore dei consumatori, infine, può giungere fino alla possibilità per questi di richiederne la cancellazione quando la conservazione non si giustifica con lo scopo per cui gli stessi dati sono stati prestati[319] o di opporsi al trattamento quando le informazioni vengono utilizzate per scopi di *marketing*[320].

Tale ultima previsione, pare, a chi scrive, essere idonea ad evitare il rischio, sopra esposto, che le banche siano incentivate a porre in essere pratiche aggressive di *marketing* o di *cross selling* a danno del consumatore[321].

Sul tema, inoltre, si segnala, che anche l'UCPD[322] e l'UTCC[323] vietano pratiche di *marketing* finalizzate a obbligare i consumatori a pagare un servizio che non hanno sollecitato, compreso le ipotesi di rinnovo automatico o tacito, dei contratti.

Per quanto riguarda il rischio che i Big Data vengano utilizzati per pratiche commerciali aggressive, l'UCPD mira a mitigare tali rischi, tramite il divieto di pratiche, come la chiamata a freddo; l'omissione di informazioni chiave[324] e tutte quelle pratiche che non consentono al consumatore di prendere un decisione ponderata.

Anche la *E-Privacy directive*[325] e la *Distance Marketing of Financial Services Directive*[326] contengono disposizioni che mirano a contrastare pratiche aggressive di *marketing*.

In particolare, la prima direttiva impone ai fornitori di ottenere il consenso preliminare dei consumatori per l'invio di comunicazioni tramite chiamate automatiche, *e-mail* o SMS[327].

---

[316] L'art. 29, Data protection working party, a pag. 35 precisa che "*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*".

[317] Art. 5, paragrafo 1, lettera a) del Regulation (EU) 2016/679.

[318] Cfr Artt. 13 e 14 del GDPR.

[319] Cfr. Art. 17 del GDPR.

[320] Cfr. Art. 21 del GDPR.

[321] Inoltre, secondo quanto previsto dal GDPR, qualsiasi trattamento dei dati personali deve basarsi sul consenso, che deve essere espresso, liberamente dato, specifico, informato . Cfr. artt. 4, comma 11 e 7, 6 e considerando 32, 42 e 43.

[322] *Unfair Commercial Practices Directive, Directive 2005/29/EC concerning unfair business-to-consumer commercial practices in the internal market.*

[323] *Council Directive* 93/13/EEC o*n unfair terms in consumer contracts.*

[324] Riguardanti ad esempio il modo in cui viene calcolato il prezzo o i motivi della comunicazione.

[325] *Directive* 2002/58/EC *concerning the processing of personal Data and the protection of privacy in the electronic communications sector ('E-Privacy Directive') – currently under review by the European Commission.*

[326] *Directive* 2002/65/EC *concerning the distance marketing of consumer financial services.*

[327] Un'eccezione (nota come "*soft opt-in*") si applica alle comunicazioni di *marketing* inviate via *e-mail*, nel contesto di una relazione cliente-fornitore già esistente, per prodotti e servizi simili, a condizione che siano soddisfatte talune condizioni di cui

Anche nel settore dei servizi bancari esistono norme che mirano ad attenuare il rischio per i consumatori di ricevere prodotti che non corrispondono al loro preciso interesse.

La direttiva MCD[328], impone ai prestatori e agli intermediari del credito di agire in modo equo, trasparente e professionale, considerando sempre l'interesse dei consumatori[329].

La stessa EBA, infine, ha adottato linee guida "*on product oversight and governance*"(POG)[330] applicabili ai prodotti bancari che rientrano nel mandato di regolamentazione dell'EBA[331] e linee guida su le politiche e le pratiche di remunerazione relative alla vendita e alla prestazione di operazioni bancarie al dettaglio[332]. Entrambe le linee guida mirano a mitigare il rischio per i consumatori di ricevere servizi bancari che non corrispondo al loro migliore interesse.

Il rischio di errori nella raccolta e elaborazione dei dati, inoltre, pare possa essere mitigato applicando le disposizioni dello stesso regolamento GDPR che attribuiscono al consumatore il diritto di accedere ai propri dati oggetto di raccolta e conservazione, allo scopo di verificarne la correttezza e la precisione, con la possibilità di richiederne in ogni momento la rettifica.

Sempre allo scopo di evitare rischi di errori, inoltre, il parere A29WP del 2013, specifica, che i consumatori dovrebbero avere libero accesso ai propri profili, nonché all'algoritmo utilizzato per elaborare le informazioni, mentre le organizzazioni che detengono tali dati dovrebbero divulgare sempre i propri criteri decisionali[333].

Anche il rischio di discriminazione o comunque di violazione del dovere di equità e di non discriminazione posto a carico delle istituzioni finanziarie pare poter essere governato facendo applicazione della disciplina prevista dal GDPR.

Tale testo, infatti, individua all'art. 14, l'obbligo, a carico di chi detiene ed elabora i dati, di informare i consumatori della possibilità che ulteriori informazioni che li riguardano possano essere estrapolate da fonti esterne.

In materia di profilazione[334], inoltre, sempre il medesimo regolamento impone di informare i consumatori in merito alle caratteristiche di tale attività, nonché in merito alle conseguenze della trasformazione di tali dati[335] .

Tali obblighi posti in capo alle banche, sono finalizzati a garantire la possibilità, per i consumatori, di ottenere un intervento umano, per esprimere il proprio punto di vista, per ottenere una spiegazione della decisione raggiunta dopo tale valutazione e per contestare l'eventuale decisione presa in virtù dei dati[336].

Per quanto riguarda i rischi sulla concorrenza nel mercato bancario, conseguenti alla possibilità di blocco derivanti dalla difficoltà di trasferimento dei Big Data tra i vari fornitori di servizi, invece, grande rilevanza assumono le nuove disposizioni sulla portabilità dei dati nel quadro del GDPR.

In particolare, l'art. 20 consente ai consumatori di ricevere in un formato strutturato, di uso comune e leggibile da di-

---

all'articolo 13, paragrafo 2 della direttiva.

[328] *La Mortgage Credit Directive, Directive* 2014/17/EU *on credit agreements for consumers relating to residential immovable property.*

[329] Cfr. art. 7 del MCD.

[330] *EBAGuidelines on product oversight and governance arrangements for retail banking products*, pubblicate il 15 luglio 2015 e applicabili ai prodotti bancari *retail* dal 3 gennaio 2017.

[331] Come ipoteche, prestiti personali, depositi, conti di pagamento, denaro elettronico e servizi di pagamento.

[332] *EBA Guidelines on remuneration policies and practices related to the sale and provision of retail banking products and services,* pubblicate il 28 Settembre 2016 e applicabili dal 13 gennaio 2018.

[333] A29WP *Opinion on Purpose Limitation, published on* 2 April 2013, 47. *See also the Statement of the A29WP on the impact of the development of Big Data on the protection of individuals with regard to the processing of their personal Data in the* EU, *published on* 16 *September* 2014.

[334] Cfr art. 22 del GDPR.

[335] Cfr. artt. 13, paragrafo 2, lett. f e 14, paragrafo 2, lett. g.

[336] Cfr il considerando 71 del GDPR dove si nota che le imprese che utilizzano la profilazione dovrebbero attuare procedure matematiche, nonché misure tecniche e organizzative finalizzate a prevenire effetti discriminatori.

spositivo automatico, i dati personali che li riguardano, in precedenza forniti a un titolare del trattamento, e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti[337].

Sulla questione, inoltre, si segnala che anche altre normative settoriali dell'UE, come il già citato PAD[338] e la PSD2[339] mirano ad attenuare il rischio di intrasferibilità dei dati.

In particolare, il PAD mira a rendere più facile per i consumatori confrontare le offerte di pagamento, facilitare la commutazione dei conti di pagamento e garantire che tutti i consumatori legalmente residenti nell'UE abbiano libero accesso a un conto bancario di base.

Per quanto riguarda i rischi per la sicurezza dei dati, invece, allo scopo di evitare che gli stessi possano essere oggetto di furto o comunque manomissione e duplicazione, il GDPR[340] richiede che i dati siano elaborati in un modo che sia possibile garantire un' adeguata sicurezza dei dati personali.

Oltre alla normativa specifica, anche altre misure settoriali hanno lo scopo di mitigare i rischi in materia di sicurezza dei dati.

Tra questi possono essere ricordate la direttiva NIS[341], adottata il 6 luglio 2016, che ha introdotto nuove misure per la sicurezza in rete per le imprese che operano in determinati settori, tra cui quello bancario, e le *Guidelines on internet payments security* dell'EBA applicabili a tutti i PSPs, compreso le banche e gli istituti di pagamento e di denaro elettronico[342].

Oltre a ciò, l'EBA di propria iniziativa ha emanato anche le *Guidelines on the ICT risk assessment under the Supervisory Review and Evaluation process* (SREP)[343], nonché raccomandazioni per *l'outsourcing* ai *cloud service providers*[344].

Con particolare riferimento al pericolo, sopra paventato, che i consumatori possano sperimentare discriminazioni o essere esclusi dall'accesso a determinati servizi finanziari a seguito di un maggiore utilizzo di Big Data, tuttavia, non pare possibile rinvenire nell'attuale assetto normativo alcuna disposizione capace di mitigare tale rischio[345].

Si tratta, in ogni caso, di preoccupazioni comuni anche al settore assicurativo e degli investimenti, per cui come ha espressamente affermato anche l'EBA, la questione dovrebbe essere affrontata tramite un lavoro congiunto con le altre autorità ESMA e EIOPA.

Tale essendo il quadro regolamentare dell'Unione, disciplinante il trattamento e l'analisi dei Big Data, è possibile conclude che la maggior parte delle criticità sopra evidenziate, conseguenti l'uso di tali informazioni nel mercato bancario, sono sufficientemente mitigati da una serie di disposizioni comunitarie, alcune ancora non attuate in pieno[346].

Si tratta, tuttavia, di una questione che evolve rapidamente, perché rapido è lo sviluppo tecnologico di questi anni.

Tale fenomeno, più che responsabilizzare il legislatore, pare dover responsabilizzare maggiormente le autorità di vigi-

---

[337] I consumatori possono anche richiedere un titolare del trattamento di trasmettere tali dati direttamente ad un altro fornitore, ove ciò sia tecnicamente fattibile.

[338] C.d. *Payment Account Directive, Directive* 2014/92/EU *on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features.*

[339] Direttiva (UE) 2015/2366 del parlamento europeo e del consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno.

[340] Artt. 5, paragrafo 1, lettera f); 33 e 34.

[341] *The Directive on security of network and information systems.*

[342] Questi indirizzi saranno ulteriormente sviluppati negli standard tecnici e le linee guida che l'EBA è stato incaricato di emettere nell'attuazione del PSD2 e del includere

[343] Pubblicate l'11 maggio 2017.

[344] *EBA draft Recommenadationson outsourcing to cloud service providers,* pubblicate il 18 maggio2017.

[345] Cfr. *Report on innovative uses of consumer Data by financial institutions* pubblicato il 28 giugno 2018

[346] Come il GDPR e la PSD2.

lanza, che dovranno essere impegnate a monitorare il fenomeno, in modo congiunto, perché i rischi derivanti dall'analisi dei Big Data coinvolgono tutti i settori.

Solo tramite la cooperazione tra autorità di vigilanza a livello internazionale sarà possibile sfruttare il pieno potenziale degli usi innovativi dei Big Data, cercando di prevenire o comunque attenuare i rischi.

A livello nazionale, ancora, l'attività dell'autorità dovrà essere indirizzata a promuovere anche iniziative di formazione, con lo scopo di aumentare la consapevolezza dei consumatori circa le opportunità e i rischi legati ad usi innovativi dei propri dati[347].

L'autorità di vigilanza del settore bancario, inoltre, a parere di chi scrive dovrà monitorare attentamente le attività delle cc.dd. FinTech , allo scopo di valutare eventuali problemi in tema di autorizzazione.

Tali imprese, cc.dd. FinTech, infatti, rappresentano non solo una sfida epocale ai modelli tradizionali di intermediazione e gestione del risparmio, ma soprattutto ai vecchi modelli nazionali di vigilanza e regolazione[348].

La BCE e la Banca d'Italia, quindi, sono chiamate ad evitare che la corsa della tecnologia finanziaria si realizzi a spese della stabilità del mercato e della sicurezza dei consumatori.

Si tratta di un tema di elevata rilevanza, tanto da meritare un approfondimento.

4.1. L'ATTIVITA' DI VIGILANZA BANCARIA E LE FINTECH: UNA QUESTIONE APERTA

Prima di analizzare le azioni intraprese dall'autorità in materia di vigilanza dell'attività delle FinTech, a chi scrive pare opportuno fornire una definizione del fenomeno, nel tentativo, per quanto possibile, di delimitare i confini del problema.

Con il termine FinTech, il Financial Stability Board (FSB) si riferisce ad un' impresa ad elevata tecnologia, capace di apportare innovazione nei servizi finanziari, determinando nuovi modelli di business, applicazioni, processi o prodotti.

Con particolare riferimento al mercato bancario, la BCE definisce una banca FinTech come un'impresa in cui la produzione di prodotti e la fornitura di servizi bancari sono fondati sull'innovazione tecnologica[349].

Per acquisire la qualifica di banca, ovviamente, l'impresa deve necessariamente ottenere, dall'autorità competente, l'autorizzazione all'esercizio dell'attività bancaria.

La BCE a settembre 2017 ha pubblicato la *Guide to assessments of fintech credit institution licence applications*, allo scopo di garantire parità di trattamento a tutte le imprese che richiedano l'autorizzazione all'attività bancaria, a prescindere dal modello di business.

L'obiettivo della BCE, quindi, è garantire che le banche che adottano un modello di business FinTech, siano tenute al rispetto delle stesse regole di tutti gli altri tipi di enti.

Ovviamente, la particolarità di tali imprese non può non ripercuotersi anche sulle valutazioni da fare per ottenere la c.d. licenza bancaria.

---

[347] Come il rischio di iper-consumismo.

[348] A. Plateroti, *Per le FinTech paletti globali*, su http://www.ilsole24ore.com/art/commenti-e-idee/2017-05-08/per-fintech-paletti-globali--224455.shtml?uuid=AEIIFKIB

349 Cfr. *Guide to assessments of fintech credit institution licence applications* pubblicata dalla BCE nel settembre 2017.

Così in tema di *governance*, se è vero che le FinTech dovrebbero soddisfare esattamente gli stessi criteri generali di qualsiasi altra banca, necessitando di organi di gestione dotati di conoscenze, competenze e esperienze pratiche e teoriche nel settore bancario e/o finanziario, per il loro modello di *business*, la BCE evidenzia che, gli stessi organi, devono necessariamente possedere anche conoscenze e esperienze in materia tecnologica.

In tema di organizzazione strutturale, inoltre, la guida rileva come le banche FinTech, per il loro modello di *business*, siano maggiormente sottoposte a particolari rischi correlati al trattamento dei Big Data, come, ad esempio, la maggiore vulnerabilità agli attacchi informatici o il deterioramento della qualità dei dati stessi.

Tali rischi, a ben vedere, nell'attività della FinTech aumentano poiché tale impresa opera, più delle altre, grazie alla condivisione dei dati fra vari soggetti e tramite servizi in *outsourcing*.

Si pensi, ad esempio, all'attività di valutazione del merito creditizio, nell'ambito del servizio di credito. In genere, la banca fondata su modelli di *business* tecnologici, essendo una *start up*, non è in possesso di informazioni relative alla capacità[350] o disponibilità[351] di rimborso del cliente che richiede un finanziamento.

Per tale motivo, le FinTech che si dedicano alla concessione del credito, o non hanno una struttura di valutazione interna del credito e si affidano così per tali servizi a imprese esterne, o, nel tentativo di creare una propria struttura, finiscono per acquisire le informazioni relative alle *performance* passate del debitore da una serie indefinita di fonti di diversa affidabilità.

Ciò che emerge, in entrambe le ipotesi, è il moltiplicarsi del rischio di *cyber* attacco o di fallacità delle informazioni, che generano operazioni finanziarie fraudolente, possibili interruzioni del servizio, perdita dei dati dei clienti.

Per ovviare a tali rischi, la BCE, nella linee guida pubblicate a settembre di quest'anno, evidenzia che le imprese FinTech che richiedono l'autorizzazione all'esercizio dell'attività bancaria dovrebbero essere in grado, già al momento della richiesta, di dimostrare quale tipo di dato o informazione verrà utilizzato nel processo di concessione del credito, nonché di indicare le procedure attraverso cui assicurare la qualità dei dati.

In particolare, l'impresa che aspira ad esercitare l'attività bancaria, anche se con modelli tecnologici, dovrebbe garantire processi e sistemi idonei ad assicurare la riservatezza, l'integrità e la disponibilità dei dati acquisiti.

Occorre a questo punto sottolineare che quanto indicato dalla BCE nelle proprie linee guida, è destinato esclusivamente alle FinTech che richiedono la licenza bancaria. Trattasi di una sparuta minoranza[352]: la maggioranza delle imprese che utilizzando gli sviluppi tecnologici, infatti, preferiscono operare nell'ambito dei singoli servizi, come quelli di pagamento o di *advisory*. In questo modo, non necessitando di autorizzazione, non sono tenute a rispettare i requisiti richiesti dalla banca centrale europea.

È proprio su tale campo che l'autorità di vigilanza è chiamata alla vera sfida.

Da analisi di mercato, infatti, emerge come il 93% delle banche tradizionali sia preoccupato dell'impatto che le FinTech, nei prossimi anni, avranno sul proprio business, essendo quest'ultime in grado di causare una possibile contrazione dei ricavi del 24 %[353].

A fronte di tali preoccupazioni, di natura strettamente settoriale, tuttavia, non può negarsi che le FinTech rappresentino un'opportunità per l'intera economia.

Tale nuovo modello di *business*, infatti, avrà effetti positivi sicuramente sui consumatori, che godranno, grazie alla tecnologia, di un aumento della qualità dei servizi, con contestuale riduzione dei costi.

---

350 Relative al reddito percepito o all'esistenza di altri debiti da rimborsare.

351 Relative allo "storico" del cliente, cioè come si è comportato in passato il cliente con precedenti creditori.

352 Nell'ultimo anno solo 6 imprese FinTech hanno ottenuto l'autorizzazione della BCE all'esercizio dell'attività bancaria.

353 Cfr. sondaggio sul FinTech 2017 di PwC.

Anche le imprese potranno godere dei benefici di questo nuovo modello, attesa la possibilità di poter accedere a nuove forme e fonti di finanziamento.

Considerate tali opportunità, l'autorità di vigilanza sarà chiamata a garantire a questi nuovi operatori parità di condizioni rispetto alle imprese finanziarie tradizionali. Per fare ciò, il regolatore dovrà attenersi, secondo chi scrive, alla vecchia regola per cui "stessa attività, stessi rischi, stesse regole".

Al riguardo, occorre evidenziare che uno dei banchi di prova sarà senza dubbio il settore dei sistemi di pagamento, al momento interessato dall'imminente adozione, nei paesi UE, della già citata direttiva PSD2.

Tale fonte normativa, infatti, introducendo nuovi servizi di pagamento quali il servizio di disposizione di ordini di pagamento, c.d. *payment initiation service*, e il servizio di informazione sui conti, c.d. *account information service*, prevede la possibilità che ad erogarli siano soggetti terzi non bancari, c.d. Third party provider o TPP.

Mentre con il servizio di informazione sui conti il pagatore può ottenere da un TPP[354] un'informativa completa su tutti i propri conti di pagamento accessibili *online*, con il servizio di disposizione di ordini di pagamento, il soggetto terzo, c.d. Pisp[355] si interpone tra il pagatore e il suo conto di pagamento accessibile *online*, avviando il pagamento a favore del beneficiario (esercente).

Grazie a questo nuovo servizio, quindi, i Pisp, generalmente società che orientano il proprio modello di *business* allo sviluppo di nuove tecnologie, potranno offrire ai propri clienti, si pensi una piattaforma di acquisti *online*, un proprio *software* per il pagamento, cercando di diventare in questo modo il *dominus* del rapporto con il cliente e offrire così ulteriori servizi, anche non finanziari.

Pare evidente, quindi, la questione che nel prossimo futuro le autorità saranno chiamate a dirimere, in un settore in cui, anche la banca tradizionale tenta di tenersi i propri clienti proprio attraverso la fornitura dei servizi non finanziari.

[354] Chiamato Account Information Service Provider.

[355] *Payment initiation service provider.*

I Big Data nel *peer to peer lending* con e senza *bitcoin*

(Giorgia Biferali)

SOMMARIO: 1. PREMESSA. – 2. SISTEMI DI INFORMAZIONE CREDITIZIA E TUTELA DELLA *PRIVACY*. – 3. *PEER TO PEER LENDING* E TUTELA DELLA *PRIVACY*. – 4. *BITCOIN PEER TO PEER LENDING* E TUTELA DELLA *PRIVACY*.

1. PREMESSA

Negli ultimi anni la società è stata travolta da una vera e propria rivoluzione digitale basata su rapporti tra miriadi di utenti ed un elevato numero di imprese che eseguono attività basate su dati. In tale realtà si assiste, da una parte, all'attività degli utenti che consiste principalmente nella più o meno consapevole fornitura di dati ai fornitori di servizi[356], dall'altra parte, all'attività dei fornitori di servizi che raccolgono dati tra gli utenti e successivamente svolgono attività di elaborazione, estrazione e sfruttamento dei dati. L'interazione tra gli utenti e i fornitori avviene tramite uno strumento informatico che è in grado sia di attingere ad una molteplicità di fonti (quali ad esempio i motori di ricerca, i negozi virtuali, le *e-mail*, i *social network*, i servizi *cloud)*, sia di aggregare una quantità elevata di dati. I dati raccolti, una volta analizzati, si prestano a fornire il quadro di un singolo utente, di grandi comunità o della società globale.

Il frutto del progresso tecnologico e scientifico di cui siamo stati spettatori e attori negli ultimi anni sono i Big Data, ossia *dataset* che per la loro estensione in volume, velocità e varietà consentono di estrarre informazioni aggiuntive[357]. Tale disponibilità di dati segna, altresì, il passaggio a una sempre più pervasiva profilazione[358] dei singoli utenti che permette ai fornitori di servizi, le aziende private o le Autorità pubbliche di risalire tramite la cronologia delle attività degli utenti alle loro preferenze, interazioni, stili di vita, al fine di proporre prodotti, di monitorare ampi gruppi sociali e di correlare fenomeni del più disparato genere con alta probabilità di conseguire risultati[359].

Le informazioni in cui i Big Data si sostanziano sono innumerevoli, di diversa natura e provengono da diverse fonti. In un immenso *database* confluiscono milioni di informazioni raccolte attraverso varie modalità da persone, computer, telecamere, e da ogni genere di strumento idoneo per poi essere sottoposti a trattamenti automatizzati. L'uso dei Big Data, oltre a fornire informazioni dettagliate dei soggetti cui dette informazioni si riferiscono (possono riguardare caratteristiche individuali, abitudini di comportamento, patologie ed ogni altra manifestazione della personalità di un individuo), permette, attraverso sofisticati sistemi informatici in grado di operare confronti, di accoppiare e di associare

[356] Ogni volta che l'utente comunica attraverso i *social network* o usufruisce dei servizi *online* (ad esempio, video su richiesta, *e- Commerce* e altri servizi basati sul *Web*) carica contenuti sulle piattaforme di rete sociale.

[357] Cfr. V. Mayer Schonberger, K. Cukier, *Big Data*, Milano, 2013, 15-16, secondo i quali "L'espressione Big Data designa delle cose che si possono fare solo su larga scala, per estrapolare nuove indicazioni o creare nuove forme di valore, con modalità che vengono a modificare i mercati, le organizzazioni, le relazioni tra cittadini e governi, e altro ancora".

[358] Per profilazione si intende "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*" (art. 4 Reg. 2016/679).

[359] Parlano di sistema "dato- centrico" A. Mantelero, *The Future of Consumer Data Protection in the E.U. Rethinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics,* in Computer Law & Security Rev., v. 30, n. 6, 2014, 643 ss.; O. Pollicino, *Un* digital right to privacy *preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel* reasoning *di Google Spain*, in Dir. info., 2014, 569 ss.

informazioni di diversa natura, di giungere addirittura fino al campo della "predizione". È lecito domandarsi quali possano essere le implicazioni negative che derivano da un uso non corretto o non "governato" dei Big Data.

L'art. 22, comma 1, del Regolamento 2016/679 ("Regolamento privacy") stabilisce che "*L'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona". Tale disposizione* sembra apparentemente rispecchiare la volontà del legislatore europeo di frenare l'utilizzo incontrollato dei *Big Data analitycs* o comunque di tentare di arginare i rischi a danno degli interessati; ma si tratta di un tentativo inidoneo a raggiungere lo scopo.

Il "dato" e le sue forme di elaborazione si pongono al centro di una nuova realtà economica[360], in cui il principio della capacità del soggetto di autodeterminarsi mediante il rilascio o il diniego del consenso rispetto alle scelte che riguardano il trattamento dei dati perde di valore[361].

Nella società della condivisione e nel particolare contesto dei Big Data, in cui le informazioni personali sono destinate alla circolazione, la tutela della persona non è l'unico obiettivo da raggiungere, ma è parte di un insieme di interessi tesi allo sviluppo del mercato e dell'economia digitale[362].

La propensione a favorire lo sviluppo dell'economia digitale rispetto alla tutela della persona è ben visibile nella nuova disciplina. Basti leggere il considerando 4 del Regolamento *privacy*, secondo il quale "*la protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerata alla luce della sua funzione sociale e va contemperata con altri diritti fondamentali, in ossequio al principio di proporzionalità*". Oppure il considerando 47, in cui è previsto che i legittimi interessi di un titolare del trattamento possano costituire una base giuridica del trattamento e che possa "*essere considerato legittimo interesse trattare dati personali per finalità di marketing diretto*".

Il Regolamento *privacy*, sebbene modifichi profondamente le regole del trattamento dei dati personali, contenute nella direttiva 95/46/CE e nella legislazione interna in relazione ai modelli organizzativi e imprenditoriali e agli adempimenti in capo ai responsabili e titolari, non fa altrettanto riguardo al fondamento giuridico che legittima il trattamento[363].

Il consenso, anche se da presupposto necessario di legittimità del trattamento dei dati[364] è divenuto semplicemente uno dei possibili presupposti di liceità del trattamento dei dati (art. 6 Regolamento *privacy*), continua a ricoprire un ruolo importante nella disciplina del trattamento dei dati (v. i considerando 32, 40, 42, 43). Esso è stato definito come "manifestazione del diritto all'autodeterminazione informativa"[365] e agisce come mezzo per superare lo squilibrio informativo tra il titolare del trattamento e l'interessato[366].

---

[360] Sul punto cfr. A. Ross, *Il nostro futuro*, Milano, 2016.

[361] A. Montelero, *Responsabilità e rischio nel Reg. UE 2016/679*, in NLCC, 1, 2017, 144 ss.

[362] Sul punto cfr. F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in NLCC, 1, 2017, 375 ss., per il quale il Regolamento *privacy* è una disciplina della circolazione dei dati personali piuttosto che disciplina di protezione della persona.

[363] Sul punto cfr. I. A. Caggiano, *Il consenso al trattamento dei dati personali tra Nuovo Regolamento Europeo (GDPR) e analisi comportamentale. Iniziali spunti di riflessione,* in Diritto Mercato e tecnologia, 2017, 8, la quale ritiene che le scelte normative del legislatore europeo "rivelano un'impostazione volta a non impedire le prospettive tecnologiche di produzione sempre più massiva di dati, le sfere di utilizzo e le tecniche che consentono la moltiplicazione dei dati stessi, ma a disciplinare i trattamenti con meccanismi, ritenuti "virtuosi", finalizzati a minimizzare i rischi di perdita, dispersione, diffusione, nella dichiarata finalità di proteggere la sfera dei soggetti cui i dati si riferiscono".

[364] D. Messinetti, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in Riv. crit. dir. priv., 1998, 353.

[365] Garante Privacy, Provv. 28 maggio 1997, in Boll. n. 1.

[366] Sul punto cfr. C. Camardi, *Mercato delle informazioni e privacy: riflessioni generali sulla L. N.675/1996,* in Eur. Dir. priv., 4, 1998, 1061, per la quale il consenso è paragonabile ad una adesione tipica dei contratti di massa uniformi stipulati tra consumatori e professionisti.

Tuttavia, nel mondo dei Big Data la circolazione dei dati è complessa e segue regole tecniche di funzionamento difficilmente controllabili dal consenso del singolo e difficilmente compatibili con il requisito della determinatezza delle finalità di trattamento (considerando 39, 50, 61). L'oscurità e complessità del trattamento dei dati vanificano completamente il ruolo riconosciuto fino ad ora al consenso, che finisce per rappresentare un mero tributo alla retorica del personalismo[367].

La vacuità del consenso si ritrova nel secondo comma dell'art. 22 del Regolamento *privacy*, in cui si prevede che il diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato viene meno se vi è il consenso esplicito dell'interessato stesso. Nessun divieto è, inoltre, previsto rispetto alla prassi imprenditoriale di porre come onere indispensabile per l'accesso a determinati servizi un consenso avente direttamente o indirettamente ad oggetto dati o modalità di trattamento non strumentali alla prestazione dei servizi stessi. In questa dimensione il requisito del consenso non è in grado di limitare i rischi di diffusione dei dati oltre un orizzonte ragionevolmente prevedibile e il consenso stesso diviene il pretesto per una silenziosa e sostanziale espropriazione interprivata dei diritti di utilizzo dei dati.

2. SISTEMI DI INFORMAZIONE CREDITIZIA E TUTELA DELLA *PRIVACY*

Tra i rischi che possono derivare da un uso non corretto dei Big Data vi è quello di effetti pratici discriminatori rilevanti nella sfera giuridica di singoli soggetti, tra i quali la limitazione della facoltà di accesso al credito.

In tema di accesso al credito, la circolazione delle informazioni rappresenta un elemento essenziale. Difatti, nei rapporti di natura creditizia la regola precontrattuale che impone al privato di comunicare tutti i dati necessari per valutare la convenienza dell'accordo viene sostituita da un sistema di rilevazione di dati esterno al soggetto interessato ad ottenere il finanziamento. Questo sistema si basa sulla rilevazione centralizzata dei rischi, ossia su "banche dati che raccolgono in modo centralizzato informazioni economiche inerenti alle caratteristiche delle posizioni debitorie degli affidati nei confronti del sistema creditizio e, più in generale, alla solvibilità dei soggetti prenditori di credito"[368].

In Italia questo sistema di centralizzazione dei rischi creditizi è svolto dalla Centrale dei Rischi gestita da Banca d'Italia, che raccoglie le informazioni fornite da banche e società finanziarie sui crediti che esse concedono ai loro clienti[369], e dai sistemi di rilevazione centralizzata dei rischi di natura privata (SIC) che agiscono nel rispetto del Codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti[370].

---

[367] F. Piraino, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato* cit., 384.

[368] A. Sciarrone Alibrandi, *Centrali dei rischi creditizi e normativa di privacy: informazione e controlli dell'interessato*, in Riv. dir. civ., 2003, I, 423 s.

[369] Cfr. Decreto d'urgenza del Ministro dell'Economia e delle Finanze - Presidente del Comitato interministeriale per il Credito e il Risparmio (CICR) dell'11 luglio 2012 n. 663. Il sistema informativo della Centrale Rischi si fonda sull'obbligo degli intermediari partecipanti di comunicare mensilmente alla Banca d'Italia i rapporti di credito in essere nei confronti di ciascun cliente, di importo pari o superiore a 30.000 euro e i crediti in sofferenza di qualunque importo. In particolare, la banca dati della Centrale Rischi è strutturata su due principali flussi informativi: le comunicazioni di dati fatte dagli intermediari alla Banca d'Italia (c.d. segnalazioni) e le comunicazioni di dati che Banca d'Italia invia agli intermediari attraverso i flussi di ritorno ed il servizio di prima informazione.

[370] Il codice di deontologia e di buona condotta per i sistemi informativi gestiti da soggetti privati è entrato in vigore il 1 gennaio 2005 e nasce dall'accordo delle associazioni rappresentative del settore con la collaborazione delle associazioni dei consumatori. Le regole in esso contenute sono il frutto dell'elaborazione compiuta dal Garante della privacy.

Questi sistemi offrono uno strumento utile per la valutazione del merito creditizio della clientela e per monitorare il rischio di sovraindebitamento. Inoltre, favoriscono l'accesso al credito e la riduzione dei relativi costi per la clientela meritevole. La corretta valutazione del merito creditizio dei clienti da parte delle banche costituisce il presupposto per ottenere la c.d. referenza creditizia, ossia "la reputazione che il cliente ha presso le banche e gli intermediari finanziari e riflette la correttezza dei suoi comportamenti nell'ambito dei rapporti di finanziamento"[371]. I sistemi informativi contengono informazioni creditizie di tipo "negativo", che riguardano soltanto rapporti di credito per i quali si sono verificati inadempimenti, e talora informazioni creditizie di tipo "positivo", riferite ai regolari pagamenti delle rate o all'estinzione del debito, o anche informazioni creditizie di tipo "positivo e negativo", che attengono a richieste o rapporti di credito a prescindere dalla sussistenza di inadempimenti registrati nel sistema al momento del loro verificarsi. Essi sono utilizzati dagli operatori del settore creditizio e finanziario al fine di condividere e scambiare informazione su finanziamenti.

Da anni si avverte ormai il problema della tutela della riservatezza degli interessati nei confronti delle centrali rischi[372]. Non sono stati pochi i casi di impossibilità o difficoltà di accesso al credito da parte degli utenti consumatori causati da un trattamento dei dati personali effettuato in modo improprio dalle centrali rischi private[373]. Per il richiedente di un finanziamento, essere considerato un "cattivo pagatore" può avere effetti negativi sull'accesso al credito, sull'iniziativa privata e sulle proprie relazioni sociali e professionali[374].

Sulla questione, l'attenzione è rivolta principalmente ai presupposti e alle modalità con cui le informazioni relative ai rapporti di credito vengono raccolte e trasmesse alle Centrali rischi e, di conseguenza, condivise all'interno del sistema bancario.

Per quanto riguarda la trasmissione dei dati che l'intermediario invia alla Centrale dei Rischi Banca d'Italia, si tratta di una comunicazione di dati personali da un soggetto privato ad un soggetto pubblico. Prima dell'entrata in vigore del Codice *privacy*, il Garante si era espresso ritenendo che "La comunicazione dei dati personali relativi all'indebitamento della clientela effettuata dagli intermediari finanziari alla Centrale dei rischi della Banca d'Italia, in quanto dovuta per legge, non è sottoposta all'obbligo della preventiva acquisizione del consenso dei singoli interessati, cui è quindi preclusa la possibilità di ottenere la cancellazione dei dati in mancanza di un accertamento dell'illiceità, anche per altri profili, del trattamento"[375]. Il fondamento normativo dell'obbligo di effettuare le comunicazioni veniva individuato negli artt. 51 e 53 del TUB e nell'art. 27, comma 2, della legge n. 675 del 1996, per i quali ai fini della legittimità della comunicazione era sufficiente che la stessa risultasse comunque necessaria per lo svolgimento delle funzioni istituzionali, tra le quali le disposizioni del TUB prevedevano il controllo di stabilità e il contenimento dei rischi a cui il servizio di centralizzazione è strumentale. Con l'entrata in vigore del Codice *privacy*, l'art. 18, comma 2, dispone che il trattamento di dati personali da parte di soggetti pubblici sia consentito solo per lo svolgimento delle funzioni istituzionali. La tutela

---

[371] Banca d'Italia, www.bancaditalia.it.

[372] Sul punto cfr. R. Cafaro, P. Pagliaro, *L'accesso al credito. Banche dati, Centrali di rischio e privacy,* Milano, 2004.

[373] Negli ultimi anni sono incrementate le controversie giudiziali riguardanti le segnalazioni presso tutte le centrali rischi creditizie, in particolare quelle relative alla sussistenza dei presupposti per la dicitura "a sofferenza" presso la Centrale Rischi della Banca d'Italia. Sul punto, cfr. Cass., 9 luglio 2014, n. 15609; Cass., 24 maggio 2010, n. 12626; Cass., 1 aprile 2009, n. 7958, in Foro it., 2011, I, 208 s.; Trib. Brindisi, 2 marzo 2011, in Nuova giur. civ. comm., 2012, I, 1 s.; Trib. Bari, 5 gennaio 2011, in Resp. civ., 2011, 314 s.
La questione delle indebite segnalazioni presso le centrali rischi è trattata anche dall'Arbitro Bancario Finanziario. Tra le più recenti cfr., ABF, 7 marzo 2017, n. 2244; ABF, 2 maggio 2016, n. 4033; ABF, 24 giungo 2016, n. 5964; ABF, 31 gennaio 2014, n. 611; ABF, 30 luglio 2012, n. 2626; ABF, 13 aprile 2012, n. 1143.

[374] V. Trib. Brindisi, 20-7-1999, secondo il quale "Una segnalazione erronea di un credito a "sofferenza", effettuata da un Istituto di Credito alla Centrale Rischi, è idonea a determinare una lesione del diritto di impresa, potendo creare difficoltà insormontabili all'imprenditore che voglia accedere al credito bancario o potendo determinare la revoca di quello già concesso".

[375] Provv. Garante per la protezione dei dati personali del 17 gennaio 2001, n. 40907.

del rischio creditizio, cui il sistema informativo della Centrale Rischi è diretto, rientra nelle funzioni istituzionali della Banca d'Italia e, in particolare, nell'attività di vigilanza regolamentare disciplinata dall'art. 53 del TUB. L'art. 18, comma 4, prevede espressamente per i soggetti pubblici l'esenzione dall'obbligo di richiedere il consenso.

Per quanto riguarda i sistemi di rilevazione centralizzata dei rischi di natura privata il codice di deontologia e buona condotta non prevede alcuna disposizione sul consenso[376].

Sul punto la dottrina è divisa tra coloro che ritengono che, per il rapporto di genere a specie che sussiste tra il Codice *privacy* e il codice deontologico, operi la regola generale stabilita dall'art. 23 del Codice *privacy* e coloro per i quali il trattamento dei dati da parte delle centrali rischi private rientra in una delle ipotesi di esenzione di cui al successivo art. 24 del Codice *privacy*. Tuttavia, se si considerano le finalità a cui mira l'intero sistema delle informazioni creditizie, ossia "*la tutela del credito e il contenimento dei relativi rischi in modo da agevolare anche l'accesso al credito al consumo e ridurre il rischio di eccessivo indebitamento da parte degli interessati*", e l'impianto di protezione disciplinato dal codice deontologico, secondo il quale "*il trattamento di dati personali effettuato nell'ambito di sistemi informativi di cui sono titolari soggetti privati, utilizzati a fini di credito al consumo o comunque riguardanti l'affidabilità e la puntualità dei pagamenti, deve svolgersi nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone interessate, in particolare del diritto alla protezione dei dati personali, del diritto alla riservatezza e del diritto all'identità personale*", il consenso preventivo al trattamento dei dati come presupposto di legittimità non risulta necessario[377]. Quest'ultimo potrebbe avere invece una funzione residuale e fungere da filtro in tutti i casi in cui il trattamento dei dati possa avvenire per finalità differenti, in virtù di quando stabilito dall'art. 2, comma 2, del codice deontologico, secondo il quale "*Non può essere perseguito alcun altro scopo, specie se relativo a ricerche di mercato e promozione, pubblicità o vendita diretta di prodotti o servizi*".

In ogni caso, come già evidenziato, il consenso non è sufficiente per tutelare l'interessato dai trattamenti dei dati illeciti e lesivi. Parte della dottrina sostiene che, in tema di trasmissione di dati dall'intermediario alle centrali rischi, il problema potrebbe essere superato tramite un'impostazione diversa, frutto di un "ribaltamento della prospettiva nella quale viene giuridicamente disciplinato il fenomeno"[378]. Nel senso che l'attività di raccolta e trasmissione di informazioni alle banche dati da parte degli intermediari ricade all'interno del rapporto banca-cliente e resta assoggettata ai principi che ne disciplinano lo svolgimento. L'intermediario procede alla raccolta e trasmissione dei dati sempre con riguardo alla propria clientela (o potenziale), sicché tale attività si innesta sulla relazione — essenzialmente negoziale — dalla quale è scaturito il rapporto di credito oggetto di segnalazione. Tale impostazione permetterebbe di considerare la segnalazione "errata" come fonte di responsabilità contrattuale per inadempimento del dovere di comportarsi secondo buona fede e correttezza.

Attraverso le tecnologie dell'informazione e delle telecomunicazioni le banche hanno aumentato la qualità e la quantità dei servizi offerti alla clientela e sono riuscite sia a sviluppare nuove tecniche di gestione dei rischi, sia a rendere più rapida e sicura la gestione dei pagamenti. Le nuove tecnologie hanno, però, anche consentito ad alcune imprese, note come imprese *FinTech*, di offrire servizi (servizi di pagamento, di investimento, di consulenza e di finanziamento)

---

[376] Per completezza di informazioni, si precisa che il codice deontologico all'art. 4, comma 7, prevede un obbligo di preavviso a carico dell'intermediario al verificarsi di ritardi nei pagamenti, al fine di avvisare l'interessato circa l'imminente registrazione dei dati in uno o più sistemi di informazioni creditizie. Inoltre, all'art. 5 è stabilito che al momento della raccolta dei dati personali relativi a richieste/rapporti di credito, l'intermediario è tenuto ad informare l'interessato del trattamento dei dati personali effettuato nell'ambito di un sistema di informazioni creditizie.

[377] Sul punto cfr. L. Bolzanini, A. Leidi, *Privacy e banche: il nuovo regime di trattamento dei dati personali (d.lgs. 28 dicembre 2001, n. 467)*, in Banca borsa e titoli di credito, I, 2003, 498, secondo i quali "lo strumento di disciplina normativa, infatti viene individuato non nella necessaria concessione del consenso, bensì nelle modalità di effettuazione dei trattamenti".

[378] C. Frigeni, *Segnalazioni presso le centrali rischi creditizie e tutela dell'interessato: profili evolutivi*, in Banca e borsa e titoli di credito, I, 2013, 364 ss. Tale tesi è stata sostenuta anche dall'Arbitro Bancario Finanziario: ABF 5 settembre 2014, n. 5947.

che fino a pochi anni fa erano esclusivo appannaggio del sistema bancario[379]. Un esempio emblematico è quello delle piattaforme on-line che facilitano il cosiddetto prestito tra pari, o *peer-to-peer lending*.

Gli sviluppi delle imprese *Fintech* hanno finora sollevato questioni di vigilanza prudenziale, ma vi sono anche altri problemi da affrontare, come la salvaguardia della *privacy*, della sicurezza IT e della tutela dei consumatori. Difatti, tali imprese si basano su modelli di business di aggregazione di dati e utilizzano i dati dei clienti per ottenere una conoscenza approfondita dei clienti stessi attraverso la cronologia delle ricerche, i dati personali e le preferenze condivise sui *social media*, le abitudini di consumo e di spesa, e così via[380].

Il successo delle imprese *Fintech*, soprattutto in chiave concorrenziale, è strettamente legato anche alla fiducia che i consumatori ripongono nelle modalità in cui i loro dati personali vengono trattati[381]. A seguito dell'emanazione del Regolamento *privacy*, tali imprese saranno obbligate a dotarsi di una serie di misure preventive per la protezione dei dati personali dei loro clienti.

3. *PEER TO PEER LENDING* E TUTELA DELLA *PRIVACY*

Come è noto, il *peer to peer lending* consiste nel prestito tra privati attraverso l'utilizzo di internet. In particolare, gli utenti di internet, mediante una piattaforma *web* gestita e messa a disposizione da una determinata società specializzata (il gestore della piattaforma di *peer to peer lending*), prestano o richiedono in prestito somme di denaro ad altri privati cittadini (c.d. *social lending*) o imprese (c.d. *direct lending*) a costi contenuti.

In tale attività si manifesta un conflitto diretto tra obiettivi economici e obiettivi di protezione della *privacy*. Il *peer to peer lending* può essere, infatti, considerato come crocevia di questioni e scelte relative alla politica economica e alla regolamentazione della *privacy*. Il fenomeno, caratterizzato dalla semplicità di utilizzo, dalla velocità di erogazione dei prestiti e dalla capacità di valutare il merito creditizio della clientela mediante un ampio numero di informazioni, da una parte agevola l'accesso al credito ma, dall'altra, può mettere a rischio la *privacy* dei soggetti coinvolti, proprio per le modalità con cui avviene la valutazione del merito creditizio.

La valutazione del merito creditizio è uno dei servizi offerti dai gestori delle piattaforme e viene effettuata consultando un ampio numero di informazioni, che possono provenire anche da internet e dai *social media*. I gestori delle piattaforme assegnano un *rating* ad ogni utente richiedente e, di conseguenza, collocano l'operazione di prestito in un certo mercato a seconda della stima del sottostante livello di rischio**.** Il *rating* viene calcolato tenendo conto di diversi fattori, quali la storia creditizia, il reddito, la situazione familiare, l'area geografica, l'età, e via dicendo.

Non sempre gli utenti che si iscrivono a tali piattaforme hanno una storia creditizia. Spesso non risultano iscritti nelle banche dati dei sistemi di informazione creditizia. In tali casi, la valutazione del merito creditizio si basa esclusivamente

[379] Le imprese *FinTech* rappresentano un forte stimolo per l'industria bancaria in quanto sono in grado di alterare in modo rilevante la struttura e il funzionamento dell'industria finanziaria. L'attività svolta dalle imprese *FinTech* in un certo senso "costringerebbe" le banche a diminuire i costi dei canali distributivi tradizionali e a offrire servizi di elevata qualità alla clientela. Sul ruolo e il potenziale per portare ad una maggiore efficienza del sistema finanziario delle imprese *FinTech*, cfr. EBA, *Discussion paper on the EBA's approach to financial technology (Fin Tech)*, 4-8-2017.
Si tratti di sistemi di pagamento che permettono di effettuare pagamenti direttamente dal proprio *smartphone*.

[380] Molte imprese *Fintech*, in particolare quelle coinvolte in *Banktech* (offrono applicazioni e servizi bancari) e *Regtech* (offrono strumenti di regolazione e conformità), si basano sulla condivisione e sull'elaborazione di dati personali.

[381] Sul ruolo che svolge la fiducia nei mercati *on line* cfr., tra gli altri, G. Smorto, *Reputazione fiducia e mercati*, in Eur. dir. priv., 2016, 199 ss.

sul **c.d.** *rating* di credito *social***,** nel senso che il rating viene assegnato sulla base dei dati raccolti dai profili *social* del richiedente insieme ai dati relativi ai pagamenti "*mobile*"[382], allo stile di vita, alle relazioni, ai desideri e agli acquisti con carte di credito.

Si prospetta allora il rischio che taluni richiedenti vedano compromesse o diminuite le proprie *chances* di accesso al credito a condizioni vantaggiose a causa di "errori cognitivi computerizzati", presunzioni o pregiudizi derivanti da erronea programmazione o da "semplificazione algoritmica" e, più in generale, da valutazioni arbitrarie, discriminatorie o comunque "eterodosse", che con l'affidabilità finanziaria possono avere ben poco a che vedere.

Inoltre, ad ulteriore differenza di quanto avviene nel caso di richieste di finanziamento rivolte ad istituti bancari, in cui il richiedente è a conoscenza del fatto che l'ente finanziatore effettuerà un'istruttoria consultando le banche dati dei sistemi di informazione creditizia al fine di valutare le capacità di adempimento, il richiedente di un *peer to peer lending* è il più delle volte sostanzialmente ignaro del fatto che il gestore lo inserirà in una determinata classe di rischio sulla base di informazioni di cui lui stesso non ha contezza.

Per giustificare i metodi di valutazione del merito creditizio adottati per il *peer to peer lending* si potrebbe rilevare che, nell'ambito limitrofo del credito al consumo (oltre che in quello dell'attività di finanziamento in generale), il finanziatore è tenuto a valutare in modo approfondito tutte le informazioni necessarie a comprendere la capacità di rimborso del soggetto richiedente[383]. Le informazioni possono essere ottenute da varie fonti, anche direttamente attraverso il consumatore, e dovrebbero essere opportunamente verificate dal creditore prima di concedere il credito.

In proposito una parte della dottrina[384] ritiene che il dovere di valutazione del merito creditizio possa essere considerato come un corollario dell'obbligo di astenersi dall'assunzione di decisioni arbitrarie e immotivate, finalizzato ad inibire al finanziatore di concedere credito ogni qualvolta emerga una scarsa capacità del consumatore di adempiere all'obbligo di restituzione della somma mutuata. Tale interpretazione permetterebbe di inquadrare l'obbligo di verifica della solvibilità del debitore quale espressione del più generale principio del dovere di sana e prudente gestione, che per vari tipi di intermediari è sancito dall'art. 5 del TUB e costituisce sempre di più una regola imprescindibile delle attività di finanziamento. In questa prospettiva la valutazione del merito creditizio effettuata dai gestori delle piattaforme di *social lending* mediante la consultazione di un'ampia gamma di informazioni, che va oltre le banche dati dei sistemi di informazione creditizia, risulta perfettamente legittima. Ciò è vero a maggior ragione se si considera che in quel contesto la valutazione del merito creditizio è effettuata dai gestori direttamente a tutela di terzi investitori, ossia dei prestatori che accedono alla piattaforma. Sotto tale profilo, all'interesse dei richiedenti ad evitare pregiudizi o presunzioni negative sulla propria solvibilità che possono eventualmente derivare dall'utilizzo dei Big Data si contrappone l'interesse dei prestatori, nella misura in cui la domanda di credito si mantenga ad un livello sufficiente, ad una valutazione "ultra-prudenziale" del merito creditizio, per la quale qualsiasi "presunzione negativa" da Big Data riguardo alla solvibilità di un richiedente dovrebbe sempre essere presa alla lettera.

Occorre inoltre tenere presente che, se i gestori delle piattaforme fossero costretti a circoscrivere le proprie indagini alla consultazione dei sistemi di informazione creditizia, il fenomeno del *peer to peer lending* riguarderebbe solo la

---

[382] I "pagamenti *mobile*" sono pagamenti effettuati mediante uno *smartphone*. La direttiva UE 2015/2366 (PSD2) ha stabilito nuove regole in tema di servizi di pagamento al fine di rendere possibile una più ampia diffusione sul mercato di nuovi mezzi di pagamento e garantire un elevato livello di protezione dei consumatori che si avvalgono di tali servizi di pagamento nel mercato europeo.

[383] A seguito del d.lgs. 19 settembre 2012 n. 169, recante ulteriori modifiche ed integrazioni al d.lgs. 13 agosto 2010, n. 141, l'art. 124-*bis*, comma 1, TUB dispone che "*Prima della conclusione del contratto di credito, il finanziatore valuta il merito creditizio del consumatore sulla base di informazioni adeguate, se del caso fornite dal consumatore stesso e, ove necessario, ottenute consultando una banca dati pertinente*".

[384] S. Pellegrino, *Le disposizioni attuative in materia di credito al consumo*, in Obbl. contr. 2011, 4, 297-298; A. Mirone, *L'evoluzione della disciplina sulla trasparenza bancaria in tempo di crisi: istruzioni di vigilanza, credito al consumo, commissioni di massimo scoperto*, in Banca borsa tit. cred., I, 2010, 592 ss.

parte di popolazione che è o è stata debitrice nei confronti di banche. Questo risultato limiterebbe un fenomeno che può svolgere un'indubbia funzione di utilità sociale.

In conseguenza di quanto si è rilevato, il problema relativo ai Big Data nella valutazione del merito creditizio per il *peer to peer lending* impone di distinguere, anche riguardo ad eventuali responsabilità per danni, due diverse questioni: quella della legittimità delle modalità di utilizzo delle informazioni reperite da parte del gestore della piattaforma e quella della legittimità delle indagini e delle ricerche che esso ha svolto per reperirle.

La prima questione si incentra sull'esigenza di un utilizzo corretto, non pregiudizievole e non discriminatorio degli stessi e sull'esigenza di trasparenza riguardo alle modalità di tale utilizzazione. In altri termini, il gestore della piattaforma potrebbe essere chiamato a mettere i richiedenti a conoscenza, attraverso idonee forme di pubblicità e informazione precontrattuale, delle tecniche adottate per il reperimento dei dati e dei criteri secondo cui, e della misura nella quale, tali dati vengono considerati rilevanti per la valutazione del merito di credito. Almeno in una fase iniziale e ad ogni evoluzione delle modalità di formazione dei Big Data, questo tipo di oneri informativi potrebbe richiedere ai gestori delle piattaforme o ad operatori specializzati da essi incaricati, per un verso, una sorta di opera di "*reverse engineering*" rispetto ai Big Data utilizzati, per individuare da quali dati e secondo quali criteri essi siano stati formati, e, per altro verso, l'elaborazione di modelli in grado di spiegare in modo relativamente semplice con quale metodo i dati ottenuti si combinano per dare luogo ad un determinato *rating* inerente al merito creditizio. Il "costo" che ne deriverebbe può essere tuttavia di gran lunga sopravanzato dai "benefici" che la trasparenza è in grado di determinare in termini di fiducia degli utenti e affidabilità dei servizi, anche sul piano della competizione tra i diversi gestori di piattaforme.

La seconda questione sopra individuata, relativa alla legittimità delle indagini che il gestore della piattaforma svolge per la valutazione del merito creditizio dei richiedenti, dovrebbe invece essere impostata prendendo atto che l'eventuale violazione di norme a tutela della *privacy* è compiuta non dal soggetto (il gestore della piattaforma) che usa le informazioni disponibili grazie ad internet, bensì dal soggetto che permette che queste ultime siano reperibili da chiunque ne abbia interesse. A questo riguardo vengono in considerazione le molte imprese che spesso non si accontentano di raccogliere dati personali dei clienti per svolgere in maniera adeguata i propri servizi, ma utilizzano tali dati anche come fonte ulteriore di ricavi tramite la rivendita degli stessi a vari livelli ad altre aziende di servizi[385].

Allo stato attuale tale fenomeno non sembra agevolmente e significativamente arginabile, anche perché legislatori e regolatori europei ed italiani temono che ciò pregiudicherebbe il mondo imprenditoriale. In una prospettiva *de iure condendo* si potrebbe considerare che dal 2009 negli Stati Uniti un importante istituto bancario utilizza un metodo che consente ai consumatori di monetizzare l'utilizzo dei propri dati**.** Segnatamente, le informazioni vengono raccolte in una banca dati chiamata "banca delle informazioni" e chi è interessato ad utilizzarle è tenuto a pagare una commissione direttamente all'interessato**,** che ha anche traccia del loro utilizzo. Questo meccanismo di "negoziazione" rappresenta un compromesso, seppure di marca monetaria o plutocratica, tra gli interessi degli utenti e quelli delle imprese in relazione al problema del trattamento dei dati e del rispetto della *privacy*.

Nel contesto dei *Big Data analytics*, in cui l'originaria definizione della *privacy* come "diritto a essere lasciato solo"[386] è mutata in il "diritto di controllare l'uso che altri fanno delle informazioni che ci riguardano" o come "diritto di mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata"[387], lo strumento della "negoziazione" potrebbe soddisfare l'esigenza di protezione dei dati personali degli interessati meglio

[385] Si pensi ad esempio alle società emittenti di carte di credito che vendono i dati grezzi relativi ai propri clienti attraverso intermediari specializzati come *Cardylitcs*.

[386] S. Warren, L.D. Brandeis, *The right to privacy*, in Harward Law Review, 5, 1980, 4 ss.

[387] S. Rodotà, *Tecnologia e diritti*, Bologna, 1995, 122.

di quanto accada mediante il semplice requisito del consenso[388].

Tuttavia, una tale apertura dovrebbe fare i conti con il fatto che nel nostro ordinamento la circolazione dei dati personali è avvenuta sempre mediante il consenso, inteso come dispositivo che permette l'accesso ad una determinata informazione personale, e che la disciplina sul trattamento dei dati personali non regola l'ipotesi di "negoziazione" di proprie informazioni personali a titolo gratuito o oneroso.

4. BITCOIN PEER TO PEER LENDING E TUTELA DELLA *PRIVACY*

I problemi di tutela della *privacy* connessi al "prestito tra pari" risultano esponenzialmente amplificati nel c.d. *bitcoin peer-to-peer lending*, ossia nel sistema di *peer-to-peer lending* che si serve dei *bitcoin*[389], i quali costituiscono l'oggetto dato o preso in prestito. Tale sistema è stato già adottato da piattaforme specializzate, che forniscono diversi servizi accessori (tra i quali la valutazione del merito creditizio), ma, in virtù dell'utilizzazione dei *bitcoin* e della connessa "*blockchain technology*", è dal punto di vista tecnico in grado di consentire i trasferimenti di valuta tra prestatore e richiedente senza alcuna intermediazione. La circolazione dei *bitcoin* avviene infatti tramite un *database* distribuito (c.d. "*blockchain*")[390] che mantiene in modo continuo una lista crescente di registrazioni, le quali fanno riferimento a registrazioni precedenti contenute nella lista stessa.

I rischi per la *privacy* sono determinati dal fatto che tali registrazioni delle transazioni in *bitcoin* sono rilevabili pubblicamente, tracciabili e impresse in maniera permanente nella rete *bitcoin*, con la conseguenza che chiunque può prendere visione delle varie transazioni effettuate da un qualsiasi indirizzo *bitcoin* e del relativo bilancio[391]. In teoria nel trasferimento di *bitcoin* ciò che viene registrato e risulta pubblicamente è solo l'indirizzo da cui la transazione è effettuata. Tuttavia, l'identità dell'utente collegata ad un certo indirizzo diviene nota appena è rivelata nell'ambito di una delle operazioni compiute. Inoltre, i *provider* di servizi internet sono in grado di rintracciare l'indirizzo IP da cui è stato effettuato il trasferimento di valuta[392]. La "democraticità" dello strumento comporta pertanto anche un ampliamento

[388] Affidare al contratto e alla sua disciplina il superamento del conflitto tra interessi delle imprese e protezione dei dati personali potrebbe permettere di valorizzare i Big Data anche nel contesto bancario. Le banche conservano traccia di un'infinità di transazioni dei clienti, contratti di mutuo ipotecario e contratti credito al consumo, ma questa enorme mole di dati è in realtà statica e spesso utilizzata solo da alcune funzioni aziendali. I dati non sono aggiornati in tempo reale e sono di difficile gestione e integrazione, mentre con un approccio incentrato sui Big Data si potrebbe fornire valore aggiunto alla raccolta e all'analisi degli stessi. Il sistema dei *Big Data analytics* potrebbe infatti consentire di elaborare strategie per reagire alla concorrenza proveniente dai nuovi operatori non bancari come le imprese Fintech**.** Esso sembra inoltre in grado di anticipare le esigenze dei clienti e di ridurre i rischi di insolvenza. La grandissima quantità di dati che si "autoalimenta" con il flusso quotidiano di dati che provengono dai *social networks*, dai *tweet*, dalle *e-mail*, e così via, potrebbe in effetti costituire un grande potenziale per le banche.

[389] Sul funzionamento tecnico dei Bitcoin, S. Nakamoto, Bitcoin: *A peer to peer electronic casch system, www.bitcoin.org.* Sui Bitcoin dal punto di vista giuridico cfr., in generale, BCE, *Virtual currency Schelemes*, ottobre 2012; Id., *Virtual currency schemese – a further analysis*, fabbraio 2015; ESMA, *Call for evidence. Investment using vitual currency or distributed ledger technology*, ESMA/2015/532, aprile 2015; Banca d'Italia, *Avvertenze sull'utilizzo delle cosiddette "valute virtuali"*, 30 gennaio 2015. Sulla natura giuridica dei Bitcoin cfr., G. Gasparri, *Timidi tentativi giuridici di messa a fuoco del bitcoin: miraggio monetario crittoanarchico o soluzione tecnologica in cerca di un problema?*, in Dir. inf., 2015, 415 s.; N. Vardi, *"Criptovalute" e dintorni: alcune considerazioni sulla natura giuridica dei Bitcoin*, in Dir. inf., 2015, 443 s.; R. Bocchini, *Lo sviluppo della moneta vituale: primi tentativi di inquadramento e disciplina tra prospettive economiche e giuridiche*, in Dir. inf., 2017, 27 s.; Tribunale di Verona, 24 gennaio 2017, con nota di M. Passaretta, *Bitcoin: Il leading case italiano*, in Banca borsa tit cred., 2017, 471 s.

[390] Si tratta di un *database* che si trova sotto il controllo di un "*Database management system*" in cui gli archivi di dati sono memorizzati, invece che su un solo elaboratore, su più elaboratori o nodi connessi tra loro.

[391] Cfr. P. Cuccuru, Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract, in NGCC, 2017, II, 110.

[392] Cfr. Id., Blockchain *ed automazione contrattuale. Riflessioni sugli* smart contract cit., 110 nt. 16.

dei problemi di protezione dei dati personali. Per evitare di fornire pubblicamente un quadro completo delle proprie attività di prestito o ricezione di fondi è possibile adoperare un indirizzo diverso per ogni nuova transazione, ma non è detto che questa accortezza venga in concreto utilizzata.

Se gli stessi indirizzi sono impiegati per più transazioni, chiunque sia venuto a conoscenza dell'identità dei relativi utenti potrà riutilizzare le informazioni raccolte, anche inserendole in una strategia di *Big Data analytics*. In questa situazione il requisito del consenso praticamente svanisce. Il controllo sull'osservanza delle norme sul trattamento dei dati personali si "disperde" e si complica, in quanto le informazioni sono diffuse nella rete *bitcoin*. Si pone il rischio della creazione di una sorta di mercato nero e parallelo delle informazioni e dei Big Data, fuori da ogni supervisione possibile in concreto. In tal modo l'effetto espropriativo in sostanziale violazione della protezione dei dati personali si moltiplica

CONSOB

(Francesco Della Rocca, Alfonso Ingenito)

Il mercato finanziario nell'era delle *fake news* e dei Big Data

Nell'era della Data economy*, non poteva tardare a manifestarsi anche sui mercati regolamentati l'impatto tanto dei Big data, quanto delle* fake news*.*

Con riferimento al primo aspetto, l'osmotico scambio di informazioni "alla" e "dalla" platea degli investitori, conseguente al recente scenario normativo, è idoneo a determinare un ampliamento dell'attività di raccolta e di analisi dei dati da parte delle imprese di investimento talmente rilevante, da non poter essere gestito in modo efficiente se non per il tramite dei Big data, il cui utilizzo è non a caso destinato a pervadere l'intero settore dei servizi di investimento, innovando a tal punto i relativi modelli di business*, da imporsi anche sulle più recenti dinamiche evolutive del FinTech, spettando, conseguentemente, alle Autorità di vigilanza europee e nazionali ricercare un adeguato bilanciamento tra i rischi ed i benefici dell'impiego sempre più massiccio dei Big Data nel settore mobiliare e della intermediazione finanziaria, affinché sia garantita adeguata protezione agli investitori e, al contempo, non sia soffocato lo sviluppo delle nuove tecnologie.*

Per quanto concerne, invece, le fake news *il presente contributo ha, come obiettivo, quello di fornirne una nozione ed un significato differenti da quelli insiti nella semplice traduzione letterale del termine, avvicinando, dunque, quest'ultimo all'accezione di stampo maggiormente "giornalistico" del concetto di "diffusioni di bufale" ed andando a vedere come detto fenomeno si manifesta nel mercato regolamentato e quali possano essere le diverse misure che l'Autorità di competenza deve adottare per contrastare un fenomeno che comunque tende ad alterare gli equilibri del mercato.*

Il ruolo della CONSOB nel "nuovo" fenomeno delle "*fake news*"

(Francesco Della Rocca)

Il presente lavoro muove dal presupposto di dare al termine "*fake news*" un significato diverso dalla semplice traduzione letterale, intendendolo nell' accezione più giornalistica del concetto di "diffusioni di bufale", andando a vedere come detto fenomeno si manifesta nel mercato regolamentato e quali possano essere le diverse misure che l'Autorità di competenza deve adottare per contrastare un fenomeno che comunque tende ad alterare gli equilibri del mercato.

" Abuso di mercato è il concetto che comprende le condotte illecite nei mercati finanziari e ai fini del presente regolamento dovrebbe essere inteso come abuso di informazioni privilegiate, comunicazione illecita di informazioni privilegiate e manipolazione di mercato. Tali condotte impediscono una piena ed effettiva trasparenza del mercato, che è un requisito fondamentale affinché tutti gli attori siano in grado di operare su mercati finanziari integrati"[393].

[393] Regolamento Europeo n. 594/2014.

Così il legislatore europeo ribadisce nelle premesse del nuovo Regolamento del 2014[394], qualora ce ne fosse bisogno, l'importanza di una corretta circolazione e diffusione di informazioni per avere un mercato finanziario efficiente e trasparente.

Prosegue individuando nel corpo del Regolamento, con una disciplina uniforme per tutti gli Stati membri, le fattispecie che debbano considerarsi illecite essendo viste con disvalore dal legislatore.

Emerge, rispetto al passato, un ampliamento delle condotte e degli strumenti utilizzabili per abusi di mercato.

Ai fini del nostro lavoro, constatato come il tema delle informazioni sia un tema sensibile per la regolamentazione europea, è necessario provare a dare una definizione specifica, per il settore di cui ci stiamo occupando, del termine di "*fake news*" e quello di "Big Data".

Se per quest'ultima detto Regolamento, integrato da fonti prodotte dall'Autorità di Vigilanza, prescrive in modo diretto i confini entro i quali è possibile effettuare ed utilizzare sondaggi di mercato, e quindi in modo indiretto, attraverso un'interpretazione sistematica, sembrerebbe possibile tentare di trovare delle regole che disciplinino la fattispecie più ampia della raccolta e il conseguente utilizzo di grandi volumi di dati, al fine di estrarre informazioni nascoste[395], o per meglio dire, utilizzando una terminologia nota al legislatore finanziario, privilegiate[396], utili per operare sul mercato, riguardo al concetto di "*fake news*" bisogna capire meglio se si tratta di una fattispecie in astratto già disciplinata, non solo dal legislatore europeo ma anche da quello italiano, o possa ricomprendersi, dentro questo termine di stampo essenzialmente giornalistico, un fenomeno leggermente nuovo per il nostro ordinamento.

Fin troppo facile è cercare nella legislazione finanziaria l'esatta traduzione in italiano del termine "*fake news*". Infatti, sia il Regolamento Europeo sopraccitato, sia tutta la regolamentazione finanziaria[397], sia addirittura il nostro codice penale contrastano la diffusione di notizie false, idonee a provocare una sensibile alterazione del prezzo di strumenti finanziari e, quindi, una manipolazione del mercato.

Orbene, collocando il termine "*fake news*" in detta fattispecie, entriamo in un settore altamente regolamentato, sul quale sono state scritte innumerevoli pagine di letteratura giuridica ed economica.

Detto fenomeno, anche se questa non è la sede adatta, è stato toccato da molto vicino dal regolamento sopramenzionato, necessitando forse di una maggiore armonizzazione delle sue fonti, ma ricondurre il concetto di "*fake news*" ad una fattispecie comunque già nota potrebbe risultare non in linea con il significato semantico che la parola "*fake news*" ha nel termine quotidianamente utilizzato.

Stesso risultato lo avremmo se provassimo a considerare la falsa informazione collegata al prospetto informativo di offerta pubblica, difatti, a prescindere dalla natura contrattuale o extracontrattuale della stessa l'analisi, si collocherebbe anche qui in un argomento già segnato dalla giurisprudenza senza cogliere le differenze che con il nuovo termine si vogliono esprimere.

Il termine espresso in lingua inglese, invece, è più corretto tradurlo con il termine "bufala".

Allora provando ad aderire alla distinzione inglese tra *disinformation*, cioè quella informazione volutamente fuorviante che spesso è frutto di manipolazione, e *misinformation*, informazione invece inattendibile ma non deliberatamente fuorviante, potremmo attribuire al termine giornalistico "*fake news*" il secondo significato.

---

[394] Detto Regolamento abroga la direttiva 2003/6/CE del Parlamento europeo e del Consiglio e le direttive 2003/124/CE, 2003/125/CE e 2004/72/CE della Commissione.

[395] Operazione chiamata *big data analytics*.

[396] Cfr. art. 181 T.U.F.

[397] Cfr. art. 185 T.U.F.

Procedendo con questo lavoro ermeneutico, si configura un fenomeno leggermente diverso da quello per il quale il legislatore italiano ed europeo si è concentrato nella legislazione finanziaria da sempre.

Il fenomeno delle *fake news* così inteso, negli ultimi anni, si è sviluppato moltissimo, usufruendo dello sviluppo della rete quale canale di informazione accessibile a tutti.

Anche i mercati regolamentati risentono di detto fenomeno, specialmente la quotazione dei titoli a forte contenuto tecnologico ed innovativo dove, anche per l'assenza di precisi parametri di riferimento, la diffusione di *fake news* è più semplice e soprattutto il suo effetto sul mercato è più tangibile.

Oltre oceano di detto fenomeno se ne sta iniziando ad occupare anche la SEC.

Individuato il fenomeno, proviamo a spostare l'attenzione sul piano della responsabilità e dei possibili rimedi.

La prima cosa che possiamo notare è che il fenomeno è caratterizzato non solo da una diversità tra il soggetto appunto che diffonde la notizie e quello che se ne avvantaggia, ma anche da una totale estraneità del secondo rispetto all'operazione di diffusione della notizia falsa.

In altre ipotesi, non è addirittura neanche individuabile un soggetto preciso che si avvantaggia della diffusione della notizia.

Anche perché se così non fosse saremmo nel campo dei reati finanziari per i quali è prevista una precisa tutela legislativa.

Analizzando il fenomeno in generale, detto dibattito è all'attenzione del nostro legislatore, essendo stato presentato al Senato un disegno di legge[398] specifico, che vada a regolamentare la cosiddetta bufala su *web*.

In assenza di una normativa *ad hoc*, la dottrina ha trovato più di una difficoltà a ritenere la condotta di diffondere la *fake news* come condotta illecita e addirittura quale fonte di responsabilità per l'autore.

Se detta situazione[399] è vera nell'ambito del diritto comune, ci dovremmo interrogare se nell'ambito delle materie regolamentate dal diritto finanziario è configurabile una riflessione simile.

Mentre, nel diritto comune, l'oggettiva valutazione negativa della diffusione dell'informazione falsa sul *web* deve subire un bilanciamento di altri valori costituzionalmente garantiti, quali per esempio la libertà di manifestazione del proprio pensiero, nel diritto finanziario, come d'altronde leggiamo da ultimo nel preambolo del nuovo Regolamento Europeo soprariportato, la corretta circolazione di informazioni è un elemento essenziale per un mercato efficiente.

Proprio per l'importanza che riveste la circolazione di corrette informazioni per un mercato efficiente, nel diritto finanziario potrebbe forse essere configurabile, anche senza modifica legislativa, una responsabilità in capo all'autore che anche senza trarne profitto diffonde la *fake news*.

Il primo problema è che detto soggetto non è nella maggior parte dei casi un soggetto vigilato, esso agisce in maniera completamente autonoma dal soggetto che si avvantaggia da detta diffusione dell'informazione e, nella maggioranza dei casi, è altresì difficile anche individuare l'autore che diffonde l'informazione falsa quando quest'ultima diventi un pensiero comune per l'operatore/risparmiatore medio, anche se del tutto infondata e priva di una qualsiasi analisi scientifica di riscontro.

Allora ci si potrebbe interrogare se e quali azioni potrebbe avere l'utente leso, soprattutto nei confronti di chi.

Sicuramente detta fattispecie non può entrare in quelle per le quali sono previste sanzioni amministrative e penali,

[398] D.D.L. n. 2688 presentato in data 7 febbraio 2017.

[399] Per una attenta riesamina si rinvia alla sezione

stante la tipicità di dette norme sanzionatorie e la loro non estensibilità analogica.

L'unica tutela a favore dell'autore che ha subito il danno è attualmente quella offerta dal codice civile in particolare quella di cui all'art. 2043 e ss del codice civile.

Ma se anche riuscissimo (in rarissimi casi) ad individuare il singolo autore o, per meglio dire, l'autore iniziale della diffusione dell'informazione non veritiera, è immaginabile configurare una responsabilità in capo all'utente che, inconsapevole e in assoluta buona fede, diffonde la falsa notizia? È possibile configurare una responsabilità in assenza di dolo e colpa?

É altrettanto incontestabile, però, la distorsione del mercato trovandosi il soggetto, a danno del quale si è diffusa la notizia, a subire dei sacrifici economici (si pensi alla difficoltà di accesso al credito per una banca dichiarata "fallita" dalla popolazione, ma in realtà con una situazione più solida di molte altre), come altresì è indubbio il vantaggio economico che indirettamente hanno i *competitor* della medesima società che subisce l'effetto della diffusione della notizia falsa.

Sicuramente gli strumenti previsti dall'ordinamento risultano inidonei, stante anche le peculiarità del fenomeno e dei molteplici interessi coinvolti.

Se le tutele offerte dal diritto comune non sembrano sufficienti, essendo impossibile configurare una responsabilità aquiliana in capo al soggetto che, senza partecipare alla diffusione di dette *fake news*, però se ne avvantaggia con operazioni speculative nei mercati regolamentati, né praticabile chiedere una tutela risarcitoria all'autore della diffusione della notizia, bisogna interrogarsi se detto fenomeno merita l'attenzione e l'intervento specifico dell'Autorità che vigila sul funzionamento del mercato regolamentato e, se sì, attraverso quale strumento o se è lo stesso mercato che si autodifende ed è insito nel concetto di contrattazione nei mercati regolamentati imbattersi in un'asimmetria informativa, lasciando il compito all'operatore di analizzare la veridicità delle informazione prima di operare sul mercato.

Allorché, l'Autorità registri una sofferenza del titolo, per via della diffusione di informazione manipolante in merito all'emittente, sospenda il medesimo dalla contrattazione, potere analogo potrebbe configurarsi qualora la medesima registri una distorsione del mercato a seguito di *fake news*.

Per fare ciò la CONSOB avrebbe bisogno di una regolamentazione che configuri il fenomeno e soprattutto circoscrivi con parametri oggettivi il suo eventuale intervento.

In assenza di una volontà politica in tal senso, l'intervento dell'Autorità di competenza potrebbe risultare alquanto arbitrario.

Un'ipotesi simile non è tra l'altro completamente fuori dai principi generali del nostro ordinamento, essendo il risparmio investito dall'investitore più piccolo a risentire nella maggior parte dei casi.

Né sarebbe in contrasto con una ricerca di stabilità del mercato.

Ma forse l'Autorità non deve spingersi oltre le fattispecie previste dalla regolamentazione europea e finanziaria, poiché sono presenti nel mercato e nel suo equilibrio, gli anticorpi per reagire ad qualsiasi disinformazione non dolosa.

Tutto il mercato finanziario si basa sulla circolazione di informazioni e le *fake news* potrebbero fare parte sicuramente della normale circolazione di esse.

A sostegno di tale tesi potrebbe esser fatto constatare che, comunque, è un operatore *non retail* ad operare nel mercato regolamentato che assume il rischio dell'investimento fatto.

I Big Data nelle attività e nei servizi di investimento

(Alfonso Ingenito)

SOMMARIO: 1.- PREMESSA. LO SCAMBIO DI INFORMAZIONI "ALLA" E "DALLA" PLATEA DEGLI INVESTITORI. – 2. LO SCAMBIO DI INFORMAZIONI "ALLA" PLATEA DEGLI INVESTITORI. L'OBBLIGO DI COMUNICAZIONE AL PUBBLICO DELLE "INFORMAZIONI PRIVILEGIATE". – 3. LO SCAMBIO DI INFORMAZIONI "DALLA" PLATEA DEGLI INVESTITORI: LA PROFILATURA DEI CLIENTI NEL REGIME DELLA MIFID I. – 3.1 LA PROFILATURA DEI CLIENTI A SEGUITO DELLA MIFID II. – 4.- BIG DATA E FINTECH: LA *ROBO-ADVISORY*. – 5. BENEFICI E RISCHI DELL'APPROCCIO "*DATA DRIVEN*" NEI SERVIZI DI INVESTIMENTO.

1. PREMESSA. LO SCAMBIO DI INFORMAZIONI "ALLA" E "DALLA" PLATEA DEGLI INVESTITORI

Nell'attuale contesto di mercato, dominato dal crescente impiego delle tecnologie informatiche e telematiche nel settore finanziario (e dalla conseguente trasformazione di quest'ultimo nel c.d. Fintech[400]), l'innovazione derivante dall'utilizzo dei Big Data non poteva tardare a manifestarsi anche con riferimento al particolare segmento del mercato mobiliare e della intermediazione finanziaria.

Non è, infatti, un caso che l'ESMA, unitamente all'EBA e all'EIOPA, nella predisposizione di un documento congiunto di consultazione appositamente dedicato al tema dell' "*Use of Big Data by Financial Institutions*", abbia affermato che la "*adoption of Big Data technologies may change the way financial services are provided*"[401].

Se, per un verso, le Autorità finanziarie europee hanno inteso rivolgere solo di recente espressa attenzione al fenomeno, come dimostrato dal fatto che il documento appena citato è stato pubblicato in data 19 dicembre 2016, per altro verso occorre evidenziare che la raccolta e la gestione dei dati dei clienti da parte degli intermediari è un aspetto tanto rilevante, da potersi attualmente definire quasi connaturato alla disciplina del mercato mobiliare.

Quest'ultima, infatti, da un punto di vista prettamente giuridico, assume quale proprio tratto distintivo la sussistenza di una notevole asimmetria informativa tra le imprese di investimento e le loro controparti contrattuali "deboli", essendosi al riguardo rilevato che qualunque sia o "il segno dell'operazione (acquisto di titoli o accensione di un mutuo)", o "la struttura temporale dello scambio delle prestazioni", od ancora "gli ulteriori dati di ingegneria finanziaria ricompresi nel contratto e che definiscono lo specifico prodotto scambiato, l'elemento centrale e caratterizzante la transazione è la disparità tra chi investe o viene finanziato rispetto chi gli offre il prodotto"[402].

Proprio al fine di colmare, o quantomeno, ridurre il *gap* conseguente a tale rilevante asimmetria informativa, le imprese di investimento sono state gravate di specifici obblighi non solo comportamentali, ma, soprattutto informativi[403], i quali vanno ad aggiungersi e ad integrare quelli derivanti dal rispetto del generale principio di buona fede tanto nella

[400] Su cui si rinvia, per ogni approfondimento a R. Ferrari, *L'era del fintech*, , Milano, 2016.

[401] EBA, EIOPA, ESMA, *Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions*, 19 dicembre 2016, reperibile al seguente link: *https://www.esma.europa.eu/press-news/consultations/joint-committee-discussion-paper-use-big-data-financial-institutions*.

[402] G. Vettori (a cura di), *Contratto e responsabilità*, Tomo II, *La disciplina del Contratto ed Il T.U.F.*, Padova, 2013, 1723.

[403] Su cui, di recente, A. Perrone, *Servizi d'investimento e regole di comportamento dalla trasparenza alla fiducia*, in *Banca Borsa tit. cred.*, 2015, 1, I, 23 ss.

fase antecedente la conclusione dei contratti di investimento, quanto in quella della loro esecuzione, ai sensi, rispettivamente, degli artt. 1337 e 1375 c.c.[404]

L'introduzione di tali obblighi, (i) si deve essenzialmente all'iniziativa del legislatore europeo, che ha provveduto a tanto non solo con il regolamento (UE) n. 596/2014 (c.d. *Market Abuse Regulation* di seguito, anche solo *MAR*[405]), ma soprattutto con la direttiva c.d. MiFID I[406] e poi, con l'altrettanto nota direttiva c.d. MiFID II[407]; (ii) è stata, in ogni caso, dettata dall'esigenza di garantire sia l'efficienza delle transazioni del mercato mobiliare, sia la massimizzazione della tutela e della protezione dell'investitore, soprattutto al fine di rendere quest'ultimo "edotto (…) degli errori che ne inficiano le scelte in via sistematica, ed aiutarlo a controllare l'emotività"[408] in sede di conclusione dei contratti di investimento.

Per quel che qui più rileva, la previsione di tali regole informative e di condotta ha altresì comportato un vero e proprio obbligo per gli intermediari di effettuare una attività di raccolta e gestione dei dati relativi ai propri clienti, nell'ambito di uno scambio di informazioni che assume un carattere biunivoco, "alla" e "dalla" platea degli investitori[409].

2. LO SCAMBIO DI INFORMAZIONI "ALLA" PLATEA DEGLI INVESTITORI. L'OBBLIGO DI COMUNICAZIONE AL PUBBLICO DELLE "INFORMAZIONI PRIVILEGIATE"

Al fine di colmare le asimmetrie informative sussistenti tra le imprese di investimento e l'indistinta platea dei clienti, il legislatore europeo ha innanzitutto previsto, a carico degli emittenti, specifici obblighi di comunicazione "*al pubblico di informazioni privilegiate*".

Tali obblighi erano già disciplinati dalla c.d. *Market Abuse Directive*[410] (di seguito, anche solo "*MAD 1*"), direttiva che, "*in considerazione degli sviluppi legislativi, tecnologici e di mercato intervenuti*", i quali "*hanno comportato cambiamenti notevoli nel panorama finanziario*", è stata sostituita dal MAR, quale un nuovo "*strumento legislativo*" adottato

[404] Cfr., al riguardo, F. Annunziata, *La disciplina del mercato mobiliare*, Giappichelli, Torino, 2008, 119, e, già in precedenza, B. Inzitari, *Vigilanza e correttezza nell'attività di intermediazione mobiliare*, in *L'intermediazione mobiliare*, a cura di S. Mazzamuto E C. Terranova, , Napoli, 1993, 132.

[405] Regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, relativo agli abusi di mercato (regolamento sugli abusi di mercato) e che abroga la direttiva 2003/6/ Ce del Parlamento europeo e del Consiglio e le direttive 2003/124/Ce, 2003/125/ Ce e 2004/72/ Ce della Commissione.

[406] Direttiva 2004/39/Ce del Parlamento europeo e del Consiglio del 21 aprile 2004 relativa ai mercati degli strumenti finanziari, che modifica le direttive 85/611/Cee e 93/6/Cee del Consiglio e la direttiva 2000/12/Ce del Parlamento europeo e del Consiglio e che abroga la direttiva 93/22/Cee del Consiglio.

[407] Direttiva 2014/65/UE del Parlamento europeo e del Consiglio del 15 maggio 2014 relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/Ce e la direttiva 2011/61/UE.

[408] N. Linciano, *La consulenza finanziaria tra errori di comportamento e conflitti di interesse*, in *Analisi Giuridica dell'economia*, 1, 2012, 135.

[409] F. Capriglione, *Intermediari finanziari. Investitori. Mercati*, Padova, 2008, 147 ss.

[410] Direttiva 2003/6/Ce del Parlamento europeo e del Consiglio, del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato (abusi di mercato). Oltre alla MAD 1, gli abusi di mercato erano, inoltre, disciplinati dai seguenti provvedimenti di secondo livello, poi abrogati dal MAR: *(i)* dalla direttiva 2003/124/Ce della Commissione, del 22 dicembre 2003, recante modalità di esecuzione della direttiva 2003/6/Ce del Parlamento europeo e del Consiglio per quanto riguarda la definizione e la comunicazione al pubblico delle informazioni privilegiate e la definizione di manipolazione del mercato; (ii) dalla direttiva 2003/125/Ce della Commissione, del 22 dicembre 2003, recante modalità di esecuzione della direttiva 2003/6/Ce del Parlamento europeo e del Consiglio per quanto riguarda la corretta presentazione delle raccomandazioni di investimento e la comunicazione al pubblico di conflitti di interesse; 3) dalla direttiva 2004/72/Ce della Commissione, del 29 aprile 2004, recante modalità di esecuzione della direttiva 2003/6/Ce del Parlamento europeo e del Consiglio per quanto riguarda le prassi di mercato ammesse, la definizione di informazione privilegiata in relazione agli strumenti derivati su merci, l'istituzione di un registro delle persone aventi accesso ad informazioni privilegiate, la notifica delle operazioni effettuate da persone che esercitano responsabilità di direzione e la segnalazione di operazioni sospette.

all'espresso fine di garantire in via immediata, diretta e cogente per tutti gli Stati membri "*regole uniformi e chiarezza dei concetti di base*"[411] nel settore in parola.

Attualmente l'art. 17, par. 1, MAR dispone che ciascun emittente è tenuto a pubblicare tutte "*le informazioni privilegiate*" che lo "*riguardano direttamente*".

Tale obbligo, già previsto dalla MAD 1, è stato esteso dal MAR: (i) agli emittenti strumenti finanziari negoziati sui sistemi multilaterali di negoziazione (MTF) e sui sistemi organizzati di negoziazione (OTF)[412]; (ii) ai partecipanti al mercato delle quote di emissione[413].

L'art. 7, par. 1, lett. a) dello stesso regolamento precisa che ciascuna "*informazione privilegiata*", per essere tale: (i) deve avere "*carattere preciso*"; (ii) non deve essere "*stata resa pubblica*"; (iii) deve concernere "*direttamente o indirettamente, uno o più emittenti o uno o più strumenti finanziari*"; ed infine, (iv) "*se resa pubblica*", è necessario che sia idonea a comportare "*un effetto significativo sui prezzi di tali strumenti finanziari o sui prezzi di strumenti finanziari derivati collegati*".

Tale obbligo di comunicazione sorge, dunque, non appena le *inside informations* (che non siano state ancora divulgate al pubblico e che possano influire in modo significativo sul prezzo di uno strumento finanziario), assumono contorni "precisi" e siano pertanto suscettibili di un indebito utilizzo.

In questo modo, il legislatore europeo ha inteso perseguire il duplice obiettivo di "*evitare l'abuso di tali informazioni*", e, al contempo, di "*assicurare che gli investitori non vengano fuorviati*", come enunciato dal Considerando n. 49, MAR.

Proprio a tale scopo, l'art. 17, par. 1, MAR prevede che la pubblicazione delle informazioni in parola debba avvenire "*quanto prima possibile*" ("*as soon as possible*" nella versione inglese del regolamento), secondo "*modalità*" che consentano non solo un "*accesso rapido*" ad esse, ma anche una loro "*valutazione completa, corretta e tempestiva*" ossia, come precisato dalla Consob, "entro il lasso temporale necessario per la redazione del comunicato stampa". Ciò, al fine di permettere sia "una valutazione completa e corretta dell'informazione da parte del pubblico" sia una "sua successiva trasmissione al Sistema per la Diffusione delle Informazioni Regolamentate ("SDIR") o ai media"[414].

Le modalità con cui gli emittenti sono tenuti a pubblicare le *inside informations* sono poi disciplinate in modo più analitico dal Regolamento di esecuzione (UE) 2016/1055[415], il cui Considerando n. 1 afferma emblematicamente (i) che, al fine di "*tutelare gli investitori*" è necessario che gli emittenti comunichino al pubblico le informazioni privilegiate "*efficacemente e tempestivamente*"; (ii) e che, per "*assicurare a livello di Unione parità di accesso a tutti gli investitori*", le medesime informazioni devono "*essere comunicate al pubblico gratuitamente, simultaneamente e quanto più rapidamente possibile, raggiungendo tutte le categorie di investitori in tutta l'Unione, e dovrebbero essere comunicate ai mezzi di informazione ai fini dell'effettiva divulgazione al pubblico*".

Quale novità ulteriore rispetto alla MAD 1, il MAR disciplina con maggiore analiticità due ordini di ipotesi in cui l'obbligo di immediata pubblicazione può subire una deroga.

La prima, di carattere generale, è prevista dall'art. 17, par. 4, MAR, ai sensi del quale ciascun emittente ha la facoltà di ritardare, "*sotto la sua responsabilità*", la comunicazione al pubblico di informazioni privilegiate, subordinatamente

---

[411] Cfr. il Considerando n. 3 MAR.

[412] Cfr. art. 17, par. 1, MAR.

[413] Cfr. art. 17, par. 2, MAR.

[414] Consob, *Gestione delle informazioni privilegiate, Guide operative*, aprile 2017, disponibile al seguente link: www.consob.it/documenti/…/lavori…/GuidaOperativa_gestione_20170406.pdf.

[415] Regolamento di esecuzione (UE) 2016/1055 della Commissione del 29 giugno 2016, che stabilisce norme tecniche di attuazione per quanto riguarda gli strumenti tecnici per l'adeguata comunicazione al pubblico delle informazioni privilegiate e per ritardare la comunicazione al pubblico di informazioni privilegiate ai sensi del regolamento (UE) n. 596/2014 del Parlamento europeo e del Consiglio.

al verificarsi di "*tutte*" le condizioni previste, ossia: (i) che "*probabilmente*" la comunicazione, se immediata, pregiudicherebbe i "*legittimi interessi*"[416] dello stesso emittente; (ii) che "*probabilmente*" il ritardo nella comunicazione non avrebbe "*l'effetto di fuorviare il pubblico*"; (iii) che in ogni caso l'emittente sia "*in grado di garantire la riservatezza di tali informazioni*". L'emittente è tenuto a notificare *ex post* il ritardo all'Autorità competente (ossia "*immediatamente dopo che le informazioni sono state comunicate al pubblico*"), fornendo "*per iscritto una spiegazione delle modalità con cui sono state soddisfatte*" le già elencate condizioni.

La seconda ipotesi di deroga, prevista dall'art. 17, par. 5, MAR all'espresso fine di "*salvaguardare la stabilità del sistema finanziario* , è invece riservata unicamente agli emittenti che siano *enti creditizi o istituti finanziari*. Ciascuno di essi può ritardare, ugualmente "*sotto la sua responsabilità*", la comunicazione al pubblico di *inside informations*, ivi "*comprese le informazioni legate a un problema temporaneo di liquidità e, in particolare, la necessità di ricevere assistenza temporanea di liquidità da una banca centrale o da un prestatore di ultima istanza*".

Ciò, ancora una volta subordinatamente al verificarsi di "*tutte*" le condizioni previste, ossia: (i) che alla comunicazione *de qua* consegua "*il rischio di compromettere la stabilità finanziaria dell'emittente e del sistema finanziario*"; (ii) che il ritardo è "*nell'interesse pubblico*"; (iii) che è possibile garantire la "*riservatezza delle informazioni*"; (iv) che il ritardo è stato autorizzato dalla "*autorità competente*". Con riferimento a tale ultima condizione, è opportuno evidenziare che l'emittente è tenuto, in tal caso, a notificare *ex ante* la propria intenzione di avvalersi della facoltà di ritardare la pubblicazione all'Autorità competente, la quale "*provvede affinché la comunicazione di informazioni privilegiate sia ritardata solo per il tempo necessario per il pubblico interesse*" e "*valuta almeno su base settimanale*" se le condizioni elencate sono "*ancora soddisfatte*". Viceversa, nel caso in cui l'Autorità competente non autorizzi il ritardo della pubblicazione, l'emittente è tenuto a comunicare "*immediatamente le informazioni privilegiate*"[417].

Resta fermo che gli emittenti, anche nelle ipotesi in cui abbiano inteso avvalersi della facoltà di ritardo di cui agli artt. 4 e 5, MAR, sono in ogni caso tenuti a comunicare "*quanto prima*" le informazioni *de quo*, in concomitanza di *rumors* che siano sufficientemente precisi e comunque tali "*da indicare che la riservatezza di tali informazioni non è più garantita*"[418].

3. LO SCAMBIO DI INFORMAZIONI "DALLA" PLATEA DEGLI INVESTITORI: LA PROFILATURA DEI CLIENTI NEL REGIME DELLA MIFID I

Per quanto concerne, invece, lo scambio di informazioni "dalla" platea degli investitori l'art. 21 del t.u.f., dispone, in generale e nel rispetto della c.d. "*know your customer rule*", che gli intermediari, nella prestazione dei servizi e delle attività di investimento, oltre a comportarsi con diligenza, correttezza e trasparenza, per servire al meglio l'interesse degli investitori e ad operare in modo che questi ultimi siano sempre adeguatamente informati, sono obbligati ad "*acquisire, le informazioni necessarie dai clienti*"[419].

---

[416] Un elenco "*indicativo*" e "*non esaustivo*" dei "*legittimi interessi*" degli emittenti che potrebbero essere pregiudicati dalla comunicazione immediata al pubblico di informazioni privilegiate e delle situazioni in cui il ritardo nella comunicazione di informazioni privilegiate può indurre in errore il pubblico, ai sensi dell'art. 17, par. 11 del regolamento (UE) n. 596/2014 è stato predisposto dall'ESMA (cfr. ESMA/2016/1478 IT *Orientamenti relativi al regolamento sugli abusi di mercato (MAR) Ritardo nella comunicazione al pubblico di informazioni privilegiate*, 20 ottobre 2016, disponibile al seguente link: https://www.esma.europa.eu/system/files_force/library/esma-2016-1478_it.pdf?...1

[417] Cfr. l'art. 17, par 6, MAR.

[418] Cfr. l'art. 17, par 7, MAR.

[419] Sull'informazione nella prestazione di servizi di investimento, cfr. per tutti, B. Inzitari, V. Piccinini, *La tutela del cliente nella negoziazione di strumenti finanziari*, Padova, 2008 e A. Albanese, *L'informazione pre-contrattuale degli intermediari*, in *Contr. impr.*, 2010, 103.

Nello scenario normativo conseguente all'introduzione della MiFID I, tale obbligo è poi ulteriormente integrato e specificato in sede regolamentare dalla CONSOB. Ed infatti, il Regolamento intermediari[420] impone alle imprese di investimento non trascurabili obblighi di profilazione della clientela.

In particolare, nella prestazione dei servizi di consulenza in materia di investimenti o di gestione di portafogli, con riferimento al giudizio di c.d. adeguatezza, l'art. 39 del Regolamento intermediari dispone che, al fine di raccomandare i servizi di investimento e gli strumenti finanziari più adatti, gli operatori abilitati devono ottenere dal cliente (anche solo potenziale) "*le informazioni necessarie*" relative: a) "*alla conoscenza ed esperienza nel settore di investimento rilevante per il tipo di strumento o di servizio*"; b) "*alla situazione finanziaria*"; c) "*agli obiettivi di investimento*". La norma aggiunge che tali informazioni devono includere anche ulteriori "*elementi, nella misura in cui siano appropriati tenuto conto delle caratteristiche del cliente, della natura e dell'importanza del servizio da fornire e del tipo di prodotto od operazione previsti*", quali, in particolare: a) "*i tipi di servizi, operazioni e strumenti finanziari con i quali il cliente ha dimestichezza*"; b) "*la natura, il volume e la frequenza delle operazioni su strumenti finanziari realizzate dal cliente e il periodo durante il quale queste operazioni sono state eseguite*"; c) "*il livello di istruzione, la professione o, se rilevante, la precedente professione del cliente*"; d) ulteriori dati ("*ove pertinenti*"), "*sulla fonte e sulla consistenza del reddito del cliente, del suo patrimonio complessivo, e dei suoi impegni finanziari*"; e) nonché "*sul periodo di tempo per il quale il cliente desidera conservare l'investimento, le sue preferenze in materia di rischio, il suo profilo di rischio e le finalità dell'investimento*".

Per quanto concerne, invece, la prestazione dei servizi diversi da quelli di consulenza e di gestione dei portafogli, in relazione al giudizio di c.d. appropriatezza, l'intermediario deve altresì verificare, ai sensi dell'art. 42 del Regolamento intermediari, che "*il cliente abbia il livello di esperienza e conoscenza necessario per comprendere i rischi che lo strumento o il servizio di investimento offerto o richiesto comporta*".

Da tali brevi cenni, risulta chiaro come già lo scenario normativo conseguente alla MiFID I legittimi gli intermediari ad una puntuale attività di raccolta dei dati e ad una conseguente profilazione dei clienti, in relazione ai giudizi di adeguatezza ed appropriatezza, nonché ai fini della classificazione degli stessi nelle note categorie di: a) "clienti al dettaglio", ovvero dei soggetti che, ai sensi dell'art. 26 del Regolamento intermediari, sono differenti dai clienti professionali o dalle controparti qualificate; b) "clienti professionali" ovvero persone fisiche e giuridiche che rispondono agli specifici presupposti previsti dal Regolamento intermediari, relativi sia alla frequenza con cui svolgono determinate operazioni di investimento, sia alle dimensioni di queste ultime; c) "controparti qualificate" le quali, ai sensi dell'art. 58 del Regolamento intermediari, sono, ad esempio, le imprese di investimento, le banche, le società di gestione del risparmio, le imprese di assicurazione, gli organismi di investimento collettivo, i fondi pensioni, ecc.[421]

3.1. SEGUE. LA PROFILATURA DEI CLIENTI A SEGUITO DELL'ENTRATA IN VIGORE DELLA MIFID II

Se questo è lo scenario conseguente alla disciplina della MiFID I, occorre evidenziare che la MiFID II, la cui entrata in vigore è prevista per il mese di gennaio 2018, legittima le imprese di investimento a procedere ad una raccolta dei dati dei clienti ancor più penetrante, incisiva ed omnicomprensiva.

Ed infatti, l'attività di profilatura degli investitori *(i)* se da un canto, con la MiFID I è essenzialmente funzionale (e dunque limitata) alla fase conclusiva di collocazione dei prodotti finanziari, al fine di indirizzare i clienti verso gli strumenti più consoni alle loro esigenze e/o al loro profilo di rischi; *(ii)* d'altro canto, a seguito della MiFID II, è suscettibile di essere

[420] Regolamento adottato dalla Consob con delibera n. 16190 del 29 ottobre 2007.

[421] Al riguardo, cfr. per tutti U. Minneci, *Servizi di investimento e gradazione dei clienti*, Milano, 2013.

estesa anche alle fasi precedenti, relative alla ideazione, alla predisposizione ed alla distribuzione dei medesimi prodotti.

Ciò, è una conseguenza della introduzione di ulteriori obblighi, il cui principale obiettivo è quello di garantire che la tutela degli investitori sia "incorporata nelle dinamiche organizzative dell'intermediario"[422] e, più in particolare, "nell'ambito della c.d. *product governance*, ossia quella fase finalizzata a divenire l'elemento organizzativo fondamentale atto a guidare l'intero ciclo di vita del prodotto", allo scopo di "impedire e ridurre, fin dal momento iniziale, i potenziali rischi legati all'esistenza di prodotti che non siano corrispondenti alla protezione dei potenziali investitori"[423].

Il procedimento relativo alla *product governance* è sostanzialmente disciplinato dal combinato disposto degli artt. 16, par. 3 e 24, par. 2 della MiFID II.

In base alla prima delle due norme, le imprese di investimento emittenti prodotti finanziari sono tenute ad adottare ed a sottoporre a verifiche un "*processo di approvazione*" sia "*per ogni strumento finanziario*", sia "*per ogni modifica significativa agli strumenti finanziari esistenti*". La medesima disposizione prevede, inoltre, che nell'ambito di tale "*processo di approvazione del prodotto*" occorre non solo precisare "*per ciascuno strumento finanziario il determinato mercato di riferimento di clienti finali all'interno della pertinente categoria di clienti*", ma anche garantire "*che tutti i rischi specificamente attinenti a tale target siano stati analizzati e che la prevista strategia di distribuzione sia coerente con il target stesso*". Inoltre, gli emittenti sono tenuti a mettere "*a disposizione dei distributori tutte le necessarie informazioni sullo strumento finanziario e sul suo processo di approvazione, compreso il suo mercato target*".

Dal proprio canto, l'art. 24, par. 2 della medesima direttiva stabilisce che le imprese di investimento emittenti strumenti finanziari: (i) "*fanno sì che tali prodotti siano concepiti per soddisfare le esigenze di un determinato mercato di riferimento di clienti finali individuato all'interno della pertinente categoria di clienti e che la strategia di distribuzione degli strumenti finanziari sia compatibile con il target*"; (ii) sono inoltre tenute ad adottare "*misure ragionevoli per assicurare che lo strumento finanziario sia distribuito ai clienti all'interno del mercato target*"; (iii) infine, devono "*conoscere gli strumenti finanziari offerti o raccomandati, valutarne la compatibilità con le esigenze della clientela cui fornisce servizi di investimento tenendo conto del mercato di riferimento di clienti finali (…) e fare in modo che gli strumenti finanziari siano offerti o raccomandati solo quando ciò sia nell'interesse del cliente*".

È dunque chiaro che la disciplina relativa alla *product governance*, incentrandosi sul concetto "chiave" rappresentato dalla nozione di "*mercato di riferimento di clienti finali*" o "*mercato target*"("*identified target market of end clients*", nella versione del provvedimento in lingua inglese) comporti un ampliamento delle informazioni relative ai clienti, che le imprese di investimento sono obbligate a raccogliere ed elaborare.

Proprio l'individuazione (*ex-ante* e per ogni singolo prodotto da collocare) di tale "*mercato target*", è idonea a determinare non solo una applicazione anticipata della "*know your customer rule*", ma anche una conseguente estensione degli obblighi di profilatura degli investitori da parte degli intermediari.

Tale circostanza trova conferma nel *Consultation Paper* lanciato dall'ESMA in data 5 ottobre 2016[424], all'esito del quale l'Autorità europea ha predisposto un *Final Report* relativo alle *Guidelines on MiFID II product governance requirements* pubblicato il 2 giugno 2017[425].

---

[422] S. Molino, *La product governance nel nuovo regime MiFID 2*, in *Dirittobancario.it*, aprile 2016.

[423] F. Mattassoglio, *La profilazione dell'investitore nell'era dei Big Data. I rischi dell'estremizzazione della regola del "know your customer"*, in *Riv. trim. dir. econom.*, Supplemento n. 4/2016, 240.

[424] ESMA/2016/1436, *Consultation Paper. Draft guidelines on MiFID II product governance requirements*, 5 ottobre 2016, disponibile al seguente link: https://www.esma.europa.eu/sites/default/files/library/2016-1436_cp_guidelines_on_product_governance.pdf

[425] ESMA35-43-620, *Final Report. Guidelines on MiFID II product governance requirements*, 2 giugno 2017, disponibile al seguente link: https://www.esma.europa.eu/sites/default/files/library/esma35-43-620_report_on_guidelines_on_product_governance.pdf

In tale documento, l'ESMA non solo afferma ripetutamente che il "*target market assessment*" rappresenta l'aspetto "*most important (…) for ensuring the common, uniform and consistent application of the new requirements*", ma, ai fini della sua individuazione e delimitazione, esorta le imprese di investimento all'utilizzo di ben cinque "*categories*", in base alle quali procedere ad una accurata profilatura della clientela, ovvero: 1) il "*type of clients to whom the product is targeted*"; 2) la "*Knowledge and experience*"; 3) la "*Financial situation with a focus on the ability to bear losses"*; 4) la "*Risk tolerance and compatibility of the risk/reward profile of the product with the target market*"; 5) i "*Clients' Objectives and Needs*"[426].

Oltre a ciò, la MiFID II contiene anche esplicite previsioni relative ad un incremento dei *database* dei clienti, atteso che essa sancisce a carico delle imprese di investimento l'obbligo di conservare, "*per un periodo di cinque anni e, se richiesto dall'autorità competente, per un periodo fino a sette anni*", tutte le registrazioni "*delle conversazioni telefoniche o delle comunicazioni elettroniche che riguardino almeno le operazioni concluse in caso di negoziazione per conto proprio e la prestazione di servizi di ordini della clientela connessi alla ricezione, trasmissione ed esecuzione di tali ordini*", con l'ulteriore precisazione che tali conversazioni telefoniche e comunicazioni elettroniche "*comprendono anche quelle intese a concludere operazioni con negoziazione per conto proprio o nella fornitura alla clientela servizi di ricezione, trasmissione ed esecuzione di ordini, anche se tali conversazioni o comunicazioni non conducono alla effettiva conclusione di operazioni o alla prestazione di servizi*"[427].

4. BIG DATA E FINTECH: LA *ROBO-ADVISORY*

È, dunque, evidente come l'osmotico scambio di informazioni "alla" e "dalla" clientela sia idoneo a determinare un ampliamento dell'attività di raccolta e di analisi dei dati da parte delle imprese di investimento talmente rilevante, da non poter essere gestito in modo efficiente se non per il tramite dei Big Data.

Non a caso, il crescente impiego di tale tecnologia è destinato a pervadere l'intero settore dei servizi di investimento, innovando a tal punto i relativi modelli di *business*, da imporsi anche sulle più recenti dinamiche evolutive del FinTech, quale ulteriore volano di sviluppo e progresso delle tecnologie informatiche e telematiche applicate ai servizi finanziari.

Ed infatti, i Big Data consentono una implementazione pressoché illimitata dei *software* e degli algoritmi predittivi alla base delle più sofisticate tecniche di *trading* quantitativo e, più in generale, di *goal-based wealth management*, nella acquisita consapevolezza che, attualmente, nel mercato mobiliare si è inclini non più solo (e tanto) a massimizzare la collocazione dei prodotti finanziari presso il pubblico degli investitori, ma anche (e soprattutto) a fornire sempre più accurati servizi relativi all'analisi dei bisogni di questi ultimi, al fine di individuare le soluzioni d'investimento più adattate alla soddisfazione delle esigenze di ogni singolo cliente[428].

In tale contesto innovativo ed in continua trasformazione, uno tra i principali effetti del processo di digitalizzazione dei servizi finanziari è dato dalla tendenza verso la loro crescente disintermediazione, come è possibile riscontrare soprattutto a proposito della consulenza in materia di investimenti.

Al riguardo, infatti, la più ampia attività di sperimentazione di soluzioni tecnologicamente avanzate può essere riscontrata proprio nell'ambito della *digital adivice*, ove si assiste al moltiplicarsi dei cc.dd. "*Robo-advisors*".

Con tale termine "si fa riferimento ad un fenomeno di ampia e variegata portata, che include molteplici fattispecie talora diversificate, unite, però, dal comune denominatore di sfruttare le più moderne tecnologie, piattaforme ed algoritmi

[426] ESMA35-43-620, *Final Report*, 34 s.
[427] Cfr. l'art. 16, par. 6 e par. 7, MiFID II.
[428] Cfr. P. Sironi, *FinTech Innovation: From Robo-Advisors to Goal Based Investing and Gamification*, John Wiley & Sons, 2016.

per la creazione di portafogli modello da raccomandare agli investitori, riproponendo così le diverse sfaccettature della consulenza intesa in senso lato, a partire da quella generica con l'*asset allocation* sino alla consulenza finanziaria vera e propria"[429].

Innegabile è, dunque, l'impatto "*disruptive*" della *Robo-advisory*, la quale, essendo un servizio di *wealth management* semplificato e meno oneroso rispetto alla consulenza tradizionale, ha la potenzialità di conquistare nuovi segmenti di mercato, se non altro, attraendovi la clientela *retail* meno propensa (o, *tout court*, impossibilitata) a rivolgersi ai soggetti istituzionali del settore.

Altrettanto evidente è il carattere non solo estremamente complesso e variegato della *Robo-advisory*, ma anche "camaleontico"[430], nella misura in cui essa può giovarsi delle ampie possibilità di sviluppo offerte dal "limbo regolamentare" in cui si muove l'intera "rete del FinTech", favorendone "l'azione"[431].

Ciò spiega il motivo per cui le Autorità di vigilanza, tanto europee[432], quanto nazionali[433], si sono finora essenzialmente limitate a porre il fenomeno sotto una attenta lente di osservazione, alla stregua di un "sorvegliato speciale in attesa di giudizio regolamentare"[434].

In ogni caso, tali nuove tecnologie FinTech non sono scevre di rischi per i consumatori, nel momento in cui non solo possono comportare un annichilimento del modello classico di consulenza, intesa come relazione di natura prettamente personale e fiduciaria, ma affidano pressoché esclusivamente ad *automated tools* ogni attività di profilazione dei clienti, sia pur utilizzando "appieno la capacità di data analysis e gli elevati standard di *user experience* digitali tipici dei migliori tool di *personal finance management*"[435].

Ed infatti, è forse proprio in combinazione con la *Robo-advisory* che i Big Data giungono a svolgere "un ruolo attivo, non meramente servente", essendosi al riguardo acutamente osservato che non "è la prima volta nella storia dell'Occidente che la macchina fa irruzione sullo scenario (…) economico", laddove però la "differenza con il passato è … che stavolta la macchina conduce i giochi, non l'uomo. L'algoritmo è sovrano"[436].

---

[429] M.T. Paracampo, *Robo-advisor, consulenza finanziaria e profili regolamentari: quale soluzione per un fenomeno* in fieri*?* in *Riv. trim. dir. econom.*, Supplemento n. 4/2016, 258.

[430] Ivi, 261.

[431] Consob, *Incontro annuale con il mercato finanziario*, *Discorso del Presidente al mercato finanziario*, Milano, 8 maggio 2017, 21, disponibile al seguente link: http://www.consob.it/documents/11973/1102412/dsc2017.pdf/4b129aa8-b702-4f6f-91e8-94d38e-de6114

[432] Le Autorità di vigilanza europee, infatti, al fine di monitorare il fenomeno in oggetto, hanno lanciato un apposito *Discussion Paper* (cf. ESMA, EBA, EIOPA, *JC/2015/080, Joint Discussion Paper on automation in financial advice*, 4 dicembre 2015, disponibile al seguente link: https://eiopa.europa.eu/Publications/Consultations/JC%202015%20080%20Discussion%20Paper%20on%20automation%20in%20financial%20advice.pdf).
Al riguardo, si rinvia a D. Siclari, G. Sciascia, *Innovazione finanziaria e rafforzamento del mercato unico per i servizi finanziari retail: sfide, rischi, risposte della regolazione*, in *Riv. Trim. Dir. Econom.*, 2016, I, 184 ss.

[433] Cfr. Consob, *Piano strategico 2016-2018*, disponibile al seguente link: www.consob.it/documents/11973/...pdf/7a462189-574c-4a20-9dc2-198c08a29956, ove è dato leggere che l'Autorità è, tra l'altro, "impegnata nello studio dell'impatto (…) della digitalizzazione sui processi di intermediazione finanziaria e sulla nuova concezione del rapporto intermediario - cliente (es. *robo advice*)".

[434] Cfr. M.T. Paracampo, *Robo-advisor, consulenza finanziaria e profili regolamentari: quale soluzione per un fenomeno* in fieri*?* in *Riv. trim. dir. econom.*, Supplemento n. 4/2016, 266.

[435] R. Ferrari, *L'era del fintech*, FrancoAngeli, Milano, 2016, 79.

[436] S. Mannoni, G. Stazi, *Un'antitrust per difendere le democrazie dai Big data*, *ilsole24ore.com*, disponibile al seguente link: http://www.ilsole24ore.com/art/commenti-e-idee/2017-06-14/un-antitrust-difendere-democrazie-big-data-195044.shtml?uuid=AErsybdB

5. BENEFICI E RISCHI DELL'APPROCCIO "*DATA DRIVEN*" NEI SERVIZI DI INVESTIMENTO

Alla luce dei brevi cenni che precedono, è chiaro come le tecnologie alla base dei Big Data saranno sempre più necessarie per favorire un approccio "*data driven*" nei servizi di investimento e che le c.d. quattro "*V*", che notoriamente contraddistinguono questa tecnologia (volume, varietà, velocità e valore) sono idonee a determinare una maggiore accuratezza nella prevedibilità del comportamento degli investitori proprio attraverso la raccolta, l'analisi e l'elaborazione di una ingente quantità di informazioni, anche di carattere strettamente personale, fornite in modo più o meno consapevole e diretto da parte dei medesimi clienti.

Innegabili sono i benefici che tale penetrante attività di profilatura è in grado di comportare in termini di riduzione dei costi dei servizi prestati, nonché all'auspicabile fine indicato dalla stessa direttiva MiFID II di "*garantire che gli strumenti finanziari siano offerti o raccomandati soltanto se sono nell'interesse*"[437] degli investitori, con il conseguente abbandono delle offerte "di massa" di identici prodotti finanziari ad una indistinta platea di consumatori *retail*, a favore di una attività di collocamento di prodotti personalizzati, creati in funzione della soddisfazione delle specifiche esigenze dei clienti, e calibrati sulla base delle informazioni da questi ultimi forniti.

Altrettanto evidenti sono, tuttavia, anche i rischi che possono derivare dalla medesima tecnologia, la quale può, in primo luogo, risolversi un una vera e propria barriera all'accesso al mercato mobiliare da parte di quegli investitori (o categorie di investitori) che (i) non corrispondano ai "profili" elaborati sulla scorta dei dati processati, (ii) o che, più semplicemente, non siano in possesso delle necessarie conoscenze di tipo informatico e telematico.

Inoltre, non può escludersi che i Big Data siano utilizzati dai *players* del mercato mobiliare (fisici o virtuali che siano) al fine di selezionare i clienti migliori, perché maggiormente corrispondenti alle strategie di mercato di ciascuno di essi, escludendo al contempo dai servizi di investimento determinati soggetti (o gruppi di soggetti) meno attraenti da un punto di vista remunerativo.

Spetta, conseguentemente, alle Autorità di vigilanza europee e nazionali ricercare un adeguato "punto di equilibrio" tra i rischi ed i benefici dell'impiego sempre più massiccio dei Big Data nel settore mobiliare e della intermediazione finanziaria, affinché, per un verso, sia garantito "agli investitori e al mercato un livello appropriato di protezione", e, per altro verso, non sia soffocato lo sviluppo di "innovazione e competitività", anche al fine "di abbattere i costi per i risparmiatori"[438].

Tali obiettivi sembrano, attualmente, raggiungibili laddove si acquisisca la piena "consapevolezza che una parte importante, forse addirittura la parte più importante della vigilanza, partecipa già oggi e a pieno titolo alle sfide del Big Data e non può non fondarsi che su avanzati meccanismi di raccolta, verifica e comunicazione al mercato di dati: milioni di dati e migliaia di algoritmi e metodologie private di trattamento degli stessi, che a loro volta richiedono sofisticati e costosi strumenti algoritmici e metodologie complesse di analisi".

Se ciò è vero, ne consegue, come la dottrina non ha mancato di rilevare, che "solo un'autorità in grado di effettuare di tempo in tempo gli investimenti, assai cospicui, in tecnologia, necessari per rispondere all'evoluzione di mercato, può ambire a svolgere una vigilanza quantomeno ragionevolmente credibile sui mercati dei capitali"[439].

---

[437] Considerando n. 71, par. 2, MiFID II.

[438] Cfr. Consob, *Incontro annuale con il mercato finanziario*, Milano, 8 maggio 2017, disponibile al seguente link: http://www.consob.it/documents/11973/1102412/dsc2017.pdf/4b129aa8-b702-4f6f-91e8-94d38ede6114

[439] M. Lamandini, *La vigilanza diretta dell'Esma. Un modello per il futuro?*, in *Giur comm.*, 2016, I, 453 s.

IVASS

(Alessandra Camedda, Andrea Luberti)

Big Data e assicurazioni. Profilazione degli assicurandi e problemi di tutela della *privacy* *

Gli obblighi informativi, tradizionalmente incombenti sugli assicurati nei confronti delle imprese, pongono specifici problemi soprattutto in relazione alla diffusione ai nuovi strumenti di diffusione e conservazione delle informazioni.

*Nell'ambito della rivoluzione tecnologica che ha investito il mercato assicurativo (c.d. "*Insurtech"*) un ruolo centrale è svolto dai* Big Data*, la cui raccolta da parte delle imprese di assicurazione agevola la conoscenza della potenziale clientela, consentendo una più efficace individuazione del corrispondente profilo di rischio e un miglioramento della competitività dei prodotti offerti. Lo sfruttamento dei* Big Data *presenta, tuttavia, numerosi profili di criticità: il carattere personale dei dati e le insidie connesse all'uso dei dispositivi deputati alla loro acquisizione determinano il rischio che il trattamento dei dati dei clienti possa tradursi in una violazione della disciplina sulla* privacy*. Le Autorità di vigilanza sul settore assicurativo, sia europee che nazionali, sono pertanto chiamate a valutare l'adeguatezza dell'attuale quadro normativo rispetto all'utilizzo dei* Big Data *nonchè l'opportunità di nuovi e più rigorosi interventi di regolamentazione e vigilanza sulla gestione dei dati da parte degli operatori.*

SOMMARIO: 1. I PROFILI DI ASIMMETRIA INFORMATIVA NEL CONTRATTO DI ASSICURAZIONE. – 2. LE INNOVAZIONI LEGISLATIVE. – 3. *INSURTECH*: LA RIVOLUZIONE TECNOLOGICA NEL SETTORE ASSICURATIVO. L'APPROCCIO DELLE *AUTHORITIES*. – 4. PROFILI DI CRITICITÀ: PROFILAZIONE E TUTELA DELLA *PRIVACY*. IL NUOVO REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (REGOLAMENTO 2016/679/UE). – 5. CONCLUSIONI.

1. I PROFILI DI ASIMMETRIA INFORMATIVA NEL CONTRATTO DI ASSICURAZIONE

(Andrea Luberti)

Le tematiche correlate alla corretta distribuzione delle informazioni, contrariamente a quanto potrebbe apparire da un'analisi superficiale, nel settore assicurativo non costituiscono una novità connessa alla recente espansione della circolazione dei dati personali. Semmai, può essere al massimo affermato che nell'ultimo ventennio sia riscontrabile una prolifica tendenza legislativa diretta a riequilibrare l'asimmetria informativa in favore del contraente-consumatore.

Tali tematiche, invece, costituiscono un problema costantemente avvertito dal legislatore, sin dall'epoca della codificazione civilistica, e ciò anche in relazione alla particolare funzione assunta dal sinallagma nel contratto di assicurazione.

Esso, in base a una normativa considerata di ordine pubblico, è infatti contraddistinto dal trasferimento di un *rischio* (inteso, secondo una nozione non espressamente fornita dal legislatore, ma desumibile in forza delle norme conferenti, come un *potenziale effetto economico negativo*) che può derivare da un evento, a sua volta, negativo, qualificabile come *sinistro* (come la morte, la malattia o un infortunio), ma anche neutro o addirittura positivo (come la sopravvivenza o la nuzialità).

L'art. 1895 del codice civile prevede, appunto, in modo solenne e inderogabile, la nullità del contratto di assicurazione, laddove il rischio non esista, o abbia cessato di esistere.

Minuziose indicazioni normative disciplinano inoltre la corretta allocazione del rischio tra le parti, anche in relazione alle informazioni fornite da parte del contraente (artt. 1896-1898 del codice civile). In linea di principio, deve essere sottolineato che sull'assicurato (anche nel corso del rapporto contrattuale) grava un generale obbligo di trasparenza e buona fede, che impone la comunicazione degli elementi essenziali (ai fini della delimitazione del rischio) che possano influire sulla decisione relativa all'assunzione dell'operazione contrattuale.

Per contro, l'assicuratore (a seguito della intervenuta ottemperanza a tale obbligo) vanta un altrettanto generale diritto di recesso, e conserva quindi la libertà di decidere se mantenere in vita il rapporto contrattuale anche in un momento successivo alla stipulazione del contratto. Risulta evidente, allora, la maggiore tutela di cui l'assicuratore gode rispetto al meccanismo previsto dall'art. 1467 del codice civile. Nel mercato assicurativo, infatti, l'impresa è tutelata anche rispetto a quegli eventi che potrebbero alterare anche in modo solo *potenziale* la propria valutazione sulla convenienza economica del contratto.

Il motivo per cui il legislatore ha sempre ritenuto di disciplinare tale tema in modo particolarmente approfondito è ricavabile intuitivamente se si prende in considerazione l'art. 1883 del codice civile, che riserva in modo espresso la stipulazione di contratti di assicurazione ai soli soggetti autorizzati, che, per espressa menzione normativa, possono essere solo *imprese*.

Dall'art. 2082 del codice civile è poi possibile ricavare agevolmente che elemento essenziale dell'attività di impresa è la professionalità.

Dal combinato disposto delle due disposizioni si desume in modo alquanto agevole che il meccanismo (non solo economico, ma anche) giuridico preso in considerazione dal legislatore è quello consistente nella stipulazione di una massa omogenea di contratti, tra cui ripartire eventuali devianze rispetto a criteri statistici predefiniti.

2. INNOVAZIONI LEGISLATIVE

(Andrea Luberti)

Le considerazioni sopra profuse risultano ancora più pregnanti se riferite a uno specifico settore del mercato assicurativo, quello dell'assicurazione (obbligatoria) RC auto.

Se, in apparenza, tale settore del comparto presenta l'indubbio vantaggio, per le imprese, di un obbligatorio ricorso alla stipulazione di contratti RC auto (pena la preclusione a circolare tramite veicoli a motore) non bisogna dimenticare che, ai sensi dell'art. 132, comma 1, del decreto legislativo 7 settembre 2005, n. 209 (Codice delle assicurazioni private), la stessa impresa di assicurazioni non ha la facoltà di rifiutare la stipulazione dei contratti offerti, con conseguente riequilibrio della forza contrattuale.

In effetti, l'evidenza empirica e giuridica tende a suggerire l'esistenza di una *doppia* asimmetria informativa: i) da un lato, il numero sostanzialmente ristretto degli operatori economici rende plausibile la possibilità di intese restrittive *sub specie* di scambio reciproco di informazioni (sovente sanzionate dall'Autorità garante della concorrenza e del mercato; ii) dall'altro, e all'opposto, il numero elevato degli assicurati rende pressoché impossibile un adeguato controllo sui comportamenti, sotto forma di legalità della guida o anche di denuncia di sinistri inesistenti. Risulta, allora, del tutto evidente lo scarso incentivo alla virtuosità dei contraenti, e la complessiva inefficienza economica del settore.

Per la verità, di recente, il legislatore ha tentato di innovare il settore tramite specifiche disposizioni contenute nella

legge 4 agosto 2017, n. 124 (legge annuale per il mercato e la concorrenza).

In particolare, al mercato della RC auto sono dedicati ben trentasette commi dell'unico articolo (secondo una deprecabile quanto frequente tecnica normativa) in cui si manifesta la legge.

Le norme dedicate alla RC auto ripercorrono soprattutto la strada dell'incentivo all'installazione di dispositivi idonei a rilevare i movimenti dei veicoli coinvolti nei sinistri (cc.dd. *scatole nere*), già prevista da precedenti interventi normativi.

Le innovazioni più importanti hanno riguardato l'art. 132-*ter* del codice delle assicurazioni, e hanno imposto l'obbligo di praticare riduzioni tariffarie in presenza del consenso ad: i) ispezioni del veicolo; ii) installazione di *"scatole nere*"; iii) installazione sul veicolo di dispositivi che precludano l'accensione del medesimo in presenza di superamento del tasso alcolemico consentito da parte del guidatore.

Soprattutto la terza fattispecie pone delicati problemi di tutela della riservatezza del contraente-consumatore, evidentemente spinto ad aderire a tali forme di controllo, in linea di massima meritevoli di tutela, dalla finalità di conseguire riduzioni tariffarie.

Il comma 20 della legge sul mercato e la concorrenza, inoltre, ha introdotto nel codice delle assicurazioni private un articolo 145-*ter*, che disciplina non solo la (piena) valenza probatoria delle "*scatole nere"*, ma anche la previsione di sistemi di *"interoperabilità"* che, nell'ottica del legislatore, dovrebbero consentire di scindere, in modo sempre più frequente, l'impresa di assicurazione da quella che provvede alla fornitura degli strumenti e delle applicazioni di controllo.

L'idoneità dei meccanismi descritti a migliorare l'efficienza del mercato assicurativo è stata recisamente contestata[440], anche con l'arguta osservazione che la forzata diffusione di tale tipologia di strumenti rischia di spostare le distorsioni del mercato dall'offerente la copertura assicurativa al produttore dei dispositivi di controllo, e si è dubitato della correttezza del loro inserimento in un atto normativo destinato a migliorare la concorrenza.

A ben vedere, tuttavia, se le finalità legalitarie ed efficientistiche dell'intervento non sembrano poter essere messe in discussione, maggiori dubbi riguardano la (sopra accennata) scissione tra titolarità del rapporto contrattuale e titolarità della trasmissione dei dati relativi al veicolo (si noti che, ai sensi del successivo comma 6, il titolare del veicolo non ha la possibilità giuridica di influire sul funzionamento del dispositivo di controllo).

Nel caso del controllo del tasso alcolemico ai fini della partenza del veicolo, come accennato, la preclusione all'utilizzo di automobile di propria titolarità, apparentemente ineccepibile, pone poi delicati spunti di tutela della proprietà personale nel caso di situazioni marginali (malfunzionamento del dispositivo, ovvero impedimento alla partenza pur in presenza di un superamento lieve e di una situazione di emergenza).

Ai sensi del comma 5 del nuovo art. 145-*ter* è, comunque, garantita l'applicazione della normativa di protezione dei dati personali, anche se andrà verificata l'idoneità di tale apparato normativo ad influire non già sulla mera titolarità delle informazioni, quanto sulla creazione di un vero e proprio mercato delle abitudini di guida e, nel caso del tasso alcolemico, persino delle abitudini di vita del contraente.

La crescente diffusione di obblighi informativi da parte degli assicurati, unitamente ai più recenti mutamenti tecnologici, pone ulteriori problemi di tutela della riservatezza che saranno esaminati nei paragrafi seguenti.

[440] D. Porrini, *La concorrenza? Non è in una scatola nera*, consultabile su www.lavoce.info del 5 settembre 2017.

3. *INSURTECH*: LA RIVOLUZIONE TECNOLOGICA NEL SETTORE ASSICURATIVO. L'APPROCCIO DELLE *AUTHORITIES*

(Alessandra Camedda)

I Big Data, espressione con la quale si è soliti definire l'enorme patrimonio di informazioni e dati personali reperibili sul *web*[441], assumono un ruolo centrale nell'ambito della rivoluzione tecnologica che ha recentemente investito il mercato assicurativo (c.d. "*Insurtech*").

La raccolta di tali dati da parte delle imprese di assicurazione può, infatti, agevolare la conoscenza dei potenziali clienti, consentendo una più efficace individuazione del corrispondente profilo di rischio e l'adattamento dell'offerta, in termini di qualità e prezzo, alle loro specifiche esigenze[442]. Essa, inoltre, può incidere positivamente sulla distribuzione dei prodotti[443] e sulla gestione e liquidazione dei sinistri, agevolata dalla possibilità di ricostruirne con precisione la dinamica e di scongiurare, in tal modo, il rischio di frodi[444].

I vantaggi sopra illustrati hanno indotto le imprese di assicurazione ad incrementare i propri investimenti nello sviluppo di nuove applicazioni tecnologiche, anche al fine di consentirne un'efficace integrazione con i più tradizionali sistemi di raccolta dei dati e di distribuzione dei propri prodotti e servizi[445].

Il legame tra le assicurazioni e la tecnologia è, dunque, destinato a divenire sempre più stretto; l'IVASS ne è consapevole e intende seguire con particolare attenzione il processo innovativo, anche al fine di individuarne i profili di rischio e di apportare eventuali adattamenti al quadro organizzativo e regolamentare[446].

Numerose sono le iniziative già intraprese in tal senso dall'Autorità di vigilanza. Tra queste, occorre segnalare l'istituzione di un apposito gruppo di lavoro incaricato di individuare misure idonee a garantire un bilanciamento tra l'apprez-

---

[441] Come evidenziato da M. Bogni, A. Defant, *Big Data: diritti IP e problemi della* privacy, in Il Diritto industriale, 2015, 2, 117, le fonti dei Big Data sono molteplici ed eterogenee; esse non si riducono al *web*, nell'ambito del quale i dati sono generati principalmente dai motori di ricerca, dai cc.dd. "*cookies"* e dai *social network*, ma possono essere costituite anche dalle più comuni carte fedeltà dei negozi e dal c.d. *Internet of Things* (*breviter*: IoT). Proprio l'IoT è destinato a divenire la principale fonte di generazione dei Big Data, trattandosi di un sistema caratterizzato dalla connessione ad internet di qualsivoglia oggetto della quotidianità come i telefoni cellulari, le automobili e le case. Più precisamente, ogni oggetto viene dotato di un *chip* interno che gli consente di registrare informazioni e di trasmetterle ad altri dispositivi, con i quali va a costituire una vera e propria rete. Le principali caratteristiche dei Big Data sono: 1. *Volume* (quantità); 2. *Viscosity* (varietà di fonti); 3. *Variety* (varietà di tipologie dei dati); 4. *Velocity* (elevata velocità di generazione); 5. *Virality* (velocità di trasmissione e diffusione).

[442] In particolare, lo sfruttamento dei Big Data è destinato ad incidere sulle modalità di determinazione del premio, destinate ad evolversi in tre direzioni: 1. progressiva personalizzazione, con abbandono del criterio di determinazione su base statistica; 2. determinazione di tipo predittivo (c.d. *forward-looking*) fondata sull'analisi dei dati personali e comportamentali raccolti e delle previsioni altamente attendibili che ne scaturiscano; 3. dinamicità, ossia periodico adeguamento del premio al variare del profilo di rischio del cliente. Così L. Servidio, *Big Data. Siamo solo all'inizio*, in *Insurance Review*, 2015, 51 ss.

[443] Anche grazie allo sfruttamento di nuovi canali quali le piattaforme *peer to peer*. Cfr. Ivass, *Relazione sull'attività svolta dall'Istituto nell'anno 2016*, Roma 23 giugno 2017, 141.

[444] Il ricorso ai Big Data è molto diffuso nel settore della RC auto mediante offerta di polizze che prevedono l'installazione, a bordo del veicolo, di dispositivi elettronici in grado di registrarne l'attività (scatole nere e localizzatori GPS); i dati memorizzati dai *devices*, spesso combinati con quelli provenienti da "fonti esterne" (ad esempio, i dati forniti dai GPS relativamente al traffico e alle caratteristiche delle strade) consentono, infatti, alle imprese di assicurazione di godere di un ampio margine di personalizzazione del premio, ossia di determinarne l'entità in base all'effettiva condotta di guida dell'assicurato secondo il modello del "*pay how you drive*".

[445] Secondo quanto riportato dall' *Italian AXA Paper n. 8 – Le sfide dei dati. Editoriale*, cit., 4, gli investimenti nella c.d. l'InsurTech ammontavano a circa 2 miliardi di dollari nei primi 9 mesi del 2016 e già nel 2015 si erano sostanzialmente triplicati a livello mondiale, passando da 0,8 nel 1024 a 2,6 miliardi.

[446] Ivass, *Relazione sull'attività svolta dall'Istituto nell'anno 2016. Considerazioni del* Presidente Salvatore Rossi, Roma 23 giugno 2017, 14.

zabile progresso tecnologico e la doverosa tutela dei consumatori. Inoltre, tenendo conto dei documenti in materia pubblicati dal G7 e dall'IAIS[447], l'IVASS ha recentemente sottoposto alle imprese nazionali un nuovo questionario sul *cyber risk*, i cui esiti hanno evidenziato una crescente vulnerabilità dell'industria assicurativa al rischio di attacchi informatici[448] e la necessità per gli operatori del settore di attivare adeguati processi di mitigazione e gestione del suddetto rischio[449].

Con riguardo ai Big Data merita di essere segnalata anche l'attività intrapresa dall'IVASS in vista dell'applicazione, a partire dal 25 maggio 2018, della nuova disciplina europea in tema di tutela dei dati personali introdotta dal Regolamento 2016/679/UE. Dinanzi ai numerosi profili di novità della disciplina, sui quali ci si soffermerà nel prosieguo, l'IVASS ha avviato studi sul tema nonchè i primi contatti con il Garante per la protezione dei dati personali volti ad individuare gli adeguamenti organizzativi e procedurali eventualmente necessari per garantire agli utenti la protezione dei dati personali raccolti[450].

4. PROFILI DI CRITICITÀ: PROFILAZIONE E TUTELA DELLA *PRIVACY*. IL NUOVO REGOLAMENTO EUROPEO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (REGOLAMENTO 2016/679/UE)

(Alessandra Camedda)

Le attività dell'IVASS, sopra sinteticamente descritte, evidenziano le criticità legate all'uso dei Big Data e, segnatamente, la possibile incidenza negativa del fenomeno sulla sicurezza dei dati e sulla tutela della *privacy*. Infatti, i dati raccolti hanno carattere personale e sono spesso acquisiti durante la navigazione in rete con strumenti altamente tecnologici e non percepibili dagli utenti; questi ultimi, altrettanto spesso, cedono i propri dati al fine di ottenere servizi apparentemente gratuiti[451]. Gli stessi dati sono, inoltre, esposti alla minaccia del *cyber crime*, come dimostrato dalla diffusione del fenomeno dell'*hackeraggio* dei dati salvati sul *cloud*.

La rilevanza del problema è evidenziata anche dai significativi interventi del legislatore europeo secondo cui la *privacy* e la sicurezza dei dati devono governare lo sviluppo e l'uso delle nuove tecnologie. Tra questi, occorre rammentare il c.d. "Pacchetto protezione dati", con il quale le Istituzioni europee hanno delineato un nuovo quadro comune in materia di tutela dei dati personali[452]. Il Pacchetto consta di due fondamentali provvedimenti: a) il nuovo Regolamento europeo in materia di protezione dei dati personali[453]; b) la Direttiva in materia di trattamento dei dati personali nei settori di prevenzione, contrasto e repressione dei crimini[454].

---

[447] *International Association of Insurance Supervisors.*

[448] Trova conferma quanto già rilevato da EIOPA, *Risk Dashboard April 2017*, p. 10, pubblicato lo scorso 16 maggio, ove si legge: "*Market analysts expect the insurance marketplace to change more drastically in 2017 than before, also due to the rising threat of cyber-attacks*".

[449] IVASS, *Relazione sull'attività svolta dall'Istituto nell'anno 2016*, cit., 141 ss.

[450] IVASS, *Relazione sull'attività svolta dall'Istituto nell'anno 2016*, cit., 145 ss.

[451] Basti pensare alle *App* per i telefoni cellulari, agli *account* di posta elettronica o all'accesso a siti di vendita *online*. Così M. BOGNI, A. DEFANT, *Big Data: diritti IP e problemi della* privacy, cit., 118.

[452] Sul tema, v. A. MANTELERO, *La riforma della* Data protection *in Europa: un'opportunità per le imprese*, in questa *Rivista*, Approfondimento del 03 marzo 2014.

[453] Si tratta del Regolamento 2016/679/UE *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*, con il quale è stata abrogata la direttiva 95/46/CE (recante il regolamento generale sulla protezione dei dati). Pubblicato sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) lo scorso 4 maggio ed entrato in vigore il 24 maggio 2016, il nuovo Regolamento UE in materia di *privacy* diventerà definitivamente applicabile in via diretta a tutti gli Stati membri dell'UE a partire dal 25 maggio 2018; termine entro il quale i vari Stati dovranno adeguare le rispettive disposizioni interne in materia di protezione dei dati alla nuova disciplina comunitaria.

[454] Anche la Direttiva 2016/680/UE è stata pubblicata sulla GUUE il 4 maggio 2016; è in vigore dal successivo 5 maggio e

Merita un cenno in questa sede, per le significative ricadute sul tema in esame, il Regolamento sopra citato, il quale mira a contemperare il diritto fondamentale delle persone fisiche alla tutela dei dati personali[455] con altri valori di pari rango e, segnatamente, con il diritto alla libertà d'impresa[456]. In particolare, preso atto dell'incremento dei flussi di dati personali e dello scambio, anche transfrontaliero, dei medesimi derivante dallo sviluppo tecnologico, il nuovo Regolamento europeo sulla *privacy* rafforza il quadro normativo comunitario in materia al fine di garantire ai soggetti interessati un adeguato controllo dei propri dati; il mercato digitale, infatti, potrà esprimere le proprie potenzialità in Europa soltanto attraverso la creazione di un clima di fiducia verso le nuove tecnologie[457].

Al fine di responsabilizzare le aziende a vario titolo coinvolte nel trattamento dei dati personali[458], il Regolamento prescrive l'adozione di misure particolarmente rilevanti sul piano della profilazione dei soggetti interessati[459].

Si segnala, *in primis*, l'istituzione della nuova figura professionale del "Responsabile della protezione dei dati" (il c.d. *Data Officer Protection*; *breviter*: DOP).

L'art. 37 del nuovo Regolamento prevede, infatti, l'obbligatoria designazione del DOP, ad opera del titolare e del responsabile del trattamento, ogni qualvolta le attività principali di questi ultimi consistano in "*trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala*" [460].

Si tratta di una novità di rilievo in quanto il responsabile della protezione dei dati è chiamato a svolgere un ruolo fondamentale all'interno dell'azienda titolare o responsabile del trattamento dei dati. Egli dovrà fornire consulenza al titolare o al responsabile del trattamento (e ai dipendenti incaricati) circa gli obblighi derivanti dal Regolamento e dalle altre disposizioni dell'Unione o nazionali in tema di protezione dei dati; vigilare sulla loro osservanza; cooperare con l'Autorità di controllo e sorvegliare sullo svolgimento della c.d. valutazione d'impatto sulla protezione dei dati introdotta, come vedremo a breve, dall'art. 35 del Regolamento[461]. Ciò con notevoli margini di autonomia e tenendo in debita

---

dovrà essere recepita dagli Stati membri dell'UE nel termine 2 anni.

[455] L'articolo 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'articolo 16, par. 1, del Trattato sul funzionamento dell'Unione europea (TFUE) sanciscono il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardino.

[456] Il Considerando n. 4 del nuovo Regolamento europeo recita: "*Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica*.

[457] Cfr. Considerando n. 7 del nuovo Regolamento europeo.

[458] L'art. 4 del Regolamento europeo sulla *privacy* distingue due figure: quella del "titolare del trattamento" ossia "*la persona fisica o giuridica, l'autorità pubblica, il servizio o 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 di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri*" (n. 7); e quella del "responsabile del trattamento", ossia "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*" (n. 8).

[459] Ai sensi dell'art. 4, n. 4, del Regolamento in esame, per "profilazione" si intende "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*".

[460] Art. 37, lett. b). Il Regolamento impone al titolare del trattamento e al responsabile del trattamento di designare un "responsabile della protezione dei dati" in due ulteriori ipotesi: quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali (lett. a)); e quando le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 (i cc.dd. dati sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

[461] V. art. 39, rubricato "Compiti del responsabile della protezione dei dati".

considerazione i rischi inerenti al trattamento dei dati, anche in ragione della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo[462].

Un'altra novità meritevole di un cenno è costituita dalla sopra menzionata valutazione di impatto sulla protezione dei dati: l'art. 35 del Regolamento pone a carico del titolare del trattamento dei dati personali l'obbligo di effettuare la suddetta valutazione preventiva ogni qualvolta il trattamento – anche per effetto delle nuove tecnologie impiegate e della natura, dell'oggetto, del contesto e delle finalità del medesimo – presenti un rischio elevato per i diritti e le libertà delle persone fisiche[463].

In particolare, il legislatore europeo impone la valutazione preventiva dell'impatto del trattamento sulla protezione dei dati personali qualora esso implichi una "valutazione sistematica e globale di aspetti personali relativi a persone fisiche basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche"[464].

5. CONCLUSIONI

(Alessandra Camedda)

Alla luce di quanto esposto, è auspicabile che le Autorità di vigilanza sul settore assicurativo rafforzino la tutela offerta ai clienti-consumatori effettuando un più incisivo controllo sulla gestione dei dati da parte degli operatori economici e valutando attentamente l'adeguatezza dell'attuale quadro normativo al fenomeno in esame.

È opportuno segnalare che iniziative in tal senso sono già state intraprese in ambito europeo dal *Joint Committee* dell'ESAs - *European Supervisory Authorities* (EBA, EIOPA ed ESMA).

Nello specifico, il Comitato congiunto delle Autorità di vigilanza europee ha avviato una pubblica consultazione sul possibile impatto dei Big Data sul tradizionale svolgimento delle attività delle imprese assicurative (e delle Istituzioni finanziarie) al fine di conoscere le opinioni e i suggerimenti dei principali *stakeholders* in ordine ai rischi e ai benefici derivanti dall'uso dei dati e all'opportunità di nuovi e più rigorosi interventi di regolamentazione e vigilanza a tutela dei consumatori[465].

---

[462] L'art. 38, par. 3, del Regolamento stabilisce, infatti, che "*Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento*".

[463] Il regolamento ammette anche la possibilità di effettuare una singola valutazione al fine di esaminare un insieme di trattamenti simili aventi rischi analoghi. Inoltre, l'art. 35 precisa che, nello svolgimento della valutazione d'impatto sulla protezione dei dati, il titolare del trattamento deve consultare il responsabile della protezione dei dati, qualora designato. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati.

[464] Art. 35, par. 3, lett. a), Regolamento. La valutazione d'impatto sulla protezione dei dati è richiesta anche in caso di trattamento, su larga scala, di categorie particolari di dati personali sensibili (individuati dall'art. 9, par. 1) o di dati relativi a condanne penali e a reati di cui all'art. 10 (lett. b)) nonché in caso di sorveglianza sistematica su larga scala di una zona accessibile al pubblico (lett. c)). La valutazione dovrà contenere almeno quattro elementi: *a)* una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; *b)* una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; *c)* una valutazione dei rischi per i diritti e le libertà degli interessati; *d)* le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al Regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

[465] *Joint Committee Discussion Paper on the Use of Big Data by Financial Institutions* consultabile all'indirizzo: *https://esas-joint-commit-*

Il *Joint Committee* ha, inoltre, ribadito l'impegno delle tre Autorità di vigilanza europee in tema di innovazione tecnologica e relativo impatto sui modelli di *business* delle istituzioni finanziarie nel recente *Report* sui rischi e le vulnerabilità del sistema finanziario europeo[466]. Il Rapporto evidenzia, in particolare, la necessità di rivolgere particolare attenzione a problematiche quali l'*outsourcing* ai fornitori di servizi *cloud* e *robo-advice*, l'uso di strumenti di analisi dei Big Data e di informazioni sui consumatori nonchè lo sviluppo di nuovi strumenti di gestione del rischio utilizzati nel settore assicurativo[467].

tee.europa.eu/Publications/Discussion%20Paper/jc-2016-86_discussion_paper_Big_Data.pdf. La pubblica consultazione si è chiusa il 17 marzo 2017.

[466] *Joint Committee Report on Risks and Vulnerabilities in the Eu Financial System*, 21 settembre 2017.

[467] V. *Joint Committee Report on Risks and Vulnerabilities in the Eu Financial System*, 21 settembre 2017, cit., 16: "*The ESAs continue to work on assessing the impact of FinTech on financial institutions' business models and their strategic response. With the rapid growth of FinTech, supervisors should ensure compliance with regulatory obligations, while policy makers should consider amending and extending the regulatory framework where necessary. The particular challenge to policy makers is that innovations such as Big Data and robo-advice affect a wide range of services across the different sectors of financial services. Supervisors should closely monitor these developments and ensure access to information for consumers, and protect customers in the light of cyber-crime and the increased use of potentially private Data*".

PRIVACY

(Angelica Saccoccio, Susanna Sandulli)

La *privacy* nella *social economy* fra Big Data e *fake news*

L'espressione Big Data, ovvero "grandi dati", usata per descrivere una raccolta dati di estese dimensioni, ha assunto ruolo predominante nell'evoluzione della moderna economia. Le imprese raccolgono, elaborano, trasformano le informazioni liberamente cedute dai consumatori al fine di accedere ad un dato servizio, per anticiparne i comportamenti, le necessità e le scelte. Quali strumenti possono essere adottati, al fine di sensibilizzare gli utenti circa il valore dei dati ceduti e quali, invece, al fine di garantirne un corretto utilizzo da parte degli operatori del settore, è il principale quesito che si vuole analizzare.

La diffusione dei Big Data risulta, inoltre, strettamente connessa al fenomeno delle fake news *il quale, sebbene abbia origini remote, sta interessando il misura sempre maggiore il legislatore e il Garante per la protezione dei dati personali; si è, infatti, compreso che con il diffondersi delle più evolute tecnologie ed il ruolo sempre più rilevante che i dati personali hanno assunto nella* social economy*, sia necessario predisporre un piano d'azione a livello europeo che sia volto non solo a contrastare il fenomeno delle* fake news*, ma anche tutte le conseguenze negative da esse derivanti, come l'hate speech e la disinformazione.*

Social economy e Big Data, tra opportunità e minacce

(Angelica Saccoccio)

SOMMARIO: 1. LA GESTIONE DEI BIG DATA. IL PROBLEMA DELLA CONDIVISIONE DELLE INFORMAZIONI. – 2. BIG DATA E NUOVE FRONTIERE DEL *MARKETING*. – 3. TRA PROGRESSI TECNOLOGICI E TUTELA DELLA *PRIVACY*.

1. LA GESTIONE DEI BIG DATA. IL PROBLEMA DELLA CONDIVISIONE DELLE INFORMAZIONI

Nell' epoca della *social economy,* sempre più spesso si parla del ruolo predominante, nell'evoluzione non solo dei settori economici ma altresì della vita quotidiana di ognuno di noi, dei Big Data. La definizione del termine induce a ritenere che si tratti dei "grandi dati", ossia della quantità abnorme di dati a disposizione dei vari *business*; in realtà, il termine Big Data[468] si riferisce all'esistenza di algoritmi in grado di elaborare innumerevoli variabili in breve tempo, per

[468] Sebbene il termine "Big Data" sia relativamente nuovo, la tendenza a raggruppare e immagazzinare ampi volumi di informazioni, per un eventuale analisi futura, è molto antica. Il concetto prende piede nei primi anni 2000 quando Doug Laney, analista di settore, formula la ormai nota definizione delle tre V dei big data: volume, velocità e varietà. In proposito https://www.sas.com/it_it/insights/big-data/what-is-big-data.html

cui alla base dei Big Data vi sono strumenti di statistica inferenziale che consentono di dedurre previsioni di risultato e di comportamento.

Pertanto, i Big Data possono supportare al meglio la raccolta, la classificazione, l'analisi e la sintesi dei dati di un determinato settore, offrendo informazioni preziose che vanno al di là del semplice dato grezzo.

Il crescente utilizzo dei Big Data ha consentito lo sviluppo di nuovi prodotti, servizi e processi, generando una profonda innovazione, tanto da poter parlare di "*data driven innovation*"[469]; quest'ultima può essere considerata un'opportunità di sviluppo non solo per le imprese, ma anche per i consumatori.

Ad ogni modo, è necessario evidenziare che i Big Data nascondono delle insidie in materia di tutela della *privacy* degli utenti. In particolare, la *social economy* ha permesso ai consumatori interconnessi di condividere dati ed informazioni di ogni genere, evidenziando una carenza di consapevolezza da parte degli stessi circa il valore delle informazioni condivise o memorizzate. Spesso, infatti, gli utenti apprezzano la gratuità dei servizi offerti dagli operatori, sottovalutando in parte il valore dei dati forniti per accedere al servizio, poiché, frequentemente, sono utilizzati dalle imprese che li detengono per finalità di profilazione ed analisi comportamentale, tanto da riuscire ad anticipare i desideri degli utenti.

A tal proposito, in occasione della Giornata Mondiale del Consumatore, in collaborazione con le organizzazioni di Spagna OCU e Portogallo Deco, l'associazione dei consumatori Altroconsumo ha aderito alla campagna "*Better Digital World*"[470], lanciando il manifesto "*I miei dati contano*".

In particolare, la Dichiarazione sottoscritta successivamente a Bruxelles, oltre che dalle organizzazioni di cui sopra, anche dalle organizzazioni partner del Belgio e del Brasile, ha i seguenti obiettivi: i) assicurarsi che i dati personali e la *privacy* dei consumatori siano rispettati; ii) che sia prevista l'opportunità per le persone di giocare un ruolo chiave nella nuova economia; iii) che siano stabilite le condizioni di un'economia digitale che garantisca ai consumatori la giusta parte dei profitti in un ambiente economico stabile e sicuro.

Tale iniziativa, sicuramente, evidenzia la necessità a livello europeo e non solo di individuare un sistema flessibile orientato a tutelare i consumatori, le libertà fondamentali e il libero mercato.

Tra gli attori di principale rilievo nel campo Big Data, è possibile annoverare il noto motore di ricerca Google che negli ultimi anni ha elaborato versioni di *software* sempre più aggiornate per la gestione dei dati.

In particolare, nel corso dei 18 mesi concessi dal Garante per la protezione dei dati personali al motore di ricerca per dare attuazione alle prescrizioni del provvedimento 10 luglio 2014 n. 353, lo stesso ha implementato una serie di misure a tutela degli utenti, offrendo maggiori informazioni in merito al trattamento dati, semplificandone la fruizione ed esplicitando le diverse finalità per cui i dati sono raccolti, compresa l'attività di profilazione.

Il motore di ricerca, in virtù di una specifica prescrizione dell'Autorità, ha, altresì, adottato misure idonee non solo ad acquisire il consenso degli utenti autenticati, ma anche di quelli non autenticati. Gli utenti autenticati possono, infatti, nella sezione *My account* accedere alle informazioni sulla *privacy*, la sicurezza e gli strumenti a disposizione per controllare i propri dati, mentre quelli non autenticati possono usare una versione semplificata che consente anche di scegliere di non ricevere la pubblicità mirata.

Google, pertanto, ha costantemente rincorso il progresso tecnologico raggiunto nella gestione dei dati, adeguando ed implementando un valido sistema di tutela della *privacy* degli utenti, in linea con quanto prescritto dal Garante.

Allo stato dell'arte, siamo, tuttavia, in presenza di un modello asimmetrico, in cui i rapporti tra chi fornisce e chi sfrutta

---

[469] R. VERGANTI, *Design driven innovation: changing the rules of competition by radically innovating what things mean*, in Harvard Business Press, 2009.

[470] Progetto promosso da *Consumer International,* organizzazione non governativa che rappresenta gruppi e associazioni di consumatori in tutto il mondo.

le informazioni e i dati volontariamente condivisi si risolvono a favore di coloro che gestiscono le piattaforme digitali e dispongono degli strumenti tecnologici necessari per elaborare la quantità enorme di dati a disposizione.

2. BIG DATA E NUOVE FRONTIERE DEL *MARKETING*

La rivoluzione Big Data interessa non solo il settore dell'*Information Tecnology* ma tutti i settori nei quali assume un ruolo preminente l'attività di pianificazione strategica ed in particolare il *marketing*[471]. In generale, il *marketing* può essere considerato come l'insieme delle azioni che l'impresa pone in essere al fine di raggiungere obiettivi prestabiliti sul mercato. Il principale risvolto dell'uso dei Big Data nel *marketing*[472] è rappresentato dai "metodi di raccomandazione" anche detti "sistemi di raccomandazione[473]", nei quali gli utenti si imbattono quotidianamente soprattutto nell'uso dei *social network* e dei portali *e-commerce*. Spesso, assumono la forma di consigli quali ad esempio: "ti piacerebbe acquistare …" o, ancor più banalmente, di raccomandazioni in forma musicale, cinematografica e da parte di soggetti terzi o potenziali acquirenti, provenienti da qualsiasi ambito, i quali esercitano una determinata influenza nelle scelte degli utenti. Questi ultimi sono anche denominati *"influencer"* e la diffusione di tale fenomeno è stata attribuita appunto al *marketing*[474]. Pertanto, i sistemi di raccomandazione forniscono agli utenti consigli personalizzati di probabile interesse riguardo un set di prodotti o servizi. Nel contesto economico odierno tali sistemi rappresentano per le imprese un valido strumento al fine di aumentare le vendite con pubblicità e promozioni su misura per ciascun utente.

Esistono diverse tipologie di sistemi di raccomandazione, che si differenziano principalmente per il modo con cui le stesse sono prodotte. Possiamo distinguere quattro grandi categorie di sistemi di raccomandazione: i)sistemi *content-based*, all'utente sono raccomandati prodotti o servizi simili a quelli scelti in passato; ii) sistemi collaborativi, all'utente sono raccomandati prodotti o servizi graditi in passato da altri utenti con gusti simili; iii) sistemi ibridi, combinano elementi dei precedenti sistemi; iv)sistema sociale, considera un insieme di persone ed uno di prodotti o servizi dove le persone sono connesse da una rete sociale e sia queste ultime sia gli oggetti sono descritti da una tassonomia.

Ad ogni modo, le raccomandazioni possono essere paragonate alle comunicazioni commerciali indesiderate che, generalmente, gli utenti ricevono tramite *e-mail*, oggetto di valutazione da parte del Garante nel corso del 2016.

L'Autorità ha, inoltre, effettuato verifiche preliminari volte a valutare progetti per la realizzazione di piattaforme in grado di aggregare dati provenienti da diverse fonti per fini di profilazione o riprofilazione.

A tal proposito, il Garante ha evidenziato che, ove realmente i dati trattati fossero stati anonimi, la fattispecie non sarebbe stata oggetto della disciplina del Codice, mentre, con riferimento alla trattazione preliminare dei dati che avrebbe condotto alla anonimizzazione degli stessi, nonché alla fase di associazione dei profili elaborati, ha sottolineato che tali profili risultano meritevoli di ulteriore approfondimento e a tale scopo l'Autorità ha richiesto alle società

---

[471] Numerose sono le definizioni di questo ramo dell'economia, fra cui: "Il marketing è l'intera azienda dal punto di vista della clientela" (P. Drucker); "Il marketing consiste nello svolgimento delle funzioni d'impresa che orientano il flusso di beni dal produttore al consumatore" (P. Kotler); "Il marketing è la funzione di interscambio tra azienda e mercato"(J. Stanton, R. Varaldo).

[472] "I cambiamenti sociali, con i quali i *marketing manager* devono confrontarsi, hanno origine dall'azione di alcuni importanti fenomeni, talvolta interconnessi, che si presentano come vere e proprie forze evolutive. Tali forze hanno prodotto nuovi comportamenti, nuove opportunità e vere e proprie sfide per il *marketing*. (…) Tecnologie di rete. La rivoluzione digitale ha creato un'Era dell'Informazione che promette di farci raggiungere livelli di produzione maggiori e pure migliori, comunicazioni più mirate e scelte di prezzo più appropriate. (…)" Marketing Management, XIV edizione, Kotler, Keller, Ancarani, Constabile, 2012.

[473] C. Tasso, P. Omero, *La personalizzazione dei contenuti web, e-commerce, i-access, e-government*, Milano, 2012.

[474] R. Subramani, Balaji Rajagopalan, *Knowledge-Sharing and Influence*, in *Online Social Networks via Viral Marketing*.

partecipanti al progetto di integrare le informazioni fornite.

Dunque, è evidente che le attività di segmentazione o più in generale di profilazione degli utenti rappresentano il principale *output* dell'analisi dei dati a disposizione di qualsiasi operatore e, in particolare, possiamo affermare vi sia una diretta correlazione tra uso dei Big Data e profilazione degli utenti. Pertanto, il *marketing* rappresenta un settore fortemente interessato dall'uso dei Big Data, poiché quest'ultimi consentono all'impresa che li utilizza di anticipare i comportamenti, le decisioni nonché le necessità dei consumatori.

3. TRA PROGRESSI TECNOLOGICI E TUTELA DELLA *PRIVACY*

Attualmente, i Big Data sono protagonisti indiscussi delle strategie aziendali, poiché, come evidenziato, dalla loro analisi scaturiscono le decisioni determinanti la crescita aziendale. Il Presidente del Garante per la protezione dei dati personali Antonello Soro, ha, infatti, affermato in un suo intervento quanto segue: "I Big Data sono un fattore strategico nella produzione, nella competizione dei mercati, nelle innovazioni di importanti settori pubblici e nella nostra vita quotidiana. Tutto ciò comporta il dover affrontare sfide molto complesse che solo in parte sarà possibile risolvere attraverso una maggiore regolamentazione"

In questo scenario, in data 23 gennaio 2017, in attuazione dei principi della Convenzione 108[475], il Comitato esecutivo della Convenzione ha adottato specifiche linee guida in materia di tutela dei dati personali con riferimento ai Big Data.

Il documento risulta essere il primo strumento di portata internazionale ad aver inquadrato il tema della tutela dei dati personali nello scenario Big Data e, infatti, lo stesso Regolamento (UE) 2016/679 non contiene indicazioni a riguardo. Le linee guida costituiscono utili indicazioni nonché istruzioni pratiche non solo per gli Stati membri ma, altresì, per gli operatori del settore, evidenziando la necessità per quest'ultimi di considerare il contesto sociale e tecnologico, ossia la non conoscenza da parte degli utenti del funzionamento e degli impieghi dei Big Data.

L'aspetto fondamentale delle linee guida è, sicuramente, costituito dalla procedura di valutazione del rischio, che considera non solo la dimensione individuale della protezione dei dati, bensì anche quella collettiva in termini di potenziale conflitto fra impiego dei dati e valori etici e sociali. In tale ottica, il diritto del singolo ad avere il controllo sui propri dati personali evolve in una più ampia nozione di controllo; infatti, tramite un processo di valutazione del rischio più complesso, si analizza l'impatto dell'impiego dei dati nella rappresentazione della società.

Le linee guida, inoltre, prevedono la possibilità per le singole autorità nazionali di coadiuvare i responsabili del trattamento, fornendo informazioni e dati circa i metodi di sicurezza. Con riferimento al tema del consenso, esse propongono, al fine di una maggiore efficacia informativa, la possibilità di ricorrere ad un'interfaccia che simuli l'uso dei dati e il loro potenziale impatto sulla persona interessata. Inoltre, le stesse chiariscono che, in un contesto di evidente squilibrio di potere tra utenti e operatori del settore, il consenso non può considerarsi liberamente dato.

Le linee guida rappresentano uno strumento originale ed innovativo e dimostrano come il Consiglio d'Europa, nonostante i vincoli posti da un quadro normativo non aggiornato rispetto al contesto tecnologico, abbia profuso notevole impegno per suggerire linee d'azione nuove rispetto alla protezione dei dati.

Dunque, le linee guida delineano un sistema innovativo che favorisce la collaborazione tra i responsabili del trattamento e le autorità nazionali, facendo supporre altresì una maggiore collaborazione tra quest'ultime, data la portata del fenomeno Big Data, nonché un maggiore ricorso all'autoregolazione da parte degli operatori.

[475] Primo strumento internazionale cogente in materia di protezione dei dati personali, a carattere tendenzialmente universale; infatti, l'art. 23 della stessa prevede che possano essere invitati ad aderire anche Stati non membri del Consiglio d'Europa.

Fake news: il mercato delle informazioni

(Susanna Sandulli)

SOMMARIO: 1. IL COMPLESSO FENOMENO DELLE *FAKE NEWS* E IL RUOLO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. – 2. I TENTATIVI DI REGOLAMENTAZIONE A LIVELLO NAZIONALE ED EUROPEO. – 3. UTENTI, OPERATORI ECONOMICI E *FAKE NEWS:* QUALI TUTELE?

1. IL COMPLESSO FENOMENO DELLE FAKE NEWS E IL RUOLO DEL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Con l'espressione "*fake news*" facciamo riferimento a fenomeni molto diversi fra loro quali, ad esempio, la diffusione di notizie false e l'*hate speech*, accumunati dalla circostanza per cui l'attendibilità della notizia dipende dalle condivisioni effettuate dagli utenti.

Sebbene, dunque, la prima accezione da dare a tale terminologia sia di origine prettamente comunicativa, in quanto attiene, fondamentalmente, all'attività giornalistica, possiamo notare l'assenza di una definizione univoca; si pone, quindi, un problema di inquadramento giuridico, in quanto da tale nozione così generica occorre trarre, comunque, delle indicazioni al fine di accostare tale fenomeno a quelli già regolati dall'ordinamento.

Se, senza dubbio, in alcuni casi si tratta semplicemente di una "cattiva informazione" che prescinde dall'intenzione del soggetto di diffondere un'informazione non veritiera, in altre ipotesi l'assenza di colpevolezza non pare, invece, ravvisabile; pertanto, sarà necessario prevedere, a seconda del comportamento doloso o colposo, differenti forme di responsabilità di natura civile, penale ovvero amministrativa.

Si pone, inoltre, un problema di libertà e di bilanciamento di interessi: la libertà di espressione, tutelata all'art. 21 della Costituzione, costituisce uno dei cardini del sistema democratico, ma quando si trasforma in disinformazione sortisce l'effetto contrario, limitando la stessa democrazia e venendo meno alla sua funzione primaria.

Le *fake news* sono, in realtà, diffuse sin da tempi molto lontani e rappresentano il costo del pluralismo, ma di recente hanno catturato l'attenzione mediatica e del legislatore, in quanto lo sviluppo di strumenti di comunicazione digitale sempre più invasivi ha aumentato in maniera esponenziale la rapidità di circolazione delle informazioni; rispetto al passato, difatti, la notizia falsa rimane digitalizzata, divenendo pressoché impossibile garantire una sua completa eliminazione dal mondo della rete e ciò richiama, inevitabilmente, il problema mai sopito della tutela del diritto all'oblio.

Tutto ciò da vita ad un meccanismo che desta giustificate preoccupazioni, in quanto dalle *fake news* deriva una strumentalizzazione dell'opinione pubblica che trae la sua maggior forza nel rapporto di sfiducia che lega i cittadini allo Stato, ma anche gli utenti alle banche e agli altri operatori economici.

Conseguentemente, un primo effetto da attribuire alla diffusione di questo fenomeno, che fonda le sue radici in una pluralità di fattori concorrenti, è di natura sociale e ciò è dimostrato dal fatto che gli utenti tendono a fidarsi maggior-

mente all'opinione degli *influencers*[476] piuttosto che di quella di soggetti qualificati[477]; la libertà della fonte incide, dunque, profondamente sul presunto e discutibile grado di attendibilità della stessa.

Da ciò deriva la necessità di creare un sistema imperniato sulla trasparenza: trasparenza da parte degli ISP, delle imprese, dei *social network* e, soprattutto, da parte dello Stato; di certo, il livello di veridicità di una notizia deve essere preteso in maniera più stringente da coloro che ricoprono un ruolo istituzionale, ma è necessario che anche gli internauti collaborino al fine di comprendere realmente il grado di attendibilità di una notizia[478].

In questo panorama così caotico un ruolo centrale non può che essere attribuito al Garante per la protezione dei dati personali.

Questo, difatti, si è sempre posto in prima linea nella lotta alle *fake news* e al *cyberbullismo*, evidenziando la necessità di pervenire a una corretta alfabetizzazione digitale come strumento di auto-difesa per l'internauta.

Come sottolineato in numerose dichiarazione dal Presidente dell'Autorità Antonello Soro, fra gli aspetti che destano maggiori preoccupazioni e sui quali è necessario intervenire rileva, in particolar modo, la viralità e la rapidità con cui si diffondono le *fake news* che lasciano il legislatore incerto sugli strumenti di contrasto da esperire.

Il problema è identificabile in quella che potremmo definire "*informazione selfie*", nel senso che l'utente non è interessato ad una ricerca della verità, ma vuole una mera conferma delle proprie convinzioni; pertanto, come detto, l'attendibilità della notizia non dipende dalla sua veridicità, bensì dalla quantità di condivisioni: nella logica dell'utente, tanto maggiore è la quantità di siti o *blog* che riportano la notizia, tanto più alte saranno le probabilità che essa sia fondata.

Questo *meccanismo autoconfermativo* può portare anche a ledere la dignità di un individuo, magari neppure più in vita e, dunque, la questione delle *fake news* fa emergere l'altrettanto rilavante problema dell'*hate speech*, perché spesso la diffusione di notizie false costituisce solo l'estremizzazione di una strategia di odio.

Ciò che deve essere assicurato, quindi, è che anche nella rete, nel mondo virtuale, il diritto alla dignità personale e alla verità siano garantiti in egual misura, in quanto la libertà di espressione non può certamente costituire una limitazione assoluta degli altrui diritti, né Internet può divenire luogo in cui il rispetto per gli altri individui viene abolito.

Occorre, a questo punto, indagare in merito alle ragioni che portano alla diffusione così repentina delle *fake news*.

La risposta a tale interrogativo è riconducibile ai guadagni economici che i siti, i forum e i *blog* possono ottenere mediante la diffusione di qualsiasi tipologia di notizia, anche quelle false.

Difatti, il fulcro dell'intera questione è da rinvenire nell'importanza che hanno assunto le informazioni e i dati personali per lo svolgimento dell'attività imprenditoriale; invero, anche il semplice collegamento al sito garantisce profitti, in quanto anche i *banner* pubblicitari hanno un valore economico e, quindi, tanto più virale è la notizia, tanto maggiori saranno i riscontri economici.

Il possesso delle informazioni personali relative alle abitudini e ai gusti dei consumatori è, dunque, divenuto fondamentale per lo svolgimento dell'attività da parte delle imprese, le quali, venendo a conoscenza delle preferenze degli utenti,

---

[476] Con tale espressione facciamo riferimento ad utenti che hanno sui diversi *social network* un numero estremamente ampio di *followers* che ripongono particolare fiducia nelle opinioni da loro espresse; pertanto, la condivisione di un *post* è in grado di influenzare l'opinione degli altri internauti, determinando, ad esempio, il successo o il fallimento di un bene o di un servizio.

[477] Un esempio emblematico in tal senso è fornito dalla questione dei vaccini in Italia in cui la diffusione di false notizie ha portato a risultati tragici.

[478] Per tale ragione si è tenuta a San Pietroburgo la tavola rotonda "*Informazione credibile vs informazione falsa: una sfida per i media moderni*", nella quale si è voluto sottolineare come l'epoca moderna si caratterizzi per la presenza di uno *tsunami informativo* che porta alla luce la questione della tutela del diritto ad una corretta informazione; durante l'incontro, si è rimarcata, difatti, la necessità di procedere ad un'educazione digitale, la quale deve prendere avvio dalle stesse scuole di giornalismo.

possono garantirsi maggiori possibilità di guadagno[479].

Il dato personale assume, di conseguenza, la valenza di un bene economico commerciabile sul mercato, un vero e proprio oggetto di scambio il quale, tuttavia, viene spesso ceduto senza un'effettiva consapevolezza da parte del suo titolare e senza una controprestazione adeguata[480].

Le problematiche che si riverberano a seguito della nascita di questo *mercato delle informazioni* sono, quindi, molteplici e rilevano sotto diversi profili.

Innanzitutto, in ragione dell'estrema velocità della circolazione delle informazioni nella rete, i titolari dei dati personali sono sottoposti al forte e costante rischio che venga leso non soltanto il loro diritto alla *privacy*, ma anche la loro dignità, soprattutto attraverso le *fake news*.

Sebbene, dunque, il consumatore sia il soggetto maggiormente esposto ai rischi derivanti dalla diffusione delle *fake news*, anche le imprese commerciali possono risultare fortemente danneggiate da questa pratica. Difatti, con la nascita di piattaforme come Tripadvisor, il concetto di *feedback* si è notevolmente dilatato, ma altrettanto è avvenuto in merito ai giudizi negativi effettuati da concorrenti poco corretti e, difatti, numerose aziende, subiscono costantemente danni all'immagine a seguito di recensioni false e negative.

Con riferimento, infine, al mercato, dobbiamo rimarcare che sono pochissimi i soggetti che possono disporre dei Big Data, i quali, come esposto nel paragrafo precedente, costituiscono il nuovo fondamento della *social economy*; si parla, a tal proposito, degli *Over The Top*, i quali assumono un potere di mercato estremamente ampio, anche in campi molto diversi da quello originario e, possedendo un numero esorbitante di informazioni, sono in grado di dar vita a situazioni di monopolio[481].

Il possesso di tali dati personali comporta una sorta di un controllo sociale da cui deriva un modellamento del comportamento degli utenti[482] ; dunque, presa consapevolezza della necessità di un intervento immediato, il 30 maggio 2017 il Garante per la protezione dei dati personali, l'Autorità Garante della Concorrenza e del Mercato e l'Autorità per le Garanzie nelle Comunicazioni hanno avviato un'indagine conoscitiva al fine di individuare gli strumenti di tutela più idonei a creare un adeguato sistema di protezione dei consumatori e del mercato che, tenendo conto del propagarsi del fenomeno dei Big Data, dia vita ad un sistema incentrato sul pluralismo informativo.

2. I TENTATIVI DI REGOLAMENTAZIONE A LIVELLO NAZIONALE ED EUROPEO

La lotta alla circolazione delle *fake news* è un problema che necessita, dunque, di una rapida soluzione[483] ma permane ancora un grande interrogativo in merito alle forme di protezione da adottare, in quanto gli strumenti tradizionali di

[479] L. Mormile, in *Libera circolazione e protezione dei dati personali*, Milano, 2006, 534.

[480] P. Manes, *Il consenso al trattamento dei dati personali*, Padova, 2001; V. Grippo, *Analisi dei dati personali presenti su Internet. La legge n. 675/96 e le reti telematiche*, in Rivista critica del diritto privato, Napoli, 1997, 640-645.

[481] In questo modo, tuttavia, l'identità personale ed il suo valore sembrano perdere la loro rilevanza, facendo sì che il dato personale divenga solamente una "cifra", un bene da sfruttare economicamente.

[482] Dallo studio di Trend Micro sulle *fake news*, denominato "*The Fake news Machine: How Propagandists Abuse the Internet and Manipulate the Public*", emerge chiaramente la portata dirompente che esse hanno assunto grazie all'avvento di Internet, ponendosi come fattori di manipolazione dell'opinione pubblica. http://www.trendmicro.it/newsroom/pr/-dollari-per-influenzare-il-risultato-di-unelezione/index.html

[483] Un precedente al tentativo di disciplinare una materia così complessa è offerto dalla Germania la quale, in vista delle elezioni, ha predisposto un nuovo apparato regolamentare che prevede multe sino 500.000 euro a carico delle aziende che non provvedono all'eliminazione della *fake news* entro 24 ore dalla segnalazione.

tutela appaiono obsoleti e sono messi fortemente alla prova dalla nuova era digitale.

La disciplina del reato di diffamazione[484], ad esempio, non tiene conto della circostanza per cui nella *social economy* ogni individuo digitale "fa informazione": il rilancio delle notizie sui *blog*, la condivisione dei *post* sui *social network*, in sostanza ogni attività svolta nella rete da vita a informazioni che vengono diffuse ad un' incredibile velocità, senza che la veridicità delle stesse venga sempre appurata.

Al fine di superare tale situazione, è stato presentato il disegno di legge "*Disposizioni per prevenire la manipolazione dell'informazione online, garantire la trasparenza sul web e incentivare l'alfabetizzazione mediatica*" volto a garantire un bilanciamento tra la protezione degli utenti e la tutela del diritto alla libertà di espressione[485].

Nonostante le intenzioni del legislatore siano, di certo, apprezzabili, il progetto presenta alcuni aspetti che destano perplessità, in quanto la disciplina risulta applicabile soltanto ai privati cittadini, escludendo, invece, dal novero dei destinatari le testate giornalistiche.

Un ulteriore dubbio deriva dal fatto che il decreto prevede che i gestori debbano eliminare prontamente la notizia qualora "ne stabiliscono la non attendibilità"; in tal modo, sembra equipararsi il ruolo dei privati a quello dei tribunali, mentre, forse, sarebbe stato più opportuno prevedere la devoluzione di tale attività di monitoraggio alle *Authorities* competenti.

Il disegno di legge, inoltre, non pare affrontare direttamente una delle tematiche principali derivanti dalle *fake news*, ossia l'incitamento all'odio, la quale, invece, è stata oggetto di un'apposita azione a livello europeo.

Difatti, il 31 maggio 2016 la Commissione europea, Facebook, Twitter, Microsoft e Youtube hanno adottato un Codice di condotta[486] contenente l'assunzione di una serie di impegni da parte delle piattaforme *social* volti a contrastare il fenomeno dell'*hate speech*[487], dimostrando che tale questione, insieme a quella delle *fake news*, non può essere affrontata in un'ottica meramente nazionale, avendo assunto connotati globali.

Tuttavia, anche tale Codice di condotta suscita qualche perplessità, soprattutto con riferimento all'obbligo per le aziende di porre in essere un'attività consistente nell'"*identifying and promoting independent counter-narratives, new ideas and initiatives and supporting educational programs that encourage critical thinking*", consentendo, in altre parole, alle stesse di modificare il flusso informativo e di preferire alcune notizie rispetto ad altre. Ciò, inevitabilmente, lascia alle aziende la possibilità di dar vita a una manipolazione delle informazione e delle opinioni degli internauti, incidendo, quindi, su valori costituzionali e sullo stesso concetto di democrazia.

---

[484] Si è, infatti, ipotizzato un accostamento con il reato di diffamazione, disciplinato dall'art. 595 c.p., posto a presidio della tutela dell'onore in senso oggettivo e, in particolare, con la fattispecie di cui all'art. 596-bis c.p. che riguarda l'ipotesi in cui l'offesa venga effettuata con il mezzo della stampa.

[485] Il testo, sull'onda dell'esperienza tedesca, prevede sia multe che sanzioni penali: chi diffonde notizie false "*esagerate o tendenziose che riguardino dati o fatti manifestamente infondati o falsi*", potrebbe incorrere in un'ammenda fino a 5.000 euro; qualora, inoltre, le notizie false rechino "*pubblico allarme o nocumento agli interessi pubblici*" la pena, oltre all'ammenda, consisterà nella reclusione non inferiore a 12 mesi.
Il decreto introduce, inoltre, l'art. 656-*bis* c.p., il quale si sostanzia in una duplicazione della norma precedente relativa al reato di diffusione di notizie false, esagerate o tendenziose, prevedendo un'applicazione all'utilizzo di mezzi elettronici ovvero telematici. È prevista, inoltre, l'aggiunta degli artt. 265-*bis* e 265-*ter c.p.* volti a punire con la carcerazione la diffusione di "*voci o notizie false, esagerate o tendenziose che possano destare pubblico allarme*" o "*recare nocumento agli interessi pubblici*" o "*fuorviare settori dell'opinione pubblica*"; l'aspetto che lascia maggiormente perplessi consiste nel fatto che l'attuale art. 265 c.p. è applicabile qualora tale diffusione avvenga "*in tempo di guerra*", mentre con il decreto si estenderebbe l'utilizzabilità della norma in tempo di pace.

[486] http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

[487] Mediante la sottoscrizione di tale Codice, le società hanno assunto l'impegno di riesaminare entro 24 ore la maggior parte delle notifiche relative ad attività di incitamento all'odio e di rimuoverne il contenuto, utilizzando un approccio che garantisca una maggior educazione dell'internauta.

Sarebbe stato, forse, preferibile prevedere un sistema di pubblicazione *online* delle decisioni relative alle rimozioni dei contenuti, garantendo non solo una maggior conoscenza da parte dei cittadini, ma anche una maggior sensibilizzazione degli utenti in tema di *hate speech* e *fake news*.

Pertanto, al fine di garantire una maggior efficienza di tale approccio basato sulla logica di autoregolamentazione, il 10 maggio 2017, nell'ambito della revisione dell'attuazione della strategia per il mercato unico digitale[488], si è confermata la necessità per l'Unione europea e gli Stati membri di attivarsi ulteriormente al fine di tutelare al meglio il diritto alla libertà di espressione degli internauti senza che esso sfoci in una *illibertà* per gli altri individui[489].

In conclusione, ad oggi non esiste ancora una disciplina nazionale ed europea in materia di *fake news* e *hate speech* e né il disegno di legge né il Codice di condotta sembrano ancora sufficienti, in quanto non si è creata una normativa uniforme, bensì un sistema frammentato che lascia gli internauti incerti sulle conseguenze derivanti dalle proprie attività *online*.

3. UTENTI, OPERATORI ECONOMICI E *FAKE NEWS*: QUALI TUTELE?

Le osservazioni svolte finora fanno comprendere la portata dirompente della disinformazione e la necessità impellente di procedere con azioni volte a tutelare non solo i consumatori, ma anche il mercato che risulta, inevitabilmente, indebolito da tali fenomeni.

La protezione della propria sfera privata, difatti, non può presentarsi come un diritto anacronistico passibile di essere accantonato in nome dello sviluppo digitale e del progresso tecnologico e, pertanto, la tutela *online* deve essere garantita al pari di quella *offline*.

Ricercare una soluzione concreta al fenomeno delle *fake news* è tutt'altro che facile, perché, come sottolineato da Antonello Soro, il rischio di cadere nella censura, nella violazione del diritto alla libertà di espressione e nella reminiscenza di un *tribunale della verità* è particolarmente elevato.

Una soluzione potrebbe, forse, essere quella proposta dal Garante per la protezione dei dati personali di concentrare l'azione legislativa non tanto sulla creazione di organismi terzi, bensì su una politica di coordinamento fra Stato e cittadino in cui l'educazione digitale assume un ruolo centrale; la risposta penale, così come prevista dal citato disegno di legge, non pare, infatti, sufficiente, poiché è necessario realizzare un quadro regolamentare caratterizzato dalla responsabilizzazione degli utenti.

Occorre, dunque, dare una risposta efficace e concreta ai problemi delle *fake news* mediante l'utilizzazione di un approccio preventivo e regolamentare allo stesso tempo, come è avvenuto con la disciplina in tema di *cyberbullismo*[490]. Non si potrebbe, in altre parole, agire in un'ottica di semplificazione e di praticità, piuttosto che mediante la previsione di ulteriori regolamentazioni, dato che la proliferazione delle norme, unita all'inevitabile anacronismo legislativo, si è già dimostrata inefficace?

---

[488] http://europa.eu/rapid/press-release_MEMO-17-1233_en.htm

[489] Il problema principale deriva dalla estrema diversità che caratterizza i sistemi normativi nazionali: la definizione di ciò che è illegale diviene, per certi aspetti, soggettiva, risultando il contesto giuridico, sociale e culturale degli Stati membri estremamente variegato.

[490] Facciamo riferimento alla Legge del 29 maggio 2017, n. 71 recante "*Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo*".

Ciò è stato evidenziato anche da Mark Zuckerberg, fondatore di Facebook, il quale ha rimarcato che la lotta contro le *fake news* richiede un ruolo attivo degli stessi utenti, i quali debbono incrociare le varie notizie, consultare più fonti possibili e approfondire la lettura dell'intero articolo senza soffermarsi ai sedicenti titoli, poiché è difficile "*identificare la verità*".

Alla luce delle problematiche ora esposte, l'ottica in cui il legislatore nazionale dovrebbe agire è quella di applicare un eguale sistema di tutela al mondo virtuale rispetto a quello "reale", in quanto le istanze di protezione non solo hanno la medesima importanza, ma pongono, anzi, maggiori problematiche in ragione dell'immaterialità della rete in cui le insidie sono molto più celate; Internet è lo spazio in cui si sviluppa la nostra personalità, la dimensione in cui i diritti possono essere esercitati e violati e, andando ad una velocità diversa rispetto al mondo fisico, richiede altrettanta rapidità nell'adozione di strumenti d'intervento adeguati.

L'impegno politico dovrebbe, dunque, dirigersi verso un'ottica di educazione digitale, facendo sorgere nel cittadino una logica di pensiero critico: se, oramai, siamo un paese che fonda la propria economia sui dati personali e sulle informazioni, perché non investire anche nella loro protezione?

Gli Autori

GLI AUTORI

Antonio Affinito
Dottorando di ricerca in Mercati, Impresa e Consumatori - Università Roma Tre

Valentina Angelini
Dottore di ricerca in Consumatori e Mercato – Università Roma Tre

Fabio Bassan
Professore ordinario di Diritto internazionale – Università Roma Tre

Giorgia Biferali
Assegnista di ricerca in Grande distribuzione organizzata e abuso di dipendenza economica – Università Roma Tre
Dottore di ricerca in Diritto Privato per l'Europa – Università Roma Tre

Alessandra Camedda
Dottore di ricerca in Mercati, Impresa e Consumatori - Università Roma Tre

Marco Cappai
Dottorando di ricerca in Mercati, Impresa e Consumatori - Università Roma Tre

Aldo Corvino
Dottore di ricerca in Consumatori e Mercato – Università Roma Tre

Francesco Della Rocca
Dottorando di ricerca in Mercati, Impresa e Consumatori - Università Roma Tre

Vincenzo Floccari
Dottorando di ricerca in Mercati, Impresa e Consumatori - Università Roma Tre

Alfonso Ingenito
Dottore di ricerca in Consumatori e Mercato – Università Roma Tre

Cristiana Lauri
Dottoranda di ricerca in Diritto dei mercati e dei consumatori – Università Roma Tre

Andrea Luberti
Magistrato
Dottore di ricerca presso la Scuola dottorale internazionale di diritto ed economia "Tullio Ascarelli"

Maria Letizia Magno
Assegnista di ricerca in La regolazione delle nuove forme di comunicazione - Università Roma Tre
Dottore di ricerca in Consumatori e Mercato – Università Roma Tre

Paolo Occhiuzzi
Dottore di ricerca in Consumatori e Mercato – Università Roma Tre e Funzionario a contratto presso l'Autorità Garante della Concorrenza e del Mercato

Francesca Pellicanò
Dottore di ricerca in Consumatori e Mercato – Università Roma Tre
Funzionario di ruolo presso l'Autorità per le Garanzie nelle Comunicazioni

Rosaria Petti
Dottorando di ricerca in Mercati, Impresa e Consumatori - Università Roma Tre

Sara Perugini
Dottore di ricerca in Consumatori e Mercato – Università Roma Tre
Funzionario di ruolo presso l'Autorità Garante della Concorrenza e del Mercato

Maddalena Rabitti
Professore ordinario di Diritto dell'economia – Università Roma Tre

Liliana Rossi Carleo
Professore emerito di Diritto privato – Università Roma Tre

Angelica Saccoccio
Dottoranda di ricerca in Mercati, Impresa e Consumatori - Università Roma Tre

Susanna Sandulli
Dottoranda di ricerca in Mercati, Impresa e Consumatori - Università Roma Tre

Maria Chiara Sole
Dottore di ricerca in Consumatori e Mercato – Università Roma Tre

Imprese e loro associazioni di categoria

AGOS

ASSTRA

CENTROMARCA
Associazione Italiana dell'Industria di Marca

FEDERDISTRIBUZIONE
LE AZIENDE DELLA DISTRIBUZIONE MODERNA

federfarma

FERROVIE DELLO STATO ITALIANE

INTESA SANPAOLO

Posteitaliane

TIM

UPA
UTENTI PUBBLICITÀ ASSOCIATI

vodafone

WIND
Più vicini.

Istituzioni

UNIONCAMERE
CAMERE DI COMMERCIO D'ITALIA

Associazioni di Consumatori

ACU
Associazione Consumatori Utenti
Organizzazione senza scopo di lucro

ADICONSUM

Adoc

Associazione Utenti dei Servizi Radio Televisivi

ASSO-CONSUM

ASSOUTENTI

Casa del Consumatore

CITTADINANZATTIVA

CODACONS

CODICI
CENTRO PER I DIRITTI DEL CITTADINO

CONFCONSUMATORI
CONFEDERAZIONE GENERALE DEI CONSUMATORI

Federconsumatori

Lega Consumatori

MOVIMENTO CONSUMATORI

MOVIMENTO DIFESA DEL Cittadino

1955
UNC
CONSUMATORI.IT

U.Di.Con.
UNIONE per la DIFESA dei CONSUMATORI

CONSUMERS' FORUM

Consumers' Forum è un'associazione indipendente e unica in tutta Europa che dal 1999 riunisce imprese e consumatori per facilitare il dialogo, promuovere le politiche consumeriste e migliorare la qualità di vita dei cittadini.

Fanno parte di Consumers' Forum le più importanti associazioni di consumatori, istituzioni, università, numerose imprese industriali e di servizi e le loro rappresentanze.

L'associazione è luogo di confronto sui diritti dei consumatori e favorisce il "dialogo aperto" tra le parti.

Consumers' Forum
Via degli Scipioni,8 00192 Roma RM
tel.06-39725486 fax 06-39887519
segreteria@consumersforum.it
www.consumersforum.it

consumforum

@ConsumForum

consumersforumtv

consumers'-forum