LUISS Università Guido Carli

Dipartimento di Impresa e Management

Diritto di Internet: social media e discriminazione

Le FANGs; il valore dei dati e la tutela della privacy

Relatore
Prof. Pietro Santo Leopoldo Falletta

Candidato
Giulia Caputo
Matr. 200021

ANNO ACCADEMICO 2017-2018

Le FANGs; il valore dei dati e la tutela della privacy

Giulia Caputo

A mio fratello, il mio piccolo cuore.

INDICE

Introduzione

Il mondo della comunicazione vive una fase di vorticosa accelerazione.

Gli sviluppi tecnologici degli ultimi due decenni spingono una rivoluzione che ha bruciato i paradigmi tradizionali, travolto interi sistemi, rimodulato canali, e che è tuttora in corso.

Si parla di "new economy", intendendo l'insieme dei fenomeni economici, ma anche sociali e culturali, associati all'impetuoso sviluppo delle tecnologie dell'informazione e delle comunicazioni.

L'"interconnessione su scala globale *anytime* and *anywhere*[1] sta cambiando radicalmente non solo il modo di accedere alle informazioni e creare conoscenza, ma anche quello di interagire e comunicare.

I social network, le app, i blog, infatti, modificano i circuiti di creazione e trasmissione dell'informazione, anche, commerciale; gli smartphone, i tablet e le *connected TV* sono i primi impulsi di un futuro che promette di essere *always on*, sempre connesso, con indubbi riflessi sulle modalità del commercio (elettronico o meno) e di relazione. La rete Internet diventa, quindi, uno spazio economico-sociale digitale o "mercato virtuale" sempre più integrato con il "mercato fisico", o mercato tradizionale. Internet, che spesso viene definita come terza rivoluzione industriale, non sembrerebbe, però, avere molte caratteristiche in comune con le precedenti rivoluzioni, in termini non solo di durata ma anche di creazione di benessere e di impatto sulla produttività. Vediamo l'era dei computer ovunque tranne che nelle statistiche della produttività, questa frase nota come il paradosso di Solow sembrerebbe definire più che correttamente l'era di Internet.

Facebook, Amazon, Google e Netflix: le *FANG's*, rappresentano il vero e proprio emblema della new economy. Esse generano enormi ricchezze che però restano in mano a pochi, non si diffondono. Le FANGs si presentano come i nuovi leader dell'economia globale.

Ci sono 7,3 miliardi di persone su questo pianeta. 1,45 miliardi usano Facebook attivamente ogni giorno. 5 miliardi di spedizioni sono state elaborate da Amazon nel 2017. 118 milioni sono attualmente abbonati Netflix. 3,5 miliardi di ricerche vengono fatte ogni giorno sul motore di ricerca di Google.

Ognuna delle FANGs presenta strategie differenti, con diversi punti deboli e punti di forza, ma, senza dubbio, tutte concentrano la loro attività sul cosiddetto advertising digitale. L'advertising online è caratterizzato da elementi completamente diversi rispetto a quello tradizionale.

Il ruolo centrale è assunto dai dati e dalla loro disponibilità, in base ai quali chi effettua la pubblicità può decidere in anticipo come impostare la propria strategia di comunicazione, ma anche modificarla in tempo reale per meglio rispondere alle esigenze del consumatore. Proprio questa

---

[1] Mattiacci A., Pastore A., *Marketing. Il management orientato al mercato*, Hoepli, 2013, pp. 56-57.

“centralità dei dati” sta facendo aprire gli occhi a molti. In un’ epoca in cui i dati personali e la privacy hanno assunto un valore non soltanto intrinseco per gli interessati, bensì anche economico-aziendale preponderante, le norme del Regolamento sono probabilmente appena sufficienti a garantire la protezione dei dati personali. Ci si chiede se l’utente di un qualsivoglia abbonamento o servizio si senta davvero al sicuro, protetto per quanto attiene alla sfera dei suoi dati personali.

Sono molti a credere che “l’evoluzione dell’antidoto” non riuscirà a tenere il passo al progredire della “malattia”. Nella fase di avvio, Internet, sembrava essere una tecnologia orizzontale e democratica. Ad oggi l’utente scambia informazioni in cambio dell’accesso ai contenuti.
Il bilancio è in genere a vantaggio dei leader della rete, a danno della privacy.

Capitolo 1

Facebook, Amazon, Google e Netflix: le FANGs

1.1 La rivoluzione della “net” economy

Internet segna una svolta nel vero e proprio senso del termine: la rete sta cambiando radicalmente il modo di lavorare, di comunicare, di studiare, il modo di vivere. Per i giovani tutto ciò è qualcosa di ovvio, ma nella realtà concreta delle imprese, delle banche, degli enti pubblici e in generale della società solo da poco tempo si è avvertita la portata rivoluzionaria di questo strumento. Oggi si può percepire la coesistenza di old economy e new economy, di vecchie abitudini e di nuove iniziative. Lo scenario molto spesso può rivelarsi incerto e contraddittorio, ma la direzione è chiara: sta avvenendo l’ingresso nel mondo on-line. Quando si parla di Internet e di *new economy*[2] è possibile cadere in errore e credere che i problemi dell'economia e della società si possano risolvere da soli; ricordando il libero mercato di Adam Smith[3] governato dalla 'mano invisibile' della concorrenza perfetta[4]. In termini generali, si può parlare del sorgere di una “new economy” ogniqualvolta l’introduzione e la diffusione di nuove tecnologie determina cambiamenti profondi a livello economico e sociale, con una conseguente accelerazione della crescita della ricchezza, della produttività, dello sviluppo sociale, associata a una trasformazione degli stessi modi di vita. Con questo termine si definisce quindi l’insieme dei fenomeni economici, ma anche sociali e culturali, associati all’improvviso sviluppo delle tecnologie dell’informazione e delle comunicazioni *(Information and Communication Technologies, ICT).* Sembrerebbe, però, essere più corretto parlare di net economy o di economia della rete, sottolineando al meglio l'aspetto più rilevante del cambiamento, che è appunto la connessione in rete di tutti gli operatori.

Dalla nascita del *World Wide Web*[5] ai giorni nostri, il mercato non ha fatto altro che evolversi. Tim Berners-Lee, co-inventore del *World Wide Web*, in occasione del discorso al Knight Foundation nel

---

[2] Insieme dei fenomeni economici, ma anche sociali e culturali, associati all’impetuoso sviluppo delle tecnologie dell’informazione e delle comunicazioni che ha caratterizzato l’ultimo scorcio del 20° sec.

[3] Adam Smith è considerato il fondatore dell’economia politica perché fu il primo a studiare, nel tardo Settecento, i fattori che determinano l’accrescimento e la diminuzione della ricchezza complessiva di un paese. Spiegò perché nelle società moderne la ricerca che ciascun individuo fa del proprio tornaconto personale può essere compatibile con il benessere collettivo: è la teoria della «mano invisibile» del mercato e della concorrenza.

[4] Secondo la teoria neoclassica, la concorrenza perfetta è il meccanismo ottimale per l'allocazione efficiente delle risorse in quanto il prezzo di vendita che va a formarsi sul mercato è quello che remunera tutti i fattori di produzione in base alla loro produttività marginale, non consente la creazione di extra profitti, ma garantisce la massimizzazione del benessere dei consumatori.

[5] Sistema, soprannominato «ragnatela intorno al mondo», che permette la condivisione di documenti ipertestuali multimediali, visuali e audio/video, sfruttando l’infrastruttura di Internet. Per accedere al world wide web si utilizza un opportuno software, detto browser.

2008 definisce così il risultato di anni di studi e ricerche che hanno portato alla nascita del WWW: "Il Web non si limita a collegare macchine, connette delle persone".

Si sviluppa un nuovo modo di "stare sul mercato": nasce l'e-commerce. Il commercio elettronico permette ad imprese e consumatori di superare le barriere spaziali: dallo scambio fisico e locale si passa, infatti, all'incontro di potenziali acquirenti che risiedono dall'altra parte del mondo. Caratteristica principale è l'ubiquità: prodotti o servizi sono disponibili pressoché dovunque e in ogni momento. Il mercato non è più ristretto ad uno spazio fisico ma ora è possibile portare a termine acquisti direttamente dal proprio smartphone. Le tecnologie dell'e-commerce permettono di superare i limiti geografici e culturali che tradizionalmente caratterizzavano ogni transazione. Le tecnologie nel commercio elettronico permettono, inoltre, un alto grado di interattività, intesa come comunicazione diretta tra i commercianti e i consumatori. Oltre, il cambiamento delle dimensioni di tempo e spazio, quindi si avvertono: lo spostamento dalla centralità della produzione industriale alla centralità dei servizi, e lo spostamento dalla centralità dell'offerta alla centralità del cliente.

La Rete permette un grado maggiore di personalizzazione del messaggio pubblicitario, che non si deve necessariamente riferire a una massa indistinta con un'unica offerta ma può adattarlo ad ogni singolo target individuabile. L'*advertising*, infatti, è la tipologia di comunicazione che è stata maggiormente coinvolta dal vento di cambiamento innescato dalla rivoluzione digitale e ha concesso all'impresa nuovi spazi per raggiungere e colpire l'attenzione del consumatore. Appare del tutto evidente allora, come l'advertising online sia caratterizzato da elementi completamente diversi rispetto a quello tradizionale.
In quest'ottica, un ruolo di primo piano è assunto dai dati e dalla loro disponibilità, in base ai quali chi effettua la pubblicità può decidere in anticipo come impostare la propria strategia di comunicazione.

Quando si parla di "*cloud computing*", la cosiddetta "nuvola", si vuole indicare l'archiviazione, l'elaborazione e l'uso di dati su computer remoti e il relativo accesso via Internet. Si configurano così un insieme di servizi, accessibili *on demand*[6] e in modalità *self-service* tramite la connessione Internet, basati su risorse condivise, caratterizzati da flessibilità nell'infrastruttura. Nella pratica il *cloud* soddisfa l'esigenza degli utenti di avere sempre e ovunque a disposizione i propri dati, anche nei casi in cui si è lontani da casa o dal proprio ufficio. Per il giurista, il *cloud computing*, rappresenta uno strumento di grande interesse, sotto vari profili, tuttavia suscita anche molte preoccupazioni, alla luce dei rischi che presenta. Si evidenziano, nel particolare, quelli relativi alla conservazione dei dati personali e tutte le informazioni riservate di cui inevitabilmente, con il *cloud*, l'utente perde il controllo diretto. Il trasferimento di quest'ultimi avviene, difatti, su server remoti, server che sottostanno a differenti sistemi giuridici nazionali, di qui l'incertezza circa la legge applicabile. Necessario è, quindi, predisporre un

6 *On demand*, letteralmente "su richiesta"

sistema di regole volte a garantire la tutela al diritto dell'utente a mantenere il controllo. La tecnologia *cloud*, in realtà solo parzialmente nuova, renderà sempre più netta la separazione fra la titolarità dei dati e dei trattamenti, e il possesso e il controllo fisico dei dati trattati o conservati. Ogni trattamento, anche il più semplice, richiederà comunque la circolazione sulla rete. Molti sono i pericoli non solo per il mondo delle imprese e per gli individui, ma anche per le grandi strutture pubbliche e private e, in particolare, quelle di giustizia e sicurezza. Sempre maggiori quantità di dati potranno essere allocate fuori dal controllo fisico e diretto delle autorità nazionali.

Tra questi innumerevoli cambiamenti, l'*Internet of Things*[7] si presenta come possibile evoluzione dell'approccio alla connettività. *IoT* si riferisce all'interconnessione in rete di oggetti di uso quotidiano, che sono spesso dotati di intelligenza onnipresente. L'*IoT* aumenterà l'ubiquità di Internet integrando l'interazione di ogni oggetto tramite sistemi integrati, arrivando a quella che sarà una rete altamente distribuita, costituita da dispositivi che comunicano con esseri umani e altri dispositivi. Le società si compongono, quindi, di strutture " flessibili " con miliardi di persone connesse. Necessario è prendere atto del cambiamento del sistema di valori, centrale è il valore che assumono i dati. Quei dati costantemente raccolti dalla Rete vanno a formare un'informazione preziosa, che necessita di protezione.

L'informazione è potere. Chiunque al giorno d'oggi detenga più informazioni possibili riguardanti un altro o tanti altri individui, ha potere su quel singolo o addirittura su quella moltitudine. Con la crescente propagazione dell'informazione su larga scala supportata dai progressi tecnologici dei computer, si passa da un diritto alla riservatezza ad un diritto del controllo dei propri dati, della diffusione degli stessi. L'informazione allora non è più soltanto potere, ma può diventare un grande business. L'attività di controllo, e dunque implicitamente di violazione della privacy, può ritenersi addirittura agevolata quando essa è ritenuta astrattamente lecita: consultare motori di ricerca o mappe tramite *GPS* (Global Positioning System) sul web, navigare in Internet, inviare documenti tramite mail sono attività ordinarie, ma che contemporaneamente possono essere oggetto di facile controllo da chi si trova al di là dello schermo. Ciò può avvenire in modo limpido attraverso politiche tecnologiche come cookies, bensì tecnologie che permettono di memorizzare le attività compiute su uno specifico computer, oppure in modo malevolo, illecito attraverso malware, spyware, cavalli di Troia e così via discorrendo.
Il Grande fratello vi guarda! Una minaccia, una intimidazione che rende ancora più consapevoli di essere osservati, di essere controllati e ancor più di essere desiderosi del ripristino di un valore fondamentale che è quello della privacy.

---

[7] L'espressione «Internet delle cose» è stata coniata nel 1999 da Kevin Ashton. Si intende una rete di oggetti dotati di tecnologie di identificazione, collegati fra di loro, in grado di comunicare sia reciprocamente sia verso punti nodali del sistema, ma soprattutto in grado di costituire un enorme network di cose dove ognuna di esse è rintracciabile per nome e in riferimento alla posizione.

La progressiva digitalizzazione ha spinto verso l'adozione di una disciplina normativa unitaria per tutti i mezzi di comunicazione elettronica, sollevando, tuttavia, numerose questioni giuridiche. Basti pensare come Internet abbia gradualmente determinato il venir meno della distinzione tra libertà di comunicazione tra due soggetti (art. 15 Cost.) e libertà di manifestazione rivolta a un pubblico indeterminato (art. 21 Cost.), poiché sulla Rete trovano applicazione entrambi i principi contemporaneamente. La net economy è, quindi, il futuro e chi non cresce in questa direzione sembrerebbe essere senza futuro. Ma sia ben chiaro che Internet non deve essere visto come un fenomeno senza possibili "danni collaterali". Intraprendere questa strada non presenta solo dei benefici, infatti, tutto ciò ha un costo, un prezzo molto elevato che sembrerebbe essere proprio la privacy degli utenti. Sarà necessario trovare il modo di rispettare la natura di Internet, spontanea, ma al tempo stesso è doveroso evitare che il cambiamento imposto dalla net economy venga subito passivamente e avanzi senza regole; il cambiamento va guidato e governato, a livello mondiale.

1.2 Facebook, Amazon, Google e Netflix

Grandi aspettative sono state poste negli ultimi venti anni sulla cosiddetta new economy trainata da Internet e dalle tecnologie dell'informazione. Ciò nonostante stiamo vivendo una lunga fase di ristagno economico che ha riportato indietro di decenni non solo i redditi della maggior parte degli abitanti dei paesi industrializzati, e ha provocato anche tassi molto elevati di disoccupazione mentre i divari tra le classi sociali si sono ampliati. Dopo aver analizzato sommariamente la new economy, non si può far altro che andare ad indagare i''protagonisti'' di questo momento storico, analizzandone i vari profili. Emblema della new economy sono Facebook, Amazon, Google e Netflix. Sono considerati i più grandi player di questa nuova era, e sono stati raggruppati dagli analisti finanziari americani in un acronimo: *FANGs*, in inglese, letteralmente zanna[8]. Le *FANGs* generano enormi ricchezze che però non si diffondono. Ognuna di esse presenta strategie differenti, con diversi punti deboli e punti di forza, lo sfruttamento dei dati degli utenti, si pone però alla base di tutte le dissimili strategie. Tutte sono senza dubbio modelli ispiratori di questo periodo storico. Le *FANGs* hanno sperimentato sul mercato azionario una crescita formidabile negli ultimi cinque anni più che raddoppiando il loro valore rispetto a risultati assai più modesti delle principali aziende quotate a Wall Street. Queste high tech company tendono a non distribuire dividendi reinvestendo la maggior parte dei loro utili, dominando da tempo il mercato azionario americano.

---

[8] Sul punto, cfr. Menghini F., *Le FANGs: Facebook, Amazon, Netflix, Google: I grandi gruppi della new economy nell'epoca della stagnazione economica*, GoWare, 2017.

1.2.1 Facebook

Facebook è un social media e social network lanciato il 4 febbraio 2004, posseduto e gestito dalla società Facebook Inc. Il sito, fondato ad Harvard negli Stati Uniti da Mark Zuckerberg e diversi colleghi era originariamente stato progettato esclusivamente per gli studenti dell'Università di Harvard, ma fu presto aperto anche agli studenti di altre scuole della zona.Successivamente fu aperto anche agli studenti delle scuole superiori e poi a chiunque dichiarasse di avere più di 13 anni di età. Il "Digital in 2018 Report"[9] realizzato da We Are Social mostra che, nel mondo, il numero di persone che utilizzano i social è oltre 3,3 miliardi: quasi la metà della popolazione mondiale, quindi, è presente su almeno un canale social e lo utilizza quotidianamente.

Facebook ha realizzato una crescita importante sebbene raggiungendo dimensioni minori degli altri big player della new economy. La missione di Facebook recita: *to give people the power to share and make the world more open and connected.* Anche in questo caso però, ampliare il numero di persone che si connette a Facebook, sembra essere un semplice mezzo per incrementare i propri guadagni. Guadagni basati sulla vendita di spazi pubblicitari sulle sue piattaforme di social networking. Nel 2010 il fatturato dell'azienda ammontava a 1,97miliardi di dollari. Quattro anni dopo 12,466 miliardi, con una crescita media del + 58% ogni anno. La pubblicità, nel 2014, arriva a rappresentare il 92% dell'intero fatturato. La parte restante è rappresentata prevalentemente dai ricavi derivanti dai produttori di app che immettono i loro prodotti nelle piattaforme di Facebook. La strategia di Facebook per sostenere ed ampliare la propria crescita si basa su: l'espansione del numero di utenti nei differenti mercati, l'offerta di nuovi prodotti, l'incremento del tasso di attività degli utenti, insieme all'aumento del numero di investitori pubblicitari (grazie alla fornitura di strumenti sempre più sofisticati di profilazione del cliente) con un conseguente incremento del *Cost Per Click* (CPC). La crescita dell'azienda non è stata sempre estranea a possibili crisi. L'inarrestabile crescita del mobile, ad esempio, a danno del personal computer comporta una più bassa redditività per Facebook (lo si è rilevato anche per Google) dovuta sia ai minori spazi pubblicitari disponibili che alla perdita dei ricavi derivanti dai produttori di video games attivi soprattutto sui personal computer. Secondo il Trefis Report nel 2014 le *ad impression*[10], cioè i messaggi pubblicitari realmente visti sono calati del 40% proprio per il crescente passaggio al mobile. Nello stesso tempo il prezzo medio per *impression* si è incrementato del 173% grazie alla più elevata performance raggiunta attraverso le informazioni raccolte sui clienti. Il potere negoziale, probabilmente, di Facebook nei confronti degli inserzionisti ha giocato il suo ruolo. Facebook ha cercato di contrastare una possibile tendenza negativa in diversi modi. Ha acquistato Instagram prima e WhatsApp poi, con l'obiettivo di

---

9 URL: https://wearesocial.com/it/blog/2018/01/global-digital-report-2018

10 Le impression pubblicitarie sono il conteggio delle visualizzazioni di ogni singola pubblicità da parte dell'utente.

rafforzare la propria posizione nel mobile. Nel 2013 Mark Zuckerberg ha annunciato con un *white paper* in cui affermava che la connettività rappresenta un diritto umano, la partecipazione all'iniziativa di internet.org[11], intrapresa insieme ad altri player, tra cui ad esempio Samsung, Ericsson, l'obiettivo è portare Internet nelle zone più povere del pianeta. Per oltre due miliardi di dollari, Facebook ha concluso l'acquisto di Oculus, una società specializzata nello sviluppo di tecnologie connesse alla realtà virtuale, che sta sviluppando prodotti destinati a rivoluzionare la realtà dei video giochi. Infine nel gennaio del 2016 Zuckerberg ha annunciato di voler costruire Jarvis, un assistente computer che potrebbe mettere a frutto gli investimenti compiuti da Facebook nell'intelligenza artificiale.Il free cash flow, di Facebook, è passato da 188 milioni di dollari nel 2010 a 3, 6 miliardi di dollari nel 2014. A fine 2015 si è arrivati a un utile netto di 1,56 miliardi di dollari, su ricavi superiori a 5 miliardi. Il 2017 non è stato esattamente positivo per Facebook dal punto di vista finanziario, dato che, nonostante la società di Zuckerberg abbia superato ogni record e previsione, con gli utili più alti mai registrati, a bilanciare la redditività vi sono stati i grossi investimenti che l'azienda ha previsto nella sicurezza per combattere fake news e abusi sul social network. «Proteggere la nostra community è più importante che massimizzare i nostri profitti» ha dichiarato Zuckerberg annunciando investimenti "significativi" nel 2018, con un aumento delle spese per migliorare il settore video della piattaforma e rafforzare gli sforzi contro abusi e fake news. La pubblicità su Instagram e l'impegno di Facebook per monetizzare i video attraverso Facebook Watch sono però considerati tali da garantire la crescita nel breve periodo.

1.2.2 Amazon

Amazon.com, Inc. è un'azienda di commercio elettronico statunitense, con sede a Seattle, Washington. Viene fondata nel 1994, e lanciata nel 1995. Il fatto che prenda il nome dal corso d'acqua più lungo del pianeta la dice lunga sulle ambizioni del suo fondatore e CEO Jeff Bezoz, l'azienda è, ad oggi, uno dei maggiori *retailer on line* del mondo. Dopo un avvio basato sulla vendita dei libri online Amazon ha gradualmente ampliato le categorie di prodotti venduti via web introducendo materiale informatico, elettronico e via via una serie di altre categorie merceologiche. Le famiglie di prodotto sono oggi più di quindici. L'obiettivo dell'azienda è di riuscire a vendere via web tutto quello che è materialmente possibile acquistare con un pc, un tablet o uno smartphone e consegnare attraverso il proprio sofisticato sistema di logistica. Oltre a questa linea di business, oggi prevalente, Amazon è anche un operatore leader nella fornitura di servizi di cloud alle imprese. La piattaforma è diventata la preferita di Uber a Airbb e Netfix. Anche lo stato americano è un cliente: pochi anni fa la CIA ha siglato un accordo di 600 milioni di

[11] URL: https://info.internet.org/en/

dollari per usufruire di servizi sul cloud. Si tratta di un settore che contribuisce al conto economico di Amazon con margini più elevati della vendita retail nonostante i servizi siano offerti ad un prezzo molto competitivo per far fronte alla concorrenza di Google e Microsoft. La strategia di Amazon nel retail è quella di comprare all'ingrosso e vendere al dettaglio con una politica molto aggressiva di sconti imposti ai propri fornitori la cui dipendenza dall'azienda è diventata crescente nel tempo. Le piattaforme operative sono principalmente due, il *Marketplace* che vede i produttori vendere direttamente la loro merce e Prime che offre vantaggi di prezzo e di consegna ai clienti i quali e pagano una *fee* (canone) annuale per abbonarsi al servizio, oggi il servizio Prime registra più di 100 milioni di clienti. La natura dei business[12] di Amazon la porta a generare un forte cash flow che finora è stato massicciamente investito dal management per garantire la crescita futura. Investendo soprattutto nella tecnologia e nei sistemi di logistica, Amazon Robotics (precedentemente KIVA), acquisita nel 2012, ha costruito più di 15.000 robot per i propri centri.

Il modello di Amazon è evidente che si focalizza sulla distruzione, all'interno della catena del valore di molti business, il *publishing* per primo, dell'anello rappresentato dal retail, per poi risalire a monte verso la creazione e la produzione del prodotto. Il fatturato del 2014, di circa 73 miliardi di euro, era cresciuto del 20% rispetto a quello del 2013, che a sua volta era cresciuto del 22% rispetto al 2012.
Nel 2017 le entrate sono state pari a 43,7 miliardi di dollari, contro i 42,19 miliardi previsti; i guadagni sono stati di 0,52 dollari per azione. Il colosso dell'e-commerce solo per quanto riguarda Amazon Web Services, intanto, ha registrato entrate per 4,6 miliardi di dollari, rispetto ai 3,2 miliardi di dollari del 2016, con una crescita superiore a quella prevista. Il bilancio del primo trimestre 2018 registra entrate superiori ai 51 miliardi di dollari (+43% rispetto allo stesso periodo dello scorso anno), e un utile netto che raddoppia e raggiunge la cifra di 1,6 miliardi di dollari. La società di investimenti Bespoken[13] ha messo a punto l'indice *"Death by Amazon"*. Misura l'andamento di 54 società di retail tradizionale e dopo l'acquisto di Whole Foods[14] da parte di Amazon è sceso ai valori minimi. Queste sono le parole dell'ex presidente degli Stati Uniti Barack Obama: «L'innovazione è inarrestabile e sta accelerando. Amazon e le vendite online stanno uccidendo il retail tradizionale, e quello che è vero lì, sta per diventare vero attraverso tutta la nostra economia». La tecnologia, molto più della concorrenza del Messico o della Cina, mette a rischio il lavoro, necessario è trovare dei modi nuovi per gestire questo cambiamento, da affiancare alle tradizionali lotte sindacali. Warren Buffet definisce Amazon quasi come un fenomeno

---

12 Sul punto, cfr. Rao V., *Why Amazon is the best strategic player in tech*, Forbes, 2011.

13 Società di consulenza specializzata nel digitale, URL: https://www.bspkn.it

14 Whole Foods Market è una società alimentare statunitense con sede ad Austin, in Texas. Nel dicembre 2017 la società gestiva oltre 473 supermercati negli Stati Uniti, in Canada e nel Regno Unito. Il 16 giugno 2017 Amazon ne ha annunciato l'acquisizione.

naturale. «È una grande, grande forza, e ha già distrutto *(disrupted)* un sacco di persone e ne distruggerà di più». Amazon ha economie di scala, di scopo e di apprendimento che nessun player tradizionale ha. Laddove viene applicata la piattaforma Amazon, la quota del valore aggiunto che resta alla distribuzione si riduce drasticamente[15].

1.2.3 Google

Nell'agosto del 2015 è stata annunciata la costituzione di Alphabet, la holding che ha assunto il governo di Google e delle altre società da essa controllate. Alphabet da allora controlla, oltre all'omonima creata da Page e Brin, Nest (*smart thermostats*), Google Fiber (*broadband service*), Calico (*longevity research*), Life Sciences (*contact lenses*), Google Ventures (*startup investments)*, Google X, (*self driving car*, intelligenza artificiale). Google, l'azienda diventata il simbolo del nuovo millennio, crea quindi una conglomerata, anche se fortemente sbilanciata. Questo perché il business dell'advertising, principale per Google, è così grande che sovrasta rispetto agli altri che sono entità ancora allo stadio di laboratori di ricerca o poco più che start-up. Questo sarà ricordato come un avvenimento, perché dalla fine degli anni novanta le più grandi società di consulenza mondiali avevano celebrato la morte delle conglomerate, poiché ritenute troppo diversificate, presenti in business tra loro differenti e non correlati, considerate dunque meno efficienti delle aziende mono-prodotto. Non vi è dubbio che la ragione principale possa essere legata all'esigenza di gestire al meglio il gigantesco cash flow generato.

Larry Page and Sergey Brin affermano : *"keep tremendous focus on the extraordinary opportunities we have inside of Google"*[16]. Google, o meglio, la sua parent company Alphabet, definisce così il suo core business: *"generate revenues primarly by delivering online advertising that consumers find relevant and that advertisers find cost-effective."* Il 2015 è stato chiuso con un fatturato di 74 miliardi di dollari ed un cash flow di oltre 64 miliardi di dollari. L'attività di vendita pubblicitaria, che offre pubblicità online che i consumatori ritengano pertinente e che gli inserzionisti trovino economicamente conveniente, trae origine da un motore di ricerca progettato dai fondatori di Google. Dai dati disaggregati disponibili nell'Annual Report del 2014, ben l'89% del fatturato di Google era generato dall'advertising.
Steve Faktor[17], un blogger americano sintetizza efficacemente la strategia di Google: la vera natura di Google è un network *B2B*[18] che consente ad un circolo chiuso di clienti di "colpire" gli utenti di Google

---

15 Sul punto, cfr. *How far Amazon go?*, The Economist, 2014.

16 Brin S., Page L., *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, Journal Computer Networks, 1998.

17 Sul punto, cfr. Faktor S., *Deconstructing Google'Strategy*, Forbes, 2013.

18 Business-to-business, spesso indicato con l'acronimo B2B, è una locuzione utilizzata per descrivere le transazioni commerciali elettroniche tra imprese.

con la propria pubblicità. Ogni servizio offerto da Google ai propri utenti nasce per raggiungere l'obiettivo principale: creare il più grande mercato possibile per distribuire pubblicità, aumentando il numero degli utenti, la loro frequenza di visita, il tempo di permanenza. Ecco spiegato il perché Google offra un mix di servizi gratuiti o economici, unicamente per accrescere il mercato dell'advertising.

I free product non sono altro che dei "cavalli di troia", usati per raccogliere dati che consentono a Google di vendere pubblicità più mirata. Sempre nell'intento di ampliare tale mercato, Google si sta muovendo al fine di rendere possibile la connessione a Internet per nuovi territori e intere popolazioni. Oppure cercando di allargare il tempo libero a disposizione di chi a Internet è già connesso, ad esempio negli USA Google sta realizzando importanti investimenti per dotare interi stati della sua fibra ottica. Infine Google è sicuramente l'azienda che più sta spingendo verso la cosiddetta intelligenza artificiale. Il suo tasso di crescita mostra però un andamento decrescente, non solo a causa dello stato generale dell'economia ma anche per la concorrenza di altri operatori. e della Da tenere in considerazione è la crescita esponenziale dell'accesso a Internet attraverso il mobile, infatti, le app rappresentano un formidabile mezzo per bypassare Google. La mossa di Google per contrastare il declino tendenziale dei propri ricavi si chiama *Moonshots*. Con questo termine, letteralmente lancio sulla luna, (ma anche palla battuta molto alta nel baseball) Brin e Page definiscono gli investimenti ad alto rischio e potenzialmente ad elevata redditività, essenzialmente per acquisti di centinaia di start up e brevetti.

Google ha oggi sette prodotti che dichiarano più di un miliardo di utenti e che includono il motore di ricerca, le mappe, Gmail, You Tube, Google Play Store, Android e Chrome. Più gli utenti passano il tempo sui servizi di Google più l'azienda apprende i loro comportamenti e vende più pubblicità. I sostenitori di Alphabet sostengono che essa è stata creata "per aggiungere forza a forza".

L'opinione di molti analisti finanziari è che una serie di successi può improvvisamente venir meno. Ken Favaro afferma: alla fine essi inevitabilmente compiranno un percorso casuale che potrà essere razionalizzato solo ex post.

Scott Cleland, presidente di Precursor una società di ricerca e consulenza americana, definisce in questo modo Google: mai è esistita tra le maggiori corporation una che abbia in modo sistematico ignorato i diritti di proprietà degli altri: i brevetti di Android, libri, musica, TV e filmati e marchi registrati. Ci sono ampie evidenze che Google spadroneggi su Internet come il rapinatore del ventunesimo secolo che crede di poter fare quello che vuole con poca paura e riguardo nei confronti della legge[19].

[19] Cleland S., *Why you can't trust Google Inc*., Telescope Books, 2011; e dello stesso autore l'articolo *The Top Ten Threats to Google*, Forbes, 2011.

Anche Kira Radisky commenta, su Harvard Business: l'accesso di player affermati a grandi quantità di dati proprietari, affligge la competitività dell'intero settore e ciò danneggia l'economia[20].

Google ha rivoluzionato i motori di ricerca quando ha introdotto nel 1996 il suo famoso algoritmo "Page Rank Algorithm". I motori di ricerca da allora si sono significativamente evoluti e oggi la maggior parte di essi è basata su "machine learning algorithms". Gli studi condotti in questo ambito mostrano come la sequenza storica delle ricerche migliori i risultati dei *search engine*[21] di oltre il 31%. Non si raggiungono oggi risultati di qualità senza una conoscenza passata del comportamento degli utenti che si basa appunto su larghe basi di dati e soprattutto lunghe serie storiche di comportamenti. È chiaro dunque come questo fattore diventi una formidabile barriera all'entrata per ogni concorrente. Forse, conclude Kira Radinsky, è arrivato il tempo di realizzare uno Sherman Act[22] per i dati. Ruth Porat, CFO di Alphabet, a inizio 2017 aveva parlato di "ottimi risultati" con ricavi in crescita del 22% rispetto al primo trimestre del 2016.

Al termine del 2017, i dati numerici più interessanti per Google, infatti, sono stati: entrate pari a 27,77 miliardi di dollari altre entrate ovvero di servizi hardware e cloud, sono state di 3,4 miliardi di dollari, rispetto a 2,43 miliardi del 2016 le perdite operative di altre società di Alphabet come X, Nest e Waymo, sono state di 812 milioni di dollari.

1.2.4 Netflix

Netflix è una *media and entertainment company*, ovvero un'impresa operante nella distribuzione via internet di film, serie televisive e altri contenuti d'intrattenimento. Fondata nel 1997 da Reed Hastings e Marc Randolph in California. Nasce come attività di noleggio di DVD e videogiochi. Gli utenti potevano prenotare i dischi via internet, ricevendoli direttamente a casa tramite il servizio postale. Questo primo business come noleggio di DVD per corrispondenza oltre ad offrire un incredibile vantaggio al cliente, permette l'assenza di investimenti iniziali per aprire punti vendita, in questo caso non necessari. Netflix nasce quindi con una struttura di costi molto ridotta. Dal 2008 l'azienda ha attivato un servizio di streaming online on demand, accessibile tramite un apposito abbonamento, questo diverrà presto il suo campo d'attività principale. Netflix poi deciderà, dal 2013, di integrarsi anche a monte per affiancare un propria produzione al catalogo offerto. Una delle serie targate Netflix di maggior successo è *House of Cards*. L'azienda a fine 2015, con 3500 dipendenti, ha avuto un fatturato di circa 6,8 miliardi di dollari.

---

[20] Radinsky K., *Data monopolists like Google are threatening the economy*, Harvard Business Review, 2015.

[21] Un motore di ricerca Web è un sistema software progettato per cercare informazioni sul World Wide Web. I risultati della ricerca vengono generalmente presentati in una serie di risultati spesso denominati pagine dei risultati dei motori di ricerca (SERP).

[22] Lo Sherman Antitrust Act del 1890 è la più antica legge antitrust degli USA.

Ovviamente rispetto a Google, Amazon , Facebook è un operatore minore. In ogni caso però è il più grande cliente di studios e canali televisivi, investendo circa il doppio rispetto ai suoi concorrenti diretti. Solo nel 2015 sono stati difatti spesi ben 3,3 miliardi di dollari in acquisizione di contenuti e diritti.
Nel 2016, dopo un lungo periodo di focalizzazione sul mercato americano, Netflix riesce a raggiungere una copertura virtuale di 130 paesi, esclusa la Cina.

"Watch what you want, when you want", quindi nessun vincolo di quantità, tempo o orario. Questa è la formula che ha portato l'azienda al successo, basti confrontare questa libertà data al consumatore con la programmazione televisiva, basata su palinsesti rigidi. Altro punto forte dell'offerta dell'azienda è che i prodotti in questione possono essere visti su qualsiasi tipo di apparecchio, senza bisogno di alcuna parabola satellitare ad esempio. I suoi maggiori concorrenti sono Hulu e Amazon Prime. All'inizio Netflix aveva spuntato prezzi bassissimi per le concessioni dei diritti da parte delle case cinematografiche e delle grandi reti televisive, quest'ultime non si rendevano ancora conto della portata dello streaming, ritenendolo un fenomeno marginale. A fine 2015 Netflix aveva circa 45 milioni di sottoscrittori. Di questi 33 milioni, quindi circa il 75%, sono americani. Ogni cliente americano genera 82,3 dollari di fatturato l'anno, e rappresenta un costo, marketing, advertising e operativo, di quasi 56 dollari. Per ogni cliente estero, invece, l'azienda realizza 65 dollari contro circa 72 dollari di costo del venduto, generando una perdita, comprensibile vista l'internazionalizzazione di Netflix molto recente. A chiusura del 2017 la società guidata da Reed Hastings ha pubblicato un bilancio "record", la capitalizzazione di mercato di Netflix per la prima volta è salita sopra i 100 miliardi di dollari. Netflix, infatti, nonostante abbia aumentato il costo dell'abbonamento, cresciuto soprattutto nella versione *premium*, la quale consente di accedere ai contenuti in alta definizione e di condividere la visione su più schermi, la risposta del pubblico sembra essere stata positiva. Questo, in una visione a lungo termine, significa che Netflix è sempre più apprezzato e può contare su un pubblico fedele; che potrà solo che migliorare i propri margini. Nel 2017, infatti, sono stati aggiunti globalmente 24 milioni di nuovi utenti, contro i 19 milioni del 2016. Le azioni ora sono al massimo storico, oltre i 220 dollari. In 12 mesi hanno guadagnato più del 60%.

David Molofsky di It Proportal commenta così l'incredibile crescite della media and entertainment company: "Netflix sa cosa state osservando. Perché raccoglie moltissime informazioni dai suoi utenti e con grande livello di dettaglio. Questi dati sono stati impiegati prima di tutto per migliorare la propria piattaforma e poi per la creazione di contenuti. *House of Cards* per esempio, è un tenebroso thriller politico con personaggi affascinanti ma immortali, *Orange is the New Black* è una commedia con forti protagoniste femminili. Ognuno è un genere specifico anche se popolare, è stato quindi costruito sull'audience." Fin dalla sua nascita, Netflix, ha infatti lavorato sul proprio motore di ricerca

Reccomendation Engine finalizzato a individuare prima e indirizzare poi le scelte dei suoi utenti. Oggi l'azienda è in grado non solo di riconoscere i generi preferiti dai suoi clienti, ma molto più nel dettaglio, riesce ad "entrare nei film" dando un rating ai singoli contenuti: azione, amore, ecc.. e al loro mix in una singola opera, selezionando in modo specifico l'offerta da proporre a ogni singolo sottoscrittore.

1.3 Un conto è essere giganti un altro è essere monopolisti

Uber, Amazon e gli altri? Non sono ancora monopolisti, parola di Antitrust. «Chi ha molto potere economico non necessariamente controlla il mercato come un monopolista.» Un conto è essere dei giganti, un altro è essere monopolisti. E un conto è essere monopolisti per un lungo periodo e un altro è esserlo per poco tempo, prima di essere scalzati da nuovi concorrenti. In altre parole, «il gigante in quanto tale non dà fastidio, è quando diventa troppo forte che va controllato». Parte da qui il direttore generale della Direzione concorrenza dell'autorità Antitrust italiana, Andrea Pezzoli, per parlare dei colossi tecnologici che abbiano delle posizioni di dominio sui mercati di riferimento. Parliamo di Google, ma non solo. Uber, l'app per il trasporto alternativo ai taxi, è tra gli esempi più citati: la sua capitalizzazione in Borsa è talmente alta che potrebbe permettersi perdite miliardarie. Ci si preoccupa di come i prezzi possano essere applicati in modo diverso per ogni singolo consumatore[23], sulla base delle informazioni che lo riguardano circa il reddito ma anche circa le sue esigenze contingenti. Questo sia che si tratti di trasporti sia social network sia di commercio elettronico. Le analisi degli economisti si dividono su come considerare i confini dei mercati rilevanti[24], e quindi quando cominciare a considerare un'azienda come Google o Uber monopolista. Per l'autorità Antitrust italiana «da un punto di vista concettuale non c'è nulla di nuovo sotto il sole. Si stanno affrontando in una nuova prospettiva, con una battuta potremmo dire 4.0, argomenti che si sono già affrontati. Da un punto di vista fattuale, però, ci sono parecchie novità e su queste ci si sta interrogando». Che i colossi del tech abbiano un potere economico enorme è fuori discussione, ma «Il gigante in quanto tale non dà fastidio, è quando diventa troppo forte che va controllato». Il potere economico, infatti, non è sinonimo di posizione dominante. Bisogna essere più cauti, soprattutto perché, a fronte di cambiamenti tecnologici sempre più rapidi, è sempre più difficile andare a definire il mercato rilevante, che da sempre è lo strumento principale per l'operato dell'Antitrust.

---

[23] Si pensi alla cosiddetta discriminazione perfetta di prezzo, studiata in economia. In tale forma, detta anche discriminazione perfetta, l'impresa riesce a ottenere da ciascun consumatore il prezzo massimo che è disposto a pagare per l'acquisto di quel determinato bene (prezzo di riserva).

[24] Il mercato rilevante può essere definito come il più piccolo contesto, insieme di prodotti, area geografica, nel cui ambito è possibile, tenendo conto delle esistenti opportunità di sostituzione, la creazione di un significativo grado di potere di mercato.

«Affinché si possa esercitare il potere di mercato e un'eventuale posizione di monopolio possa pericolosa per la concorrenza, questa condizione di monopolio deve anche persistere.» Altrimenti si parlerebbe solo di competizione, che è caratteristica di modelli di business basati su "effetti rete" e su tecnologie in continua evoluzione.Alcuni di questi giganti, tuttavia, è da tempo che sono presenti sul mercato in posizione di forza. «Google in particolare, ma anche altri, non sono sul mercato da poco ma da qualche anno e qualche preoccupazione appare legittima». Tra i molti interrogativi, l'analisi va ad incentrarsi su quella che è una questione molto importante, che un caso come quello di Google solleva, ma si potrebbe parlare anche di Facebook: ossia che sul versante dei rapporti con gli utenti non c'è uno scambio monetario. I consumatori "pagano" Google con i propri dati.

È possibile che se i consumatori sapessero esattamente come vengono trattati i dati, potrebbero limitare i dati messi a disposizione. Finora le autorità per la concorrenza si sono dovute basare sul valore dei fatturati delle aziende che comprano e che vengono acquisite. Ma la cronaca racconta di società con un fatturato modesto si sono rilevate di svariati miliardi (qui la lista infinita delle sole acquisizioni di Facebook). Questo perché sono società gonfie di informazioni e di dati che un domani potranno essere vendute sul mercato e trasformarsi in fatturati significativi. A livello comunitario e non solo, ci si sta interrogando se nei settori innovativi, dove contano non tanto i fatturati ma le idee, i dati, le informazioni, forse non bisognerebbe cambiare le soglie di notifica e avere un controllo delle concentrazioni ad hoc.

L'antitrust oltre che intervenire con regole ad hoc sulle acquisizioni del settore hi-tech, potrebbe usare la strategia di "punire il gigante". In termini più tecnici significa non concentrarsi sul controllo delle concentrazioni o sulla struttura ma applicare le regole contro gli abusi di posizione dominante. In altri casi possono utilizzare le norme a tutela dei consumatori, che rientrano tra le competenze dell'Agcm. In Germania, per esempio, a Facebook è stato contestato un abuso di posizione dominante perché non aveva reso chiare le finalità del trattamento dei dati degli utenti. Il dirigente dell'Agcm aggiunge però, che «il consumatore va tutelato ma va soprattutto emancipato. Un eccesso di protezione rischia di entrare in contraddizione con il buon funzionamento del processo competitivo».

1.4 La lettura dei dati come punto di forza

Fin qui abbiamo cercato di comprendere chi siano, come siano nati e come agiscono sul mercato i big player di questa nuova era: Facebook, Amazon, Netflix, Google.

I "magnifici quattro" dell'era digitale, come si è visto, hanno diverse strategie, e quindi diversi punti di forza e punti deboli. Quello che si può notare, però, è che tutte le quattro diverse aziende tendono a sfruttare i dati forniti, in maniera automatica, dai propri utenti.

Il viaggio inizia nell'archivio di Google (Alphabet). Chi usa una email di Gmail, il servizio di posta elettronica, ha inevitabilmente attivato un account che dà accesso a decine di altri servizi, dall'archivio di foto e documenti. Google conosce anche i diversi dispositivi con cui ogni utente si collega all'account e quando, il fine, a detta di Google, è aiutare l'utente a tenere sotto controllo gli accessi, e impedire movimenti non autorizzati. Ogni consumatore ha un personale archivio sulle sue abitudini di ricerca. Nella sezione "Personalizzazione degli annunci" c'è l'elenco dei possibili interessi, catalogati tenendo traccia di tutte le ricerche e della navigazione online con il browser Google Chrome e le app collegate a Google. Se l'utente ha attivato la localizzazione gps, si dà la possibilità a Google incamerare anche posizioni e spostamenti. Google con questi dati perfeziona il servizio e 'nutre' gli inserzionisti.

Anche Amazon conosce molto bene i propri utenti. Ogni giorno, i "Consigli per gli acquisti di Amazon", ricordano ai consumatori prodotti precedentemente ricercati ma, finora, non acquistati, configurandosi quindi come come il *personal shopper* che sa cosa cerca il cliente. "I dati – spiega Amazon – servono per gestire gli ordini, fornire prodotti e servizi, elaborare pagamenti, comunicare con l'utente, aggiornare i registri e, in genere, gestire l'account, mostrare contenuti e consigliare prodotti e servizi che potrebbero essere di interesse". Amazon conserva ogni dato che viene inserito nel sito o che l'utente fornisce in un mal specificato "qualsiasi altro modo". La piattaforma segue la navigazione dell'utente con i cookie, in alcuni casi Amazon acquisisce anche la localizzazione geografica, se abilitata dall'utente. La maggior parte dei dati personali vengono ovviamente forniti con le ricerche, la registrazione, l'iscrizione a Prime, gli ordini. Ma se si guarda più a fondo si scopre che Amazon assimila molto di più: l'indirizzo Ip del computer del consumatore, le informazioni sulla sua connessione internet e anche tipo e versione di browser. La piattaforma spiega di non cedere i suoi dati ad altri, con l'eccezione ovviamente delle società poste sotto il suo controllo. Le pagine a cui viene messo il "mi piace", le amicizie, le foto, i messaggi, tutto ciò è raccolto da Facebook. Se l'utente autorizza l'accesso ai contatti il social network allora ha iniziato ad accumulare anche tutti i metadati di telefonate e messaggi.

Per aiutare gli inserzionisti a personalizzare la pubblicità e a far in modo di rendere gli annunci più efficaci il social assegna agli utenti delle categorie di interesse, dettagliate e numerose. L'advertising online può infatti sfruttare ogni singola espressione di preferenza. È il 12 dicembre 2017: il social media

manager di Netflx pubblica un tweet: “Alle 53 persone che hanno guardato Un principe a Natale ogni giorno negli ultimi 18 giorni: chi vi ha fatto del male?”. Interesse della piattaforma è fornire un palinsesto su misura al suo cliente per fargli vedere film e serie di suo gusto, contenuti tali da controbilanciare il pagamento di un canone. I principali dati che raccoglie sono infatti quelli “di utilizzo”, questi dati però, Netflix lo dichiara, potrebbero essere integrati con informazioni ottenute da altre fonti, comprese le informazioni ottenute da fornitori di dati sia online sia offline.

Quest’enormità di dati, raccolti automaticamente attraverso il servizio offerto agli utenti, costituiscono la vera ricchezza delle cosiddette FANGs. Grazie alla mole di informazioni a loro disposizione, come detto, possono vendere nelle loro piattaforme pubblicità digitale, garantendo ai loro clienti campagne search, rese possibili dall’acquisto di *keywords.* Google e Facebook hanno registrato entrate pubblicitarie nel 2017 per circa 94 miliardi di dollari (Google) e poco meno di 40 miliardi di dollari (Facebook). Antonio Montesano, direttore digital Omd, afferma però che è Amazon il player che sta crescendo di più in termini percentuali, aggiungendo che solo ora sta iniziando a sfruttare a pieno le sue potenzialità di advertising. A metà agosto, Michael Olson, analista di Piper Jaffray, in una comunicazione agli investitori ha dichiarato che il business nell’advertising di Amazon spingerà molto in alto gli affari. «Essere il motore di ricerca di prodotti più grande al mondo ha i suoi vantaggi e Amazon sta iniziando a sfruttarli», ha scritto. Jaffray si aspetta che i ricavi da pubblicità arrivino a 8 miliardi di dollari nel 2018 contribuendo a sostenere gli utili operativi per oltre 3 miliardi. «Entro il 2020, ci aspettiamo vendite pubblicitarie di Amazon pari a 16 miliardi di dollari ed entro il 2021 crediamo che sia altamente probabile che i profitti generati dall’advertising superino quelli di ASW[25]» Si parla delle potenzialità di un gigante che ha dalla sua il vantaggio della vendita al consumatore finale, si tratta del cosiddetto completamento dell’offerta. La pubblicità è la stessa rispetto a quella garantita ad esempio da Google, ma nel market place l’*adv* viene fatto negli stessi luoghi dove si completa l’acquisto.

[25] Amazon Web Services (Aws)

Capitolo 2

La tutela della privacy

2.1 Evoluzione del significato di privacy; significato, valore, diritto.

Com'è definita l'identità? In passato si diceva: "Io sono quello che dico di essere".
Oggi, siamo quello che Google dice che siamo. Siamo sempre meno persone, sempre più profili. Oggi, la libertà è diventata quella non essere discriminati, non essere schedati, non diventare oggetto di controllo continuo per quanto riguarda il consumo o il lavoro. cit. Stefano Rodotà[26]

Quello dei dati personali è un tema che nel contesto che è stato precedentemente delineato, ha guadagnato una sempre maggior rilevanza, soprattutto per via dell'ampliamento della capacità di conservare dati e informazioni. Non è più necessario archiviare in voluminosi scaffali migliaia di carte: tutto viene caricato e salvato nel web risultando più che facilmente accessibile. Al giorno d'oggi "i dati personali sono il nuovo petrolio di internet e la nuova moneta del mondo digitale". Il web essendo nato senza limiti e restrizioni, rappresenta un'area grigia ancora scarsamente regolamentata. Le esigenze di tutela della privacy sono state per lungo tempo intese coincidenti con quelle di riservatezza. È il progresso tecnologico che ha fatto sì, poi, che fosse necessario un rafforzamento della stessa. Il termine privacy descrive quell'ambito "gelosamente circoscritto della vita personale e privata", vi é un bisogno intrinseco di differenziare una sfera individuale privata ed una sfera individuale pubblica, nella quale ad ogni propria azione verrà dato un peso da parte della società. É un concetto estremamente moderno, che risale a non più di 150 anni circa, ma allo stesso tempo anche un aspetto da sempre inerente la natura umana.
Ripercorrendone l'evoluzione storica, dalle origini sino agli ultimi interventi legislativi, risulta evidente la sua natura poliedrica, non é una nozione unificante. "Non è cioè un concetto che esprime esigenze uniformemente e coerentemente diffuse nella storia e nella collettività"[27]. Gli antichi greci ritenevano fondamentale la necessità per ognuno di avere una sfera privata, nell'ambito strettamente limitato all'espletamento dei propri bisogni e delle proprie necessità. La polis riteneva e tutelava come sacri i confini della "casa", ogni uomo necessitava di un "luogo che fosse propriamente suo". Proseguendo nella propria evoluzione, il termine privato divenne sinonimo di familiare, nell'età medievale caratterizzata dalla società feudale. Si andava via via sviluppando il senso di intimità. Intimità durante il sonno; intimità

---

26 Sia consentito rinviare all'articolo di Giovanni Zagni, URL: https://www.linkiesta.it/it/article/2016/03/12/stefano-rodota-la-trasparenza-totale-e-unidea-da-dittatori/29592/

27 Niger S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, 2006, p. 40 ss.

durante i pasti; intimità nel rituale religioso e sociale; arrivando poi all'intimità nel pensiero. Con la progressiva costruzione dello stato moderno e lo sviluppo dell'alfabetizzazione si andò affermandosi il concetto di privacy nella connotazione a noi più vicina.

La nascita concettuale del diritto alla privacy viene solitamente attribuita a due giovani avvocati, Samuel D. Warren e Louis D. Brandeis. In un momento in cui la carta stampata si stava evolvendo, con il passaggio al fotogiornalismo, i due pubblicarono nel dicembre 1890 un saggio intitolato *'The right to privacy'*. Warren e Brandeis definirono la privacy come un'estensione del diritto di proprietà che andava ad includere aspetti non materiali come i sentimenti, i pensieri e le emozioni, che fino a quel momento non avevano ancora ricevuto alcuna tutela. Lo definirono come un diritto negativo, nello specifico usarono l'espressione *"right to be let alone"*[28], cioè un diritto a essere lasciati soli. L'evoluzione del concetto di privacy non si arresta soprattutto grazie all'interpretazione giurisprudenziale, «trovando esplicazione in situazioni profondamente differenti che vanno dal diritto del singolo ad impedire comportamenti intrusivi nella propria vita privata ad opera dei media, al diritto di aborto, alla libertà sessuale»[29], manifestando, così, tutta la propria natura poliedrica. Si giunge, così, a parlare di *informational privacy* e di *decisional pivacy*. Entrambe hanno come fulcro il riconoscimento e la garanzia del potere di autocontrollo in capo al singolo. Tra i "diritti della personalità" il diritto alla privacy non è, quindi, nato per primo. A lungo sullo sfondo, ha progressivamente conosciuto un'evoluzione che ne ha modificato struttura e contenuto. È stato invocato sempre più spesso a tutela di interessi già protetti da altri diritti personali. Tra questi ha così acquistato un ruolo primario, diventando uno tra gli strumenti più importanti di tutela della persona[30]. Il concetto di right to privacy finisce per diventare un "contenitore concettuale" all'interno del quale confluiscono tutte le modalità di tutela della libertà personale garantite al singolo dallo Stato. Definendo la riservatezza un valore essenziale della persona, il diritto alla privacy viene fatto rientrare tra i diritti inviolabili della persona e, quindi, tutelato dall'art. 2 della Costituzione. In questa prospettiva l'art. 2 Cost. è una clausola generale attraverso la quale operare il continuo adeguamento delle garanzie giuridiche alle sempre nuove esigenze di tutela della persona. Dette esigenze sono mutevoli nel tempo e il loro incremento si presenta come direttamente proporzionale alla "distribuzione" dell'informatica. Se da un lato la diffusione dei computer rappresenta un'indubbia conquista del progresso, non si può nascondere il rischio che tale diffusione accompagna: il consolidamento di quello che taluno definisce un "potere occulto"[31]. Un nuovo potere informatico,

---

28 Dorothy J. Glancy, The invention of the right to privacy, Arizona Law Review, 1979.

29 Mantelero A., Il costo della privacy tra valore della persona e ragione d'impresa, Giuffré editore, 2007, p.1

30 Umbertazzi T. M., *Il diritto alla privacy. Natura e funzione giuridiche,* Cedam, Padova, 2004.

31 Niger S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, 2006, p. 43 ss.

consistente nel controllo sui singoli, reso possibile dall'acquisizione e dall'elaborazione di informazioni, spesso anche apparentemente neutre. Un potere spesso "occulto", sia per le modalità di esercizio, sia in ragione dell'ignoranza da parte delle persone a cui le informazioni si riferiscono di quelli che sono le modalità tecniche ed i meccanismi di gestione delle stesse»[32] . Secondo i giuristi De Hert e Gutwirth[33] la privacy e la protezione dei dati personali sono due facce della stessa medaglia, due diritti differenti eppure complementari. Tuttavia, per funzionare in modo efficace questi due ambiti devono restare distinti. De Hert e Gutwirth facendo un confronto evidenziano che il diritto alla privacy è, in termini generali, un diritto sostanzialmente negativo, di non interferenza, che protegge la zona d'ombra (ciò che è privato) dell'individuo; all'opposto, il diritto alla protezione dei dati personali si esprime come una richiesta di trasparenza da parte dei detentori di dati personali. Il diritto alla protezione dei dati è nato con due caratteristiche peculiari che lo contraddistinguono: il consenso e la proporzionalità. In ogni caso è noto che il consenso sia spesso un atto formale, raramente libero e in molti casi inevitabile; mentre, per quanto riguarda la proporzionalità, essa non è talvolta un criterio sufficientemente limitante. La privacy può essere analizzata attraverso con un modello di "costo opportunità", la sua tutela viene contrapposta ad altri diritti, in particole la sicurezza nazionale e la libertà di espressione. Basti pensare che nel momento in cui un individuo autorizza al trattamento dei suoi dati personali ha già acconsentito ad una riduzione della sua privacy in cambio dei servizi ottenuti.

2.2 La protezione dei dati come diritto fondamentale

Il catalogo dei diritti della persona viene definito "aperto"nel senso che nuovi diritti e maggiori tutele della persona sono creati con la lettura costituzionalmente orientata che opera la giurisprudenza. Il catalogo aperto dell'art. 2 della Costituzione afferma che "La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità". Sui (nuovi) diritti e le (nuove) tutele è d'obbligo ricordare l'opera preveggente di Stefano Rodotà, il primo in Italia a intuire già all'inizio degli anni '70 la gravità del problema. In "Elaboratori elettronici e controllo sociale " (Bologna, 1973), Rodotà anticipò i nuovi confini dei diritti della persona. alla vigilia della rivoluzione tecnologica, dei computer e poi della Rete e dei Social, Rodotà affermava esser necessaria non solo una difesa per così dire tradizionale[34], ma anche una difesa "attiva ", sotto forma di

---

[32] Mantelero A., *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffré editore, p. 14.

[33] Gutwirth, De Hert, *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power,* Bepress, 2006.

[34] Forme tradizionali intendendo la mera difesa per così dire statica affidata ai tradizionali mezzi risarcitori ed ai provvedimenti d'urgenza di inibitoria (quando vi è rischio di reiterazione dell'illecito)

controllo della raccolta dei dati personali[35]. Il 7 dicembre 2000 a Nizza viene proclamata la Carta dei diritti dell'Unione europea, o "Carta di Nizza", dal Consiglio d'Europa, essendo parte del Trattato di Lisbona, è pienamente vincolante per le istituzioni europee e gli Stati membri. Con essa per la prima volta si è voluta elevare la protezione dei dati personali a diritto fondamentale. Nel preambolo si legge che l'Unione Europea pone la persona al centro della sua azione e i valori cui la Carta si ispira sono quelli della dignità e della libertà, dell'uguaglianza e della solidarietà. Rodotà ha definito la Carta dei diritti fondamentali dell'UE come il punto finale di un'evoluzione che ha portato ad una separazione della privacy e della protezione dei dati personali[36]. Il diritto della persona alla protezione dei dati di carattere personale che la riguardano è considerato, quindi, un "diritto fondamentale"e il trattamento dei dati personali viene configurato come al servizio dell'uomo. Si tratta di un diritto che nasce dapprima come riferimento etico riconnesso alla dignità della persona; in epoca moderna diventa diritto sancito giuridicamente e si trasforma da enunciazione di principio a diritto esigibile attraverso la disciplina prevista da norme giuridiche. Non si tratta solo del diritto alla riservatezza ma anche di tutela dei propri dati e di determinare quando, come, e in che misura, le informazioni personali possano essere comunicate ad altri. La Carta di Nizza, quindi, oltre a prevedere l'inviolabilità della dignità umana, della libertà, dell'uguaglianza e della solidarietà, sancisce anche il diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni, e il diritto di ogni persona alla protezione dei dati di carattere personale che la riguardano (art. 8). L'articolo 8 recita:

- *Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano*.
- *Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge.*
  Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
- *Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*

Nel momento in cui si è diffusa una gestione automatizzata dei dati, la maggior quantità di informazioni in circolazione ha posto in primo piano la questione della protezione dei dati personali, evolvendo ulteriormente l'ambito di riservatezza dell'individuo ed il concetto di privacy. Si tratta delle fondamenta da cui poi sono successivamente scaturiti ulteriori trattatati sulla protezione dei dati personali. L'articolo 8 è stato meglio definito in seguito alle sentenze della Corte europea dei diritti dell'uomo (Corte EDU), segue l'analisi di alcune tra le più importati.

---

[35] Sia consentito rinviare all'articolo di Magnani C., I nuovi diritti nella Carta dei diritti fondamentali dell'Unione Europea. URL: http://ojs.uniurb.it/index.php/studi-A/article/view/294

[36] Rodotà S., *Data Protection as a Fundamental Right in S. Guthwirth e altri, Reinventing Data Protection?*, Springer, 2009.

Sentenza della Corte EDU del 9 ottobre 2012 nel caso Alkaya contro Turchia.

In seguito ad un furto a casa di una nota attrice turca un quotidiano nazionale scrisse un articolo sull'effrazione nel quale riportava anche l'indirizzo esatto dell'abitazione. L'attrice chiese i danni al quotidiano, ma la richiesta non venne accolta dalla corte domestica. L'indirizzo di residenza di una persona è un'informazione prettamente personale e dunque viene tutelata dall'articolo 8 della CEDU. Dall'altra parte il quotidiano basava la sua difesa sull'articolo 10 della medesima Convenzione, cioè la garanzia della libertà di espressione. Si trattava di pubblicazione di informazioni personali in assenza di consenso. La Corte valutò che non vi erano ragioni di pubblico interesse per pubblicare l'indirizzo dell'attrice, sebbene costei fosse una "figura pubblica". Inoltre, pubblicare tale informazione poteva avere ripercussioni negative sulla sicurezza del soggetto, oltre che sulla sua vita privata.

Sentenza della Corte EDU del 3 aprile 2007 nel caso Copland contro il Regno Unito.

La sentenza Copland contro il Regno Unito specificò che la vita privata include non solo la privacy delle telefonate ma anche la riservatezza delle e- mail, e dell'uso di Internet. La signora Copland lavorava come assistente personale in un college scozzese. Per sei mesi le sue telefonate, la cronologia della sua navigazione web e le sue e-mail furono monitorate dall'università.L'università giustificò le sue azioni con due scuse: la prima riguardava la protezione dei diritti e delle libertà degli altri, assicurandosi che le strutture non fossero usate per scopi personali, e in secondo luogo l'università riteneva di poter esercitare un ragionevole controllo sulle sue strutture e di fare quanto necessario per provvedere a garantire un'istruzione di elevato livello. La Corte dichiarò che controllare le chiamate è un'azione protetta dall'articolo 8 della CEDU a prescindere che ciò avvenga sul luogo di lavoro. La Corte poi ritenne che la sorveglianza applicata a e-mail e internet doveva essere trattata allo stesso modo delle chiamate.
L'articolo 8 venne dunque espanso dalla sentenza a protezione della corrispondenza non solo domestica, ma anche sul luogo di lavoro.

Sentenza della Corte EDU del 25 febbraio 1997 nel caso Z. contro Finlandia

La protezione dei dati personali riguardanti la salute di un individuo viene analizzata nello specifico nella sentenza del caso Z. contro Finlandia. Il caso ha origine in seguito al fatto che una sentenza di una Corte d'appello finlandese rende pubbliche l'identità della moglie del condannato e la sua sieropositività. La pubblicazione di tali informazioni aveva violato il rispetto della vita privata e familiare della donna. La Corte aggiunse che il rispetto della confidenzialità dei dati personali sulla salute è un principio essenziale nei sistemi legali di tutti gli Stati parte della Convenzione.

Sentenza della Corte EDU del 2 dicembre 2008 nel caso K.U. contro Finlandia

In un caso più recente vengono messi in evidenza gli obblighi positivi nel contesto di Internet: la vicenda K.U. contro Finlandia. Nel 1999 un individuo sconosciuto pubblicò un'inserzione in un sito di dating utilizzando il nome e altre informazioni del ricorrente, che a quel tempo aveva 12 anni. Il padre di quest'ultimo dopo esser divenuto consapevole di ciò, chiese alla polizia di identificare la persona che aveva pubblicato l'annuncio a nome del figlio, tuttavia il provider di internet si rifiutò di rilasciare quelle informazioni alla polizia, in quanto si riteneva vincolato dalla confidenzialità delle telecomunicazioni secondo la legge finlandese. Il 19 gennaio 2001 anche la Corte distrettuale di Helsinki rifiutò la richiesta della polizia di obbligare il provider di internet a fornire l'identità dell'uomo che aveva pubblicato l'inserzione. Il caso venne poi preso in carico dalla Corte EDU il 27 giugno 2006. La Corte rilevò che l'azione di pubblicare un'inserzione a nome del ricorrente era stata un'azione criminale, che aveva reso il minore un obiettivo di pedofili. I minori e altri individui vulnerabili devono ricevere dallo Stato protezione contro interferenze nella loro vita privata.Secondo la Corte nel 1999 era già chiaro che la rete poteva essere usata per fini criminali e dunque il Governo finlandese aveva colpa di non aver messo in atto dei meccanismi di protezione. La normativa doveva essere in grado di soppesare da una parte la confidenzialità del servizio Internet e dall'altra l'importanza della prevenzione dei crimini e la protezione dei diritti e delle libertà degli individui. La Corte ritenne dunque che la Finlandia era venuta meno al suo dovere di proteggere la vita privata del ricorrente, poiché era stata data la precedenza alla confidenzialità rispetto al benessere psico-fisico della vittima. Vi era dunque stata una violazione dell'articolo 8.

Sentenza della Corte EDU del 26 marzo 1987 nel caso Leander contro Svezia.

Un'altra sentenza che è stata essenziale per lo sviluppo dell'articolo 8 della CEDU, fu quella del caso Leander contro Svezia del marzo 1987. Il caso riguardava un carpentiere svedese che desiderava lavorare in un museo adiacente ad un'area militare ad accesso ristretto. La sua applicazione per il posto di lavoro gli venne però rifiutata durante le procedure di selezione del personale sulla base di alcuni file segreti della polizia. Il ricorrente chiese di accedere ai file ma gli fu negato. La Corte ritenne che l'uso di file segreti della polizia e il susseguente rifiuto a consentire l'accesso a tali informazioni costituisse un'ingerenza nel diritto alla vita privata del soggetto e quindi una violazione dell'articolo 8. Il giudizio in questione è di particolare importanza perché viene dichiarato che anche la sola conservazione di dati personali costituisce una violazione dell'articolo 8, a prescindere da un possibile utilizzo o meno di tali dati. Nonostante la violazione dell'articolo 8, la Corte valutò infine che nel caso in questione tale violazione era giustificata da motivi di sicurezza nazionale.

Sentenza della Corte EDU del 13 novembre 2012 nel caso M.M. contro Regno Unito.

Infine un caso riguardante la conservazione di dati personali su registri criminali è quello di M.M. contro Regno Unito. Nel 2000 la ricorrente fu arrestata dopo essere scomparsa per un giorno con il nipote nel tentativo di evitare la sua partenza per l'Australia in seguito alla separazione avvenuta nel matrimonio del figlio. Le autorità decisero di non perseguire penalmente la donna ma di limitarsi ad una diffida che sarebbe dovuta rimanere nei registri per cinque anni, ma poiché la parte danneggiata era un minore fu estesa a tempo indefinito. Nel 2006 aveva ricevuto un'offerta di lavoro ma in seguito ad un controllo dei registri criminali tale offerta venne ritirata. La Corte EDU valutando il caso trovò una violazione dell'articolo 8. La conservazione dei dati ne permetteva l'accesso pubblico anche in un momento molto distante dall'evento, Come la diffida diventa un elemento del passato, allo stesso tempo diventa parte della vita privata di una persona che deve essere rispettata.

2.3 Dalla Direttiva 95/46/CE al nuovo Regolamento 679/16

Fondamentale è disciplinare le innumerevoli fattispecie giuridiche che trovano spazio sul web, individuando nuovi punti di equilibrio tra "sfruttamento" della rete e tutela di altri diritti, in particolare quelli di rango costituzionale afferenti la sfera civile, politica ed economica[37]. Questo ventennio rivela il ricorso a soluzioni non sempre uniformi e non ancora definitive. Il primo significativo documento, che tratta i diritti del web, risale al 1996, è la Comunicazione della Commissione europea sul contenuto nocivo su Internet (COM (96) 487 def.). La Commissione si dimostra consapevole che un "certo volume d'informazioni di contenuto potenzialmente nocivo ed illegale" si presta ad abusi finalizzati allo svolgimento di attività criminali[38]. I settori che potevano dimostrarsi più "sensibili" sono: sicurezza nazionale, tutela dei minori, tutela della dignità umana, sicurezza economica, sicurezza dell'informazione, tutela della sfera privata, tutela della reputazione personale, tutela della proprietà intellettuale. La Comunicazione, al fine di affrontare questi problemi, spinge verso la cooperazione tra gli Stati membri, favorendo la definizione di un quadro giuridico comune. Segue la Risoluzione del Consiglio e dei rappresentanti dei Governi e degli Stati membri, del 17 febbraio 1997. Con essa si invitano i singoli Stati ad agevolare processi di autoregolamentazione tra le associazioni dei fornitori di accesso alla rete, favorendo il coordinamento su scala europea. Con la decisione n. 276/99/CE del Parlamento Europeo e del Consiglio del 25 gennaio 1999, viene adottato il primo, tra i vari, piani pluriennali d'azione

[37] Mensi M., Falletta P., *Il Diritto del Web*, Cedam, 2015, p. 129 ss.

[38] Si pensi alle attività terroristiche, alla pornografia, all'incitamento all'odio razziale e alla discriminazione, alle frodi, o all'uso fraudolento delle carte di credito, alla distribuzione non autorizzata di opere soggette a diritto d'autore.

comunitari per promuovere l'uso sicuro di Internet, facendo leva su azioni di sensibilizzazione piuttosto che di reale controllo. Il fenomeno del web, però, era ancora circoscritto a piccole realtà territoriali e sociali. All'aumentare della dipendenza della società dalle reti di comunicazione, pubbliche o private, all'aumentare della quantità di dati trasmessi, aumentano i potenziali rischi, e si mostra quindi sempre più necessaria una cornice normativa adeguata.

Il 24 ottobre 1995, a Lussemburgo, veniva adottata la Direttiva 95/46/CE, essa si prestava ad essere il principale strumento giuridico dell'Unione europea in materia di protezione dei dati. L'esigenza di armonizzazione nasceva dalla frammentazione in materia tra i diversi paesi aderenti all'Unione, per cui si è reso necessario procedere ad un ravvicinamento delle normative nazionali che garantisse uniformemente un elevato grado di tutela. Nell'Art. 1 viene enunciato l'oggetto della direttiva: *"Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali"*. All'articolo 28 si prevede la formazione di un organismo di controllo indipendente per ciascuno Stato membro, che vigilasse a livello nazionale sulla protezione dei dati: questo portò alla nascita della autorità nazionali di protezione dei dati. Invece con all'articolo 29 veniva istituito il Gruppo di lavoro, formato da un rappresentante di ognuno di esse e da un rappresentante della commissione. I suoi compiti sono elencati all'articolo 30 e sono principalmente quello di: (a) esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della presente direttiva per contribuire alla loro applicazione omogenea; (b) formulare, ad uso della Commissione, un parere sul livello di tutela nella Comunità e nei paesi terzi; (c) consigliare la Commissione in merito a ogni progetto di modifica della presente direttiva, ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di dati personali; (d) formulare un parere sui codici di condotta elaborati a livello comunitario.

Nel 2001 venne formulato il Regolamento sulla protezione dei dati da parte nello specifico delle istituzioni comunitarie (regolamento 45/2001/CE). In particolare con questo Regolamento viene istituito il Garante europeo della protezione dei dati (GEDP), un'autorità di controllo che deve valutare l'applicazione di normative sulla protezione dei dati. Il Garante europeo della protezione dei dati (GEPD), autorità di sorveglianza indipendente istituita nel 2004, con sede a Bruxelles , è chiamato a cooperare con altre autorità garanti della protezione dei dati per promuovere un approccio coerente alla tutela dei dati in tutta l'Europa. Quasi tutti gli stati europei hanno così adottato apposite legislazioni per la tenuta e l'utilizzo dei dati. Per quanto concerne l'Italia bisogna però aspettare sino al 1996. Il 31 dicembre 1996 entra in vigore la legge n. 675, legge con cui viene istituita l'autorità amministrativa indipendente, il Garante per la protezione dei dati personali ,volta ad assicurare la tutela dei diritti e delle libertà

fondamentali e il rispetto della dignità nel trattamento dei dati personali. Con il decreto legislativo n. 196 del 30 giugno 2003, viene approvato il Codice in materia di protezione dei dati personali, meglio noto come Codice della privacy[39]. Nell'art. 26, comma 1 del decreto legislativo in questione si evince che "*I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti."* Il legislatore, che ha riconosciuto sin dai primi articoli del Codice il "diritto alla tutela dei dati personali", non si è limitato ad ordinare la materia ma ha dettagliatamente regolamentato il trattamento dei dati, egli ha, quindi, voluto raccogliere in un testo unico la maggior parte delle disposizioni inerenti alla privacy e al trattamento dei dati, recependo in tal modo la Direttiva 95/46/CE e quella sull'e-privacy[40]. Qualunque trattamento di dati personali deve avvenire nel rispetto dei diritti e delle libertà fondamentali dell'individuo. Con trattamento di dati personali si intente qualunque operazione o insieme di operazioni automatizzate o meno riguardanti raccolta, registrazione, conservazione, consultazione, elaborazione ed eventuale cancellazione e distruzione di dati è da intendersi come trattamenti. I dati, oggetto di tali situazioni, possono essere catalogati in *personali*, se comprendono qualunque informazione relativa a persone fisiche identificate o identificabili anche indirettamente mediante ricorso ad altro tipo di notizie, *sensibili* qualora rivelino l'origine razziale ed etnica, le convinzioni socio-politiche, religiose, filosofiche ecc. e infine *giudiziari* nel caso in cui diffondano informazioni in materia di casellario giudiziale e di anagrafe alle sanzioni amministrative dipendenti da reato. Il "diritto alla protezione dei dati personali" viene assicurato attraverso l'introduzione di precise regole di condotta a cui l'autore del trattamento deve attenersi, nonché mediante una procedimentalizzazione del trattamento medesimo al fine di assicurare in via preventiva la conformità della gestione dei dati al dettato normativo.

La Commissione europea ha, poi, voluto rendere ancora più omogenea la protezione dei dati personali di cittadini e residenti dell'Unione europea visti gli incessanti mutamenti dell'era digitale, con il regolamento generale sulla protezione dei dati, *"General Data Protection Regulation"*. Il testo del nuovo Regolamento è stato siglato il 27 aprile 2016 e pubblicato il 4 maggio 2016, in tutte le lingue ufficiali dell'Unione, sulla Gazzetta Ufficiale dell'Unione Europea. Come disposto dall'art. 99, esso è entrato in vigore il 25 maggio 2016, ma l'effettiva applicazione avverrà solo dal 25 maggio 2018, con l'abrogazione

---

[39] Il Codice della Privacy "garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali con particolare riferimento ma non esclusivamente al diritto di riservatezza, all'identità personale e alla protezione dei dati personali" (art. 2, d. lgs. n. 196/2003). Sulla definizione del diritto alla protezione dei dati personali si veda sul punto *La protezione dei dati personali e la tutela dell'identità*, in G. Finocchiaro – F. Delfini (a cura di), Diritto dell'informatica, Utet Torino, 2014, pp. 151 -152.

[40] La Direttiva 2002/58/CE, cosiddetta *e-privacy,* si applica al "trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazione" (art. 3 n. 1)

della Direttiva 95/64/CE. Il presupposti del Regolamento sono contenuti nei 173 considerando che precedono l'enunciazione dei 99 articoli . Non si tratta solo di una regolamentazione di carattere procedurale: il GDPR intende contribuire *"alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica"*, come pure *"al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche"*. Si tratta, cioè, dell'ambizioso obiettivo di coniugare la protezione dei dati dei cittadini con lo sviluppo economico e tecnologico, e in questo senso il Regolamento rappresenta probabilmente la più avanzata struttura normativa a livello internazionale. Nel nuovo "ordinamento europeo della privacy" si abrogano adempimenti formali, si rimodulano quelli di tutela sostanziale prescrivendo un nuovo modo di concepire la protezione dei dati personali in cui viene fortemente responsabilizzato il Titolare del trattamento. Si affida a ciascuno Stato membro il compito di prevedere e assicurare la protezione dei diritti e delle libertà con riferimento al trattamento dei dati personali.

Il confronto tra la prospettiva in cui si colloca la Direttiva e quella che caratterizza il nuovo Regolamento consente un'analisi tra finalità, caratteristiche e differenze tra questa nuova normativa e la precedente. La scelta di sostituire un sistema basato su una Direttiva di armonizzazione con uno incentrato ora su un Regolamento direttamente applicabile trova il suo perché, prima di tutto nelle trasformazioni socio-economiche dei due decenni che ci separano dall'adozione della Direttiva 95/46, poi per il ruolo sempre più importante che assume la protezione dei dati. Con la Direttiva 95/46 si affermava "i sistemi di trattamento dei dati sono al servizio dell'uomo" e, di conseguenza, "debbono rispettare le libertà e i diritti fondamentali dello stesso, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui". Il nuovo Regolamento, pur operando in un contesto nel quale ormai la protezione dei dati personali è riconosciuta dalla Carta dei diritti fondamentali dell'Unione Europea come diritto fondamentale della persona, pone in relazione il rispetto di questo diritto con la sua funzione sociale e con la necessità di contemperarlo con altri diritti di pari grado, in ossequio al principio di proporzionalità. Tre disposizioni del nuovo testo, nello specifico, possono considerarsi come simboliche di questa nuova impostazione. Il paragrafo 1 dell'art. 24 obbliga al titolare del trattamento di assicurare tutte le misure organizzative e tecniche "adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato in conformità al Regolamento". L'art. 33 disciplina la notifica di violazione dei dati personali: "in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55", ove la notifica "non sia effettuata entro 72 ore, essa deve essere correlata dai motivi del ritardo". Il diritto dell'interessato, a conoscere le violazioni dei propri dati personali, è, quindi, in subordine, rispetto alla comunicazione all'Autorità. Il successivo art. 34 specifica che la notificazione della violazione

all'interessato è obbligatoria solo "quando la violazione è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche" ovvero quando lo richieda l'Autorità. La violazione dei dati che comporti rischi per i diritti e le libertà delle persone fisiche deve in ogni caso essere denunciata all'Autorità che esercita la funzione di controllo. La violazione va, invece, notificata all'interessato solo se il rischio è "elevato". È richiesta di fatto una valutazione case by case del grado di rischio. Oltre a quanto già detto, i legami tra la Direttiva 95/64/CE e il nuovo Regolamento sono numerosi. La decisione di adottare un nuovo strumento normativo nella forma del Regolamento immediatamente applicabile in tutti gli Stati membri, in sostituzione alla Direttiva 95/64/CE, trova la sua radice nel fatto che, nel corso del tempo, questa si è dimostrata sempre meno idonea a garantire l'uniformità di applicazione che invece la rapidità dell'evoluzione tecnologica e la globalizzazione richiedono. L'art. 99 del Regolamento dichiara esplicitamente che esso sarà applicato solo a decorrere dal 25 maggio 2018, è quindi ad "applicazione differita". È chiaro che la regolazione e la legislazione europea e nazionale incompatibili con il Regolamento devono essere adeguate ad esso, salvo che i settori regolati siano oggetto di esplicita riserva di competenza a favore degli Stati. Spetta alla Commissione assumere le iniziative necessarie alla piena armonizzazione con il nuovo Regolamento, in tutti quei casi in cui non vengano richieste di per sé modifiche ma solo forme di armonizzazione. L'art. 97 precisa che la Commissione, entro il 25 maggio 2020, e successivamente ogni quattro anni, deve presentare una relazione di valutazione, eventualmente orientata anche al riesame, del Regolamento e dei suoi effetti, "tenuto conto in particolare dello sviluppo delle tecnologie dell'informazione e dei progressi della società dell'informazione". L'obiettivo dichiarato del Regolamento è quello di assicurare un'applicazione coerente e omogenea e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. Si tratta quindi di un apparato di disposizioni che , data la natura regolamentare, si applica direttamente in tutta l'Unione, ma affida allo stesso tempo, un ruolo rilevante alle Autorità di controllo e al Comitato europeo di protezione dati. Inoltre si dedica un intero Capo, il VII, alla normativa di "cooperazione e coerenza", che contiene le disposizioni relative alla cooperazione tra le Autorità e quelle che concernono i meccanismi di coerenza e di assistenza reciproca. L'obiettivo è uniformare ed armonizzare questa disciplina all'interno dell'Unione Europea, eliminando numerose asimmetrie e "barriere" che si erano create nel corso del tempo con normative nazionali frammentarie e diverse tra loro, le quali ostacolavano la libera circolazione dei dati tra una nazione e l'altra.

Con l'emanazione del decreto legislativo 101/18 è finalmente avvenuto l'adeguamento al nostro ordinamento, con l'abrogazione del precedente decreto legislativo 196/2003, noto come Codice della Privacy. Ci si lascia alle spalle un Codice "basato su una direttiva europea di oltre vent'anni fa e scritta per un'epoca in cui la maggioranza delle persone si scambiava ancora la corrispondenza con fax e

francobolli, con il Regolamento UE 2016/679 veniamo invece catapultati in una nuova dimensione che potremmo definire una "Privacy 2.0", pensata per gli scenari più complessi dell'Internet of Things e dei Big Data", questa è la descrizione di Nicola Bernardi, presidente di Federprivacy. Il decreto legislativo del 10 agosto 2018 è stato pubblicato nella Gazzetta Ufficiale dello scorso 4 settembre e, con esso, la normativa nazionale in materia di privacy si è adeguata alle disposizioni del Gdpr. Quanto in esso previsto entra in vigore dal 19 settembre 2018. Non vi è dubbio che gli adeguamenti e la normativa interna erano necessari. Il decreto andrà a prevedere e adeguare la normativa nazionale soprattutto in settori dove il trattamento dei dati personali è complesso, delicato. Da una prima analisi si evidenziano le principali novità previste. Innanzitutto, il decreto contiene delle importanti precisazioni circa le conseguenze dell'omesso rispetto della disciplina in materia di privacy, dedicando delle apposite previsioni alle sanzioni amministrative e a quelle penali. Per quanto riguarda quest'ultime, il provvedimento ha recuperato alcune fattispecie penali, allontanandosi dall'alleggerimento sanzionatorio. Rientrano, ad esempio, i reati di trattamento illecito di dati personali, di acquisizione fraudolenta e di false dichiarazioni rese al Garante. Riguardo invece le sanzioni amministrative: le imprese che violano gli obblighi privacy specificati dal decreto rischiano di essere assoggettate a sanzioni amministrative che vanno da 10milioni a 20milioni di euro o che sono ricomprese tra il 2% e il 4% del fatturato mondiale annuo. Il compito di applicare le sanzioni, dietro apposito reclamo o su autonoma iniziativa, è del Garante della privacy. Dopo aver ricevuto il provvedimento sanzionatorio, all'impresa sono concessi 30 giorni di tempo per inviare le proprie difese. Dovranno essere adottate misure adeguate di sicurezza, come tecniche di cifratura e di pseudonomizzazione a tutela del dato personale, misure di minimizzazione e le specifiche modalità per l'accesso selettivo ai dati. Il decreto va a toccare, poi, il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione, si dichiara che esso deve essere validamente espresso in prima persona dal soggetto che ha compiuto quattordici anni. Chi ha un'età inferiore necessita del consenso di chi esercita la sua responsabilità genitoriale. Il testo del nuovo provvedimento prende in particolare considerazione le esigenze di semplificazione delle micro, piccole e medie imprese, affidando al Garante per la protezione dei dati personali il compito di promuovere delle modalità semplificate di adempimento degli obblighi di trattamento. Merita infine di essere menzionata la norma che si occupa dei diritti delle persone decedute. Si stabilisce che i diritti in materia di privacy dettati dal *Gdpr* e riferiti ai dati personali di soggetti deceduti possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato in qualità di suo mandatario o per ragioni familiari meritevoli di protezione. Ciò tranne che nei casi previsti dalla legge.

2.4 La trasferibilità dei dati

Il profilo del trattamento dei dati personali e della tutela della *privacy* ha assunto una rilevanza tale che diversi sono stati negli ultimi tempi gli interventi legislativi a livello internazionale. Già con la Direttiva 95/46/CE si era andato a creare uno standard europeo della protezione dei dati personali. "Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva."

Per l'intensità degli scambi commerciali, si rilevò da subito necessario un accordo tra Europa e Stati Uniti. Il sistema statunitense sulla protezione dei dati era sviluppato in modo molto diverso da quello europeo, non garantiva la sicurezza dei dati personali secondo gli standard comunitari. Un primo tentativo di essere definito "approdo sicuro" per i dati dei cittadini europei si ebbe nel 2000 con l'accordo "Safe Harbour". Quest'ultimo ha consentito per più di 10 anni il trasferimento di dati personali dall'Europa ad aziende e organizzazioni americane. Sarà la battaglia contro Facebook di uno studente austriaco, Max Schrems, al fine di proteggere i propri dati personali a portare questo accordo alla decadenza. Nel 2011, Schrems aveva richiesto a Facebook di ricevere i propri dati personali conservati sui server americani di Facebook, all'epoca infatti i dati personali degli utenti europei venivano trasferiti dalla filiale irlandese di Facebook (sede europea) ai server situati sul suolo americano. Il diritto e la prassi americana non offrivano una sicurezza adeguata contro la sorveglianza svolta da autorità pubbliche. Facebook trattava ancora ogni dato a partire dall'iscrizione dell'utente, anche quelli cancellati da quest'ultimo. Preso atto della scarsa tutela della privacy garantita da Facebook, Schrems denunciò varie volte quest'ultimo al *Data Protection Commissioner*, l'Autorità garante della privacy irlandese, facendo richiesta di un blocco al trasferimento dei dati dalla filiale irlandese ai server americani. Nel 2012 l'Autorità irlandese predispone delle raccomandazioni a Facebook sull'adeguarsi alla normativa europea e garantire la cancellazione definitiva dei dati qualora richiesto. In seguito alle rivelazioni del 2013 di Edward Snowden[41], informatico e attivista statunitense, sulla sorveglianza di massa effettuata dalle agenzie di intelligence americane a scapito di tutti i dati presenti sul suolo americano, senza distinzione di provenienza, Schrems

[41] Ex tecnico della CIA e fino al 2013 collaboratore della Booz Allen Hamilton (azienda di tecnologia informatica consulente della NSA, la National Security Agency), è noto per aver rivelato pubblicamente dettagli di diversi programmi di sorveglianza di massa del governo statunitense e britannico, fino ad allora tenuti segreti. Attraverso la collaborazione con Glenn Greenwald, giornalista de The Guardian che ha pubblicato una serie di denunce sulla base di sue rivelazioni avvenute nel giugno 2013, Snowden ha rivelato diverse informazioni su programmi di intelligence secretati, tra cui il programma di intercettazione telefonica tra Stati Uniti e Unione europea riguardante i metadati delle comunicazioni, il PRISM, Tempora e programmi di sorveglianza Internet.

fece ricorso alla High Court of Ireland[42] (Alta Corte di giustizia irlandese). Quest'ultima per poter valutare la questione si rivolse a sua volta, mediante rinvio pregiudiziale, alla Corte di Giustizia Europea. La Corte nella sua sentenza del 6 ottobre 2015 reputò che l'esistenza di una decisione della Commissione che dichiara che un paese terzo garantisce un livello di protezione adeguato dei dati personali trasferiti (accordo "Safe Harbour") non può ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza della Carta dei diritti fondamentali dell'Unione europea e della Direttiva 95/46. Quest'ultima dà alle autorità nazionali i poteri di valutare se il trasferimento dei dati di una persona verso un paese terzo rispetta i requisiti comunitari sulla protezione dei dati, anche qualora vi sia una decisione della Commissione che dichiara adeguato il livello di sicurezza di quel paese. La Corte rilevò che il regime di approdo sicuro è applicabile alle imprese americane ma non alle autorità pubbliche, che non sono tenute alla sua osservanza. Si sottolineava come una normativa, quale quella statunitense, che consentisse alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche dovesse essere considerata lesiva del contenuto essenziale del diritto fondamentale al rispetto della vita privata. L'accordo, infatti, risultava applicabile soltanto alle imprese americane che vi avevano aderito, non anche alle autorità pubbliche degli Stati Uniti, con un evidente pericolo di ingerenza da parte loro nei diritti fondamentali delle persone. Inoltre, esigenze di sicurezza nazionale, di pubblico interesse e la stessa applicazione di principi normativi dell'ordinamento degli Stati Uniti d'America sarebbero prevalsi sullo Schema *Safe Harbor*; di conseguenza le organizzazioni con sede negli USA sarebbero state obbligate, senza limitazione alcuna, a disapplicare i principi di tale schema cui pure avevano aderito, in caso di conflitto con le superiori esigenze pubbliche appena descritte. La Corte giunge, così, a invalidare la decisione della Commissione del 26 luglio 2000. Il 21 gennaio 2016, Antonello Soro, Presidente del Garante privacy, parlava di possibili "pesanti conseguenze dal punto di vista economico"[43] nel caso in cui non si fosse giunti rapidamente ad un nuovo accordo che riformulasse il regime di approdo sicuro. Di lì a breve si giungerà a una forma rivisitata dell'accordo precedente, anche se permanevano forti dubbi relativi al gap tra il trattamento dei dati personali raccolti nell'Unione europea e quella che sarebbe stata la loro sorte, una volta trasferiti negli Stati Uniti.

Il 2 febbraio 2016, , la Commissione Europea e il governo degli Stati Uniti d'America raggiungono un accordo politico su un nuovo regime giuridico per gli scambi transatlantici di dati personali, per fini commerciali. Il cosiddetto scudo UE-USA del Privacy Schield per la protezione della privacy avrebbe recepito le indicazioni della sentenza del 6 ottobre 2015, con cui la Corte di Giustizia

---

[42] Sentenza Schrems vs Data Protection Commissioner della High Court of Ireland del 18 Giugno 2014

[43] Lettera del Presidente del Garante privacy, Antonello Soro, al Presidente del Consiglio dei Ministri, Matteo Renzi del 21 gennaio 2016

dell'Unione Europea ha invalidato il vecchio regime dell'accordo Safe Harbor. I punti più significativi del nuovo accordo si possono sintetizzare in tre punti: il primo è relativo agli obblighi sul trattamento dei dati e vuole che le aziende statunitensi che desiderano importare i dati personali dall'Europa dovranno impegnarsi nel mantenimento di solidi obblighi sul trattamento dei dati e sulla garanzia dei diritti individuali. Il secondo riguarda la sorveglianza di massa e richiede che l'accesso delle autorità pubbliche per questioni di ordine e sicurezza nazionale sia sottoposto a chiare limitazioni, garanzie e meccanismi di controllo. Queste eccezioni dovranno essere utilizzate solo nella misura necessaria e in maniera proporzionata, evitare ogni tipo di sorveglianza di massa dei dati personali trasferiti negli Stati Uniti. Per monitorare regolarmente il funzionamento del nuovo regime ci sarà una revisione congiunta annuale, che comprenderà anche la questione dell'accesso sicurezza nazionale. Il terzo attiene al diritto di ricorso e alla previsione del difensore civico. Viene riconosciuto ai cittadini Ue la possibilità di denunciare gli abusi, qualora dovessero ritenere che la riservatezza dei loro dati sia stata violata e le aziende avranno precise scadenze per rispondere alle accuse. Sul piano europeo, il Capo V del Regolamento 2016/679/ UE, confermando l'approccio già vigente in base alla direttiva 95/46, è intervenuto a fare chiarezza, esso disciplina i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali. Specificamente, l'articolo 44 enuncia un principio generale per il trasferimento: qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere tali dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni stabilite dal Regolamento. Il fine ultimo è quello di assicurare che il livello di protezione delle persone fisiche garantito dal Regolamento non sia pregiudicato. L'adeguatezza viene valutata sulla base di una serie di parametri tra i quali lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale; l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale; gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni. L'art. 49 elenca una serie di deroghe, quindi il trasferimento verso un paese terzo che non garantisce una tutela adeguata può avvenire se:

a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate; b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato; c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato; d) il trasferimento sia necessario per importanti motivi di interesse pubblico; e) il

trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria; f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri. Le deroghe molto spesso però rischiano di trasformare l'adeguatezza in approssimazione. La principale problematicità che emerge dall'analisi del trasferimento dei dati riguarda proprio la valutazione dell'adeguatezza. L'adeguatezza rispetto all'equivalenza può prevedere garanzie inferiori ma sufficienti. Inoltre, «le clausole contrattuali modello» rischiano di minimizzare la tutela dei dati per ridurla a un livello meno che sufficiente. Questi modelli sarebbero destinati a diventare lo strumento che traghetterà i Big Data al di fuori dell'Europa con un livello di garanzia più basso rispetto a quello del Paese di provenienza. Ci si chiede se ammettere un trasferimento dei dati a un paese terzo, qualora esso assicuri garanzie adeguate, significhi proteggere efficacemente la riservatezza dei cittadini europei.

2.5 La nuova sicurezza dei dati, fino al DPO

Con il Regolamento 679/2016 il legislatore europeo opta decisamente per un innalzamento, qualitativo e quantitativo, delle soglie di tutela, scegliendo uno strumento di unificazione (e non più di armonizzazione) e ponendolo nel quadro di più generale rinnovamento normativo[44]: accanto al Regolamento "*General Data Protection*", possono infatti considerarsi il Regolamento 910/2014 cd. e.IDAS (*Electonic Identification, Authentication, signature*) e la Direttiva 2016/680/UE relativa al "trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati". Il cd. "pacchetto protezione dati", nelle intenzioni del legislatore europeo, rappresenta dunque una priorità, anche e soprattutto in considerazione delle più recenti pronunce della Corte di Giustizia Europea che, dal caso Digital Ireland fino al cd. Caso Schrems e passando per la storica sentenza Costeja,

[44] Mariottini I., *Il pacchetto di riforma della Commissione europea in materia di protezione dei dati personali*, in Riv. dir. int. priv. proc., 2016, p. 905 ss.; Fumagalli Meraviglia M., Le nuove normative europee sulla protezione dei dati personali, in Diritto comunitario e degli scambi internazionali, 2016, p. 1 ss.

nota come caso Google Spain[45], avevano evidenziato la necessità di una serie di innovazioni, rispetto all'impianto classico della tutela dei dati, come emergente dalla normativa di derivazione dalla Direttiva 95/46/Ce. Il nuovo approccio si basa, nelle sue linee generali, su una più dinamica considerazione dei flussi di dati, sul principio di *accountability* (termine utilizzato nel linguaggio economico che presenta qualche difficoltà di traduzione nel lessico delle nostre categorie giuridiche, tanto da indurre alcuni dei primi commentatori a preferire il termine anglosassone proprio per mantenere le caratteristiche delle situazioni incombenti sul titolare e sul responsabile del trattamento), nonché sulla valutazione dei rischi che possono derivare dalle attività di trattamento, con un decisivo passaggio all'approccio precauzionale.
Ma l'innovazione riguarda anche i profili soggettivi ed oggettivi delle attività di trattamento dei dati: lasciando da parte i primi, con la considerazione delle figure del co-titolare e del *Data Protection Officer*[46].

L'introduzione della figura del responsabile della protezione dati, DPO, è una delle più rilevanti novità del Regolamento; la nuova figura professionale, che non deve confondersi con il responsabile del trattamento, risulta finalizzata, in linea con il principio di accountability, a rafforzare la tutela e la sorveglianza nelle operazioni di trattamento dei dati, ponendosi come figura apicale e di interfaccia tra i soggetti a diverso titolo coinvolti nelle stesse attività di trattamento. Gli artt. 37-39 del Regolamento che disciplinano le ipotesi di obbligatorietà della nomina (art. 37), la posizione ed i rapporti con i titolare (art. 38) ed i compiti e le funzioni (art. 39). Nel delineare i tratti caratterizzanti della nuova figura professionale, che risulta obbligatoria per le autorità pubbliche e gli organismi pubblici e per le società private che trattino notevoli moli di dati o che effettuino trattamenti su particolari categorie di dati (quali quelli contemplati all'art. 9), il Regolamento risulta, già ad una prima lettura, rifarsi alla normativa tedesca del 2003 in tema di protezione dei dati *(Bundesdatenschutzgesetz)* che aveva già introdotto e reso obbligatoria la figura del *datenschutzbeauftrager* (DSB), in tutte le ipotesi di trattamento di dati sensibili

---

45 Nel 2010 il sig. Mario Costeja González, cittadino spagnolo, ha presentato all'Agencia española de protección de datos (Agenzia spagnola di protezione dei dati, Aepd) un reclamo contro un editore largamente diffuso in Spagna, nonché contro Google Spain e Google Inc. Il sig. Costeja González faceva valere che, allorché il proprio nome veniva introdotto nel motore di ricerca del gruppo Google («Google Search»), l'elenco di risultati mostrava dei link verso due pagine del quotidiano datate gennaio e marzo 1998. Tali pagine facevano riferimento ad accadimenti che il soggetto non voleva fossero ricordati. Il gestore di un motore di ricerca su Internet fu dichiarato responsabile del trattamento da esso effettuato dei dati personali che appaiono su pagine web pubblicate da terzi. Così dice la sentenza della Corte Ue numero 131/12, definendo il cosiddetto "diritto all'oblio".

46 D'Antonio V., Sica S., Riccio G. M., *La nuova disciplina europea della privacy*, Cedam, 2016; Lambert P., *The Data Protection Officer: profession, rules and role*, CRC Press Boca Raton, 2017; Bernardi N., Perego M., *Privacy Officer. La figura chiave della data protection europea*, Ipsoa, 2017.

o di attività che implichi trattamento svolta da un numero minimo di dipendenti. A detta dei primi commentatori, però, sembra che questo possa determinare una generale indeterminatezza nella specificazione dei compiti del DPO, con possibile aumento dei costi transattivi, a fronte di altre esperienze normative europee, ad esempio quella spagnola.

2.6 Il consenso

Il nuovo Regolamento dà sicuramente un notevole apporto[47] alla disciplina dei nuovi fenomeni che hanno preso piede in Rete: è stato ampliato l'elenco delle definizioni in materia di protezione dei dati personali dell'art. 2 della previgente dir. 95/46/CE, oggi divenuto l'articolo 4 del Regolamento UE. Risultano aggiunte descrizioni più calzanti al contesto tecnologico, quali quella di profilazione, dati genetici, dati biometrici e così via. Tra le principali novità introdotte vi è il diritto a richiedere la cancellazione dei dati: il cosiddetto *Right to be forgotten* (articolo 17 del nuovo Regolamento). È cambiata altresì la definizione di «consenso dell'interessato» che l'articolo 6 configura come caposaldo di liceità di un trattamento dei dati personali. Il trattamento deve trovare radicamento in un'idonea base giuridica e in una serie di fondamenti che, in linea di massima coincidono con quelli previsti dal Codice Privacy, ossia oltre al consenso, l'adempimento degli obblighi contrattuali, gli interessi vitali della persona interessata o di terzi, gli obblighi di legge cui è soggetto il titolare, l'interesse pubblico o l'esercizio di pubblici poteri e l'interesse legittimo prevalente del titolare o dei terzi cui i dati vengono comunicati. L'articolo 4, al n. 11) definisce il consenso come «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento». Il chiarimento è teso a cancellare ogni dubbio relativo all'*opt in*[48] che richiederebbe sempre un consenso espresso preventivo al trattamento da parte dell'interessato. Resta da definire il significato di ciascuno dei requisiti richiesti per il rilascio di un consenso valido: 1) il primo requisito attiene alla libertà: il consenso può essere valido soltanto se l'interessato è in grado di operare realmente una scelta, e non c'è il rischio di raggiri, intimidazioni, coercizioni o conseguenze negative significative nel caso in cui questa persona non manifesti il proprio consenso. 2) Il secondo riguarda la specificità del consenso: «il consenso "specifico" deve riferirsi a una situazione ben definita e concreta in cui si prevede un trattamento dei dati. Pertanto un

---

[47] Tra le principali novità il nuovo pacchetto di protezione dei dati introduce il principio di «responsabilizzazione»: il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità, ma è compito dello stesso titolare. Cfr. con l'articolo 4, paragrafo 1, n. 8) e con l'intero Capo IV del Regolamento.

[48] Nell'ambiente online è il consenso esplicito manifestato con la firma elettronica o digitale o con un click di conferma su un'icona.

“consenso generale” dell’interessato non costituisce un consenso conformemente all’articolo 4 del Regolamento. 3) Il terzo requisito riguarda la necessaria informazione, la richiesta di consenso deve essere presentata in forma comprensibile, utilizzando un linguaggio semplice e chiaro. 4) Il consenso dovrebbe, inoltre, applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere dato per l’insieme delle finalità del trattamento. 5) Infine, il consenso deve definirsi come inequivocabile, deve essere «fondato su dichiarazioni o azioni intese a esprimere un consenso valido» e sembrerebbe implicare la necessità di un’azione positiva. Dunque il comportamento dell’interessato non dovrebbe lasciare adito a dubbi in merito alla sua intenzione di manifestare il suo consenso.

Il nuovo Regolamento Europeo presuppone quindi che il consenso non costituisca mai la scelta di default, ma debba essere sempre espresso. Non dovrebbe pertanto configurare consenso il silenzio, l’inattività o la preselezione di caselle. Ovviamente il consenso rilasciato per il trattamento dei dati personali differisce da quello rilasciato per il trattamento dei dati sensibili. «Meritano una specifica protezione i dati personali che, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali». Dunque quelle informative veloci che chiedono i dati personali come corrispettivo del servizio che offrono per finalità generiche e disomogenee, ma soprattutto che non fanno luce sul fatto che l’aggregazione dei dati mette in chiaro i dati «più che sensibili» della persona, sembrerebbero contrastare nettamente con le previsioni regolamentari sopra descritte.

Un consenso che diventa una «cessione di dati» e quindi trasferimento di informazioni riservate, le più intime degli utenti, non può dirsi valido tantomeno compatibile con le disposizioni del Regolamento UE, che comunque non riesce a stare al passo con le tecnologie, perché omette di regolare fattispecie ormai consolidate sulla Rete. I Big Data: quelle informazioni che quotidianamente sono raccolte e incrociate diventano nella società dell’informazione dati ipersensibili che incidono sull’esplicarsi delle libertà degli utenti al punto che esse stesse costituiscono il nucleo di quelle libertà fondamentali indisponibili.

Capitolo 3

Scambio implicito del dato

3.1 I Big Data tra sfruttamento economico e vocazione democratica

Pochi giorni fa Google ha inviato a ogni suo utente un “promemoria sulla privacy”. Il motore di ricerca ricorda quali siano i dati elaborati. Ad esempio, quando viene effettuata una ricerca di un ristorante su Google Maps o si guarda un video su YouTube, vengono elaborate le informazioni relative a quella attività, che possono includere il video visualizzato, gli ID del dispositivo, gli indirizzi IP, i dati dei cookie e la posizione. Viene aggiunto anche il perché questi dati vengano analizzati. Tra i motivi: aiutare i servizi a offrire contenuti più utili e personalizzati, come risultati di ricerca più pertinenti; mostrare annunci basati su specifici interessi, quindi migliorare la qualità dei servizi, in ultimo aumentare la sicurezza proteggendo da attività fraudolenta e illeciti. I dati dei nostri servizi e di diversi dispositivi vengono combinati tra loro per tali finalità. Infine, Google ricorda "Se accedi al tuo account prima di accettare, Google ricorderà la tua scelta per tutti i browser e i dispositivi su cui hai eseguito l’accesso". Quando utilizziamo i servizi di Google, Facebook o simili «accettiamo» di essere monitorati, in questo modo i grandi colossi di Internet utilizzano i nostri profili per fare business, e non solo.

L’utilizzo delle tecnologie informatiche ha rivoluzionato la vita quotidiana dei consumatori da ogni possibile punto di vista. Ne è risultato un mercato dei servizi e dei contenuti digitali profondamente ristrutturato in cui sono mutati il «tipo» di operatore economico, il terreno di gioco e la fonte del profitto, nonché le logiche di mercato e i paradigmi della disciplina antitrust. In questa «prateria dai confini senza limiti» della Rete di Internet, si sono affermati pochi big Player. Secondo la definizione dell’OCSE[49], con il termine *Big Data* si includono tutti quei contenuti che permettono l’identificazione di un individuo (*data subject*): i contenuti generati dagli utenti, inclusi *blog*, foto, video; dati comportamentali, incluso quello che le persone cercano in rete, e guardano su Internet, cosa comprano *online*, quanto spendono e come pagano; i dati sociali, inclusi i contatti degli amici sui *social network*; dati di geolocalizzazione, inclusi l’indirizzo di residenza, il segnale gps, l’indirizzo ip; i dati demografici, inclusi l’età, il genere sessuale, l’orientamento sessuale, le affiliazioni politiche; i dati identificativi ufficiali quali nome, informazioni finanziarie, numero di conto, informazioni sulla salute e così via. L’aggregazione di informazioni e l’accessibilità ai Big Data da parte di pochi, ottenuti attraverso forme non negoziate di profilazione degli utenti, impattano inevitabilmente sull’ecosistema digitale, modificandone assetti ed

[49] OCSE, Exploring the economics ofpersonal data: a Survey ofMethodologies for Mesauring Monetary Value, URL: http://www.oecd- ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en,

equilibri. Chi possiede i dati possiede conoscenza e quindi denaro. La raccolta delle informazioni e la loro gestione giocano un ruolo decisivo per le imprese, al punto che i dati personali sono divenuti asset strategico, attraverso forme di profilazione e definizione di algoritmi possono incidere sul mantenimento della net neutrality[50]. I dati, o meglio le decisioni legate ai dati, non hanno valore senza il calcolo automatizzato, basato su logiche algoritmiche, cioè senza software in grado di estrapolare, gestire e processare le informazioni ivi racchiuse entro un tempo ragionevole. I processi decisionali Big Data driven aumentano la produttività delle imprese poiché gli strumenti di advanced analytics - come i sistemi di machine learning e di text mining, analisi semantica e reti neurali, nonché ricercatori specializzati - producono profitto. Le informazioni vengono utilizzate principalmente per scopi commerciali: il data mining consente di perfezionare il commercio virtuale, ridurre a zero gli errori e le spese inutili, fidelizzare i clienti, personalizzando i singoli prodotti e tenendo traccia del loro comportamento. Il Rapporto Mc Kinsey[51] ha analizzato anche quelli che sono i vantaggi economici derivanti dall'impiego dei dati, gli analisti hanno studiato una serie di esempi in cui essi si sono mostrati in grado di «creare valore nelle organizzazioni pubbliche e private, nei mercati e nei prodotti e servizi in sette settori dell'economia mondiale: istruzione, trasporti, prodotti di consumo, energia elettrica, gas e petrolio, assistenza sanitaria, credito al consumo». Per comprendere il flusso di benefici, non solo economici, innescato dall'utilizzo dei dati, basti pensare che se sono note le preferenze delle persone, attraverso quello che loro dichiarano sui social network, per esempio, è possibile comprendere al meglio i loro bisogni e possono essere progettati servizi migliori, più efficienti.

Queste enormi quantità di dati diventano carburante dell'economia dell'informazione garantendo «una pluralità di fonti di informazione, libero accesso alle medesime, assenza di ingiustificati ostacoli legali, anche temporanei alla circolazione delle notizie e delle idee» . I dati, allora, si fanno strumento democratico perché i diritti fondamentali e le libertà costituzionali che essi consentono di esercitare in forma più piena, rispetto al passato, hanno un radicamento popolare: «si riferiscono al "popolo" nella totalità dei suoi componenti. In questo senso i Big Data diventano il nuovo nocciolo duro delle libertà fondamentali, ma si tratta sempre di un nucleo bifronte: da un lato la loro conoscenza è precondizione per l'esercizio delle libertà fondamentali, perché l'accesso ai dati è strumentale all'esercizio delle libertà; dall'altro i Big Data rappresentano l'intimità più profonda della persona, in grado di rivelare informazioni sull'individuo riservate, che in quanto tali dovrebbero essere protette, anonimizzate e minimizzate in modo che la persona cui si riferiscono non sia identificabile.

---

[50] La neutralità della rete, nota anche con i termini inglesi network neutrality, net neutrality, internet neutrality o NN.

[51] I benefici sono stati misurati dal Rapporto Mc Kinsey . L'impiego dei dati consente di migliorare l'istruzione scolastica, innalzando le competenze dei lavoratori e la produttività, quindi aumentando anche i salari e innescando un circolo virtuoso.

Le informazioni hanno guidato, in forma poco ortodossa, la campagna elettorale di Trump, direzionando al pubblico messaggi elettorali diversi (*microtargeting*), personalizzati per il singolo elettore[52]. Questi strumenti di analisi sono in grado di capovolgere i risultati elettorali, in danno della sana competizione democratica, alterando gli strumenti propri della sovranità popolare. Alexander Nix, responsabile della campagna di Trump, ha spiegato che «se vogliamo fare breccia su un'elettrice coscienziosa e nevrotica, converrà mostrargli l'immagine di una rapina in casa, con tanto di mano minacciosa che spacca il vetro e lo slogan "oltre che un diritto, una pistola è un'assicurazione sulla vita" […]; se invece il bersaglio è un tipo tradizionalista, ma ben disposto verso il prossimo, funzionerà meglio la foto di nonno e nipote a caccia, con un *claim* tipo "dal padre al figlio, sin dalla nascita della nostra nazione"». Similarmente: «a un pubblico di madri, sia casalinghe che in carriera, di età inferiore ai 55 anni, parlavamo di misure di supporto alle famiglie sostenuto da Donald e Ivanka Trump. A un pubblico di maschi disoccupati provenienti da zone con alto tasso di crisi e fenomeni di decentramento industriale, tipo Wisconsin e Michigan, il messaggio sarebbe ruotato intorno a misure di creazione di nuovi lavori e tassazione sulle società americane che esportano lavori all'estero». I dati consentono di «targetizzare» gli utenti per fini pubblicitari, ma anche di ottimizzare prodotti e servizi, monetizzando i dati. Le imprese che hanno un vantaggio competitivo nelle cosiddette 4 V dei Big Data (Volume, Velocità, Varietà e Valore) non sono solo nella condizione di dominare i loro stessi settori, ma anche di estendere la dominanza ad altri e abusarne. Appare evidente che una Rete ubiqua si presta da un lato a potenziali violazioni della riservatezza delle comunicazioni e dall'altra alla concentrazione del potere in capo a pochi operatori privati. Ad oggi diventa sempre più complesso, da un lato, capire fin dove si spinge la ragionevole aspettativa di privacy, dall'altro frenare il trasferimento indiscriminato dei dati, oggi divenuti, come anticipato, nocciolo duro di diritti fondamentali inalienabili.

[52] Sul punto, cfr. *Così, con i social network, abbiamo fatto vincere Donald Trump*, in La Repubblica, 2017; Booth R., *Inquiry launched into targeting of UK voters through social media*, in the Guardian, 2017.

3.2 La consapevolezza del “prezzo”

Per accedere al mondo dell’online l’utente è chiamato a pagare un prezzo. Ci si chiede sempre più spesso se l’utente “paghi”i servizi di Internet consapevolmente. Da un’indagine conoscitiva sui big data avviata dall’Autorità garante delle comunicazioni (Agcom), dall’Autorità garante della concorrenza e del mercato (Agcm) e dal Garante per la protezione dei dati personali, emerge che la maggior parte degli intervistati sono consapevoli circa i rischi legati alla privacy ma, più della metà, sembra preferire che i servizi siano gratuiti rispetto alla sicurezza. Lo studio, svolto in collaborazione con l’Università La Sapienza di Roma e realizzato su oltre un milione di app, pari all’80% di quelle presenti sullo store di Google Play, mostra la presenza di uno “scambio implicito del dato“ . I dati diventano così il vero elemento della transazione digitale in corso. All’aumentare del numero di permessi richiesti sull’uso dei dati sensibili, diminuisce statisticamente il prezzo delle app. Allo stesso tempo, la domanda di download da parte degli utenti risulta negativamente correlata con il numero di permessi richiesti. L’incidenza sui propri dati viene quindi in ogni caso considerata dall’utente. Nel complesso, spiega il rapporto, più della metà degli utenti sono consapevoli della stretta relazione esistente tra la concessione del consenso e la gratuità del servizio e circa il 75% degli intervistati si dichiara disponibile a rinunciare ai servizi gratuiti per evitare lo sfruttamento dei propri dati. Allo stesso tempo però, solo poco meno della metà dichiara che sarebbe disposto a pagare per app oggi fornite gratuitamente, pur di difendere la propria privacy. In altre parole la scelta del servizio a costo zero vince, quando, però, il rischio per la privacy viene avvertito come alto il consumatore preferisce rinunciare al servizio. Il timore degli utenti è legato all’utilizzo dei dati a fini pubblicitari (46,7%) e, ancor di più, all’utilizzo per altre finalità (50,2%). Dallo studio poi, emergono ulteriori dati sull’uso delle piattaforme digitali da parte degli utenti e la loro attenzione al tema della privacy. In particolare, al 33% degli italiani non interessa leggere le informative sulla privacy e il 54% ne legge solo una minima parte.

Il presunto valore dei dati che oggi viene usato come mezzo di pagamento, si potrebbe definire quindi “moneta personale”. "Ogni giorno, utenti più o meno ignari cedono i propri dati mentre consultano pagine web o guardano un video online; perché non permettergli di usare i propri dati per acquistare una t-shirt o un altro oggetto?” Questa è la provocazione di Kaspersky Lab, una società di cybersecurity che ha aperto a Londra "The Data Dollar Store”[53]. I clienti seguono regole curiose imposte dallo store per l'acquisto dei gadget disponibili, senza dover aprire il portafoglio, “tre screenshot per una tazza, due foto per una maglietta”. L'idea sembra una provocazione futurista, ma potrebbe anche essere una non lontanissima realtà, potrebbe non restare un caso isolato, visto il valore che tutti, banche fintech, istituzioni, addetti ai lavori, cominciano a dare ai Big Data, i dati personali.

[53] URL: www.datadollarstore.com

Già un'inchiesta pubblicata nel 2013 dal Financial Times[54] ha cercato di stabilire il valore dei dati personali: mediamente, nome, età, etnia e livello di istruzione di 10.000 persone diverse, affermava valessero 5.139 euro.

In questo contesto rischia di esplodere uno scandalo sull'uso dei dati degli utenti da parte di un colosso del web: Google avrebbe pagato milioni di dollari per avere dati da Mastercard.
Se l'accordo fosse vero la maggior parte dei possessori di Mastercard sarebbe stata inconsapevole di questo, ulteriore, tracciamento. La vicenda ancora una volta solleva questioni di privacy: "Le persone non si aspettano che le cose comprate nei negozi fisici siano collegate a quelle comprate online, non c'è abbastanza informazione ai consumatori su cosa stanno facendo e che diritti hanno", spiega Christine Bannan, dell'Electronic Privacy Information Center (EPIC). In seguito alla notizia Unicredit ha interrotto le interazioni con Facebook giudicando il social network "non etico".

Scegliendo la strada che conduce al godimento del paradiso tecnologico che muta di giorno in giorno l'utente, come è stato discusso, si impegna a sostenere un costo, un prezzo molto elevato, rappresentato dallo scambio implicito dei dati personali. Tutto ciò, ad ogni modo, comporta dei rischi che sembrano andare oltre rispetto alla semplice, come è stata fino ad ora intesa, violazione della sfera personale. Affrontando l'analisi su quanto gli utenti paghino un "prezzo" piuttosto alto, vanno citati il caso Dragonfly ed il caso Maven, entrambi con protagonista Google[55]. Tra i dipendenti di Google sono stati oltre mille i firmatari della lettera di protesta, con la quale chiedevano una ridefinizione dei principi etici e di trasparenza dell'azienda. Tutto ciò in risposta al progetto, cosiddetto "Dragonfly", relativo ad un motore di ricerca ad hoc per la Cina che la multinazionale starebbe sviluppando. Google avrebbe offerto il proprio supporto a sviluppare un software di ricerca sulla base delle esigenze del governo cinese, censurando l'accesso ai contenuti che il regime di Xi Jinping reputa come sfavorevoli, per mezzo di un sofisticato sistema di filtraggio, blocco e reindirizzo. Il tradizionale motore di ricerca di Google, infatti, è fuori uso in gran parte della Repubblica Popolare Cinese, poiché bloccato dal Great Firewall (防火 长城), sottosistema del più ampio disegno di censura e di sorveglianza Golden Shield, implementato dal Ministero di pubblica sicurezza cinese per bloccare dati potenzialmente sfavorevoli provenienti dai paesi stranieri. I dipendenti del colosso informatico hanno denunciato di non poter compiere scelte responsabili nel proprio lavoro, poiché molto spesso, come in questo caso, tenuti all'oscuro di informazioni rilevanti. Vengono quindi sollevate "urgenti questioni etiche e morali". Con una simile lettera di denuncia, circa quattromila funzionari hanno espresso la loro disapprovazione in merito

---

54 Si veda: *Big data, tre profili a confronto sul valore dei dati personali*, 2013, URL: https://www.ilsole24ore.com/art/tecnologie/2013-06-14/data-profili-confronto-012622.shtml?uuid=AbTdmq4H

55 Si veda: Il caso Dragonfly ed il caso Maven: Google e la negoziazione coi principi etici di Lezzi I., in www.medialaws.eu

all'accordo tra l'azienda ed il Dipartimento di Difesa statunitense. Il cosiddetto progetto "Maven" (o AWCFT – Algorithmic Warfare Cross-Functional Team) consiste nello sviluppare sistemi di intelligenza artificiale per i droni militari di prossima generazione, incrementando l'integrazione tra le tecnologie per il riconoscimento di obiettivi sensibili ed i processi di elaborazione di big data. Sebbene non palesati i limiti del supporto di Google, se cioè circoscritti a migliorare la capacità di sorveglianza dei droni o se estesi anche a dotare gli stessi di avanzate capacità di attacco autonomo, la sola collaborazione tra Google e il Pentagono è bastata a far scatenare la tensione. Al centro il timore che il progetto potesse avere direttamente o indirettamente finalità belliche; la sua attuazione, quindi, ignorerebbe la responsabilità etica e morale dell'azienda. La questione ha condotto a conseguenze tangibili: i vertici della multinazionale hanno manifestato l'intenzione di non rinnovare il contratto col Pentagono. Google, successivamente, ha rassicurato, affermando che si impegnerà a non fornire supporto per lo sviluppo di armamenti ed applicazioni di sorveglianza e a circoscrivere piuttosto il suo impegno a progetti in grado di apportare benessere condiviso, ridurre l'ingiustizia sociale e che, nel complesso, rispettano l'integrità dell'individuo ed i principi del diritto internazionale[56]. Questi episodi rilevano l'esistenza di trade-off considerevoli e creano il precedente per la definizione di nuovi standard di regolamentazione. Progettare e distribuire soluzioni tecnologiche implica trovare un compromesso con l'etica ed i diritti individuali.

3.3 Ragionevoli aspettative di anonimato

Obiettivo è individuare una soluzione condivisa per una penetrazione di garanzie a tutti i livelli, si propongono una serie di possibili soluzioni alla tutela della ragionevole aspettativa di *privacy* del consumatore sui dati che immette in Rete ogni giorno. La tutela della *privacy* delle persone potrebbe avvenire in sede di progettazione senza annullare la potenza dei dati, mediante la *privacy by design*[57]. Silver Nate in "Il segnale e il rumore"[58] scrive che quello che cerchiamo è la conoscenza e non le informazioni. Silver è l'autore di un *software* che utilizzando i dati gli ha consentito di prevedere correttamente l'elezione di Obama in 49 Stati su 50, analizzando i dati numerici di affluenza al voto. Si ritiene sia superata l'era degli exit poll per il fatto che *Facebook, Google* e T*witter* sono in grado di dire molto di più delle tradizionali previsioni. In questa direzione sembra si sia mosso il Regolamento 679 con la previsione dell'articolo 25, il quale stabilisce che, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, il titolare del trattamento mette in atto misure

---

56 Si veda AI at Google: our principles. URL: https://www.blog.google/technology/ai/ai-principles/

57 Si veda: D'Acquisto, *Privacy by design in big data*. *An overview of privacy enhancing technologies in the era of big data analytics*, in www.enisa.europa.eu, dicembre 2015.

58 Nate S., *Il segnale e il rumore. Arte e scienza della previsione,* traduzione di Giffone, Fandango Libri, 2013.

tecniche e organizzative adeguate, quali la *pseudonimizzazione*, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente Regolamento e a tutelare i diritti degli interessati. La vera sfida è, dunque quella di riuscire ad anonimizzare[59] gli utenti senza cancellare l'interesse dei dati raccolti. Una proposta potrebbe essere quella dei *Topic Data* di *Facebook.* Si tratta di dati anonimi raccolti in forma aggregata che riguardano attività specifiche, marche, prodotti, eventi etc. che le persone seguono. Tuttavia, si tratta di sistemi complessi perché la raccolta, la conservazione e l'elaborazione dei dati si scontrano con le operazioni per rendere i dati anonimi. Si potrebbe utilizzare la crittografia «omomorfica», che consente di eseguire calcoli su dati cifrati senza prima decrittarli. È evidente che dati e anonimato rimangono un ossimoro perché il dato è tanto più interessante quanto più dettagli può dare sulla persona osservata, ma sembra una delle poche strade percorribili, al fine di mantenere bilanciati gli interessi dei vari attori. Tralasciando che, questo problema, sia percepito da molti come evanescente: sono gli stessi utenti a rinunciare alla tutela della *privacy* condividendo sui *social* i momenti più intimi della propria vita. L'interesse verso il processo che rende i dati non associabili a un individuo identificato o identificabile potrebbe essere soddisfatto da appositi sistemi. Il dato trattato con il cd. processo di *Big Data Anonymization* diventerebbe di origine ignota, esso si avvale di crittografia, *hashing* e generalizzazione, e serve a consentire il trattamento dei dati nel rispetto della *privacy*. Seguono alcuni esempi di *software importanti* nel settore. *SimilarWeb* è una *startup* israeliana, con sede a Londra che ha raccolto 400 milioni di dollari di investimenti per finanziare un servizio basato sull'analisi dei dati anonimi, provenienti da cento milioni di dispositivi e migliaia di siti in tutto il mondo. Esso traccia una sorta di "*traffic ranking*" cui sono interessati migliaia di clienti che pagano per avere accesso a *benchmark* e rapporti dettagliati per lo studio della concorrenza al fine di individuare rapidamente *trend* e strategie migliori sul *web*. Con *DataSift* vengono analizzati gli *status* degli utenti e i *post* delle pagine, compresi quelli privati, commenti e "mi piace", da queste analisi è possibile sapere quante persone parlano di un determinato argomento, il loro sesso, la loro età, la loro residenza, la loro istruzione, il loro grado di soddisfazione su un evento o marca, i *link* più condivisi, la materia che sta loro più a cuore al momento. Il sistema *DataSift* anonimizza i dati prima di processarli sulla piattaforma *Facebook*, inoltre analizza una soglia minima di cento unità di utenti maggiorenni per evitare analisi individuali. I risultati che il sistema restituisce sono dati aggregati e anonimi, che dopo trenta giorni vengono cancellati.

---

[59] Skopek J. M., *Reasonable expectations of anonymity*, in 101 Va. L. Rev. 691 2015, p. 692 ss.

Tim Berners Lee ha suggerito nel suo progetto Solid[60], un insieme di proposte di convenzioni e strumenti per la creazione di applicazioni sociali decentrate, basate sui principi *linked data*. Il progetto si muoverebbe lungo tre direttrici:

1)*True data owner ship*: gli utenti dovrebbero avere la libertà di scegliere dove i loro dati devono risiedere e chi è autorizzato ad accedervi scollegando i contenuti che non intende condividere o cedere dall'applicazione stessa.

2) *Modular design*: poiché le applicazioni sono scollegate dai dati che producono, gli utenti saranno in grado di evitare il *vendor lock-in* - il blocco da fornitore, cioè il rapporto di dipendenza che si instaura tra un cliente e un fornitore di beni o servizi - cambiando *app* senza difficoltà e *server* di archiviazione dei dati personali, senza alcuna perdita di dati o di connessioni sociali.

3) *Reusing existing data*: Gli sviluppatori saranno in grado di innovare facilmente con la creazione di nuove applicazioni riutilizzando dati esistenti creati da altre applicazioni.

Da quanto finora argomentato, si evince che oggi diventa più complesso, da un lato, capire fin dove si spinge la ragionevole aspettativa di *privacy*, dall'altro frenare il trasferimento indiscriminato dei dati, oggi divenuti, come anticipato, nocciolo duro di diritti fondamentali inalienabili. Per adattarsi a questo rapido mutamento sociale e tecnologico è necessario che la garanzia dei diritti non venga rimessa al singolo consumatore, confidando nella sua prudenza, ma, al contrario, che sia il legislatore a imporre condizioni contrattuali chiare e *privacy designed* nonché fermi divieti. Piuttosto, le nuove forme di consenso dovrebbero mirare a educare i soggetti della ricerca su ciò che i dati raccolti su di loro possono dire e il grado con cui possono o non possono essere protetti. Quanto al modello europeo, esso si presta a un'applicazione meramente formalistica che facilmente si riduce ad un modulo di informativa e alla prestazione di un consenso vuoto e non effettivo. L'interessato cui viene richiesto di esprimere un consenso è la parte più debole del rapporto contrattuale sotto ogni profilo: culturale, economico, tecnologico e conoscitivo.

60 Solid è modulare ed estensibile e si basa il più possibile su *standard* e *protocolli W3C* esistenti.

Conclusioni

Per millenni dimenticare è stata la norma, e ricordare l'eccezione. L'era digitale cambia questo rapporto, creando un fenomeno completamente nuovo: oggi rimane traccia di tutto. Tutto oggi può essere richiamato con il semplice clic di un mouse. Il progresso tecnologico si inserisce trasversalmente ed in maniera sempre più incisiva nelle sfide globali: il corso dell'innovazione e degli scenari futuri è imprevedibile ed in continua evoluzione. Lo sviluppo tecnologico va quindi considerato come mezzo per il raggiungimento di soluzioni ottimali e non fine da perseguire in quanto tale. Attribuendovi una connotazione valoriale si ridurrebbe il margine di rischio per esiti incontrollabili. Andando verso la progressiva consapevolezza dell'impatto sociale, economico, strategico e di sicurezza, permetterebbe di agire responsabilmente affinché i benefici risultino complessivamente superiori rispetto gli svantaggi del tutto prevedibili. È indubbio il tentativo di tutelare, almeno formalmente, il corretto trattamento dei dati personali, tuttavia, nessuna particolareggiata disciplina normativa sarà sufficiente per recepire la natura dinamica del contesto economico e sociale. Al fine di garantire una solida tutela della privacy sarebbero necessari continui interventi legislativi e normativi, sempre aggiornati. Tanto più il progresso tecnologico e l' innovazione aumentano, tanto più grandi ed insidiose saranno le minacce di invasione della nostra sfera privata.

Vittorio Frosini in Informatica, diritto e società, già nel 1992, affermava "il progresso tecnologico può essere apportatore di benefici come pure di malefici, nell'ordine fisico come in quello morale: può aumentare il grado di libertà umana o comprimerla, creare il nuovo uomo artificiale ad immagine di un'umanità più ricca di valori ma può anche irrigidirlo in una vita povera di energia morale"[61]. Occorre che si radichi una cultura della "privacy", fondata sulla consapevolezza dell'importanza dei dati personali e, più in generale, su un maggior rispetto per l'individuo. Per prevenire il "male" della privacy, occorre studiarlo, conoscerlo in modo così da poter applicare un vero e proprio antidoto. Oggi siamo come dinanzi ad un bivio: ad una strada che conduce al rispetto e alla tutela della privacy personale e ad un'altra che invece porta al letterale godimento del paradiso tecnologico che viene presentato sempre diverso giorno dopo giorno, in costante evoluzione. Tuttavia è stato analizzato che percorrere quest'ultima strada non presenta solo dei benefici. Tutto ciò ha un costo, un prezzo molto elevato, perché per vivere in un mondo colmo di vantaggi tecnologici, bisogna sacrificare qualcosa, rinunciare a qualcosa: quel "qualcosa" è proprio la privacy.

---

61 Frosisi V., *Informatica, diritto e società*, Giuffrè, 1992.

Bibliografia

Testi:

Acciai, *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo Codice*, Maggioli, Rimini, 2004.

Baldassarre, *Diritto della persona e valori costituzionali*, Giappichelli, Torino, 1997.

Bernardi, Perego, *Privacy Officer. La figura chiave della data protection europea*, Milano, 2017.

Biaisotti, *Il nuovo regolamento europeo sulla protezione dei dati*, Roma: EPC editore, 2016.

Bolognini, Fulco, Paganini, *Next privacy: il futuro dei nostri dati nell'era digitale*, Etas, Collana Economia, 2010.

Ciccia Messina, Bernardi, *Privacy e Regolamento europeo*, Milano: Wolters Kluwer Italia, 2016.

Cirillo, *Il codice sulla protezione dei dati personali*, Giuffrè, Milano, 2004.

Cleland S., *Why you can't trust Google Inc*., Telescope Books, 2011.

Comandè G. ,Pascucci G., *Diritto e informatica*, Giuffrè, Milano, 2002.

Costanzo P. - De Minico G. - Zaccaria R., *I «tre codici» della Società dell'informazione. Amministrazione digitale. Comunicazioni elettroniche Contenuti audiovisivi*, Torino, 2007.

Cuffaro V., Ricciuto V., Zeno-Zencovich V*., Trattamento dei dati e tutela della persona, Giuffrè, Milano, 1998.*

De Hert e Gutwirth, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in S. Guthwirth e altri, Action in Reinventing Data Protection?*Springer, 2009.

De Hert, Gutwirth, *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power*, Bepress, 2006.

Delfini F., Finocchiaro G., *Diritto dell'informatica*, Utet giuridica, 2014.

Dizionario Devoto-Oli Digitale 2016

Faro S., *Trattamento dei dati personali e tutela della persona*, in Digesto delle discipline pubblicistiche, Utet, Torino, 2000.

Faulkner, *Privacy*, Piccola Biblioteca Adelphi, 1955.

Fischer P. E., *Will Privacy Law in the 21st Century be American, European or International?*, GRIN Verlag, Munich, 2012.

Frosisi V., *Informatica, diritto e società*, Giuffrè, 1992.

Gianniti P., *La CEDU e il ruolo delle corti*, Zanichelli, 2015.

Glancy D. J., *The invention of the right to privacy*, Arizona Law Review, 1979.

Lambert P., *The Data Protection Officer: Profession, Rules, and Role,* CRC Press, 2016.

Maccarelli M., *Regolamento Privacy: Regolamento (UE) 2016/679,* Certifico S.r.l.

Mantelero A., *Il costo della privacy tra valore della persona e ragione d'impresa*, Giuffrè, 2007.

Mattiacci A., Pastore A. , Marketing. *Il management orientato al mercato*, Hoepli, 2013, Milano.

Messi M., Falletta P., *Il diritto del web, casi e materiali*, Cedam, 2015

Menghini*, Le FANGs: Facebook, Amazon, Netflix, Google: I grandi gruppi della new economy nell'epoca della stagnazione economica*, GoWare, 2017.

Nate S., *Il segnale e il rumore. Arte e scienza della previsione,* traduzione di Giffone, Fandango Libri, 2013.

Niger S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, 2006.

Orefice M., *I Big Data. Regole e concorrenza, in Politica del diritto*, 4/2016.

Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali: dalla Direttiva 95/46 al nuovo Regolamento europeo,* Torino: Giappichelli, 2016.

Pizzetti F. , *Il percorso del Consiglio d'Europa che porta al riconoscimento del diritto alla protezione dei dati personali*, LUISS.

Rampini F., *Rete padrona. Amazon, Apple, Google & co. Il volto oscuro della rivoluzione digitale*, Feltrinelli Editore, 2015.

Resta G., Zeno-Zencovich V., *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press, 2015.

Rodotà S., *Data Protection as a Fundamental Right in S. Guthwirth e altri, Reinventing Data Protection?,* Springer, 2009.

Rosen J., *The right to be forgotten*, Stanford law review online, 2012.

Sica S., D'Antonio V., Riccio G. M., *La nuova disciplina europea della privacy,* Cedam, 2016.

Umbertazzi T. M., *Il diritto alla privacy. Natura e funzione giuridiche,* Cedam, Padova, 2004.

Wacks, R., *Privacy Una sintetica introduzione*, Pescara: Monti & Ambrosini editori, 2016

Westin, A. F. *Privacy and freedom*, 1968, New York: Atheneum.

Ziccardi G., I*nformatica giuridica*, Giuffrè, Milano 2012.

Articoli :

Brin S., Page L., The Anatomy of a Large-Scale Hypertextual Web Search Engine, Journal Computer Networks, 1998.

Magnani C. , "I nuovi diritti nella Carta dei diritti fondamentali dell'Unione Europea" Studi urbinati di scienze giuridiche politiche ed economiche.

Cleland S., The Top Ten Threats to Google, Forbes, 2011.

Roger Clarke, 1997, Introduction to Dataveillance and Information Privacy, and Definitions of Terms, Xamax Consultancy, Consultabile su: http://www.rogerclarke.com/DV/Intro.html

Radinsky K., Data monopolists like Google are threatening the economy, Harvard Business Review, 2015.

Stefano Rodotà, 16 settembre 2004, Discorso conclusivo della Conferenza internazionale sulla protezione dei dati: Privacy, libertà e dignità

Intervista a Stefano Rodotà del 12 marzo 2016 a Linkiesta, Consultabile su: https://www.linkiesta.it/it/article/2016/03/12/stefano-rodota-la-trasparenza-totale-e-unidea-da-%20dittatori/29592/

Mariottini I., Il pacchetto di riforma della Commissione europea in materia di protezione dei dati personali, in Riv. dir. int. priv. proc., 2016.

Fumagalli Meraviglia, Le nuove normative europee sulla protezione dei dati personali, in Diritto comunitario e degli scambi internazionali, 2016.

Polly Sprenger, 26 gennaio 1999, Sun on Privacy: 'Get Over It', Wired, Consultabile su: https://www.wired.com/1999/01/sun-on-privacy-get-over-it/

Bobbie Johnson, 11 gennaio 2010, Privacy no longer a social norm, says Facebook founder, Consultabile su: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Rosen, J. ,21 luglio 2010, The web means the end of forgetting, The New York Times, Consultabile su: https://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all

Guido Scorza, 9 ottobre 2015, Costeja Gonzalez: negato l'oblio all'uomo che lo ha regalato all'Europa, Il fatto quotidiano, Consultabile su: https://www.ilfattoquotidiano.it/2015/10/09/costeja-gonzalez-negato-loblio-alluomo-che-lo-ha-regalato-alleuropa-2/2111057/

Garante della privacy, Newsletter n. 397 del 22 dicembre 2014 Consultabile su: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3623678

Comunicato stampa della Commissione Europea del 2 febbraio 2016, Consultabile su http://europa.eu/rapid/press-release_IP-16-216_it.htm

Pubblicità digitale: Amazon lancia la sfida a google e Facebook. Consultabile su: http://www.ilsole24ore.com/art/impresa-e-territori/2018-08-31/pubblicita-mercato-ora-fa-conti-amazon-155626.shtml?uuid=AEbL9zhF

Le sfide della privacy, 2018. Consultabile su: https://www.federprivacy.org/informazione/item/364-le-sfide-della-privacy-nell-era-dell-internet-of-things

«Così, con i social network, abbiamo fatto vincere Donald Trump», in il Venerdi di Repubblica, 7 febbraio 2017.

R. Booth, Inquiry launched into targeting of UK voters through social media, in the Guardian, 17, maggio 2017.

Faktor S., Deconstructing Google'Strategy, Forbes, 2013.

Rao V., Why Amazon is the best strategic player in tech, Forbes, 2011.

How far Amazon go?, The Economist, 2014.

Facebook, per capire qual è la pubblicità giusta per te basta un Like, di Michela Rovelli, Consultabile su: https://www.corriere.it/tecnologia/social/17_novembre_14/facebook-capire-qual-pubblicita-giusta-te-basta-like-e8541538-c918-11e7-8a54-e86623f761be_preview.shtml?

Uccisi e sopravvissuti, l'indice che misura l'impatto di Amazon sulle aziende, di Mauro Del Corno. Consultabile su: https://www.ilsole24ore.com/art/finanza-e-mercati/2017-09-02/indici%20amazon-174954.shtml?%20uuid=AEGNxgMC

Google-Mastercard, accordo segreto per scambiarsi i dati sui clienti, La Repubblica. Consultabile su: https://www.repubblica.it/economia/finanza/2018/08/31/news/google-mastercard_accordo_segreto_per_scambiarsi_i_dati_sui_clienti-205302785/

Google, la Corte Ue: motore di ricerca responsabile del trattamento dati. Link «indesiderati» vanno rimossi, 2014. Consultabile su: https://www.ilsole24ore.com/art/norme-e-tributi/2014-05-13/google-corte-ue-articoli-indesiderati-vanno-rimossi--105050.shtml?uuid=ABvy3qHB

Il caso Dragonfly ed il caso Maven: Google e la negoziazione coi principi etici, di Lezzi I., Consultabile su: http://www.medialaws.eu/il-caso-dragonfly-ed-il-caso-maven-google-e-la-negoziazione-coi-principi-etici/

La vera nuova moneta sono i Big Data di Roberto Sommella, Consultabile su: https://www.huffingtonpost.it/roberto-sommella/la-vera-nuova-moneta-sono-i-big-data_a_23234648/

Titolarità e contitolarità dei dati personali alla luce della decisione della Corte di giustizia sulle fanpage di Facebook. Consutabile su: http://www.medialaws.eu/titolarita-e-contitolarita-dei-dati-personali-alla-luce-della-decisione-della-corte-di-giustizia-sulle-fanpage-di-facebook/

G. D’Acquisto, Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics, dicembre 2015. Consultabile su: https://www.enisa.europa.eu/news/enisa-news/privacy-by-design-in-big-data-an-overview-of-privacy-enhancing-technologies-in-the-era-of-big-data-analytics

Reasonable Expectations of Anonymity by Jeffrey M. Skopek, 101 Va. L. Rev. 691 (2015) Article, Consultabile su: http://www.virginialawreview.org/volumes/content/reasonable-expectations-anonymity

Big data, tre profili a confronto sul valore dei dati personali, 2013, Consultabile su: https://www.ilsole24ore.com/art/tecnologie/2013-06-14/data-profili-confronto-012622.shtml?uuid=AbTdmq4H