LUISS

Dipartimento
di Giurisprudenza

Cattedra di Informatica giuridica

Come lo scandalo "Cambridge Analytica" ha cambiato il modo in cui le multinazionali, del web e non, trattano i dati personali.

Chiar. mo Prof. Francesco Romeo

RELATORE

Chiar. mo Prof. Stefano Russo

CORRELATORE

Vincenzo Lanzetta Matr. 136913

CANDIDATO

Anno Accademico 2019/2020

INTRODUZIONE

Quella in cui viviamo oggi potremmo definirla "la società dell'informazione e della comunicazione", un tipo di società che fa della conoscenza e della sua condivisione gli elementi cardine attorno ai quali sviluppare le attività caratterizzanti il vivere sociale ed economico.

La crescente possibilità offerta dai supporti tecnologici di scambiare agevolmente contenuti di vario tipo, superando le tradizionali barriere spazio-temporali, ha, negli anni, profondamente innovato il tradizionale modo di intendere l'attività economica, le modalità di interazione tra i consociati e l'erogazione di servizi pubblici che si nutrono ormai pienamente dell'interattività, versatilità, speditezza e globalità dei servizi offerti dalla Rete[1].

Nell'ultimo decennio, tuttavia, tale peculiare processo estremamente dinamico e mutevole ha compiuto un ulteriore passo in avanti con il diffondersi di tecnologie sempre più avanzate, fondate sullo scambio dei dati e delle informazioni.

Si fa riferimento, in primo luogo, al fenomeno dell'*Internet of Things (IOT*) che consente di trasformare oggetti, come auto, edifici, ma anche televisori ed elettrodomestici, in beni tra loro strettamente connessi, capaci di immagazzinare, trattare e scambiare reciprocamente migliaia di dati al fine di garantire esperienze di consumo sempre più avanzate e personalizzate[2].

Anche le stesse città, attraverso l'impiego di tali tecniche, diventano anno dopo anno sempre più "*smart*", perché in grado di trasformare le potenzialità offerte dalle nuove piattaforme digitali in servizi sempre più efficienti per i cittadini[3], ottimizzando

---

[1] Sul concetto di società dell'informazione e della comunicazione, cfr., tra gli altri, A. PAPA, Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico, Torino, 2009; P. CARETTI, Diritto dell'informazione e della comunicazione. Stampa, radiotelevisione, telecomunicazioni, teatro e cinema, Bologna, 2005; M. CUNIBERTI (a cura di), Nuove tecnologie e libertà della comunicazione, Milano, 2008; ZACCARIA R., I tre codici della Società dell'informazione, Torino, 2006; A. VALASTRO, Libertà di comunicazione e nuove tecnologie, Milano, 2001; S. RODOTÀ, Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione., Roma, 1997; G. OLIVIERI – V. FALCE, Smart cities e diritto dell'innovazione, in Quaderni di giurisprudenza, Milano, 2016.

[2] Per un'analisi della portata rivoluzionaria dell'Internet of things si rinvia, fra gli altri, allo studio realizzato dalla Commissione Europea tramite DG Communications Networks, Content & Technology nell'ambito dell'"Agenda Digitale", una delle sette iniziative principali individuate nella più ampia Strategia EU2020, che punta alla crescita inclusiva, sostenibile ed intelligente entro l'anno 2020. COMMISSIONE EUROPEA, DG Communications Networks, Content & Technology, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Final Report, 2013. L'analisi ha evidenziato che l'impiego di tale tecnologia garantirà una crescita economica di oltre 20 miliardi di euro all'interno dell'Unione Europea entro l'anno 2020 e rappresenta uno dei pilastri della creazione del mercato unico digitale europeo (c.d. Digital single market).

[3] Sulla nascita delle nuove realtà urbane basate sull'utilizzo delle tecnologie dell'informazione e della comunicazione

l'uso delle risorse a disposizione e garantendo in alcuni casi anche un minor impatto ambientale[4].

Un ulteriore fenomeno è rappresentato dal proliferare dei *Big Data*, enormi quantità di dati ed informazioni di vario tipo che, prodotti a grande velocità a partire da una pluralità di fonti differenti, vengono utilizzate in maniera combinata per l'erogazione di prestazioni altamente avanzate e modellate sulle necessità degli utenti[5].

Ed infine è da sottolineare la diffusione delle tecnologie di *cloud computing* (letteralmente nuvola informatica), che permettono, sfruttando le straordinarie potenzialità di immagazzinamento della Rete *Internet*[6], di archiviare queste imponenti masse di dati in remoto.

---

cfr. G. OLIVIERI – V. FALCE, Smart cities e diritto dell'innovazione, in Quaderni di giurisprudenza, op. cit. Rileva sottolineare che il progetto a livello sovranazionale della realizzazione di smart cities all'interno del panorama europeo ha trovato la sua più compiuta realizzazione con la creazione del partenariato "Città e comunità intelligenti" (CCI) - Smart Cities and Communities (EIP-SCC) che mira a stimolare la crescita tecnologica nei settori in cui "la produzione, la distribuzione e l'uso dell'energia, la mobilità e i trasporti e le tecnologie di informazione e comunicazione (TIC) sono strettamente legati e possono offrire nuove opportunità interdisciplinari di migliorare
i servizi, riducendo il consumo di energia e risorse e le emissioni di gas a effetto serra e di altre sostanze inquinanti". Sul punto v. COM (2012) 4701, Comunicazione della Commissione, Città e Comunità Intelligenti Partenariato Europeo di innovazione, 2012.

[4] Il conseguimento di "un'Europa efficiente sotto il profilo delle risorse" rappresenta una delle sette iniziative "faro" promosse a livello sovranazionale e degli Stati membri nell'ambito della strategia H2020 che, come è noto, punta alla realizzazione di una crescita intelligente, attraverso lo sviluppo delle conoscenze e dell'innovazione; sostenibile, basata su un'economia più verde, più efficiente nella gestione delle risorse e più competitiva; inclusiva, volta a promuovere l'occupazione e la coesione sociale e territoriale. V. COM (2010) 2020, Comunicazione della Commissione, Europa 2020 - Una strategia per una crescita intelligente, sostenibile e inclusiva. A tal proposito, come si legge nella tabella di marcia stilata nel 2011 dalla Commissione europea, per la realizzazione di tale iniziativa risulta necessario definire "un quadro strategico che premi l'innovazione e l'efficienza delle risorse e che crei le condizioni per nuove opportunità economiche per una maggiore sicurezza di approvvigionamento grazie alla riprogettazione dei prodotti, alla gestione sostenibile delle risorse ambientali, alla promozione del riciclaggio e del riuso, alla sostituzione di materiali e al risparmio di risorse". V. COM (2011) 0571, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle regioni, Tabella di marcia verso un'Europa efficiente nell'impiego delle risorse, 2011.

[5] Sul significato dei big data e sul relativo impatto sulla tutela dei dati personali cfr. da ultimo CONSIGLIO D'EUROPA, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data; Strasburgo, 2017. Sul ruolo dei big data all'interno delle moderne società digitali cfr. COM (2014) 442 Final, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Verso una florida economia basata sui dati, 2014; RUBINSTEIN IRA S., Big Data: The End of Privacy or a New Beginning? in International Data Privacy Law, 2013, Vol. 3, No. 2; B. VAN DER SLOOT - S.VAN SCHENDEL, Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study in Jipitec, Journal of Intellectual Property, Information Technology and E-Commerce Law, n.7 (2)/2016. A testimonianza della trasversalità delle problematiche connesse all'utilizzo dei Big Data, in data 30 maggio 2017 è stata avviata un'indagine conoscitiva congiunta che coinvolge l'Autorità Garante della Concorrenza e del Mercato (AGCM), il Garante per la protezione dei dati personali e l'Autorità per le Garanzie nelle Comunicazioni (AGCOM). Lo studio, ancora in corso, è finalizzato all'individuazione di eventuali criticità concorrenziali connesse ai Big Data e alla definizione di un quadro di regole atto a promuovere e tutelare la concorrenza dei mercati della economia digitale, consentendo al contempo una più efficace realizzazione dei compiti istituzionali di ciascuna Autorità.

[6] Per cloud computing si intende un insieme di tecnologie e di modalità di fruizione di servizi informatici che consentono l'archiviazione, l'elaborazione o la trasmissione di dati, in modalità on demand, attraverso Internet, a partire da un insieme di risorse preesistenti e configurabili. Sul tema si faccia riferimento al documento COM (2012) 529 final,

IOT, big data e cloud computing rappresentano, quindi, le tre direttrici su cui si sta muovendo l'attuale evoluzione tecnologica[7] ed il loro combinato agire sta completamente modificando la fisionomia delle società contemporanee, favorendo la nascita di una nuova era caratterizzata da collettività "iper-connesse".

È evidente che, in tale peculiare scenario, il "Dato" assurge a risorsa strategica e fattore di sviluppo economico; elemento di crescita collettiva e di ricchezza culturale, ponendo l'individuo al centro della società digitale.

Nel mondo in cui viviamo, in cui siamo sempre più connessi, tutto (o quasi) ruota intorno alla persona ed al relativo bagaglio di informazioni.

Tuttavia, nonostante la personalizzazione dei servizi porti con sé una serie di straordinari vantaggi, dietro alla stessa si cela il rischio che i diritti fondamentali del singolo vengano eccessivamente compressi, attraverso la sovraesposizione di aspetti estremamente delicati della propria sfera personale[8].

Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Sfruttare il potenziale del cloud computing in Europa, 2012. Rileva sottolineare che in Italia il Garante per la protezione dei dati personali nel maggio 2012 ha stilato un vademecum per le imprese e la pubblica amministrazione relativamente alla scelta e all'utilizzo del cloud computing dal titolo "Cloud computing. Proteggere i dati per non cadere dalle nuvole".

[7] Internet of things, Big data e cloud computing sono gli assi portanti della strategia nota come Digital single market. V.COM (2015) 192 final, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, A Digital Single Market Strategy for Europe. Adottata il 6 maggio 2015, tale progetto include 16 specifiche iniziative eterogenee che ruotano intorno a tre pilastri fondamentali: 1) l'accesso: finalizzato a garantire ai consumatori e agli operatori del mercato un accesso efficiente ai beni e ai servizi digitali in tutta l'Unione Europea; 2) il contesto: finalizzato a garantire le migliori condizioni e un level playing field che sia in grado di far emergere servizi e reti digitali innovative; 3) l'economia e la società: finalizzata alla massimizzazione della crescita potenziale dell'economia digitale. L'obiettivo perseguito è la creazione di un mercato unico digitale che si fondi sullo sfruttamento delle potenzialità e della straordinaria pervasività delle tecnologie dell'informazione e della comunicazione. Le iniziative che si collegano a tale strategia risultano, infatti, ampie ed eterogenee, muovendosi dal campo del e- commerce a quello della tutela dei dati personali, passando per la tutela del diritto d'autore, l'evoluzione del mercato audiovisivo fino alla digitalizzazione dei servizi della pubblica amministrazione. Una trasformazione, quindi, ad ampio spettro imperniato sui vantaggi derivanti dalla sempre più avanzata digitalizzazione della società europea. Sul tema cfr. tra gli altri, la prima valutazione degli obiettivi raggiunti sino ad ora nell'ambito della suddetta strategia realizzata nel 2017. COM/2017/0228 final, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Sulla revisione intermedia dell'attuazione della strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti, 10 maggio 2017. Ulteriori informazioni e tutti i documenti prodotti sino ad ora possono essere reperiti su questa pagina: https://ec.europa.eu/commission/priorities/digital-single-market_en

[8] Sulla portata rivoluzionaria delle nuove tecnologie e la necessità di ridefinire regole in grado di tutelare diritti fondamentali del singolo cfr. G. BUSIA - L. LIGUORI - O. POLLICINO (a cura di), Le nuove frontiere della privacy nelle tecnologie digitali, Roma, 2016; M. OREFICE, I Big Data e gli effetti su privacy, trasparenza e iniziativa economica, Roma, 2018; M. R. ALLEGRI - G. D'IPPOLITO (a cura di), Accesso a internet e neutralità della rete, tra principi costituzionali e regole europee, Roma, 2017, S. WACHTER, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, in Computer law & security Review, n. 34/2018, pp. 436–449; I. S. RUBINSTEIN, Big Data: The End of Privacy or a New Beginning?, in International Data Privacy Law, n. 2/2013; ; G. - NALDI M., Big data e privacy by design, Torino, 2017; V. MAYER - SCHÖNBERGER - K. N. CUKIER, Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà, Milano, 2013; O. POLLICINO – T. E. FROSINI – E. APA, Diritti e libertà in Internet, Milano, 2017; R. BIFULCO - O. POLLICINO - G. D'ACQUISTO - M. NALDI - M. BASSANI - F. PIZZETTI (a cura di), Intelligenza artificiale, protezione dati personali e regolazione, Milano, 2018.

Con il digitalizzarsi della società, sta seguendo un sempre maggior frazionamento dell'identità dell'individuo in migliaia di piccoli tasselli, che attraverso il dato si riflettono all'esterno proiettando aspetti più o meno intimi della propria persona. Il fluire incessante di tali informazioni personali ha favorito negli ultimi anni il sorgere di tecniche di profilazione sempre più affinate che, attraverso l'aggregazione, l'incrocio e la riorganizzazione dei dati raccolti, consentono di suddividere gli utenti in categorie distinte in base a caratteristiche omogenee, al fine di fornire prodotti "su misura" attraverso la previsione delle decisioni di consumo e dei relativi comportamenti.

Potenziate dalla straordinaria rapidità evolutiva degli strumenti tecnologici, tali particolari attività di trattamento dei dati personali non solo possono creare situazioni di discriminazione e di stereotipizzazione già esistenti, ma rischiano di condurre a fenomeni di "penalizzazione delle propensioni"[9], limitando le effettive possibilità di scelta del singolo, sino a condurre all'estrema conseguenza di inibire l'esercizio delle relative libertà fondamentali o di limitare l'erogazione di servizi essenziali[10].

Inoltre, basandosi su tecniche statistiche, tali meccanismi di classificazione possono condurre a previsioni imprecise o errate favorendo a loro volta ulteriori fenomeni discriminatori.

Tutto ciò di cui abbiamo parlato si verifica specialmente nel panorama dei social network, le quali svolgono intense attività di profilazione che si basano su manifestazioni di interesse e diffusioni di opinioni molto spesso estemporanee o peggio incentivate dall'apparente carattere ludico e riservato delle piattaforme che, se decontestualizzate ed aggregate, rischiano di favorire la delineazione di identità virtuali completamente diverse da quelle reali.

---

[9] Così V. MAYER-SCHÖNBERGER - K. N. CUKIER, Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà, op. cit.

[10] Come evidenziato dalle Linee guida tracciate dall'Article 29 Working Party in materia di profilazione e di processi decisionali automatizzati tali peculiari trattamenti non solo possono accentuare situazioni di discriminazione sociale già esistenti, ma sono potenzialmente in grado di incardinare una persona all'interno di una determinata categoria, limitandone le possibili alternative di scelta. Ad esempio, in seguito ad un'attività di profilazione, un sito tende inevitabilmente a proporre ai propri clienti prodotti e servizi affini alle loro esigenze e preferenze, escludendone altri e limitando così drasticamente la libertà di scelta di tali soggetti. E' evidente che con l'affinarsi delle tecniche di profilazione soprattutto in maniera automatizzata e, quindi, in assenza dell'intervento umano, e l'ampliarsi degli strumenti messi a disposizione dei soggetti titolari del trattamento, tale attività, se non regolata rischia di ledere anche la sfera dei diritti fondamentali dei singoli, incidendo, ad esempio, sulla relativa libertà di associarsi ovvero sul cosciente esercizio del diritto di voto, nonché influenzare le posizioni contrattuali dei soggetti all'interno di un contratto. Infine, basandosi su calcoli previsionali, le profilazioni possono condurre a predizioni non accurate provocando ulteriori danni in termini di limitazioni di accesso a determinati servizi o prodotti. Sul punto cfr. ARTICLE 29 WORKING PARTY, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, ultima versione adottata il 6 febbraio 2018.

È evidente, quindi che l'attuale processo di "frantumazione" della sfera personale dell'individuo e di ricomposizione della stessa da parte di soggetti terzi per l'erogazione di servizi e prodotti di vario genere ovviamente presenta inevitabili profili di rischio che impongono l'individuazione di nuove e soprattutto efficaci modalità di tutela e di garanzia a favore del singolo.

La piena e consapevole realizzazione del singolo all'interno delle moderne società data-centriche corre oggi lungo i binari della protezione dei dati personali, con la finalità di tutelarlo dal pericolo di acquisizione occulta delle informazioni, di intrusione nella propria sfera privata e di utilizzazione impropria dei dati raccolti[11].

[11] Con riferimento all'ordinamento italiano, come è noto, il diritto alla protezione dei dati personali ha iniziato a farsi strada in seguito al riconoscimento del diritto alla riservatezza sancito per la prima volta dalla Corte di Cassazione con sentenza n. 2129 del 1975 e al crescente interesse a livello sovranazionale sul tema della tutela delle informazioni personali sancito dall'emanazione di tre rilevanti direttive in materia: la Direttiva 95/46/CE (relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati), la Direttiva 97/66/CE (sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni) e la Direttiva 2002/58/CE (relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche). Il combinato agire di questi due aspetti ha condotto all'adozione di una prima organica regolamentazione legislativa sul tema con la legge 31 dicembre 1996, n.675 (c.d. "legge sulla privacy"), in seguito assorbita ed implementata dal "Codice in materia di protezione dei dati personali" adottato con decreto legislativo 30 giugno 2003 n.196 e comunemente identificato come "Codice della Privacy". In seguito all'adozione del Regolamento 2016/679, con legge 25 ottobre 2017, n.163, il Governo ha ricevuto delega dal Parlamento all'emanazione di uno o più decreti legislativi di adeguamento del quadro normativo nazionale alle nuove disposizioni europee. L'opera di coordinamento è stata compiuta mediante l'adozione del d.lgs. 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 delParlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" in G.U. 4 settembre 2018 n. 205. Sull'evoluzione della tutela dei dati personali nell'ordinamento italiano, senza pretesa di esaustività, V.P. PATRONO, voce Privacy e vita privata (dir. pen.), in Enc. Dir., XXXV, Milano, 1972; A. BARBERA, Art. 2 della Costituzione, in Commentario della Costituzione (a cura di) G. BRANCA, Bologna, 1975; T.A. AULETTA., Riservatezza e tutela della personalità, Milano, 1978; F. BARTOLOMEI, La dignità umana come concetto e valore costituzionale, Torino, 1987; G. ALPA, Diritti della personalità emergenti, diritto all'identità personale, in Giurisprudenza di merito, 1989, IV, pp. 464 e ss.; A. CERRI, voce Riservatezza (diritto alla), in Dig. disc. pubbl., vol. IV, Torino, 1989; A. CLEMENTE (a cura di), Privacy, Padova, 1999; G. GIACOBBE, Riservatezza (diritto alla), in Enc. Dir., vol. XL, Milano, 1989; P. RESCIGNO, Personalità (diritti della), in Enciclopedia Giuridica, XXIII, Roma, 1990; V. ZENO-ZENCOVICH, Personalità (diritti della), in Digesto delle Discipline Privatistiche–Sez. civile, vol. XIII, 1995; B. MARKESINIS -G. ALPA, Il diritto alla "privacy" nell'esperienza di "common law" e nell'esperienza italiana, in Riv. Trim. dir. proc. civ. 1997; R. PARDOLESI (a cura di), Diritto alla riservatezza e circolazione dei dati personali, Milano, 2003; S. STANZIONE –S. SICA, La nuova disciplina della privacy, Bologna, 2004;A. BARBERA, "Nuovi diritti": attenzione ai confini, in L. CALIFANO (a cura di), CorteCostituzionale e diritti fondamentali,, Torino, 2004; AA.VV., Codice della privacy, commento al decreto legislativo 30 giugno 2003, n. 196, Milano, 2004; T. M. UMBERTAZZI, Il diritto alla privacy: natura e funzione giuridica, Padova, 2004; G. RESTA, Privacy e processo civile, in Il Diritto dell'informazione e dell'Informatica, 2005, pp. 681 e ss.; S. RODOTÀ, Intervista su privacy e libertà, Roma-Bari, 2005; R. PANETTA (a cura di), Libera circolazione e protezione dei dati personali, Milano, 2006; D. CALDIROLA, Il diritto alla riservatezza, Padova, 2006; S. NIGER, Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali, Padova, 2006; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, (a cura di), Il codice del trattamento dei dati personali, Torino, 20017;S. RODOTÀ, La vita e le regole. Tra diritto e non diritto, Milano, 2006; A. M. GAMBINO –A. STAZI, Diritto dell'informatica e della comunicazione, Torino, 2009; M. MEZZANOTTE, Il diritto all'oblio –un contributo allo studio della privacy storica, Napoli, 2009; A. PAPA, Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico, Torino, 2009; R. RAZZANTE, Manuale di diritto dell'informazione e della comunicazione: privacy, diffamazione e tutela della persona -libertà e regole nella rete, Padova, 2011; V. ZENO-ZENCOVICH -G. RESTA (a cura di), La protezione transnazionale dei dati personali dai "safe harbour principles" al "privacy shield", Roma, 2016; F. PIZZETTI, Privacy e il diritto europeo alla protezione dei dati personali –dalla Direttiva 95/46 al nuovo

L'esigenza, dunque, è quella di evitare che il dato, trattato per finalità che esulano dalla volontà del soggetto, possa cagionare situazioni di discriminazione, furto o usurpazione di identità; pregiudicare la propria reputazione o comportare un qualsiasi significativo danno economico o sociale.

Inoltre, alla luce delle sempre più invasive tecniche di profilazione, come è stato efficacemente evidenziato[12], in tale complesso panorama la tutela del dato assume un significato ulteriore al di là della protezione del singolo, affermandosi come strumento di tutela della collettività.

Il corretto trattamento dei dati personali, soprattutto di carattere sensibile, costituisce premessa, infatti, irrinunciabile al pieno e consapevole esercizio degli altri diritti fondamentali allontanando fenomeni di compressione dei momenti di interazione tra i soggetti, non accettabili all'interno delle società democratiche.

Ne consegue che la previsione di un ragionato sistema di regole destinato a quello che è stato definito "il nuovo petrolio dell'economia digitale"[13] trova giustificazione e legittimazione nel suo essere funzionale al carattere democratico delle moderne società.

Non solo ha un valore in sé[14], ma opera al fine di garantire che la collettività sia in grado di convogliare le potenzialità delle nuove tecnologie verso nuovi e desiderati livelli di crescita, senza però mai sacrificare i valori fondamentali a cui essa stessa si ispira e che rappresentano causa e fine ultimo della sua esistenza.

Regolamento europeo, Milano, 2016; A. PAPA, Il diritto dell'informazione e della comunicazione nell'era digitale, Torino, 2018.

[12] Come evidenziato da F. PIZZETTI in Privacy e il diritto europeo alla protezione dei dati personali – dalla Direttiva 95/46 al nuovo Regolamento europeo, op.cit., p. 10 e ss., partendo dalla consapevolezza che l'uomo è un animale sociale e come tale al centro di una rete di relazioni "rinunciare alla protezione dei dati personali da ogni indebita ingerenza, significa rischiare di vanificare ogni altra forma di libertà e mettere in pericolo tutti i diritti fondamentali". D'altra parte, rileva sottolineare che lo stesso Regolamento europeo oggetto di analisi al considerando 4) dichiara che "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica". Sul punto si veda anche V. BOEHME-NEßLER, Privacy: a matter of democracy. Why democracy needs privacy and data protection, in International Data Privacy Law, Vol. 6, n. 3/2016.

[13] Così sono stati definiti i dati personali dall'attuale Presidente del Garante italiano per la protezione dei dati personali, Antonello Soro, durante un'intervista relativa all'attuale debolezza delle imprese nei confronti di attacchi di carattere cyber. L'intervista è reperibile sul sito del Garante, documento web n. 8136779, Le imprese sono troppo deboli nelle difese contro gli hacker, del 26 marzo 2018.

[14] E. CARLONI –M. FALCONE, L'equilibrio necessario. Principi e modelli di bilanciamento tra trasparenza e privacy, in Diritto Pubblico, Fascicolo 3, settembre-dicembre 2017, p. 731.

CAPITOLO PRIMO

Connessione tra manipolazione di dati particolari e processi elettorali

1. Il caso Cambridge Analytica

1.1 Attori in scena di questo celebre caso mediatico: SCL Group e Cambridge Analytica

Nel 1993, il pubblicitario Nigel Oakes fondò la società *Strategic Communication Laboratories* (in seguito SCL Group), che si occupava di pubbliche relazioni, ricerche comportamentali e comunicazione strategica per governi, politici ed anche eserciti[15].

Sul sito online della società, nella sezione dei servizi offerti ai clienti, SCL Group indicava la "guerra psicologica" e asseriva di poter "influenzar le elezioni".

Nel 2013 nasce *Cambridge Analytica*, come branca di SCL Group, con il fine di occuparsi di consulenza politica.

Uno dei maggiori finanziatori della società era il miliardario statunitense Robert Mercer, anche noto per essere uno dei più grandi finanziatori delle campagne dei conservatori; Cambridge Analytica, tra il 2013 e il 2018, ha lavorato ad oltre 200 campagne elettorali in giro per il mondo[16].

La SCL Group e Robert Mercer vennero a contatto grazie al consigliere politico della famiglia Mercer, Steve Bannon, all'epoca direttore di Breitbart News, un giornale online e piattaforma dell'"Alt-Right"[17], l'estrema destra statunitense[18].

Uno dei dirigenti di SCL Group, Alexander Nix, venne nominato CEO di *Cambridge Analytica*, mentre Steve Bannon ne divenne il vicepresidente.

---

[15] Prokop, A. (2 maggio 2018). Cambridge Analytica shutting down: the firm's many scandals, explained. Vox https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-analytica-trump-russiamueller.

[16] BBC News. (22 marzo 2018). Cambridge Analytica: The data firm's global influence. https://www.bbc.com/news/world-43476762.

[17] Sterling, J. (17 novembre 2016). White nationalism, a term once on the fringes, now front and center. CNN. https://edition.cnn.com/2016/11/16/politics/what-is-white-nationalism-trnd/.

[18] Il Post. (14 agosto 2017). Breve storia della "alt-right". https://www.ilpost.it/2017/08/14/breve-storiadella-alt-right/

Durante i primi anni di attività, *Cambridge Analytica* collaborò con il *SuperPAC*[19] del repubblicano John Bolton, che alle elezioni midterm del 2014 finanzia, in particolare, la campagna elettorale di Thom Tillis per il seggio del Senato del North Carolina, quella di Tom Cotton per un seggio del Senato in Arkansas e quella di Scott Brown per un seggio del Senato in *New Hampshire*.

In quegli anni la società si occupò, inoltre, della campagna del presidente Keniota Uhuru Kenyatta nel 2013, della campagna di Nerendra Modi alle elezioni generali indiane del 2014 e della campagna del 2015 per la rielezione del presidente uscente della Nigeria Goodluck Jonathan[20].

Nel 2013 *Cambridge Analytica*, alla vigilia delle elezioni politiche del 2013, ha lavorato anche per un partito italiano; tuttavia, non venne mai divulgato quale fosse il partito in questione: le uniche informazioni che sono note riguardano il fatto che il partito aveva avuto successo per l'ultima volta negli anni '80 e che grazie alle proposte della società, elaborate a seguito di una "*audience target*", alle elezioni politiche sarebbe riuscito a raggiungere un risultato oltre le aspettative[21].

Tra il 2015 e il 2016, la società ha lavorato per conto di Leave.EU, un'organizzazione che ha fatto campagna a favore del "*leave*" nel voto per il referendum sull'uscita del Regno Unito dall'Unione Europea.

Stando alle parole dello stesso Alexander Nix, *Cambridge Analytica* si occupava della campagna sui *social media*, assicurandosi che "i messaggi giusti arrivassero agli elettori giusti"[22].

Nel marzo del 2017 il *Guardian* trovò un altro legame tra *Cambridge Analytica* e la campagna a favore della *Brexit*: tra le società che hanno collaborato alla campagna "*Vote Leave*" figura, infatti, anche la società canadese "*AggregateIQ*", il cui presidente,

[19] Un Political action committee (PAC) è un gruppo registrato presso la Federal Election Commission che, con alcune limitazioni, può raccogliere fondi per finanziare campagne politiche, a sostegno o contro i candidati. Un SuperPAC può raccogliere fondi, senza limiti per le donazioni, da persone, società, sindacati e altri gruppi, con l'unico obbligo di agire in maniera formalmente indipendente e di non potersi coordinare direttamente con i candidati o i partiti.
[20] BBC News. Op. cit.
[21] AGI. (26 marzo 2018) Perché non salta fuori il nome del partito italiano per cui lavorò Cambridge Analytica? https://www.agi.it/politica/partito_italiano_cambridge_analytica_intervista_wylie-3684939/news/2018- 03-26/
[22] Reuters. (21 marzo 2018) What are the links between Cambridge Analytica and a Brexit campaign group? https://www.reuters.com/article/us-facebook-cambridge-analytica-leave-eu/what-are-the-linksbetween-cambridge-analytica-and-a-brexit-campaign-group-idUSKBN1GX2IO.

come scoperto dal quotidiano britannico, aveva lo stesso numero di telefono della sede canadese di SCL Group[23].

Alla fine del 2015, *Cambridge Analytica* aveva anche incominciato a lavorare alla campagna di Ted Cruz alle elezioni primarie del partito repubblicano.

Le opinioni sull'efficacia del lavoro di Cambridge Analytica sono divergenti: inizialmente, i responsabili della campagna di Cruz hanno lodato i servizi offerti da Cambridge Analytica, sottolineando come il loro modello psicografico avesse contribuito a far emergere la campagna del Senatore texano[24].

Successivamente, però, alcuni consulenti che hanno lavorato alla campagna di Cruz hanno minimizzato il lavoro della società britannica, dichiarando che si fosse dimostrata poco affidabile[25] e raccontando come non potessero interrompere il contratto che li legava solamente per non perdere l'appoggio di Mercer[26].

Cambridge Analytica ha avuto un ruolo minore e più circoscritto anche nella campagna per un altro candidato alle primarie repubblicane del 2016, Ben Carson: anche in questo caso, lo staff di Carson descrive l'esperienza con la società come "frustrante"[27].

Dopo le sconfitte di Carson, prima, e Cruz, poi, il 23 giugno del 2016 Cambridge Analytica ha cominciato a lavorare alla campagna elettorale del candidato Repubblicano alle elezioni presidenziali statunitensi del 2016, Donald Trump.

Sebbene Nix si sia vantato che ci fosse *Cambridge Analytica* dietro la ricerca, la raccolta dei dati, le analisi, il targeting, la campagna digitale e televisiva e in definitiva la strategia della campagna di Trump[28], il ruolo della società di consulenza è stato pesantemente ridimensionato nel tempo.

---

[23] Doward, J. & Gibbs A. (4 marzo 2017). Did Cambridge Analytica influence the Brexit vote and the US elections? The Guardian. https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridgeanalytica-what-role-brexit-trump.

[24] Hamburger, T. (13 dicembre 2015). Cruz campaign credits psychological data and analytics for its rising success. The Washington Post. https://www.washingtonpost.com/politics/cruz-campaign-creditspsychological-data-and-analytics-for-its-rising-success/2015/12/13/4cb0baf8-9dc5-11e5-bce4-708fe33e3288_story.html?utm_term=.d88e13292410.

[25] Confessore, N. & Hakim, D. (6 marzo 2017). Data Firm Says 'Secret Sauce' Aided Trump; Many Scoff. The New York Times. https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html?_r=1.

[26] Kroll, A. (Giugno-Luglio 2018). Cloak and Data: The real story behind Cambridge Analytica's Rise and Fall. Mother Jones. https://www.motherjones.com/politics/2018/03/cloak-and-data-cambridge-analyticarobert-mercer/

[27] Kroll, A. Ibidem.

[28] Channel 4 News. (20 marzo 2018). Cambridge Analytica: Undercover Secrets of Trump's Data Firm. https://www.youtube.com/watch?v=cy-9iciNF1A

Secondo il *New York Times*, per esempio, *Cambridge Analytica* ha gestito una parte della campagna degli spot televisivi, ha lavorato al fundraising e al targeting delle pubblicità online ed ha svolto sondaggi negli *swing states*[29].

Il giornalista Jonathan Swan ha sottolineato che tutte le persone che hanno lavorato con Cambridge Analytica con cui ha parlato si sono lamentate del lavoro svolto, mentre Kenneth Vogel del *New York Times* ha scritto che i servizi della società di consulenza politica venivano comprati solamente perché visti come prerequisito per ottenere finanziamenti dalla famiglia Mercer[30].

Quel che è certo è che la vittoria contro ogni aspettativa di Trump ha contribuito alla fama della società, che ha approfittato dell'improvvisa pubblicità enfatizzando quello che era in grado di fare.

Il lavoro della società, tuttavia, sarebbe diventato di interesse pubblico solamente qualche anno più tardi, quando nel marzo del 2018 Christopher Wylie, ex dipendente di *Cambridge Analytica*, raccontò alla stampa il suo lavoro e le tecniche che aveva utilizzato[31].

Wylie spiega che nel 2014 Alexsander Kogan, un ricercatore del Dipartimento di Psicologia dell'Università di *Cambridge*, si mise in contatto con il suo collega Michal Kosinski, uno degli ideatori del modello di profilazione psicometrica basato sul metodo *OCEAN*, per proporgli una collaborazione con una società interessata al suo modello e al suo database, l'SCL Group.

Kosinski, insospettito dal fatto che Kogan non potesse rivelargli quale l'utilizzo che la società aveva pianificato di fare del suo modello, cominciò a informarsi sull'SCL Group: non volendo che né lui né il suo gruppo di lavoro fossero coinvolti nelle attività della società, decise di rifiutare l'offerta.

Questo non fermò Kogan, che riuscì a replicare il modello elaborato dai ricercatori del Centro di Psicometria dell'Università di *Cambridge*.

Nel 2015, infatti, Kogan creò un'applicazione dal nome "*thisisyourdigitallife*" (letteralmente, "questa è la tua vita digitale"), che permetteva alle persone di "scoprire"

[29] Confessore, N. & Hakim, D. Op. cit.

[30] Prokop, A. Op. cit.

[31] "[…] il 17 marzo 2018, il Guardian, il New York Times e Channel 4 News hanno pubblicato i risultati di un'indagine durata un anno, nata dalla mia decisione di svelare quanto stava accadendo dentro a Cambridge Analytica e Facebook", Christopher Wylie ne il "Il mercato del consenso. Come ho creato e poi distrutto Cambridge Analytica".

il loro profilo psicometrico dopo aver risposto alle domande di un questionario sui cinque tratti della personalità (*Big Five*).

A chi voleva utilizzare l'applicazione era richiesto di collegarsi attraverso il proprio profilo Facebook e autorizzare gli sviluppatori dell'applicazione ad accedere alle informazioni presenti sul social network.

Cone le informazioni ottenute tramite l'applicazione e le risposte del questionario, Kogan aveva costruito un database di utenti con i loro tratti della personalità e i loro "mi piace": a questo punto, non fu difficile elaborare un modello per la profilazione psicometrica.

Più di 270.000 utenti di Facebook hanno utilizzato l'applicazione nel periodo in cui era attiva, ma Kogan ebbe accesso ai dati personali di un numero ancora maggiore delle persone: all'epoca, infatti, Facebook permetteva agli sviluppatori di applicazioni di ottenere anche le informazioni presenti nei profili degli amici delle persone che utilizzavano un'applicazione, senza che fosse richiesto il loro consenso.

Oltre ai dati dei 270.000 utenti che avevano risposto al questionario, quindi, Kogan ottenne anche i dati dei loro amici, per un totale di informazioni su circa 87 milioni di utenti[32],[33].

Se la raccolta di dati non era contro i termini di Facebook, non li rispettava, invece, la condivisione con terze parti.

Per questo, quando Facebook scoprì il passaggio di dati, intimò *Cambridge Analytica* di cancellarli, senza mai però rilasciare una dichiarazione pubblica.

Secondo quanto dichiarato da Wylie, inoltre, *Facebook* non si impegnò particolarmente per recuperarli, finché il 16 marzo 2018, qualche giorno prima della pubblicazione delle interviste dell'ex dipendente di *Cambridge Analytica*, *Facebook*, improvvisamente, sospese dal *Social Network* gli account degli individui delle società legate a questa vicenda.

[32] Wagner, K. (17 marzo 2018). Here's how Facebook allowed Cambridge Analytica to get data for 50 million users. Recode. https://www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trumpexplained-user-data.

[33] Fonti stampa inizialmente avevano calcolato che il numero di utenti coinvolti fosse inferiore, intorno ai 50 milioni, ma una nota pubblicata da Facebook ha precisato che gli utenti esposti sono stati 87 milioni. Si veda Schroepfer, M. (4 aprile 2018). Facebook Newsroom. An update on our plans to restrict data access on Facebook. https://newsroom.fb.com/news/2018/04/restricting-data-access/

Viste le responsabilità di Facebook e la sua scarsa proattività nel risolvere la questione, il quotidiano online Vox sottolinea che questo è "più uno scandalo Facebook, che uno scandalo Cambridge Analytica"[34].

Qualche giorno dopo la pubblicazione delle interviste di Wylie, *Channel 4 News*, un programma televisivo britannico, ha pubblicato una serie di inchieste frutto di quattro mesi di indagini su Cambridge Analytica.

In uno dei video trasmessi, Nix spiega a un potenziale cliente quali servizi possono offrirgli per screditare un politico, come per esempio tentare di corromperlo e riprenderlo in caso accettasse la tangente, o ancora mandare delle prostitute a casa sua[35].

A causa della trasmissione delle inchieste, Nix viene sospeso.

La sua situazione si è ulteriormente aggravata quando alcuni giornali hanno scoperto che potrebbe essere potenzialmente coinvolto nello "scandalo e-mail", dal momento che, qualche giorno prima di siglare il contratto con la campagna di Donald Trump, Nix aveva contattato Julian Assange, caporedattore di *Wikileaks*, per ottenere le e-mail sottratte dagli account di personalità in vista del Partito Democratico[36].

Sia Nix che Assange hanno negato che ci sia stato alcun accordo tra i due.

A causa del peggioramento della sua reputazione e della sua situazione finanziaria (e secondo alcuni in un tentativo di non affrontare le indagini[37]), il 4 maggio 2018 Cambridge Analytica è costretta a cominciare le procedure per dichiarare bancarotta.

Tutte le sue figure chiave, però, si sono spostate in una nuova società, Emerdata: oltre a Jennifer e Rebekah Mercer, figlie di Robert Mercer, entrate nella società con un ruolo nella direzione, ci sono anche Julian Wheatland, presidente di SCL, e Alexander Tayler, CEO di Cambridge Analytica dopo la sospensione di Nix.

---

[34] 5 Chang, A. (2 maggio 2018) The Facebook and Cambridge Analytica scandal, explained with a simple diagram. Vox. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridgeanalytica-trump-diagram

[35] Channel 4 News. Op. cit.

[36] Ballahus, R. (25 ottobre 2017). Trump-liked company reached out to Wikileaks on hacked emails. The Wall Street Journal. https://www.wsj.com/articles/wikileaks-assange-says-he-rejected-overture-fromtrump-linked-group-1508961298.

[37] Simonetta, B. (5 maggio 2018). Cambridge Analytica fallisce, ma i personaggi chiave si spostano in Emerdata. Il Sole 24 Ore. https://www.ilsole24ore.com/art/tecnologie/2018-05-05/cambridge-analyticafallisce-ma-personaggi-chiave-si-spostano-emerdata-192526.shtml?uuid=AEXw0ijE&refresh_ce=1.

1.2 Sviluppo della vicenda e regolamentazione

Le Big Tech Companies che dominano l'attuale panorama digitale, come Facebook, Yahoo, Google e Amazon, basano la propria attività sulla circolazione delle informazioni in uno spazio apparentemente privo di confini geografici come quello della Rete; a tal proposito, il primo e rilevante aspetto da chiarire in merito al Regolamento europeo non può che riguardare l'ambito di applicazione delle nuove regole.

Negli anni abbiamo assistito la portata della condivisione e della raccolta dei dati raggiungere livelli talmente elevati su scala mondiale da richiedere un rinnovamento ed ampliamento dell'orizzonte di riferimento dell'efficacia delle nuove norme in materia.

Esigenza che emerge chiaramente nel nuovo quadro normativo e risulta pienamente soddisfatta dall'agire congiunto dell'art.3 e tenendo in considerazione gli artt. 22,23,24.

Fermo restando che le nuove regole hanno ad oggetto esclusivamente dati personali delle persone fisiche, con riferimento all'ambito di applicazione territoriale, infatti, il testo specifica che le norme si applicano non solo ai casi in cui il titolare o il responsabile del trattamento siano stabiliti nell'Unione Europea, "indipendentemente dal fatto che il trattamento sia effettuato o meno all'interno dei confini europei", ma anche a tutte quelle attività che coinvolgono dati personali relativi a soggetti che si trovano nell'Unione ed il cui titolare o responsabile non sia stabilito in uno degli Stati europei.

In questo caso, i trattamenti in questione debbono riguardare oltre all'offerta di beni o alla prestazione di servizi ai suddetti interessati all'interno del territorio europeo, indipendentemente dall'obbligatorietà di un pagamento dell'interessato, anche il monitoraggio del loro comportamento nel caso in cui abbia luogo nell'Unione.

Il Regolamento con l'art.3, quindi, recependo l'orientamento della Corte di Giustizia e del Gruppo Articolo 29, introduce un importante elemento di rottura rispetto al passato attraverso l'ampliamento del principio di stabilimento che dominava la precedente normativa in materia[38].

[38] La determinazione dell'ambito territoriale di applicazione della direttiva n.95/46/CE ruotava essenzialmente intorno al tradizionale principio di stabilimento. Ai sensi dell'art. 4, par.1, lett. a) le norme nazionali di recepimento della direttiva operavano in caso di trattamenti effettuati "nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro". In tal senso, l'applicabilità del quadro normativo dipendeva dallo svolgimento di un'attività realizzata da un'impresa stabilmente presente all'interno di uno degli Stati europei. Nel caso di soggetti extra-europei, le regole operavano solo nel caso il responsabile disponesse di "strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro". Con lo straordinario incremento

In un'era contraddistinta dal carattere transfrontaliero dei servizi erogati online, non è, o almeno apparentemente non è solo il luogo di stabilimento, infatti, a determinare l'applicabilità della norma, ma è il bene tutelato che diventa fonte di legittimazione della relativa applicabilità: il solo fatto che i dati oggetto di analisi siano relativi a soggetti che si trovano nell'Unione o i cui comportamenti si realizzino all'interno dei confini europei impone il rispetto della normativa in questione indipendentemente dal luogo dello stabilimento del titolare o del responsabile dei dati.

Così, all'interno di un universo tendenzialmente infinito come quello della Rete, il legislatore è arrivato a delimitare un'area "europea" di tutela dei dati personali che non si piega alla logica del fluire incessante delle informazioni, ma che è completamente dedicata ai cittadini europei indipendentemente dal luogo in cui il trattamento dei dati viene materialmente eseguito.

L'applicazione delle regole, infatti, esula dai confini nazionali, legittimata dal carattere a-territoriale di Internet, e trova piena giustificazione nel fine ultimo di tutela dell'identità personale dei singoli utenti.

A rafforzare l'applicabilità del nuovo Regolamento, in particolare, alla piattaforma *Facebook* vi è poi la previsione, ripresa anche dal considerando articolo 23, secondo cui la valutazione deve tenere conto della destinazione d'uso dei beni e dei servizi dell'azienda "indipendentemente dal fatto che vi sia un pagamento correlato".

In questo caso, è evidente che si faccia riferimento al funzionamento dei grandi Social Network e in primis alla piattaforma oggetto di analisi che fanno uso dei dati personali sfruttando l'apparente gratuità dei servizi erogati.

---

dell'utilizzo della rete Internet e, soprattutto, dei social network che della a-territorialità fanno il proprio punto di forza, tale approccio in vista di una effettiva tutela dei dati personali è risultato via via sempre meno efficiente. Dal campo di applicazione della normativa sfuggivano, infatti, proprio i grandi colossi extra-europei che da anni dominano il panorama mondiale del mercato delle comunicazioni. Supportato dal parere n. 8/2010 dell'Article 29Working Group e dalle sentenze "Google Spain" e "Weltimmo" entrambe orientate ad un'estensione dell'applicabilità delle norme europee al di là del principio di stabilimento, il legislatore europeo ha ampliato l'ambito di efficacia della nuova disciplina, dichiarando in maniera specifica al considerando 23) che tale scelta è finalizzata ad evitare che una persona fisica possa essere privata dalla protezione cui ha diritto ogni volta che il trattamento venga effettuato da un soggetto non stabilito dell'Unione e si connetta all'offerta di beni o servizi indipendentemente dal fatto che vi sia pagamento correlato ovvero al monitoraggio del comportamento di interessati che si trovano nell'Unione. Inoltre, rileva sottolineare che il Regolamento chiarisce che la nozione di stabilimento affermando al considerando 22) che lo stesso "implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica". Sul punto cfr. la sentenza "Google Spain", Google Inc./Agencia Española de Protección de Datos, (AEPD) and Mario Costeja González", causa C-131/12; Sentenza Weltimmo s. r. o/ Nemzeti Adatvédelmi és Információszabadság Hatóság, causa C-230/14; ARTICLE 29DATA PROTECTION WORKING PARTY,Opinion 8/2010on applicable law (WP179), adottato il 16 dicembre 2010; PIZZETTI F., Privacy e il diritto europeo alla protezione dei dati personali –dalla Direttiva 95/46 al nuovo Regolamento europeo, op. cit.

La riferibilità a tale piattaforma e a quelle che condividono con essa un'attività di profilazione è ricavabile anche dalla lettura del considerando 24) in cui si specifica che "per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su Internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali".

Le tecniche di aggregazione dei dati personali, pertanto, se rientranti nell'attività tipica del soggetto titolare impongono a quest'ultimo l'assoggettamento al nuovo quadro di disciplina[39].

1.3 Il modello di accountability del titolare del trattamento dei dati personali applicato allo scandalo "Cambridge Analytica"

Come descritto in precedenza, la vicenda ha avuto origine non da una violazione dei sistemi di sicurezza della piattaforma, bensì dalla divulgazione non autorizzata dei dati degli utenti a favore di terzi da parte di una società che operava con Facebook.

Un trasferimento resosi possibile, a detta dei soggetti coinvolti dalla mancata implementazione di adeguate tecniche di controllo ulteriori e successive con riferimento al flusso dei dati acquisiti dai partner commerciali che con la piattaforma operano e cooperano.

In tal senso, la violazione perpetuata non è da individuarsi nell'illecito utilizzo dei dati da parte dello sviluppatore dell'app, bensì nella successiva trasmissione degli stessi ad una società terza la cui attività primaria, per di più, consiste nella profilazione degli utenti a fini politici.

A peggiorare ulteriormente la situazione già di per sé grave, vi è stata la decisione del CEO di Facebook, Mark Zuckerberg, di non avvertire immediatamente le autorità

[39] Il considerando 23) del GDPR ritiene rilevanti, a tale scopo, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione.

competenti di quanto fosse accaduto, nonostante la violazione fosse nota già dal 2015, ma di limitarsi a chiedere alla società di profilazione politica la distruzione delle informazioni ottenute in maniera illecita, senza per altro averne avuto successiva conferma[40].

In regime di piena applicazione del Regolamento europeo, tale mancata sollecita comunicazione avrebbe di per sé integrato una grave violazione della normativa perché in contrasto con il sistema degli obblighi generali previsti a carico del titolare del trattamento e, segnatamente, con il dovere di notifica all'autorità di controllo di cui all'art. 33.

La disposizione in questione impone al soggetto di attivarsi entro 72 ore, e in ogni caso senza ingiustificato ritardo, specificando la natura della violazione, le categorie di dati coinvolti ed il presunto numero di soggetti interessati, nonché di descrivere le possibili conseguenze dannose.

La tempestività, infatti, è ritenuta vitale ai fini della limitazione dei danni che potenzialmente possono abbattersi sui soggetti, in quanto la dilazione dei tempi di intervento rischia di depotenziare l'efficacia dei rimedi previsti, esacerbando situazioni già estremamente critiche connesse alla perdita di controllo dei propri dati personali[41].

È evidente che con la mancata osservanza di tale sistema di regole viene ad incrinarsi quella rete di cooperazione attiva tra autorità di controllo e titolari del trattamento, la cui creazione il Regolamento ritiene cruciale per la tutela attuale delle identità personale degli interessati all'interno di un panorama estremamente mutevole e complesso.

Accanto alla violazione dei suddetti obblighi di comunicazione, in caso di applicazione del nuovo quadro normativo sarebbe risultato violato anche l'art. 34, che, come è noto, impone al titolare di informare in maniera dettagliata gli interessati circa l'avvenuta violazione delle proprie informazioni.

---

[40] *Zuckerberg*, in occasione delle due udienze presso il Congresso americano, ha pubblicamente ammesso di non aver effettuato alcun controllo successivo circa l'effettiva avvenuta distruzione dei dati illecitamente sottratti e trasferiti dalla società che ha sviluppato l'applicazione a *Cambridge Analytica*.

[41] Come esplicitamente indicato dal considerando 85) del Regolamento "una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata".

Potendosi agevolmente ritenere che la sottrazione di dati riguardanti più di 80 milioni di profili possa ricondursi al novero dei casi che il legislatore europeo ritiene "suscettibili di presentare un rischio elevato per i diritti e le libertà delle persone fisiche" e non potendosi, al contempo, considerare applicabili le eccezioni di cui al paragrafo 3 del medesimo art. 34, il social network, contrariamente a quanto effettivamente accaduto, avrebbe dovuto obbligatoriamente informare tutti gli utenti coinvolti in maniera dettagliata e sollecita.

Anche in questo caso, il mancato rispetto di tale previsione tradisce in pieno lo spirito della normativa che mira a garantire agli interessati un pieno e consapevole controllo dei propri dati anche attraverso la costruzione di un clima di fiducia tra utenti e titolari.

1.4 Sanzioni applicabili per la violazione del Regolamento

In un quadro di disciplina fortemente incentrato sul processo di responsabilizzazione dei titolari e parallelamente sul rafforzamento del controllo dei soggetti sui propri dati personali, tuttavia, l'analisi trova il suo punto saliente non tanto nel sistema di rimedi ex post implementati dal social network, quanto nella valutazione degli strumenti tecnici ed organizzativi predisposti preventivamente al fine di evitare il realizzarsi di tali ingerenze esterne alla sfera privata dei propri utenti.

Come analizzato precedentemente, il nuovo Regolamento punta a stimolare un atteggiamento proattivo da parte di tutti i titolari, orientandoli verso un'organizzazione delle proprie attività che sia completamente orientata al rispetto della privacy, intesa come principio ispiratore in grado di permeare concretamente ed interamente l'intera filiera di utilizzazione dei dati, dal momento della loro raccolta a quello finale della loro conservazione ed eliminazione.

Analizzata in tale ottica, il modello posto in essere dalla piattaforma oggetto di analisi non rispecchierebbe evidentemente il sistema definito dal legislatore europeo. In primis, in una situazione di piena vigenza della nuova normativa, il social network, realizzando "una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e

sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche" avrebbe dovuto necessariamente procedere ad una valutazione d'impatto del trattamento sui diritti fondamentali ai sensi dell'art. 35 paragrafo 3, lett. a) del Regolamento con conseguente documentazione di tutte le misure tecniche ed operative adottate al fine di prevenire situazioni di violazione della sfera di identità degli utenti.

Inoltre, è indubbio che le profilazioni che il social network realizza a partire dai dati e dalle attività di condivisione effettuate dai propri utenti prevedano l'impiego continuo di nuove tecnologie, il cui impatto sui diritti e sulle libertà fondamentali delle persone coinvolte non è sempre prevedibile apriori.

L'utilizzo di tecniche sempre più sofisticate avrebbe obbligato la piattaforma, ai sensi dell'art. 36, a consultare l'autorità di controllo al fine di individuare i possibili rischi connessi e stabilire sistemi di tutela condivisi.

Infine, la realizzazione di un'attività di trattamento come quella realizzata da Facebook che per propria natura, ambito di applicazione e/o finalità, include il monitoraggio regolare e sistematico degli interessati su larga scala e spesso anche di categorie di dati particolari ai sensi dell'art. 9, avrebbe imposto inevitabilmente anche la nomina di un DPO (Data Protection Officer), con compiti di collaborazione e di supporto tecnico–giuridico alle decisioni relative alla tutela dei dati personali.

L'individuazione di tale figura connessa al rispetto degli obblighi poc'anzi menzionati, avrebbe consentito alla piattaforma di realizzare una prima e soprattutto incisiva rete di controlli corroborati da momenti di condivisione e di sostegno da parte delle autorità di controllo, favorendo l'implementazione di strumenti di tutela ex ante valutati in una duplice dimensione, privata da un lato, pubblica dall'altro, in uno spirito di piena collaborazione nell'interesse degli utenti.

Riassumendo, alla luce della prima parte dell'analisi, in un regime di piena applicazione del Regolamento, la piattaforma sarebbe stata riconosciuta non rispettosa del nuovo sistema di accountability del titolare previsto dal Capo IV del Regolamento.

Questo avrebbe comportato l'immediata applicazione del più rigoroso quadro di sanzioni introdotto dalla nuova disciplina, con la previsione ai sensi dell'art. 83, paragrafo 4, di pene amministrative sino a 10.000.000 di EURO, ovvero fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, a cui debbono aggiungersi

le eventuali ulteriori misure di carattere deterrente riconosciute alle autorità di controllo dall'art. 58.

2. La profilazione dell'utente

2.1 Tecniche di profilazione usate da Cambridge Analytica e test di personalità: "scala dei Big Five"

Con il termine "profilazione" si fa riferimento a quell'insieme di attività realizzate attraverso processi, software ed algoritmi che raccolgono ed elaborano dati sugli utenti che utilizzano un determinato servizio per poi raggrupparli a seconda del loro comportamento.

In ambito commerciale, questa tecnica è largamente impiegata per fornire servizi personalizzati come ad esempio la pubblicità comportamentale; inoltre, è utile anche per ottenere analisi accurate dei potenziali clienti.

Secondo il GDPR (General Data Protection Regulation), dell'Unione Europea per profilazione si intende "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di questi ultimi per valutare determinati aspetti personali relativi ad una persona fisica (…)".

Nella realtà, ai fini puramente commerciali si tende a fare uso di qualsiasi tipologia di informazione reperibile online creando una profilazione particolarmente dettagliata quasi sempre lesiva o al limite della normativa concernente la privacy.

È su questo terreno che hanno trovato applicazione le tecniche di profilazione utilizzate dalla società di consulenza britannica Cambridge Analytica, la quale, attraverso il *data mining* e l'analisi dei dati, attuava comunicazioni strategiche mirate per scopi elettorali.

Per comprendere a pieno la vicenda, bisogna tornare nel 2008, quando Michal Kocinski, un esperto di psicologia comportamentale, ottenne l'accesso ad un dottorato di ricerca nel Centro di psicometria del Campus dell'Università di Cambridge.

Li, con il suo collega David Stillwell, realizzò l'applicazione "my personality" che attraverso la piattaforma Facebook proponeva agli utenti di compilare un questionario

psicometrico basato su un modello a cinque fattori della personalità, chiamato modello dei "Big Five".

Le ricerche che hanno portato all'elaborazione del modello a cinque fattori della personalità sono identificate dall'utilizzo dell'approccio lessicale, alla base del quale vi è l'assunzione che le più rilevanti caratteristiche della personalità sono state codificate nel linguaggio, che dunque fornisce dei vocaboli per descrivere una serie ampia ma finita di attributi.

Uno tra i primi lavori ad utilizzare quest'approccio fu quello di Allport e Odbert, che nel 1936 catalogarono tutte le parole che potevano essere utilizzate per descrivere il comportamento di un individuo, arrivando a costruire un elenco contenente 18.000 vocaboli.

Per faro ordine in questo "incubo semantico", i due studiosi ordinarono i descrittori dividendoli in quattro categorie: gli stati d'animo, i giudizi sulla condotta, le caratteristiche fisiche, e i tratti della personalità, definiti come "tendenze determinanti generalizzate, consistenti e stabili".

Già in uno studio precedente Allport aveva individuato otto criteri per definire un tratto della personalità e distinguerlo, così, da inclinazioni, predisposizioni, tendenze e riflessi: tra questi, lo studioso notava che i tratti sono dinamici e determinativi, sono solo relativamente indipendenti tra loro e non si rispecchiano necessariamente in tutte le azioni che compiono gli individui.

Successivamente al primo studio di Allport e Odbert, si sviluppò un consistente filone di ricerca sui tratti della personalità: tuttavia, la mancanza di una visione comune creò un'intricata massa di concetti, scale e misurazioni.

Cattel, in una serie di studi pubblicati tra il 1943 e il 1945[42], selezionò 35 variabili della personalità tra i vocaboli collocati da Allport e Odbert nella categoria tratti della personalità.

Fiske operò un'ulteriore riduzione, arrivando a 22 fattori fondamentali: è a partire da questi che le ricerche di Tupes e Christal evidenziarono cinque variabili "Relativamente forti e ricorrenti".

Questa struttura diventò la base per gli studi successivi e venne man mano perfezionata grazie al contributo di altri studiosi.

[42] Cattell, R. B. (1943); Cattell, R. B. (1945a); Cattell, R. B. (1945b).

Il modello, nelle sue diverse sfumature, divenne noto come “Big Five”: le cinque variabili identificate rappresentano la personalità al più alto livello di astrazione e ognuna delle dimensioni riesce a riassumere un alto numero di specifiche e distinte caratteristiche della personalità.

Il modello si basa su quattro assunti della natura umana: i tratti della personalità esistono e sono misurabili, il valore dei tratti varia tra gli individui, le cause del comportamento sono radicate nell’individuo, le persone capiscono sé stesse e gli altri.

Come già accennato, la versione che si è imposta è quella elaborata da Goldberg all’inizio degli anni Novanta, mentre lo sviluppo di questionari per misurare i tratti e delle relative batterie di domande si deve soprattutto a McCrae e Costa.

Esistono diversi tipi di questionari, a seconda della precisione richiesta e delle necessità: ne esistono con lunghezza diversa, intesa come numero di domande, con diverse tipologie di domande (possono chiedere all’intervistato di indicare quanto si sente rappresentato da un aggettivo oppure da una definizione) e con numero di risposte variabili.

2.2 La profilazione psicometrica: ricostruzione dei tratti dell’attività online

Gli studiosi si sono interrogati per cercare di costruire un modello predittivo del profilo psicometrico di una persona, senza che, cioè, fosse necessario sottoporla al test del Big Five.

Il punto di partenza per costruire un modello di questo tipo sono i social network, definiti come “servizi informatici online che permettono la realizzazione di reti sociali virtuali, siti internet o tecnologie che consentono agli utenti di condividere contenuti testuali, immagini, video e audio e di interagire tra di loro”.

Oggigiorno sempre più utenti condividono contenuti sul web: per questa ragione, i social network, oltre alle informazioni strutturate come i dati sociodemografici (età, genere, lingua, provenienza), contengono informazioni sugli utenti sotto forma di contenuti testuali (post, commenti, aggiornamenti sugli stati) o audiovisivi (foto e video): riflettono la personalità “offline” degli utenti integrando queste diverse fonti di informazioni personali.

È stato dimostrato, infatti, che i social network costituiscono dei contesti sociali estesi in cui gli utenti esprimono la propria personalità, al punto che gli stessi utenti riescono a farsi un'idea accurata della personalità degli altri utenti sulla base dei loro profili online.

Dunque, come chiaramente sintetizzato da Kosinksi, "la migrazione degli esseri umani nel mondo digitale rende possibile basare le predizioni circa le loro informazioni personali sulle tracce digitali che lasciano".

Con il modello che hanno elaborato, riescono a desumere diverse caratteristiche degli utenti partendo dalle pagine a cui hanno messo "mi piace" su Facebook.

Il "mi piace" ("Like" nella versione inglese) è un meccanismo presente su Facebook che gli utenti utilizzano per esprimere il loro gradimento nei confronti di un contenuto pubblicato sul social network.

Una pagina Facebook è il profilo pubblico di una società, un brand, di un'organizzazione, di una personalità o di una causa: un utente che mette "mi piace" a una pagina, ne diventa "fan", e da quel momento riceverà informazioni e aggiornamenti sui suoi contenuti.

Le pagine possono anche esprimere un modo di essere o un tratto comune: in questi casi, il "mi piace" potrebbe anche indicare che l'utente condivide gli stessi valori della pagina.

Per l'elaborazione di questo modello vennero, prima di tutto, sottoposti circa 58mila volontari ad un questionario che comprendeva una parte con domande sociodemografiche ed un test psicometrico.

A queste persone veniva chiesto di poter avere accesso alle informazioni condivise sul loro profilo Facebook, inclusi i "mi piace".

Per ridurre l'enorme numero di "mi piace" venne utilizzata la c.d. decomposizione ai valori singolari.

Gli utenti venivano quindi rappresentati in una matrice incrociata con le pagine Facebook: per ogni utente, il valore in corrispondenza di una pagina è uguale a 1 se l'utente ha messo "mi piace" alla pagina, 0 in caso contrario.

Dai "mi piace" si possono predire attributi espressi sia sotto forma di variabili dicotomiche, vale a dire variabili che rappresentano solamente due modalità, sia sotto forma di variabili numeriche, il cui valore è indicato, cioè, da un numero.

Per le variabili dicotomiche hanno utilizzato regressioni linguistiche, mentre per quelle numeriche regressioni lineari.

Rientrano nella prima categoria informazioni come il genere (maschio/femmina), l'origine etnica (caucasico/afroamericano), la relazione sentimentale (single/in una relazione), la religione (cristiano/musulmano) e persine se si è fumatori (fumatore/non fumatore).

Per esempio, l'origine etnica può essere ricostruita con un'accuratezza del 95% e la posizione politica (democratico/repubblicano) con un'accuratezza dell'85%.

Dai "mi piace" si possono desumere anche variabili numeriche quali tratti e attributi misurabili, come l'età, la soddisfazione della vita, l'intelligenza e i cinque tratti della personalità del modello a cinque fattori.

Un "mi piace" alla pagina di Michael Jordan, ad esempio, è indice di valori maggiori nella dimensione dell'estroversione, mentre un utente che ha messo "mi piace" alla pagina di Leonardo Da Vinci ha più possibilità di essere mentalmente aperto (Kosinski et al, 2013).

Secondo Kosinski, uno dei ricercatori del Centro di Psicometria dell'Università di Cambridge, 70 "mi piace" bastano per riuscire a conoscere un numero di informazioni su una persona maggiore di quante ne conoscano i suoi amici, 150 "mi piace" sono abbastanza per saperne di più dei suoi genitori e con 300 "mi piace" si sa, addirittura, più di quanto ne sappia il suo partner.

Con più di 300 "mi piace", si supera la conoscenza della persona che ha la persona stessa.

2.3 Big Five: i cinque tratti della personalità

I tratti della personalità, come abbiamo già detto, sono dunque misurabili: ogni tratto può assumere un valore all'interno di un asse compreso tra due estremi.

La personalità di un individuo è data dal valore assunto da ognuno dei tratti.

I tratti prendono il nome da uno dei due estremi della scala di valori con cui si misurano (*OCEAN): Openess to experience (*apertura mentale), conscientiousness

(coscienziosità), extraversion (estroversione), agreeableness (amicalità), neuroticism (nevroticismo)[43].

Apertura mentale

Un valore alto in questa dimensione è correlato positivamente con la creatività, la curiosità e l'anticonformismo.

Gli individui che hanno una mentalità più aperta sono tolleranti, fantasiosi e apprezzano le novità.

Altri ne sottolineano l'originalità e la profondità o ancora il fatto che siano maggiormente disposti a entrare in contatto con nuove informazioni e fare nuove esperienze.

Al contrario, gli individui con valori bassi in questo tratto sono persone realiste, pratiche e tradizionali, che preferiscono ciò che conoscono rispetto all'ignoto.

Diversi studi hanno dimostrato come l'apertura mentale sia associata con il voto per candidati e partiti liberali e che un valore alto in questo tratto sia collegato a tassi di partecipazione politica più alti, che si tratti di un voto o nei casi di manifestazioni di protesta.

Sugli individui mentalmente aperti, inoltre, la persuasione ha un maggiore effetto.

Un alto valore di questa dimensione porta anche a preferire politiche, economiche e sociali, di stampo liberale e ad avere un maggiore senso di efficacia politica, cioè "la sensazione che l'azione politica individuale abbia, o possa avere, un impatto sul processo politico, cioè che valga la pena esercitare i propri doveri civici".

Gerber et al. (2011c) indicano che gli individui mentalmente aperti non leggono molto i giornali, ma preferiscono informarsi guardando la televisione (in particolar modo prediligono i programmi nazionali a quelli locali) o, in maniera ancora maggiore, su internet.

[43] Le traduzioni dei nomi delle dimensioni sono quelle utilizzate, tra gli altri, in Caprara, G.V., Barbaranelli, C. e Borgogni, L. (1993).

Coscienziosità

Gli individui coscienziosi cercano di tenere sotto controllo il mondo che li circonda, seguono le norme sociali e le regole, organizzano nel dettaglio la loro vita, pensano molto prima di agire.

Mondak e Haplerin (2010) aggiungono che tali individui sono persone ligie al dovere, prudenti, conformi e affidabili.

Altri tratti distintivi secondo Jost et al (2009) sono la loro efficienza, la loro laboriosità, la loro precisione, la loro attendibilità, la loro capacità a programmare e a restare concentrati sugli obiettivi.

Tutti gli autori, inoltre, sono concordi nel dire che un alto livello di coscienziosità si traduce in un maggiore senso di responsabilità.

Per Cantador et al. (2013) i coscienziosi hanno un senso dell'autodisciplina molto sviluppato e cercano di realizzare gli obiettivi che si sono posti.

Individui poco coscienziosi, invece, sono caratterizzati da un approccio spontaneo alla vita, da una maggiore tolleranza, da una maggiore affabilità e da una maggiore flessibilità.

Mondak e Haplerin (2010) sottolineano che spesso sono pigri, impulsivi e inaffidabili, mentre Jost et al. (2009) indicano che sono disorganizzati e negligenti.

La coscienziosità è politicamente legata a preferenze conservatrici, sia per i candidati e i partiti che per le politiche economiche e sociali, mentre sugli effetti che ha sulla partecipazione politica i risultati delle ricerche sono più discordanti.

Per quanto riguarda invece il modo di informarsi, Gerber et al. (2011c) scoprono che gli individui più coscienziosi si informano principalmente guardando la televisione, nello specifico i talk show politici, e che prediligono i telegiornali locali a quelli nazionali.

Dumitrescu e Blais (2010), infine, scoprono che gli individui coscienziosi sono più propensi ad esprimere un voto strategico.

Amicalità

L'amicalità è correlata con l'essere collaborativi, altruisti e comprensivi. Individui comprensivi sono più portati a essere parte di gruppi, a fidarsi degli altri, a evitare i

conflitti e a cercare di risolverli, sono disponibili, amichevoli, benevoli, compassionevoli e generalmente bonari.

Secondo alcuni sono anche modesti e rispettosi. Coloro i quali hanno valori bassi di amicalità sono, invece, più concentrati su sé stessi, meno disposti a cercare compromessi e meno ingenui.

Tendenzialmente, inoltre, sono meno interessati a soddisfare le aspettative sociali o a rispettare le convenzioni. Sono più assertivi, litigiosi, critici, rigidi, distaccati, schietti, testardi, scettici, orgogliosi e competitivi.

L'amicalità è associata con la preferenza per candidati e partiti liberali, ma anche in questo caso non ha un chiaro effetto sulla partecipazione politica, con alcuni studi che sostengono abbia effetti riduttivi e altri che ne abbia di accrescitivi.

Gli individui amicali, inoltre, hanno preferenze liberali sul piano economico e conservatrici su quello sociale.

Gli amicali si informano guardando la televisione, su internet o leggendo i giornali, con una leggera preferenza per la prima: in televisione guardano i daytime talk20 e preferiscono i programmi locali a quelli nazionali.

Come i coscienziosi, anche gli amicali sono più portati a un voto strategico.

Estroversione

Come i coscienziosi, anche gli amicali sono più portati a un voto strategico.

Gli individui estroversi hanno un "approccio energetico al mondo materiale e sociale".

All'estroversione sono legate caratteristiche come la socievolezza e la positività: un'alta estroversione è infatti presente nelle persone più loquaci, entusiaste ed espansive.

Gli estroversi fanno amicizia facilmente, preferiscono essere circondati da persone, hanno piacere a essere al centro dell'attenzione e cercano di esprimere emozioni positive, sono inoltre esuberanti.

L'estroversione è anche correlata con una maggiore capacità di leadership.

Le persone introverse sono, solitamente, più solitarie e riservate e cercano, per queste ragioni, di trovarsi in contesti caratterizzati dall'assenza, o poca presenza, di stimoli esterni. Sono silenziosi, timidi e seri.

Gli studi non sono riusciti ad attribuire con certezza una preferenza ideologica agli estroversi.

L'estroversione, inoltre, non è sempre un fattore predittivo della partecipazione politica, ma in alcune ricerche è stato associato con tassi di partecipazione più alti. Gli estroversi hanno preferenze conservatrici sulle politiche economiche e su quelle sociali e mostrano avere un maggiore senso di efficacia.

L'estroversione è correlata positivamente con la lettura dei giornali e negativamente con l'informarsi su internet. Gli estroversi guardano talk show politici e daytime talk.

Nevroticismo

A questo tratto ci si riferisce anche con il nome di "stabilità emotiva", riferendosi all'estremo opposto nella dimensione.

Le persone che presentano un alto valore di nevroticismo sono negative, ansiose, nervose, tristi, tese e inquiete.

I nevrotici sono molto emotivi e sensibili, inclini a essere agitati, nonché lunatici e volubili e più inclini a trovarsi sotto stress, a sentirsi in colpa e arrabbiarsi.

Le persone più stabili emotivamente, invece, sono più calme, rilassate e sicure di sé e riescono a gestire lo stress con maggiore facilità.

La stabilità emotiva è associata a preferenze per candidati e partiti conservatori, e anche per le politiche sociali ed economiche conservatrici, ma non ha chiari effetti sulla partecipazione politica.

È più facile persuadere gli individui meno stabili emotivamente con gli appelli al voto che fanno leva sulla pressione sociale.

Gli individui più stabili emotivamente si informano su internet e guardano talk show politici.

3. Social advertising: come si fa pubblicità sui social network

3.1 Facebook ed Instagram advertising

La pubblicità, per come la conosciamo noi, risale al 1479, quando l'editore inglese W. Caxton decide di pubblicizzare i propri libri.

Ma per il primo annuncio pubblicitario mezzo stampa si deve attendere il 1630, con la nascita di un vero e proprio servizio pubblicitario, grazie all'idea del parigino T. Renaudot che apre un ufficio e fonda una gazzetta per raccogliere e pubblicare annunci pubblicitari a pagamento.

Nel corso della storia recente, più precisamente negli ultimi 60 anni, poi, abbiamo visto il susseguirsi di diverse tipologie di pubblicità; dal classico Carosello alle pubblicità sui social network.

Si badi bene che il modo di fare pubblicità nel tempo è cambiato radicalmente; il termine pubblicità, nel senso italiano del termine, deriva da "pubblico" ed assume quindi il semplice significato di "rendere noto" ciò che fino a quel momento non lo era e tutto ciò, ancora oggi, viene attuato da molte aziende.

Ma non solo, se consideriamo il termine "pubblicità" in inglese, letteralmente "advertising", qui il significato viene stravolto.

Infatti, il termine "advertising" privilegia il processo di natura commerciale finalizzato al raggiungimento del destinatario del messaggio; spesso questo processo viene fatto attraverso la manipolazione dell'utente, il quale ignaro della personalizzazione della pubblicità stessa, è indotto a pensare che quel prodotto o quel politico da votare, rispecchino a pieno i propri valori.

Con l'avvento dei social network, come dicevamo, si è iniziato a prediligere maggiormente l'"advertising", rispetto alle classiche pubblicità.

Oggi ciò che io posso vedere nel mio feed di Facebook, o su una storia di Instagram, non è ciò che potrebbe vedere mio padre, mia sorella o un amico mio, e questo in quanto il processo di creazione di un'inserzione pubblicitaria sui social è molto sofisticato.

Quotidianamente, chiunque sia iscritto ad un social network, in particolare Facebook ed Instagram, inserisce in rete un numero elevatissimo di dati personali.

Dal momento della registrazione, in cui ci vengono rivolte domande generali per conoscere i nostri dati anagrafici, alla pubblicazione di foto e post, consentiamo ai colossi del web di trattare i nostri dati personali.

Dati che, nella stragrande maggioranza se non totalità dei casi vengono rivenduti alle società di tutto il mondo per le finalità di marketing più disparate.

La raccolta di dati permette di delineare un profilo di gusti, scelte, carattere e preferenze della nostra persona e di assoggettarci ad analisi statistiche o di mercato o a ricevere campagne pubblicitarie mirate.

Addirittura, i dati personali pubblicati sui siti di social network possono essere usati dai terzi per scopi pericolosi e lesivi, che possono comportare gravi rischi come il furto di identità, il danno economico, la perdita di opportunità commerciali e di possibilità di impiego e, per finire, pericoli per l'incolumità fisica.

Ma essendo, Facebook ed Instagram, piattaforme gratuite, come fanno a guadagnarci?

I maggiori introiti dell'azienda di Mark Zuckerberg derivano dai servizi di "Behavioural Advertising", all'interno del quale troviamo come principali il c.d. "Custom Audience" e "Look Alike".

Custom Audience

Il Custom Audience è un servizio di elaborazione del CRM (Customer Relationship Management) che permette alle aziende di abbinare alla loro lista, composta da nomi e cognomi, indirizzi e-mail o numeri di telefono, delle persone reali che possiedono un profilo Facebook[44].

Scopo di tale matching è, ovviamente, la personalizzazione delle pubblicità, affinché possano essere cucite su misura su ogni singolo utente.

Tale lista del CRM solitamente è composta da iscritti alla newsletter che non hanno mai acquistato prodotti oppure da soggetti che hanno chiamato il call center per

[44] https://www.coine.it/social-media-marketing/targeting-avanzato-facebook-custom-audience/#:~:text=Una%20Custom%20Audience%20%C3%A8%20un,possono%20essere%20online%20oppure%20offline.

avere informazioni e poi non hanno acquistato o da utenti che hanno inserito nel carrello un prodotto che all'ultimo hanno deciso di non acquistare.

La società, pertanto, gli invia "tailored advertising" al fine e nella speranza di trasformarli in clienti.

Look Alike

Il secondo servizio, il "Look Alike", mira sempre a trovare nuovi clienti per le aziende, ma questa volta permette di generare un pubblico simile all'audience di partenza (il CRM delle aziende)[45].

Partendo dalla lista fornita dall'azienda, Facebook crea un pubblico con caratteristiche, interessi e comportamenti simili.

A tali soggetti Facebook invierà pubblicità mirata.

In sostanza, mentre con il primo servizio mira a trovare nuovi clienti sulla base di dati già posseduti dalle società, il secondo mira ad aumentare il database dei potenziali clienti di una società, identificando quei soggetti che hanno caratteristiche e gusti simili ai soggetti presenti su CRM della società.

Resta dunque da capire come venga tutelata la privacy all'interno di questi servizi e quali siano le basi giuridiche per effettuare questo trattamento di dati personali.

La società di Zuckerberg nelle "Condizioni Generali di Facebook per Business" dichiara che "Ciascuna azienda si assume la responsabilità della propria conformità al GDPR, così come quella alle leggi in vigore applicabili".

Di conseguenza, sono le aziende a dover implementare i propri obblighi privacy (in qualità di titolari del trattamento) ai fini dell'invio delle suddette campagne di Adv personalizzate.

Tuttavia, Facebook compie una distinzione: per il servizio di Custom Audience si definisce Responsabile del Trattamento, mentre per il servizio di Look Alike si definisce Titolare del trattamento dei dati personali.

Ciò, ha numerose implicazioni, infatti, per il servizio di Custom Audience, definendosi Responsabile del trattamento, Facebook permette alle società che raccolgono i dati (e quindi che agiscono in qualità di Titolari del trattamento) di non chiedere il

[45] https://www.coine.it/social-media-marketing/facebook-lookalike-audience/

consenso specifico per la trasmissione dei dati ad un soggetto terzo, essendo lecito il semplice trattamento, privo di consenso, effettuato da una persona giuridica per conto del Titolare.

Il Titolare, piuttosto, è obbligato a chiedere il consenso agli interessati per eseguire attività di profilazione.

Al contrario, per il servizio Look Alike, Faceook, definendosi Titolare del trattamento, fa sì che le società che raccolgono i dati non chiedano il consenso alla profilazione ma, piuttosto, al trasferimento dei dati personali a terzi soggetti (Facebook stessa ovviamente) per la finalità di profilazione.

Alla luce di quanto illustrato, notiamo che il Custom Audience è un servizio "Client Oriented" assolutamente vantaggioso e gradito dall'utente, in quanto elimina la pubblicità superflua e fa sì che riceviamo solo pubblicità attinente ai propri interessi.

Tuttavia, tale servizio è vantaggioso solo se viene realizzato in conformità al Regolamento Europeo sul Trattamento dei Dati Personali.

È, pertanto, consigliabile porre maggiore attenzione nella lettura delle informative sul trattamento dei dati personali, verificare i destinatari o le categorie di destinatari dei nostri dati personali e le relative finalità per cui ricevono i nostri dati, riflettere sulle conseguenze dei consensi rilasciati e, soprattutto, esercitare i propri diritti ogniqualvolta si riscontri una violazione della disciplina sulla Privacy, così da indurre, necessariamente, Facebook, ma in generale qualsiasi altro social network, a conformarsi.

3.2 Political Microtargeting: il microtargeting politico applicato da Cambridge Analytica

Il Microtargeting, spesso utilizzato dai partiti politici e dalle campagne elettorali, include tecniche di data mining di marketing diretto che prevedono una segmentazione predittiva del mercato (ovvero l'analisi dei cluster).

È utilizzato dai partiti politici repubblicani e democratici degli Stati Uniti, così come dai candidati per monitorare i singoli elettori e identificare potenziali sostenitori.

Le tecniche di microtargeting si basano sulla trasmissione di un messaggio personalizzato a un sottogruppo dell'elettorato sulla base di informazioni uniche su quel sottogruppo."

Il microtargeting psicografico attuato da Cambridge Analytica è una tipologia di marketing politico innovativo, fondato sulla misurazione della personalità degli elettori in base alle loro tracce digitali e nella pratica di influenza attraverso l'invio di messaggi personalizzati.

Cambridge Analytica, dopo aver profilato milioni di cittadini americani, inizia ad inviare agli utenti Facebook annunci pubblicitari sulla base della personalità dedotta dal modello e adattando i propri annunci a persone con caratteristiche particolari.

Inoltre, grazia alla, già menzionata, funzione "LookAlike" di Facebook, avrebbe potuto rivolgersi anche a persone che non aveva profilato.

Al Concordia Annual Summit (New York), Alexander Nix, dimostra come sia possibile rivolgersi in modo differenziato agli elettori di ogni categoria psicografica; inoltre, prendendo come esempio il secondo emendamento degli Stati Uniti, che garantisce ad ogni cittadino il diritto di possedere armi da fuoco, afferma: "Per convincere le persone fortemente nevrotiche e coscienziose, serve la minaccia del furto in casa e la sicurezza rappresentata da un'arma", continua in una recente intervista, "praticamente ogni messaggio lanciato da Trump si basava su dati digitali".

Il terzo giorno del dibattito televisivo tra Donald Trump ed Hilary Clinton, la squadra del candidato Repubblicano ha testato, soprattutto attraverso la piattaforma Facebook, 175mila variazioni di inserzioni sui temi della campagna elettorale.

Nella maggior parte dei casi i messaggi differivano tra loro solo per dettagli microscopici, con l'obiettivo di rivolgersi ai destinatari nel modo più consono al loro profilo psicologico.

C'erano titoli diversi, colori e didascalie diversi, accompagnate da foto e video.

Sempre Alexander Nix ha spiegato, in un'intervista al giornale tedesco Das Magazin, che queste variazioni quasi impercettibili servono a raggiungere anche i gruppi più piccoli: "In questo modo siamo in grado di rivolgerci in modo mirato ad un intero villaggio, come ad un condominio e perfino a singole persone".

Durante le Elezioni Presidenziali Americane, lo staff che seguiva la campagna elettorale di Trump, per evitare che gli abitanti di un quartiere di Miami, chiamato Little Haiti, votassero per la Clinton, ha messo in circolazione la notizia del fallimento della Clinton Foundation in seguito al terremoto di Haiti: stavano cercando di tenere lontano dai seggi i potenziali elettori della candidata Democratica.

Obiettivo che venne raggiunto attraverso i c.d. “Dark Post”, inserzioni sponsorizzate che si presentano come “ultimissime notizie”.

I Dark Post sono comparsi su Facebook e possono essere visti soltanto dagli utenti che hanno profili specifici.

Un esempio sono i video rivolti agli afroamericani, in cui Hilary Clinton definiva “predatori” i maschi neri.

Le indagini condotte fino ad oggi hanno accertato che nel corso della campagna elettorale pro-Trump furono utilizzati numerosi account fasulli e bot per diffondere notizie false e altri contenuti finalizzati a screditare Hilary Clinton.

Ogni giorno venivano pubblicati decine di migliaia di post, soprattutto in occasione dei dibattiti tv e di altri appuntamenti elettorali: l’efficacia dei post veniva analizzata in tempo reale, così da poter privilegiare quelli che maggiormente erano in grado di influenzare le opinioni dell’elettorato.

In tutto questo, Cambridge Analytica, ha suddiviso la popolazione statunitense in 32 tipi di personalità e ha concentrato i suoi sforzi solo su 17 Stati.

Inoltre, così come Kosinski era arrivato alla conclusione che gli uomini che emettono like su Facebook ai cosmetici MAC hanno qualche probabilità in più di essere gay, la società britannica Cambridge Analytica ha scoperto che la preferenza per le automobili di fabbricazione statunitense era tipica dei potenziali elettori di Trump.

Sulla vicenda l’ex dipendente di Cambridge Analytica, Christopher Wyile, in un’intervista ha spiegato: “Invece di stare in piedi nella piazza pubblica e dire quello che pensi, stai sussurrando all’orecchio di ogni singolo elettore. E potresti sussurrare una cosa ad un elettore ed un’altra cosa ad un altro elettore”.

Ecco, dunque, perché Facebook si è dimostrata l’arma più potente per la vittoria di Trump, al quale merito va dato anche di aver investito maggiormente nella campagna digitale, a discapito di quella televisiva.

4. Brexit ed elezioni Presidenziali degli Stati Uniti: qual è il massimo comune denominatore?

La raccolta dei dati e la profilazione dell'utente, che portano all'invio di campagne pubblicitarie mirate, hanno visto molti grandi eventi concludersi con risultati inaspettati.

Primo tra tutti, il già citato "caso Donald Trump" durante le Elezioni Presidenziali degli Stati Uniti nel 2016.

A questo caso si aggiunge un altro incredibile risultato ottenuto in Gran Bretagna dal partito "Leave.eu" nel 2016, ovvero, la c.d. "Brexit".

Brittany Kaiser, dipendente di Cambridge Analytica e collaboratrice di Alexander Nix e il Dottor David Wilinkson, Chief Data Scientist di Cambridge Analytica, in quell'anno decisero di recarsi in Gran Bretagna per affiancare il partito "Leave.eu".

Durante la loro visita a Bristol, dove si trovava la sede del partito, Brittany si informò sulle attività che svolgevano, su come raccoglievano i dati degli utenti e su che tipologie di domande facessero ai cittadini britannici per capire se fossero interessati a votare per restare o uscire dall'Unione Europea.

Quando le vennero consegnate le domande si accorse che il lavoro che stavano facendo era completamente sbagliato, erano domande così tendenziose da compromettere qualsiasi modello, dunque decise, in nome di Cambridge Analytica, di fornirgli consulenza.

Alcuni mesi dopo, ricevuta la consulenza, il partito decise di rompere i rapporti con Cambridge Analytica.

Durante la primavera del 2016 il partito sembrò avercela fatta senza l'aiuto della società di consulenza britannica, pur con, all'apparenza, le tecniche da loro illustrate.

Fu solo qualche mese dopo, che il politico Arron Banks dichiarò che il risultato raggiunto fosse merito dell'impiego scientifico dei dati, citando Cambridge Analytica ogni volta che gli conveniva.

Lo stesso Banks si vantava del fatto che quella del Leave.eu fosse la campagna politica più virale del Regno Unito e che in una settimana aveva raggiunto su Facebook ben 3,7 milioni di sottoscrittori.

Un altro partito che beneficiò dell'appoggio di Cambridge Analytica fu "Vote Leave, il quale capo, Dominic Cummings, che considerava i dati una religione, ammise di aver adottato il loro approccio.

Secondo quanto rivelato da una ricerca del "Observer" il partito Vote Leave aveva ingaggiato una società affiliata a Cambridge Analytica "AggregateIQ", la quale aveva collaborato all'intera campagna fornendo aiuto anche alle associazioni connesse come BeLeave e Veterans for Britains.

L'AIQ arrivò a stabilire il suo centro operativo nella sede del Vote Leave; e così mentre Cambridge Analytica lavorava con il Leave.eu, l'AIQ, la società partner di SCL, la cui proprietà intellettuale era detenuta dai Mercer, era al servizio del suo diretto concorrente.

La campagna digitale di AIQ era molto simile a quella di Cambridge, se non nei contenuti, quantomeno nel metodo; la loro strategia era improntata sull'uso dei focus Group, della segmentazione psicografica e degli algoritmi predittivi, e i dati erano stati raccolti tramite concorsi e vari test online assolutamente legittimi.

Avevano combinato poi i dati degli utenti con quelli degli elettori registrati e avevano iniziato ad inviare messaggi personalizzati, incitando un'intera nazione.

Durante il rush finale, prima del referendum, il veleno che aveva contraddistinto la propaganda online infettò anche il mondo reale.

Il Vote Leave diffuse notizie false su paesi come la Turchia, che stava trattando per entrare a far parte dell'Europa.

Spronò gli elettori incerti suggerendo che un voto a favore del *remain* era un voto che avrebbe impoverito il sistema sanitario nazionale a cui tanto teneva la Gran Bretagna.

La campagna a favore del Leave faceva leva sulle paure della gente, sfruttando le preoccupazioni legate ai fondi per i servizi del governo e la minaccia dei migranti e dei terroristi.

Alla fine, tramite una testimonianza di una ricercatrice di nome Emma Bryant, venne fuori che il Leave.eu aveva usato le proposte che Brittany kaiser aveva illustrato durante la sua consulenza a Bristol.

L'attivista politico britannico, Andy Wigmore, si era vantato con Emma Bryant di essersi impossessato della strategia di Cambridge Analytica e, dopo ave assunto dei data scientist provenienti dall'University of Mississippi, aveva creato la propria versione

di Cambridge Analytica, chiamata Big Data Dolphins, e aveva utilizzato l'intelligenza artificiale affinché il leave trionfasse.

CAPITOLO SECONDO

Il trattamento dei dati degli utenti

1. I diritti dell'interessato

Nella Direttiva 95/46/CE il catalogo contenente i diritti dell'interessato era spalmato su più sezioni all'interno del Capo II inerente le "Condizioni Generali di Liceità dei Trattamenti di Dati Personali".

Il legislatore europeo del 2016 al contrario decide di dedicare un intero Capo, suddiviso in ben cinque sezioni[46], ai diritti facenti capo all'interessato in modo da catalogarli in maniera ordinata e sistematica.

L'obiettivo è senza dubbio quello di estrapolare dalla massa aggrovigliata delle condizioni di liceità del trattamento, la parte relativa ai diritti costruendo un sistema più chiaro, omogeneo, autonomo e coordinato, in modo tale da renderne senz'altro più agile la lettura e con lo scopo, inoltre, di far risaltare le innovazioni apportate in quest'ambito di disciplina.

Il Capo III infatti presenta rilevanti novità per il diritto alla protezione dei dati personali come il Principio di Trasparenza, tanto per quanto riguarda il trattamento (come visto ex art.6 Reg.) quanto per le comunicazioni e l'informativa, ovvero per l'introduzione di nuovi diritti come il Diritto alla Rettifica, il Diritto alla Cancellazione (il c.d. diritto all'oblio), il Diritto di Limitazione di trattamento e infine il Diritto alla Portabilità dei dati.

Per quanto riguarda il principio di trasparenza il Regolamento lo introduce in pianta stabile, in primo luogo, nell'apparato dei principi applicabili al trattamento dei dati personali dove insieme ai canonici principi di liceità e correttezza, come abbiamo visto, l'articolo 5 stabilisce che i dati personali siano trattati in modo lecito, corretto e

[46] Il Capo III intitolato "Diritti dell'Interessato" si suddivide nelle seguenti sezioni:
a) Sezione I: Trasparenza e modalità;
b) Sezione II: Informazione e accesso ai dati personali;
c) Sezione III: Rettifica e cancellazione;
d) Sezione IV: Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche;
e) Sezione V: Limitazioni.

trasparente nei confronti dell'interessato; in secondo luogo inserendolo in apertura del capo relativo i diritti dell'interessato, determinando le modalità attraverso le quali il principio si estrinseca in concreto, specialmente per quanto riguarda l'informativa e le comunicazioni all'interessato, e definendolo come un presupposto giuridico fondamentale per un efficace esercizio dei diritti appartenenti alla persona.

È indubbio, infatti, che il principio di trasparenza sia strettamente connesso in profondità con le trame di altri istituti come quello dell'informazione, delle comunicazioni destinate all'interessato, ma non solo più in generale la trasparenza è strettamente collegata all'operatività dei diritti facenti capo al soggetto in primis il diritto d'accesso.

Immaginiamo uno schema a struttura triangolare ai cui vertici troviamo rispettivamente Trasparenza, Informazione ed Esercizio dei Diritti: senza trasparenza non vi è informazione (o quantomeno è difficile ottenere un quadro completo, chiaro e perché no veritiero), se non vi è informazione non può seguire un efficiente esercizio dei diritti da parte dei soggetti interessati.

Al fine di chiudere lo schema, e renderlo completo, è necessaria la compresenza di tutti e tre gli elementi, essendo infatti l'uno il presupposto dell'altro.

L'articolo 12 a tal proposito prevede un vero e proprio obbligo in capo al titolare del trattamento che deve adottare tutte le misure appropriate per fornire a chi è legittimato a farne richiesta, le informazioni di cui agli artt. 13 e 14 (qualora i dati personali rispettivamente non siano stati ottenuti presso l'interessato, oppure siano stati raccolti presso l'interessato), ovvero le comunicazioni di cui agli artt. dal 15 al 22 (cioè tutto l'insieme di diritti e obblighi che partono dal diritto d'accesso e terminano con la disposizione relativa al processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione) e all'art. 34 (che prevede le comunicazioni in caso di violazione dei dati personali dell'interessato).

Fondamentale è che tali informazioni e comunicazioni avvengano in «forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.».

Come anche enunciato espressamente al 39esimo Considerando l'applicazione del principio di trasparenza deve essere, nello specifico, mirata a rendere il più chiaro e comprensibile possibile per l'interessato quelle che sono «le modalità con cui sono

raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati».

Non solo, necessario al fine di assicurare e garantire la correttezza del trattamento è fondamentale che sia data un'informativa chiara e precisa riguardante «l'identità del titolare del trattamento e le finalità del trattamento e ulteriori informazioni per assicurare (…) alle persone fisiche interessate e ai loro diritti, di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano».

Inoltre, in un'ottica di maggiore completezza del patrimonio informativo dell'interessato riguardo il trattamento al quale sono sottoposti i dati che lo riguardano si asserisce che «le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali» e che sia «utilizzato un linguaggio semplice e chiaro».

La trasparenza dei dati e delle modalità con cui avviene il trattamento è dunque funzionale alla possibilità per l'interessato di seguire i propri dati, di autorizzarne modifiche, richiedere aggiornamenti e fare in modo di vietare e richiedere l'intervento per evitare abusi.

Se la trasposizione dei diritti e dell'identità di una persona avviene dal tradizionale piano fisico, su di un altro completamente nuovo come quello digitale, è allora doveroso che vi sia un'adeguata tutela rafforzata tanto del corpo quanto della mente elettronica, con garanzie e responsabilità che il principio di trasparenza introduce nel nuovo Regolamento dettando chiari precetti ai titolari del trattamento, alle imprese e alle amministrazioni affinché adottino politiche concise, trasparenti, chiare e facilmente accessibili mediante informazioni rese con linguaggio semplice e chiaro[47].

Al fine di una tutela rafforzata sono previsti ulteriori obblighi in capo al titolare del trattamento come quando al par. 2 si specifica che il titolare agevola l'esercizio dei diritti dell'interessato e che non può rifiutarsi di soddisfare la richiesta dell'interessato al fine di esercitare tali diritti, o ancora quando al par. 3 è fatto obbligo al titolare di fornire le informazioni relative all'azione intrapresa senza ingiustificato ritardo nel termine massimo di un mese, prorogabile di due mesi, previa comunicazione all'interessato dei motivi di ritardo.

[47] G. DI GENIO,Trasparenza e Accesso ai dati personali, Cap VIII, in La Nuova Disciplina Europea della Privacy, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 164.

Però, così delineato, il principio di trasparenza sembra operare esclusivamente *ex post*, e cioè in un momento successivo al trattamento, che si presuppone in questo caso già avvenuto, come un requisito da rispettare affinché il complesso delle comunicazioni e delle informazioni richieste dall'interessato siano *compliant* rispetto al dettato normativo che richiede la massima comprensione e la chiara conoscibilità da parte delle persone alle quali i dati appartengono.

Invero, il principio di trasparenza deve porsi già in un momento antecedente rispetto al complesso di operazioni alle quali i dati verranno successivamente sottoposti, e cioè ancor prima che il titolare del trattamento arrivi in possesso dei dati dell'utente, in una fase in cui trasparenza e consenso dell'interessato sono strettamente correlati.

Infatti, affinché il principio di trasparenza possa dirsi completato, nell'ottica di favorire con la chiarezza massima la consapevolezza dell'interessato, in merito all'utilizzo che verrà fatto dei propri dati personali, deve necessariamente porsi prima della richiesta di acquisizione dei dati personali da parte del titolare, nella fase appunto del rilascio del consenso.

La persona alla quale appartengono i dati deve potersi prefigurare già prima di una valida prestazione del consenso (e in realtà tali informazioni a monte sono funzionali proprio affinché l'interessato presti liberamente e consapevolmente il proprio consenso) quale sarà l'utilizzo che verrà fatto dei propri dati, a quali operazioni di trattamento saranno sottoposti gli stessi, per quanto tempo, con quali modalità e quali sono le specifiche finalità per le quali sono trattati.

Soltanto in questo modo può dirsi realmente consapevole e pienamente informata la persona interessata in merito al trasferimento e all'utilizzo dei propri dati personali al quale ha acconsentito, solo in questo modo può dirsi pienamente rispettato quel diritto all'autodeterminazione informativa che è la sostanza del diritto alla protezione dei dati personali, quantomeno sotto il profilo della disponibilità, della libera gestione e della autonoma spendibilità del patrimonio informativo che appartiene ad ognuno di noi.

Inoltre, il principio di trasparenza è indissolubilmente legato al diritto d'accesso dell'interessato che, nell'ottica della tutela del diritto alla protezione dei dati personali, riveste un'importanza strategica rilevante nella dinamica procedurale, in quanto è funzionale, potremmo dire anche prodromico rispetto all'esercizio delle altre tipologie di

diritti connessi come quello di rettifica, limitazione, opposizione, oblio e portabilità dei dati.

Non di rado accade che l'utente accetti di rilasciare un consenso anticipato e generale, sopraffatto dalla forza economica schiacciante, che nella dialettica della domanda e offerta di servizi sul mercato digitale, hanno banche, multinazionali e aziende-colosso del settore (si pensi ai, già citati, social network), e che è posto come condizione indispensabile alla possibilità di usufruire del servizio.

Nella maggior parte dei casi, infatti, le istanze garantiste nei confronti del nostro patrimonio dati sono rapidamente sostituite dai benefici e dai comfort che ricaviamo da tale sottoscrizione.

Oggigiorno la consapevolezza dei nostri dati e dei danni che possono derivare da un uso illegittimo, lascia il posto alla prospettiva di una vita più facile grazie alle comodità offerte dalle nuove tecnologie e dai servizi, a quest'ultime, connessi.

È in quest'ottica che trasparenza e diritto d'accesso assumono un'importanza significativa nella nuova disciplina: trasparenza come regola metodologica da attuare nella fase pretrattamento (come una delle condizioni di validità del consenso) e nella fase post-trattamento (per quanto riguarda comunicazioni e informativa inerente le operazioni effettuate sui dati ecc..); e diritto d'accesso come verifica posta in essere dall'interessato al fine di sondare il rispetto dei principi sottesi ad un corretto trattamento dei proprio dati e di avere, inoltre piena contezza dei propri dati personali in un preciso momento[48].

La categoria dell'accesso si presenta come struttura unificante, che rende concreto l'esercizio dei poteri attribuiti alla persona in una molteplicità di situazioni dall'entrata nella rete al rapporto con le diverse categorie di beni comuni, al permanente controllo del sé elettronico e come detto in precedenza apre la porta, quale presupposto procedurale, alla possibilità di esperimento degli altri diritti dell'interessato.

L'articolo 15 prevede dunque che l'interessato abbia il diritto di ottenere da parte del titolare la conferma in merito all'esistenza o meno di un trattamento di dati che lo riguardano e in tal caso ottenere l'accesso a tali dati nonché essere informato in merito:

a) alle finalità del trattamento;

b) alle categorie di dati personali sottoposte a trattamento;

[48] Come anche esplicitato nel considerando n. 63 del Reg. quando si afferma che «Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità.»

c) ai destinatari a cui i dati personali saranno comunicati e se quest'ultimi appartengono a paesi extra UE o a organizzazioni internazionali;
d) al periodo di conservazione previsto per i dati e, quando non è possibile definirlo, quantomeno richiedere quali siano i criteri utilizzati per determinare tale periodo;
e) all'esistenza da parte dell'interessato del diritto di chiedere direttamente al titolare la rettifica, la cancellazione dei dati, oppure il diritto di richiedere la limitazione o di opporsi al trattamento;
f) al diritto di proporre reclamo a un'autorità di controllo;
g) all'origine dei dati, qualora quest'ultimi non siano stati raccolti direttamente presso l'interessato;
h) all'esistenza di un processo decisionale automatizzato, compresa la profilazione, e in tal caso richiedere informazioni in merito alla logica utilizzata nonché sulle conseguenze previste da tale trattamento.

Infine, nei successivi paragrafi è previsto rispettivamente che: qualora i dati personali siano trasferiti verso un paese terzo o un'organizzazione internazionale, l'interessato ha diritto a essere informato in base al possesso, da parte dei soggetti suddetti, dei requisiti previsti dall'articolo 46 del Reg. che subordina il trasferimento dei dati, al di fuori dell'ombrello giuridico dell'Unione europea, alla sola condizione che siano previste adeguate garanzie sul trattamento; che il titolare fornisca una copia dei dati personali oggetto di trattamento, e che se la richiesta è presentata mediante l'utilizzo di mezzi elettronici (e qui la disposizione è figlia del suo tempo), salvo indicazione diversa dell'interessato, le informazioni devono essere fornite in un formato elettronico di uso comune.

In ogni caso come affermato più volte non essendo il diritto fondamentale alla protezione dei dati personali, e di conseguenza anche tutti i diritti ad esso sottesi, dei diritti assoluti anche le prerogative dell'interessato come i diritti d'accesso, d'informazione, di rettifica, di limitazione del trattamento ecc.. soffrono delle limitazioni in base ad esigenze, spesso collettive o forse meglio dire pubbliche, ritenute prevalenti.

È quanto stabilisce infatti l'articolo 23 in tema di "Limitazioni" prevedendo che il diritto dell'Unione e di uno Stato membro può limitare, mediante misure legislative, i

diritti previsti nelle Sezioni 3 e 4 del Regolamento, se tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e consista in una misura necessaria e proporzionata in una società democratica per salvaguardare svariati interessi tra cui: la sicurezza nazionale, la difesa, la sicurezza pubblica o altri obiettivi di interesse pubblico generale specialmente per quanto riguarda l'aspetto economico e finanziario (politica monetaria, tributaria, sanità pubblica e sicurezza sociale).

Oppure quando bisogna salvaguardare la tutela stessa dell'interessato o dei diritti e delle libertà altrui, l'indipendenza della magistratura e dei procedimenti giudiziari, nonché per la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica.

1.2 Il diritto all'oblio nel Regolamento (UE) 2016/679, alla luce dei social network

Nel paragrafo seguente ci appresteremo ad analizzare la disciplina del diritto all'oblio nell'ambito del nuovo quadro giuridico dell'Unione Europea in materia di protezione dei dati.

Ci chiederemo inoltre poi quali analogie e quali differenze presenti tale disciplina rispetto alla Direttiva 95/46/CE, in modo tale da capire se siamo davvero di fronte ad un elemento così innovativo e se la denominazione di "diritto all'oblio" sia effettivamente opportuna.

1.3.1 l'Articolo 17 nell'iter che porta all'adozione del "Pacchetto"

La norma di riferimento, ovvero l'Articolo 17 del Regolamento 2016/679, ha una storia travagliata.

In ogni fase della procedura legislativa, in tale disposizione figura il "diritto alla cancellazione", considerato fin dall'entrata in vigore della Direttiva 95/46/CE un punto fermo della disciplina UE sulla protezione dei dati.

D'altro canto, non possiamo dire lo stesso del diritto all'oblio.

1.3.2 La Proposta della Commissione

Nella Proposta avanzata dalla Commissione il 25 gennaio 2012, il "diritto all'oblio" è presentato come uno degli elementi di maggior importanza e novità dell'intero Pacchetto.

Notiamo innanzitutto come la rubrica dell'Articolo 17 reciti "Diritto all'oblio e alla cancellazione": si ha quindi fin da subito l'impressione che le due espressioni non siano considerate come sinonimiche.

Tale impressione viene confermata dalla lettura della Relazione alla Proposta della Commissione, in cui si spiega che l'Articolo 17, da un lato, approfondisce e precisa il "diritto alla cancellazione", precedentemente sancito dall'Articolo 12 lettera b) della Direttiva 95/46/CE, dall'altro prevede le condizioni del "diritto all'oblio".

I due diritti, dunque, non sono equivalenti, e se il primo si pone in continuità con il passato, il secondo è un diritto "nuovo", che va "oltre" rispetto al primo.

L'importanza del diritto all'oblio è enfatizzata anche nella Comunicazione "Salvaguardare la *Privacy* in un mondo interconnesso: Un quadro europeo della protezione dei dati per il XXI secolo", che accompagna le proposte illustrando le principali novità della riforma.

Come sappiamo tale Comunicazione elenca, a titolo esemplificativo, una serie di problemi concreti che la disciplina vigente non è in grado di fronteggiare, ma che con il nuovo quadro giuridico, potranno essere risolti.

Uno degli esempi in questione riguarda proprio il diritto all'oblio: "uno studente europeo membro di un social network decide di chiedere l'accesso a tutti i dati personali che lo riguardano e che la rete ha conservato.

Tuttavia, si accorge che la mole di dati raccolti, sono molti di più rispetto a quelli che pensava e che molti dati personali che riteneva fossero stati rimossi, in realtà erano ancora lì, conservati.

La riforma delle norme dell'UE di protezione dei dati garantirà che ciò non si verifichi più".

Per far ciò vengono introdotti una serie di obblighi: "I servizi di socializzazione in rete (e tutti gli altri responsabili del trattamento) sono espressamente tenuti a ridurre al minimo il volume dei dati personali degli utenti che raccolgono e sottopongono a

trattamento"; "i sistemi devono essere configurati con impostazioni prestabilite che garantiscano che i dati non siano resi pubblici"; ma soprattutto, ai nostri fini, rileva che "i responsabili del trattamento sono espressamente tenuti a cancellare i dati di chi ne faccia esplicita richiesta, in assenza di altri motivi legittimi che ne giustifichino la conservazione.

Nella fattispecie poc'anzi illustrata, la normativa proposta obbligherebbe il provider di social network a rimuovere immediatamente e completamente i dati dello studente".

Ricordiamo che nella Proposta, con "responsabile del trattamento" si intende la figura soggettiva che nella versione definitiva del Regolamento sarà denominata "titolare del trattamento".

Per riassumere, la Commissione dimostra, sia nella Proposta che nella Comunicazione, di considerare il diritto all'oblio come un elemento di grande novità, capace di avere un impatto davvero significativo.

Tuttavia, il Parlamento non considera il diritto all'oblio altrettanto meritevole e in prima lettura, il 12 marzo 2014, decide di sopprimerlo dal Regolamento; in seguito, a questa modifica rimane il solo diritto alla cancellazione.

Infine, il testo approvato dal Consiglio il 15 giugno 2015 contiene di nuovo entrambe le espressioni, che permangono anche nella versione definitiva del Regolamento 2016/679.

Ma c'è una differenza essenziale rispetto alla Proposta originaria: la rubrica dell'Articolo 17 recita ora "Diritto alla cancellazione ("diritto all'oblio").

Una simile formulazione non lascia adito a dubbi: le due espressioni sono ora considerate come sinonimiche, e non siamo più di fronte a due diritti (uno "vecchio" e uno "nuovo"), ma a due diverse denominazioni dello stesso diritto.

Per comprendere le ragioni che hanno portato a questo cambiamento nell'interpretazione del diritto all'oblio da parte delle istituzioni europee si rimanda alla famosa Sentenza *Google Spain*[49], in cui la Corte di Giustizia dell'Unione Europea afferma che tale diritto esiste già: può essere infatti ricavato dalle disposizioni della

[49] Sentenza della Corte (Grande Sezione) del 13 maggio 2014. Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.

Direttiva 95/46/CE (lette alla luce degli articoli 7 e 8 della Carta), e non vi è dunque bisogno di una riforma[50].

Per intenderci, utilizzando lo stesso esempio della Commissione: lo "studente europeo membro di un social network", per ottenere la cancellazione dei dati da parte del "responsabile del trattamento", non avrebbe più bisogno dell'introduzione di un nuovo diritto; sarebbe sufficiente la giurisprudenza "*Google Spain".*

Proprio per questo le istituzioni europee, pur facendo riferimento al "diritto all'oblio", non ritengo necessario enfatizzare il fatto che si tratti di un elemento innovativo rispetto al passato.

1.3.3 Analisi dell'Articolo 17 del Regolamento (UE) 2016/679

Per comprendere a fondo se l'Articolo 17 del Regolamento (UE) 2016/679 rappresenti o meno una novità nel panorama europeo, procediamo con l'analisi del testo completo; a tal fine, è innanzitutto necessario riportarne il testo nella sua forma integrale:

Articolo 17

Diritto alla cancellazione (<<diritto all'oblio>>)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a. I dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati:

[50] M. KRZYSZTOFEK, Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation (EU) 2016/679, Kluwer Law International, Alphen aan den Rijn, 2017, p. 120.

b. L’interessato revoca il consenso su cui si basa il trattamento conformemente all’articolo 6, paragrafo1, lettera a), o all’articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;
c. L’interessato si oppone al trattamento ai sensi dell’articolo 21, paragrafo 1, e se non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell’articolo 21, paragrafo 2;
d. I dati personali sono stati trattati illecitamente;
e. I dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell’Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f. I dati personali sono raccolti relativamente all’offerta di servizi della società dell’informazione di cui all’articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto, della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell’interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.
3. I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario:

a. Per l’esercizio del diritto alla libertà di espressione e di informazione;
b. Per l’adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell’Unione o dallo Stato membro cui è soggetto il titolare del trattamento o per l’esecuzione di un compito svolto nel pubblico interesse oppure nell’esercizio di pubblici poteri di cui è investito il titolare del trattamento;
c. Per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell’articolo 9, paragrafo 2, lettere h) e i), e dell’articolo 9, paragrafo 3;
d. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all’articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o

e. Per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

Analizzando il paragrafo 1, osserviamo che elenca i casi in cui la persona interessata ha il diritto di chiedere ed ottenere la cancellazione dei dati personali che la riguardano.

Il primo motivo, citato alla lettera a), per cui una persona può chiedere la cancellazione dei propri dati personali, è quello in cui gli stessi "non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati".

Tale previsione è riconducibile ad uno dei principi della "limitazione della conservazione", sancito dall'Articolo 5 paragrafo 1, lettera e) del Regolamento, e precedentemente dall'Articolo 6 paragrafo 1 lettera e) della Direttiva.

Esso proibisce la conservazione dei dati, in una forma che consenta l'identificazione degli interessati, per un arco di tempo superiore al conseguimento delle finalità per le quali i dati stessi sono trattati.

Di conseguenza, al titolare del trattamento è richiesta la specificazione del periodo massimo previsto per la conservazione dei dati; ciò deve essere fatto in relazione a ciascuna categoria di dati, con l'indicazione della corrispondente base giuridica.

La motivazione elencata alla lettera b) è quella in cui l'interessato revoca il consenso su cui si basa il trattamento, e non sussiste altro fondamento giuridico per lo stesso.

È necessario, a tal proposito, ricordare che al paragrafo 3 dell'Articolo 7 del Regolamento, si garantisce che "l'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento", diritto non espressamente sancito, ma comunque ricavabile dalla Direttiva 95/46/Ce, almeno secondo il Gruppo di lavoro "Articolo 29"[51]; laddove altri, tuttavia, non sarebbero d'accordo[52].

Bisogna precisare inoltre che l'obbligo di cancellazione dovrebbe gravare in capo al titolare non solo nel caso in cui l'interessato revochi il consenso, ma anche nell'ipotesi

[51] Gruppo di lavoro "Articolo 29", parere sulla "definizione di consenso" (15/2011, WP 187)

[52] C. MARKOU, The 'Right to be Forgotten': Ten Reasons Why It Should Be Forgotten, in S. GUTWIRTH, R. LEENES e P. DE HERT (a cura di), Reforming European Data Protection Law, Springer, Dordrecht, 2015, p. 203 ss., spec. p. 208.

in cui l'interessato esprima il consenso per un periodo limitato, e tale periodo si concluda[53].

La motivazione espressa alla lettera c) è quella dell'opposizione al trattamento.
L'interessato, infatti, può opporsi:

- "per motivi connessi alla sua situazione particolare" (Articolo 21 paragrafo 1); ciò a sua volta si può verificare solo nel caso in cui la condizione che rende il trattamento lecito sia una delle seguenti:

  c) "il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (Articolo 6 paragrafo 1 lettera e)

  d) "il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi" (Articolo 6 paragrafo 1 lettera f).
  quest'ultima condizione corrisponde a quella dell'Articolo 7 lettera f) della Direttiva 95/46/CE.

Ricordiamo che in questi casi il titolare del trattamento, a seguito dell'opposizione, si astiene dal trattare ulteriormente i dati personali ed è obbligato a cancellarli, ma solo se "non sussiste alcun motivo legittimo prevalente per procedere al trattamento" (e, ovviamente, solo se l'interessato si trova effettivamente in una situazione diversa da quella degli altri).

- "qualora i dati personali siano trattati per finalità di marketing diretto" (Articolo 21 paragrafo 2).
  In questo caso, il diritto di opposizione è incondizionato. L'obbligo di cancellazione in capo al titolare, invece, sorge solo se non sussiste altro fondamento giuridico per il trattamento.

La motivazione di cui alla lettera d), fa riferimento all'ipotesi in cui "i dati personali sono stati trattati illecitamente".

[53] M. KRZYSZTOFEK, Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation (EU) 2016/679, Kluwer Law International, Alphen aan den Rijn, 2017, p. 122.

Un trattamento è illecito quando, molto semplicemente, non rispetta gli obblighi o i divieti stabiliti dal diritto sostanziale o procedurale.

Ciò si verifica soprattutto (ma non certo esclusivamente) quando il trattamento ha finalità illecite o quando esso è sprovvisto di fondamento giuridico; a tal proposito, ricordiamo, nuovamente, che deve sempre ricorrere almeno una delle condizioni elencate dall'Articolo 6 del Regolamento (in precedenza, Articolo 7 della Direttiva), e, se ad esempio il trattamento ha come fondamento giuridico il consenso dell'interessato (Articolo 6 paragrafo 1 lettera a), tale consenso deve rispettare tutti i requisisti dell'Articolo 4 numero 11); si deve quindi trattare di una "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 del trattamento".

In caso contrario, siamo di fronte a un trattamento illecito.

D'altro canto, l'Articolo17 paragrafo 1 lettera d) non chiarisce un aspetto: ossia, qualsiasi tipologia di illiceità fa sorgere in capo al titolare del trattamento l'obbligo di cancellazione? Oppure, alcune tipologie non sono sufficientemente gravi? La seconda delle due soluzioni appare più ragionevole; in modo particolare è opportuno ritenere che, in caso di violazione degli obblighi di informazione degli articoli 12 e 13, la cancellazione possa essere ottenuta solo se il trattamento richiede il consenso dell'interessato, o quantomeno la sua non-opposizione.

La motivazione espressa alla lettera e) è quella in cui "i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento".

La lettera f), infine, fa riferimento all'ipotesi in cui "i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1".

Il "servizio della società dell'informazione" è definito dall'Articolo 4 numero 25) del Regolamento 2016/679 come "il servizio definito dall'articolo 1, paragrafo 1, lettera b), della Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio"[54].

Tale disposizione, a sua volta, recita: "qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi"

In definitiva, rientra in questa nozione una vasta gamma di attività economiche svolte in rete, tra cui *l'online banking*, *l'online insurance* e la vendita online di altri servizi.

L'Articolo 8 paragrafo 1, invece, riguarda "l'offerta diretta di servizi della società dell'informazione ai minori".

Tale disposizione prevede che è lecito il trattamento di dati personali dei minori che abbiano almeno 16 anni sulla base del loro consenso, al fine di offrire loro direttamente i servizi della società dell'informazione.

Per i minori che abbiano un'età inferiore ai 16 anni, il trattamento è lecito solo se il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale (gli stati membri possono stabilire per legge un'età inferiore, purché non inferiore ai 13 anni).

Riassumendo, l'Articolo 17 paragrafo 1 lettera f) prevede il diritto all'oblio nel caso in cui i dati personali sono stati raccolti nel contesto dell'offerta diretta di servizi della società dell'informazione ai minori; tale disposizione è quindi pensata per proteggere le persone che sono minorenni nel momento in cui esprimono il loro consenso al momento del trattamento, e che di conseguenza non sono sufficientemente consapevoli delle possibili conseguenze[55].

Se passiamo ad analizzare il paragrafo 2 dell'Articolo 17, notiamo che un titolare, dopo aver pubblicato dati personali, è obbligato a cancellarli per le ragioni dell'Articolo 17 paragrafo 1, e deve anche adottare misure per informare gli altri titolari della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione di tali dati.

---

[54] "Direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio, del 9 settembre 2015, che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione"

[55] M. KRZYSZTOFEK, Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation (EU) 2016/679, Kluwer Law International, Alphen aan den Rijn, 2017, p. 124.

Nella società attuale i dati pubblicati su Internet sono messi a disposizione di un numero illimitato e indefinito di destinatari e di ulteriori titolari; si pensi, ad esempio, ai social network, che dal momento in cui effettuiamo la registrazione attraverso la nostra e-mail, nome utente e password, vengono registrati all'interno di un database e successivamente venduti agli inserzionisti che pubblicano annunci su quelle piattaforme[56].

In definitiva, è praticamente impossibile rintracciare tutti questi dati e tutti gli ulteriori titolari.

Per questo, il paragrafo 2 dell'Articolo 17 prevede che le misure, anche tecniche, per informare gli altri titolari della richiesta di cancellazione siano "ragionevoli", "tenendo conto della tecnologia disponibile e dei costi di attuazione".

Tale paragrafo, presentato in precedenza come l'aspetto più innovativo dell'articolo in esame rispetto alla Direttiva 95/46/CE, ha in realtà un predecessore nella Direttiva stessa: si stratta, cioè, dell'Articolo 12 lettera c), in base a cui la persona interessata ha il diritto di ottenere dal titolare del trattamento "la notificazione ai terzi, ai quali sono stati comunicati i dati, di qualsiasi rettifica, cancellazione o congelamento, effettuati conformemente alla lettera b), se non si dimostra che è impossibile o implica uno sforzo sproporzionato".

Ma tra le due disposizioni vi è un netto divario: un conto è dover notificare solo ai terzi a cui il titolare ha "comunicato" i dati; un conto è dover informare della richiesta di cancellazione tutti i "titolari del trattamento che stanno trattando i dati".

Ritornando all'Articolo 17 paragrafo 2, come abbiamo visto, nel corso dell'*iter legis* il diritto all'oblio non riceve sempre la stessa considerazione; una delle conseguenze più rilevanti di ciò è che, durante la procedura legislativa, la riformulazione della disposizione in esame viene modificata più volte.

Nello specifico, la versione approvata in prima lettura dal Parlamento europeo il 12 marzo 2014 obbliga addirittura il titolare ad adottare le misure ragionevoli per ottenere la cancellazione dei dati da parte degli altri titolari (e non solo per informarli della richiesta di cancellazione); d'altro canto, tale versione prevede che l'obbligo del titolare di adottare le misure in questione venga meno quando i dati sono stati resi pubblici ex articolo 6

[56] Facebook: è legale la cessione dei nostri dati personali? Come vengono vendute le informazioni? È possibile proteggere la nostra privacy su Facebook?

paragrafo 1 del Regolamento, ovverosia sulla base di un fondamento giuridico come il consenso dell'interessato, come il fatto che il trattamento sia necessario all'esecuzione di un contratto di cui l'interessato è parte, o il fatto che il trattamento sia necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento, ad esempio.

Ma tali condizioni sono i prerequisiti di un trattamento lecito; dove invece non sono presenti il trattamento è illecito *ab origine*.

In definitiva, l'obbligo del titolare di cancellare i dati da Internet è in questo modo limitato ai soli casi di pubblicazione originaria illecita.

Ma, stando ad una simile formulazione, di "diritto all'oblio" non è sicuramente possibile parlare: tale diritto non dovrebbe essere un mero strumento per rimediare ad un errore del titolare che, fin dall'inizio, ha reso pubblici i dati senza un valido fondamento giuridico; ma dovrebbe riguardare, ad esempio, anche i casi in cui i dati col passare del tempo non siano più necessari.

E, infatti, come già illustrato in precedenza, l'espressione "diritto all'oblio" in prima lettura viene completamente abbandonata, e rimane solo il "diritto alla cancellazione".

Le due cose vanno di pari passo.

Nella versione finale del Regolamento, invece, da un lato la rubrica dell'Articolo 17 fa riferimento al "diritto all'oblio", dall'altro la formulazione del paragrafo 2 è quella precedentemente riportata.

Nel Preambolo vi è inoltre un Considerando particolarmente significativo, che enfatizza l'importanza di tale paragrafo 2; si tratta del numero 66, e recita: "per rafforzare il "diritto all'oblio" nell'ambiente online, è opportuno che il diritto di cancellazione sia esteso in modo tale da obbligare il titolare del trattamento ha pubblicato dati personali a informare i titolari del trattamento che trattano tali dati personali di cancellare qualsiasi link verso tali dati personali o copia o riproduzione di detti dati personali.

Nel fare ciò, è opportuno che il titolare del trattamento adotti misure ragionevoli tenendo conto della tecnologia disponibile e dei mezzi a disposizione del titolare del trattamento, comprese misure tecniche, per informare della richiesta dell'interessato i titolari del trattamento che trattano i dati personali".

L'ultimo paragrafo, numero 3, del considerato Articolo 17 elenca alcune eccezioni all'obbligo di cancellare i dati personali e di informare gli altri titolari della richiesta di cancellazione.

In primo luogo, occorre evidenziare che i paragrafi 1 e 2 non si applicano qualora il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione e di informazione (lettera a).

Tale eccezione si ricollega:

a. Al Considerando 153 del Preambolo, secondo cui: "Il diritto degli Stati membri dovrebbe conciliare le norme che disciplinano la libertà di espressione e di informazione, comprese l'espressione giornalistica, accademica, artistica o letteraria, con il diritto alla protezione dei dati personali ai sensi del presente regolamento.

   Il trattamento dei dati personali effettuato unicamente a scopi giornalistici o di espressione accademica, artistica o letteraria dovrebbe essere soggetto a deroghe o esenzioni rispetto ad alcune disposizioni del presente regolamento se necessario per conciliare il diritto alla protezione dei dati personali e il diritto alla libertà d'espressione e di informazione sancito nell'articolo 11 della Carta. […] È pertanto opportuno che gli Stati adottino misure legislative che prevedano le deroghe e le esenzioni necessarie ai fini di un equilibrio tra tali diritti fondamentali. […] per tenere conto dell'importanza del diritto alla libertà di espressione in tutte le società democratiche è necessario interpretare in modo esteso i concetti relativi a detta libertà, quali la nazione di giornalismo".

b. All'Articolo 85 del Regolamento, che al paragrafo 1 prevede: "il diritto degli Stati membri concilia la protezione dei dati personali ai sensi del presente regolamento con il diritto alla libertà di espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria".

   Al paragrafo 2, invece, si afferma che ai fini del trattamento effettuato a scopi giornalistici o di espressione accademica, artistica o letteraria, gli Stati membri prevedono, qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione, esenzioni o deroghe

rispetto ad un elenco di Capi; tra questi Capi figura anche il numero III, quello sui "Diritti dell'interessato", all'interno del quale rientra l'Articolo 17.

Riassumendo, il trattamento dei dati personali può essere esentato da alcune regole generali dello strumento giuridico in questione al fine di tutelare la libertà di espressione e di informazione; e nello specifico, ciò può determinare la non applicazione dei paragrafi 1 e 2 dell'Articolo 17.

Aggiungiamo che il termine "giornalismo" deve essere interpretato in modo estensivo (come afferma il Considerando 153), e ciò implica che, ad esempio, devono essere ricondotti all'interno di tale nozione anche i blog gestiti da attivisti, che stanno assumendo un ruolo sempre più simile a quello della stampa locale.

Quindi possiamo dire che, tra le eccezioni elencate al paragrafo 3, quella della lettera a) è senza alcun dubbio la più significativa, soprattutto considerandone la notevolissima portata.

Per quanto riguarda le due ipotesi successive, la lettera b) prevede che i paragrafi 1 e 2 non si applichino se il trattamento è necessario per l'adempimento di un obbligo legale previsto dal diritto nazionale o dell'UE, o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare; la lettera c), invece, stabilisce una deroga diritto all'oblio per motivi di interesse pubblico nel settore della sanità pubblica in conformità con l'articolo 9[57].

[57] L'Articolo 17 paragrafo 3 lettera c), in modo particolare, richiama:

- L'Articolo 9 paragrafo 2 lettera h), che fa riferimento al caso in cui "il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3".
- - L'Articolo 9 paragrafo 2 lettera i), che fa riferimento al caso in cui "il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale".
- - L'Articolo 9 paragrafo 3, secondo cui i dati particolari del paragrafo 1 "possono essere trattati per le finalità di cui al paragrafo 2, lettera h), se tali dati sono trattati da o sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti o da altra persona anch'essa soggetta all'obbligo di segretezza conformemente al diritto dell'Unione o degli Stati membri o alle norme stabilite dagli organismi nazionali competenti".

In base alla lettera d) i paragrafi 1 e 2 non si applicano se il trattamento è necessario a fini di archiviazione del pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui il diritto di cancellazione rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento.

D'altro canto, occorre notare che la lettera d) fa riferimento all'Articolo 89 paragrafo 1.

Tale disposizione richiede, proprio per i trattamenti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o fini statistici, l'adozione di misure tecniche ed organizzative che garantiscano il rispetto del principio della minimizzazione dei dati, e che possono includere la pseudonimizzazione.

Ciò, a patto che le finalità in questione possano essere comunque conseguite.

Quindi, per questi trattamenti, il diritto all'oblio può venire meno, ma vi sono comunque garanzie adeguate per i diritti e le libertà dell'interessato.

Infine, la lettera e) del paragrafo 3 stabilisce una deroga al diritto all'oblio per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

A tal proposito ricordiamo che tale disposizione deve necessariamente essere interpretata alla stregua di un'eccezione, e non può certo giustificare una conservazione illimitata dei dati.

Ciò è enfatizzato dal Considerando 64 del Regolamento, in base a cui "il titolare del trattamento non dovrebbe conservare dati personali al solo scopo di poter rispondere a potenziali richieste".

Questo perché nella pratica tale scopo viene utilizzato da molte società come base giuridica per poter conservare i dati per tutta la durata del periodo entro il quale può esser fatta valere nei loro confronti una determinata pretesa[58].

1.3.4 Articolo 17: "passo in avanti" o semplice interpretazione?

Negli ultimi due paragrafi abbiamo analizzato nel dettaglio quella che è una delle maggiori "novità" introdotte dal nuovo Pacchetto europeo, l'Articolo 17.

[58] M. KRZYSZTOFEK, Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation (EU) 2016/679, Kluwer Law International, Alphen aan den Rijn, 2017, p. 125.

Possiamo dunque, finalmente, trarre alcune conclusioni e provare a dare una risposta a quei quesiti che ci eravamo posti in precedenza.

Prima, però, è necessario chiedersi se la disposizione in esame, se confrontata con la Direttiva 95/46/CE, risulta essere davvero un elemento tanto innovativo, e se si tratta effettivamente di un "passo in avanti" per il diritto all'oblio.

Ormai dovrebbe essere chiaro che, rispetto al mero dato testuale della Direttiva 95/46/CE, riteniamo l'Articolo 17 del Regolamento (EU) 2016/679 un elemento di grandissima novità.

La Direttiva, oltre a non utilizzare affatto l'espressione "diritto all'oblio", non sembra dare una grande importanza neanche al diritto alla cancellazione.

Basti pensare che:

a) Nessuno dei Considerando del Preambolo fa esplicito riferimento a tale diritto
b) Non vi è. In realtà, alcun articolo specificamente dedicato al diritto alla cancellazione: l'Articolo 12 è infatti rubricato "Diritto di accesso".
c) La disposizione di riferimento è estremamente scarna; la lettera b) dell'Articolo 12 si limita, come osservato in diverse occasioni, a prevedere che la persona interessata abbia il diritto di ottenere dal titolare del trattamento la cancellazione (o, a seconda dei casi, la rettifica o il congelamento) dei dati il cui trattamento non è conforme alle disposizioni della Direttiva, in particolare a causa del carattere incompleto o inesatto dei dai.

Possiamo, dunque, concludere che nella Direttiva 95/46/CE, il diritto alla cancellazione è decisamente un diritto sottovalutato.

Ciò non sorprende, soprattutto se si contestualizza la Direttiva nel periodo storico all'interno della quale è stata emanata; infatti, nella prima metà degli anni '90, l'uso di Internet è ancora agli albori: fare una previsione su quale tipo di diffusione possano avere i dati personali grazie alla rete, è pressoché impossibile.

È solo con l'avvento dei Social Network e del proliferarsi dell'uso di dispositivi elettronici all'interno delle nostre case, che finalmente si è iniziato ad aprire gli occhi su quali ripercussioni potesse avere la mancanza di una specifica disposizione di legge che prevedesse la possibilità di ottenere la cancellazione dei propri dati personali all'interno della Rete.

Ad oggi, che ci troviamo nel secondo decennio del XXI secolo, la situazione appare completamente mutata.

Infatti, come afferma la stessa Commissione europea nella già citata Relazione alla Proposta di Regolamento, in virtù delle tecnologie attuali "la portata della condivisione e della raccolta di dati è aumentata in modo vertiginoso".

Una disposizione come l'Articolo 12 lettera b) della Direttiva risulta particolarmente scarna, soprattutto se l'interessato chiede la cancellazione dei propri dati personali a seguito della condivisione su larga scala, per due motivi essenziali:

1. Non definisce in modo sufficientemente chiaro i presupposti per l'esercizio del diritto alla cancellazione;
2. Prevede esclusivamente la possibilità di rivolgersi al titolare del trattamento, e di ottenere la cancellazione da parte di quest'ultimo, ma, poiché i dati pubblicati in rete sono messi a disposizione di un numero limitato di ulteriori titolari, ottenere la cancellazione solo da parte del titolare "originario" può giovare ben poco all'interessato

I paragrafi 1 e 2 dell'Articolo 17 del Regolamento 2016/679, rispettivamente, cercano di rispondere a tali problematiche.

Infatti:

1. Il primo paragrafo definisce con grande accuratezza e puntualità i presupposti per l'esercizio del diritto alla cancellazione.
2. Il secondo paragrafo sancisce l'obbligo in capo al titolare di adottare misure ragionevoli per informare gli altri titolari della richiesta di cancellazione. In questo modo ancorché rintracciare tutti gli ulteriori titolari sia in alcune circostanze estremamente difficile, la cancellazione avrà una portata indubbiamente più ampia, e maggiori saranno i benefici che l'interessato potrà ottenere.

In conclusione: l'Articolo 17 del Regolamento, se confrontato con il mero dato testuale della Direttiva 95/46/CE, risulta davvero essere un elemento innovativo, infatti,

grazie al paragrafo 1, ma ancor più grazie al paragrafo 2, la posizione degli interessati risulta essere indubbiamente rafforzata.

2. La piattaforma Facebook e il Regolamento (EU) 2016/679: che ruolo ricopre il consenso?

L'evolversi costante del progresso tecnologico prima e della legislazione europea poi hanno portato a mettere al centro del dibattito parlamentare, in modo sempre più marcato, l'utente.

Dunque, la ricostruzione della capacità del nuovo quadro normativo di garantire una effettiva tutela della sfera di identità delle persone fisiche attraverso l'analisi di un caso concreto non può prescindere da una valutazione specifica del ruolo assunto nel nuovo panorama europeo dal consenso, perno attorno al quale, ormai, ruota inevitabilmente tutto il trattamento dei dati personali.

Solo in questo modo sarà possibile confrontarlo idoneamente con le modalità di esplicitazione del valore dell'utente previste dalla piattaforma oggetto di analisi e valutare in maniera comparativa l'efficacia del nuovo quadro normativo.

Come abbiamo già avuto modo di osservare[59], l'atto volitivo del oggetto interessato all'interno del Regolamento europeo costituisce uno dei sei requisiti alternativi alla base della liceità del trattamento ex art. 6[60], confermando l'impostazione prevista dalla vigente disciplina in materia[61].

Tuttavia, in un clima di crescente attenzione circa la capacità del soggetto di concedere consapevolmente l'uso dei propri dati personali, il ruolo affidato a tale momento risulta sicuramente rafforzato.

Affondando le proprie radici nella definizione dettata dalla previgente Direttiva 95/46/CE arricchita dai contributi apportati dall'"opinione sulla definizione del

[59] Ibid. §3.1

[60] Ai sensi dell'art. 6, infatti, il trattamento si considera lecito se si verifica almeno una delle seguenti condizioni: espressione del consenso da parte dell'interessato; il trattamento è necessario per l'esecuzione di un contratto ovvero di misure precontrattuali; è necessario adempiere ad un obbligo legale; risulta fondamentale per la salvaguardia di interessi vitali dell'interessato o di altri; è necessario per soddisfare l'interesse pubblico o per assolvere ad un pubblico potere; è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Sulla liceità del trattamento cfr. anche ARTICLE 29 DATA PROTECTION WORKING PARTY, Guidelines on Consent under Regulation 2016/679, WP259, adottate il 28 novembre 2017.

[61] L'art. 6 del Regolamento europeo ricalca infatti fedelmente l'impostazione prevista dall'art. 7 della direttiva europea 95/46/CE

consenso" adottata dal WP29 il 13 luglio 2011[62], il consenso, infatti, riemerge nel nuovo panorama normativo in maniera potenziata, grazie all'aggiunta del carattere dell'inequivocabilità accanto ai precedenti connotati di libertà, specificità ed informazione[63].

Tale nuova qualificazione impone che l'assenso si manifesti attraverso un'esplicita dichiarazione ovvero un'azione inequivocabile, che non lasci dubbi circa la volontà dell'interessato di mettere a disposizione del titolare i propri dati personali.

Ne consegue che l'attività di trattamento non possa mai avviarsi sulla base di un atteggiamento passivo od omissivo del soggetto, come spesso accade in Rete con la previsione di "*box*" preselezionati (i c.d. *opt-out),* ma richiede un'attività positiva, mirata a testimoniare la consapevole approvazione dello stesso.

Ancora più indicativo in tal senso è l'ampliamento dei casi in cui il legislatore ha imposto non solo una manifestazione di approvazione, dotata delle caratteristiche precedentemente indicate, ma anche un'esplicitazione del consenso connotata da profili di specificità.

Il c.d. consenso specifico, infatti, nel nuovo quadro normativo è richiesto non solo con riferimento al trattamento dei dati appartenenti alle categorie di cui all'art. 9 (c.d. dati particolari), caso già previsto nella precedente Direttiva, ma anche in occasione di trasferimento verso un paese terzo o un'organizzazione internazionale in assenza di adeguate garanzie ex art. 49, paragrafo 1, lett. a) e nel caso particolarmente attuale dei processi decisionali automatizzati[64], compresa la profilazione, disciplinati dall'articolo 22.

Giustificato dai più accentuati profili di rischio delle situazioni in cui viene richiesto, quindi, il consenso esplicito spinge in avanti il confine della consapevolezza degli interessati richiedendo uno sforzo aggiuntivo nel momento della manifestazione di interesse.

---

[62] ARTICLE 29 WORKING PARTY, Opinion 15/2011 on the definition of consent (WP187).

[63] Per un'analisi dettagliata degli elementi costitutivi del consenso con riferimento alla direttiva 95/46/CE v. F. PIZZETTI, Privacy e il diritto europeo alla protezione dei dati personali – dalla Direttiva 95/46 al nuovo Regolamento europeo, op.cit... Con riferimento al nuovo Regolamento v. anche Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/67, op.cit.

[64] Per un'analisi dettagliata degli elementi costitutivi del consenso con riferimento alla direttiva 95/46/CE v. F. PIZZETTI, Privacy e il diritto europeo alla protezione dei dati personali – dalla Direttiva 95/46 al nuovo Regolamento europeo, op.cit... Con riferimento al nuovo Regolamento v. anche Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/67, op.cit.

Nel silenzio del Regolamento, le Linee Guida interpretano tale ulteriore impiego, quando possibile, nella realizzazione, di un'approvazione scritta e firmata da parte dell'interessato, ovvero in caso di piattaforme o siti *online,* nella compilazione di un determinato modulo o nel caricamento di un documento personale[65].

Per completare la valutazione del ruolo del consenso nella nuova disciplina e procedere al confronto con quanto previsto nel modello adottato dalla piattaforma oggetto di analisi, è necessario, infine, collegare tale atto alle modalità di realizzazione dei dati personali.

Infatti, affinché l'assenso del soggetto interessato si espliciti come una "manifestazione di volontà libera, specifica, informata e inequivocabile" ai sensi dell'art.4, n.8 del Regolamento, risulta indispensabile che l'attività si realizzi nel pieno rispetto del quadro dei principi individuati dal legislatore europeo, individuati nella liceità, correttezza e trasparenza, nonché adeguatezza, pertinenza, limitatezza a cui si aggiunge la presenza di finalità determinate, esplicite e legittime.

È il contemporaneo agire di tali dimensioni che rende, infatti, il trattamento rispettoso della nuova normativa.

Una volta definito il significato del consenso all'interno del nuovo quadro normativo ed individuati i principi legittimanti l'utilizzo delle informazioni personali è possibile procedere all'analisi del modello adottato da *Facebook* al fine di effettuare una comparazione che permetta di individuare le criticità che hanno caratterizzato, e che per alcuni aspetti caratterizzano ancora, il trattamento dei dati personali degli utenti della piattaforma.

Le condizioni d'uso del *social network* vigenti al momento in cui si è verificato il caso "*Cambridge Analytica*", oggi oggetto di un'attenta e profonda modifica proprio alla luce del nuovo Regolamento europeo, risultavano ripartite in due distinti documenti denominati "Dichiarazione dei diritti e delle responsabilità" e "Normativa sui dati"[66].

---

[65] Cfr. ARTICLE 29 WORKING PARTY, Guidelines on consent under Regulation 2016/679 (WP259), adottate il 28 novembre 2017 ed aggiornate il 10 aprile 2018, p.18 ss.

[66] La "Normativa sui dati" aggiornata al 29 settembre 2016 e la "Dichiarazione dei diritti e delle responsabilità" del 31 gennaio 2018 costituivano la struttura portante delle regole applicate da Facebook per garantire la tutela dei dati personali dei propri utenti prima dell'entrata in vigore del Regolamento europeo e del verificarsi della vicenda "Cambridge Analytica". In particolare, il primo documento dettava le condizioni d'uso della piattaforma, regolando i rapporti tra utenti, social network ed il complesso di brand, prodotti e servizi ancillari, definiti "Servizi di Facebook". La normativa sui dati, invece, costituiva invece un documento soprattutto di carattere illustrativo in cui venivano fornite informazioni circa la tipologia dei dati raccolti e le relative modalità di utilizzo e di condivisione con partner, fornitori e soggetti terzi. Tali documenti, consultabili sino a pochi giorni prima dell'applicazione del GDPR, non sono più presenti sulla piattaforma. I nuovi termini e condizioni in materia di privacy, aggiornati al 19 aprile 2018, prevedono

Dalla lettura dei due testi era possibile estrapolare un'articolata informativa che, dietro l'apparente velo della chiarezza dettata dalla semplicità dei termini utilizzati, nascondeva però, a ben vedere, un labirinto di regole poco trasparenti e a tratti contraddittorie.

Le prime e rilevanti criticità riguardavano, e riguardano ancora, la finalità per la quale la piattaforma dichiarava di raccogliere ed utilizzare i dati personali ed il livello di trasparenza della comunicazione effettuata a favore dei destinatari del servizio.

È indubbio, infatti, che l'utente medio sia convinto che *Facebook* utilizzi le proprie informazioni personali per offrire una piattaforma in grado di mettere in contatto le persone attraverso la condivisione di immagini, pensieri, foto e notizie di vario genere, in modo da abbattere la distanza che il tempo e lo spazio tendono inevitabilmente ad erigere nel corso della vita.

D'altronde è proprio questa l'idea che il *social network* ancora trasmette ai potenziali utenti nella scarna pagina iniziale dedicata alle nuove iscrizioni[67].

Un obiettivo, inoltre, che era ribadito anche nella sezione dedicata alla "normativa sui dati", laddove si specificava che la *mission* aziendale consisteva nel "rendere il mondo sempre più aperto e connesso" consentendo "alle persone di condividere i contenuti".

È evidente che si trattava di un messaggio di inevitabile impatto sulla clientela, ulteriormente rafforzato dall'affermazione della perpetua gratuità del servizio[68].

Tuttavia, mutando due rilevanti termini dal filone degli studi aziendalistici, lo slogan "*give people the power to build community and bring the world closer together*", a ben vedere non costituisce la *mission* vera e propria dell'azienda, bensì attiene alla sua

ancora una ripartizione della normativa tra diversi documenti, secondo una logica che, a ben vedere, non differisce molto da quella precedente. L'impatto della nuova disciplina europea e della vicenda "Cambridge Analytica" è comunque ben visibile. Al di là della riorganizzazione delle voci delle condizioni d'uso sulla falsariga delle novità introdotte dal legislatore europeo, la normativa sui dati prevede una sezione esplicitamente dedicata al nuovo Regolamento europeo e denominata "Come esercitare i diritti previsti dal GDPR?". Inoltre, assume particolare rilievo la seguente nota, a dimostrazione che l'attenzione della piattaforma su tali aspetti adesso è inevitabilmente molto alta: "stiamo lavorando per limitare ulteriormente l'accesso ai dati degli sviluppatori in modo da prevenire usi impropri. Ad esempio, rimuoveremo l'accesso degli sviluppatori ai tuoi dati di Facebook e Instagram se non hai usato la loro app per tre mesi, e stiamo cambiando Facebook Login in modo che nella prossima versione vengano ridotti i dati che un'app può richiedere senza inviare l'app per l'analisi, includendo solo nome, nome utente e biografia di Instagram, immagine del profilo e indirizzo e-mail. Per richiedere altri dati, sarà obbligatoria la nostra approvazione". I nuovi termini e condizioni in materia di privacy della piattaforma Facebook possono essere consultati al seguente link: https://www.Facebook.com/about/privacy/update; le condizioni d'uso, invece, sono reperibili a questo indirizzo: https://www.Facebook.com/legal/terms?locale=it_IT.

[67] l testo che appare nella pagina iniziale della piattaforma per i nuovi utenti italiani è il seguente: "Facebook ti aiuta a connetterti e rimanere in contatto con le persone della tua vita": https://it-it.Facebook.com/

[68] Sulla pagina di iscrizione al social network compare la seguente dicitura: "È gratis e lo sarà sempre".

vision, vale a dire quel complesso di valori e principi che la piattaforma dichiara di voler realizzare in maniera prospettica e che ispira tutta la sua attività[69].

In altri termini, rappresenta l'immagine che *Facebook* vuole comunicare al mercato, ma non il modo attraverso cui la stessa aspira a raggiungere tale obiettivo.

Ai fini della valutazione delle finalità del trattamento, invece, l'attenzione non può che soffermarsi su quella che vuole chiamarsi missione aziendale e nel sistema di obiettivi strategici d'impresa che consistono nell'offerta di una molteplicità di servizi di comunicazione in senso lato in cambio dell'utilizzo dei dati personali degli utenti a scopi di profilazione.

È evidente che la *mission*, meno attraente della *vision* aziendale, ma più vicina alla realtà concreta, è rimasta volutamente per anni in penombra, perché in grado di svelare un aspetto "scomodo" per i potenziali clienti, ossia l'apparenza del carattere "gratuito" del servizio[70].

Lo scambio di utilità, servizi *social* da parte della piattaforma ed informazioni ad opera degli utenti, infatti, non si evinceva immediatamente dai documenti messi a disposizione, rafforzando la convinzione che gran parte dei soggetti utilizzano tale piattaforma non siano effettivamente consapevoli del motore sotteso al suo funzionamento.

A confermare tale ipotesi, vi è anche la valutazione che nella Dichiarazione dei diritti e delle responsabilità di Facebook, l'utilizzo dei dati per finalità eccedenti il semplice uso della piattaforma era "svelato" solo nell'articolo 9, dove per la prima volta il social network manifestava esplicitamente la volontà di offrire pubblicità e altri contenuti commerciali o contenuti sponsorizzati e a tal fine dichiarava che gli utenti utilizzando la piattaforma, di fatto accettavano di autorizzare l'utilizzo del loro nome, dell'immagine del profilo e delle informazioni condivise[71].

---

[69] Sui concetti di mission, vision e valori aziendali, v. tra gli altri G. ARMSTRONG – P. KOTLER, Marketing an introduction, Pearson education, 2016; P. KOTLER, Marketing management,15th edition, Londra, 2017; S. SABRAUTZKI, Strategies, Mission, Vision, Goals, Monaco, 2010; M. J. BAKER, Marketing Strategy and Management; 3rd Revised edition, Londra, 2000.

[70] "Se è gratis, il prodotto sei tu" ***The Social Dilemma*** - a 2020 American docudrama film directed by Jeff Orlowski and written by Orlowski, Davis Coombe, and Vickie Curtis.

[71] In particolare, nel documento intitolato "Dichiarazione dei diritti e delle responsabilità" si leggeva: "Il nostro obiettivo è quello di offrire pubblicità e altri contenuti commerciali o contenuti sponsorizzati preziosi per i nostri utenti e per gli inserzionisti. A tal fine, gli utenti accettano quanto segue: 1. Gli utenti forniscono a Facebook l'autorizzazione a utilizza re il loro nome, l'immagine del profilo, i contenuti e le informazioni in relazione a contenuti commerciali, sponsorizzati o correlati (ad es. i brand preferiti) pubblicati o supportati da Facebook. Tale affermazione implica, ad esempio, che l'utente consente a un'azienda o a un'altra entità di offrire un compenso in denaro a Facebook per mostrare il nome e/o l'immagine del profilo di Facebook dell'utente con i suoi contenuti o le sue informazioni senza ricevere

È evidente che la mancata esplicita indicazione della finalità sottesa alla raccolta e al trattamento dei dati personali è in contrasto con il principio della trasparenza di cui all'art 5, lettera b), considerato uno dei capisaldi del Regolamento europeo[72].

Non specificare che il controvalore del servizio è rappresentato dalla cessione di proprie informazioni, spesso di carattere sensibile perché in grado direttamente o indirettamente di svelare aspetti strettamente personali e riservati della persona, significa favorire l'ingannevole convinzione che la piattaforma sia gratuita, incoraggiandone per giunta un utilizzo piuttosto disinvolto.

L contrario, l'esplicita indicazione dell'esistenza di finalità di profilazione, avrebbe potuto consentire un atteggiamento più consapevole da parte degli utenti, esplicando che dietro l'apparente gratuità del servizio si cela un'intensa attività di trattamento dei dati personali, divenuti ormai una merce di scambio di straordinario valore all'interno delle moderne società "iper-connesse".

Una situazione leggermente diversa si riscontrava invece all'interno della "Normativa sui dati" della piattaforma.

Tale documento, infatti, specificava sin dall'inizio l'intento della piattaforma di raccogliere informazioni di carattere personale, evidenziando addirittura cinque macro-categorie[73] a seconda dei servizi utilizzati dall'utente.

Tuttavia, a tale maggiore chiarezza circa la tipologia dei dati ceduti non corrispondeva una adeguata trasparenza relativamente alla motivazione per cui essi venivano e vengono ancora raccolti.

La finalità del trattamento, infatti, risultava diluita in una molteplicità di obiettivi distinti e separati, considerati tutti necessari ed indispensabili per il funzionamento della piattaforma.

---

nessuna compensazione. Se l'utente ha selezionato un pubblico specifico per i propri contenuti o informazioni, rispetteremo la sua scelta al momento dell'utilizzo; 2. Facebook non fornisce agli inserzionisti le informazioni o i contenuti degli utenti senza il consenso di questi ultimi".

[72] Come indicato dal considerando 39) del Regolamento 2016/679 il principio della trasparenza si sostanzia nella trasmissione di informazioni relative al trattamento dei dati che siano per i destinatari facilmente accessibili e comprensibili, caratterizzate da un linguaggio chiaro e semplice. La trasparenza impone, inoltre, che tali comunicazioni siano complete con riferimento alle modalità del trattamento e alle relative finalità in modo da sensibilizzare le persone fisiche sui rischi che si celano dietro l'utilizzo non corretto ed illecito delle proprie informazioni personali. Per un approfondimento cfr. ARTICLE 29 WORKING PARTY, Guidelines on transparency under Regulation 2016/679, adottate il 29 settembre 2017 e modificate l'11 aprile 2018.

[73] Le cinque macro-categorie evidenziate erano le seguenti: Attività che esegui e informazioni che fornisci; attività eseguite e informazioni fornite dalle altre persone; le tue reti e connessioni; informazioni sui pagamenti; informazioni sul dispositivo; informazioni di partner terzi; aziende di Facebook.

Ciò ovviamente in violazione del quadro dei principi di cui all'articolo 5 del Regolamento, secondo cui le informazioni per essere raccolte richiedono una finalità determinata, esplicita e legittima in modo che l'utente abbia la possibilità di decidere in maniera risoluta e consapevole se fornire o meno i propri dati.

D'altronde, pur volendo ricondurre tali differenti esigenze nell'ambito di un unico grande obiettivo rappresentato dal corretto funzionamento della piattaforma, non sarebbe stato comunque possibile porre sullo stesso piano in particolare due tra le diverse finalità elencate: la garanzia della sicurezza e della tutela degli account e la creazione di inserzioni pubblicitarie personalizzate.

È evidente che la richiesta di informazioni necessarie a garantire uno spazio di condivisione sicuro e protetto da violazioni esterne presenta inevitabilmente connotazioni differenti in termini di destinazione d'uso e di tipologia di dati da trattare rispetto ad una richiesta finalizzata al perseguimento di esigenze di carattere prettamente economico.

Inoltre, è da considerare che la creazione di contenuti commerciali di interesse per l'utente sottintende un'attività di profilazione a cui il Regolamento europeo, proprio per gli elevati rischi ad esso connessi, riconosce specifici strumenti di tutela, tra cui il peculiare diritto previsto dall'art. 22 a favore dell'interessato di opporsi a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, in grado di produrre effetti giuridici che lo riguardano o di incidere in modo analogo significativamente sulla sua persona.

La concentrazione di molteplici obiettivi per altro così differenti, quindi, era evidentemente in contrasto con quanto delineato da nuovo quadro normativo europeo.

Alla luce della "granularità" del dato ed in linea con il fine di assicurare un controllo continuo e soprattutto consapevole da parte del soggetto interessato, il Regolamento stabilisce, infatti, che il consenso non solo debba essere specifico (art.4), ma nel caso in cui "il trattamento abbia più finalità, il consenso (deve) essere prestato per tutte queste" (considerando 32)[74].

[74] Con il termine "granularità" si intende indicare il carattere multiforme e plurale dei dati raccolti durante l'attività di trattamento. Secondo tale interpretazione, il controllo dei dati personali può realizzarsi concretamente solo nel caso in cui l'interessato possa esprimere un consenso granulare, vale a dire specifico per uno o più finalità determinate e distinte. Per un approfondimento cfr. ARTICLE 29 WORKING PARTY, Guidelines on Automated individual decision - making and Profiling for the purposes of Regulation 2016/679, op. cit., p.10 ss.; INFORMATION COMMISSIONER'S OFFICE (ICO), Consultation: GDPR consent guidance, marzo 2017, consultabile al link https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf Sul punto anche V. ZENO-ZENCOVICH, Dati, grandi dati, dati granulari e la nuova epistemologia del giurista, in Media Laws, Rivista di diritto dei media, 2/2018.

È solo la concreta ed effettiva possibilità di realizzarsi pienamente come "manifestazione di volontà libera, specifica, informata e inequivocabile".

Al contrario, la molteplicità dei fini in assenza di un assenso mirato imprigionava l'azione dell'utente, costretto passivamente ad accettare o rifiutare di mettere a disposizione i propri dati per utilizzi molteplici e non specificamente delineati, in evidente contrasto con il principio della centralità della persona alla base dell'attuale quadro normativo.

Infine, la previsione di un consenso omnicomprensivo valevole per tutte le finalità evidenziate impediva all'utente di esercitare un consenso esplicito come richiesto nel caso di trattamenti automatizzati dei dati dall'articolo 22.

2.1 Il lento declino del "modello del consenso" della piattaforma Facebook

Il punto in cui il "modello del consenso" delineato dal *social network* iniziava a sgretolarsi, allontanandosi definitivamente dai principi ispiratori del Regolamento europeo, tuttavia, era sicuramente rappresentato dalla parte dedicata alla "condivisione" da parte della piattaforma delle informazioni personali raccolte direttamente dai profili dei propri utenti.

A partire da tale sezione le condizioni d'uso del Regolamento si trasformavano in una difficile esposizione di regole e di condizioni.

Infatti, la sezione 2 della "Dichiarazione dei diritti e delle responsabilità" attribuiva, all'utente la proprietà "di tutti i contenuti e le informazioni pubblicati su Facebook" riconoscendogli la possibilità di controllare anche il modo in cui essi venivano condivisi.

Si tratta di un'idea che emergeva a più riprese nelle condizioni d'uso della piattaforma, ma che calata nella realtà del *social network* risultava priva di concretezza.

Bastava, infatti, proseguire nella lettura della stessa sezione per scoprire che, in riferimento ai contenuti protetti dal diritto di proprietà intellettuale, l'utente, nel momento in cui decideva di utilizzare la piattaforma, riconosceva alla stessa *"una licenza non*

esclusiva, trasferibile, che (poteva) essere concessa come sotto licenza, libera da royalty e valida in tutto il mondo, che (consentiva) l'utilizzo dei contenuti pubblicati su Facebook o in connessione con Facebook".

Al di là della limitata chiarezza del dato testuale, risulta evidente che la contraddizione che era insita in tale parte del documento: veniva, infatti, dapprima riconosciuta all'utente la proprietà dei contenuti caricati, creando la falsa convinzione di poterli effettivamente controllare, ma dopo poco tale illusione veniva a cadere dinnanzi al riconoscimento di una non ben specifica "licenza" che consentiva l'utilizzo degli stessi da parte della piattaforma.

Continuando nella lettura, la sezione 9 intitolata "Informazioni sulla pubblicità e altri contenuti commerciali pubblicitari o messi a disposizione da *Facebook*" specificava che con l'utilizzo della piattaforma, l'utente accettava di concedere "l'autorizzazione a utilizzare il […] nome, immagine del profilo, i contenuti e le informazioni in relazione a contenuti commerciali, sponsorizzati o correlati (ad es. i brand preferiti) pubblicati o supportati da *Facebook*"[75].

Subito dopo, in contraddizione con quanto appena indicato, la piattaforma si premurava di sottolineare che la trasmissione di tali dati personali agli inserzionisti era soggetta, comunque, al consenso degli interessati, ma nessuna indicazione veniva fornita circa le modalità attraverso cui gli utenti avrebbero potuto esprimere consapevolmente il proprio esplicito assenso a tale peculiare trattamento di carattere profilatorio.

Altre criticità emergevano nella omologa sezione presente nel documento "Normativa sui dati".

In tale documento, la piattaforma dichiarava di trasmettere alle aziende che fanno parte del gruppo[76], tra le quali vi sono altri importanti *social network* come *WhatsApp* e *Instagram*, una gamma di informazioni personali di straordinaria ampiezza che derivavano non solo dal monitoraggio continuo delle azioni compiute direttamente

[75] Procedendo nella lettura emergeva la seguente indicazione: "*Tale affermazione implica, ad esempio, che l'utente consente a un'azienda o a un'altra entità di offrire un compenso in denaro a Facebook per mostrare il nome e/o l'immagine del profilo di Facebook dell'utente con i suoi contenuti o le sue informazioni senza ricevere nessuna compensazione. Se l'utente ha selezionato un pubblico specifico per i propri contenuti o informazioni, rispetteremo la sua scelta al momento dell'utilizzo*".

[76] A queste, poi, si aggiungeva una serie indefinita di informazioni acquisite in maniera indiretta perché fornite dai partner esterni che collaborano con la piattaforma ovvero trasmesse dagli inserzionisti e relative ai comportamenti di consumo dell'utente. Per questo tipo di trattamento ulteriore di dati personali, la cui possibile combinazione avrebbe potuto dar vita ad informazioni più complesse e di carattere sensibile, la piattaforma non solo non prevedeva forme di consenso specifico, ma dichiarava apertamente che il loro utilizzo avrebbe seguito le diverse condizioni d'uso dei nuovi titolari.

dall'utente, come la visualizzazione di determinati contenuti, la lettura di peculiari tipologie di notizie o la localizzazione delle immagini caricate o dei luoghi visitati, ma anche dai momenti di "contatto" che collegano l'interessato a soggetti terzi come la condivisione di foto, lo scambio di commenti o di contenuti di vario genere[77].

Un'ulteriore condivisione di informazioni personali era prevista, infine, a favore di clienti, fornitori di servizi e altri partner che supportano l'azienda sotto il profilo dell'infrastruttura tecnica.

In questo caso, la piattaforma specificava che tali soggetti avrebbero dovuto rispettare gli obblighi di riservatezza senza contravvenire alla normativa sui dati e agli specifici accordi stipulati tra le parti, ma è evidente che in assenza di dettagliate indicazioni circa le finalità perseguite e la tipologia di informazioni condivise, né tantomeno del contenuto degli "specifici accordi" tra le parti, la genericità della previsione risultava chiaramente in contrasto con il quadro di principi che sono alla base del legittimo trattamento dei dati secondo il legislatore europeo.

Da quanto evidenziato, quindi, l'utente si trovava di fronte ad una miriade di regole differenti e frammentarie che impedivano di fatto un controllo effettivo del percorso seguito dal proprio dato personale, acquisito e sfruttato da soggetti diversi, per finalità distinte e troppo spesso poco trasparenti.

Ma l'apice del complesso ed aggrovigliato modello di utilizzo dei dati personali dei propri utenti era sicuramente rappresentato dal complesso di informazioni che *Facebook* dichiarava di condividere con applicazioni e siti web di terzi utilizzano i servizi della piattaforma.

Quanto ciò sostenuto, porta, a chiusura del cerchio, alla vicenda che abbiamo analizzato in precedenza: il caso "*Cambridge Analytica*".

Come indicato precedentemente, Facebook negli anni ha accresciuto notevolmente il numero di collaborazioni con soggetti esterni che sfruttano le informazioni già presenti sulla piattaforma per erogare servizi differenti, spesso di carattere ludico e soprattutto indipendenti dal funzionamento della piattaforma.

[77] È infatti da tenere presente che, come sottolineato anche dalle Linee guida, singoli dati separatamente raccolti se combinati tra loro possono dar vita ad informazioni più complesse di carattere sensibile il cui trattamento, per gli elevati profili di rischiosità ad essi associati, può essere realizzato solo nel caso in cui siano soddisfatti i requisiti stabiliti dall'art. 9, paragrafo 2.

Si tratta di attività del tutto scisse dal social network, che tuttavia si servono della relativa infrastruttura per effettuare le proprie prestazioni: dati di accesso, immagini, visualizzazioni e localizzazioni degli utenti di Facebook ed in un passato piuttosto recente anche di informazioni provenienti dai profili degli "amici".

Si apre in questo modo un ulteriore panorama di condivisioni caratterizzato da un intenso scambio di informazioni e di dati tra piattaforma e soggetti terzi che sfugge completamente da qualsiasi forma di controllo.

Tali *app* e siti *web*, come accaduto con l'applicazione che ha dato vita al caso "*Cambridge Analytica*" diventano, infatti, custodi di un elevatissimo numero di dati personali dal valore incommensurabile, ricavabile sulla base di consensi flebili non derivanti da un idoneo procedimento di formazione della volontà dell'utente.

Anche per questa peculiare forma di trattamento, potenzialmente più pericolosa delle precedenti perché realizzata completamente al di fuori della piattaforma, le condizioni d'uso previste da *Facebook* risultavano estremamente e, soprattutto, colpevolmente carenti e poco rispettose dei dati personali degli utenti.

La normativa sui dati, infatti, affermava l'assoggettamento di tutte le informazioni condivise con terzi che facevano uso della piattaforma esclusivamente alle relative "condizioni e normative".

Questo significa che l'utente con un semplice *click* ovvero utilizzando lo strumento della registrazione tramite le credenziali (c.d. *login* tramite *Facebook*) trasferiva, in maniera quasi del tutto inconsapevole, parti estremamente delicate della propria sfera personale a nuovi titolari, sacrificandole per finalità spesso ignote.

È proprio il passaggio del dato personale dal nucleo tendenzialmente più sicuro della piattaforma al variegato panorama di servizi esterni che ha costituito il nodo più critico di tutto il modello delineato da *Facebook* e che, di fatto, ha scatenato il caso "*Cambridge Analytica*".

La piattaforma non è stata in grado di prevenire situazioni lesive particolarmente gravi e connesse alla perdita completa di controllo delle informazioni dei propri utenti.

Non è stata prevista alcuna forma di consenso esplicito per questo peculiare tipo di trattamento ulteriore che eccede le dichiarate finalità della piattaforma; né tantomeno sono state individuate procedure di controllo *ad hoc* finalizzate a garantire un monitoraggio continuo dell'utilizzo legittimo dei dati personali.

In altri termini, *Facebook*, sottovalutando la rischiosità della propria attività di raccolta e trattamento dei dati, è stata carente proprio nella parte più delicata del proprio modello di consenso.

In assenza di regole ancor più rigorose per il trasferimento di tali dati e di procedure di manifestazione del consenso da parte dell'utente strutturate in modo tale da garantire l'effettiva e consapevole determinazione volitiva del soggetto, "l'universo" *Facebook* ha creato un vero e proprio "buco nero" che ha assorbito milioni di informazioni personali di carattere più o meno sensibile, lasciandole alla mercè di interessi di carattere meramente economico, con ripercussioni estremamente gravi per la sfera personale degli utenti e inammissibili per una società democratica anche nella sua evoluzione di tipo digitale.

3. Gli adempimenti connessi al trasferimento dei dati all'estero, soprattutto extra UE

Quanto analizzato finora ha fatto emergere, da un lato la fragilità delle *policy* del *social network, Facebook*, il quale "consentiva" a sviluppatori di app terze di accedere al database di dati degli utenti che si iscrivevano a tali applicazioni consentendone di conoscere anche i dati personali degli "amici", dall'altro psicologi e *data scientists*, come Aleksandr Kogan, che attraverso la creazione di app come "*thisisyourdigitallife*"[78], hanno sfruttato la falla all'interno della "macchina *Facebook*", impossessandosi di quasi 80 milioni di dati personali.

Resta ora da capire come questi dati fanno a circolare all'interno della Rete e possano "rimbalzare" da un'azienda ad un'altra all'interno del panorama europeo ed extra UE.

[78] There is an unwitting mole amongst my friends. Without my permission, they passed my personal information to a Facebook app called "This Is Your Digital Life", which eventually ended up in the hands of Cambridge Analytica, the company famed for using questionable tactics in an effort to influence election campaigns. Read more: https://www.newscientist.com/article/2166435-how-facebook-let-a-friend-pass-my-data-to-cambridge-analytica/#ixzz6i7bJSc5U

3.1 La circolazione dei dati nel panorama europeo e non

La globalizzazione, l'abbattimento di frontiere economiche e politiche e la crescente necessità di operare ovunque nel mondo ed in qualunque momento comporta inevitabilmente la circolazione dei dati personali oltre i confini nazionali e, soprattutto, fuori UE.

Basti pensare alla diffusione dei "*cloud*", account e-mail, accessi personali a siti, applicazioni di telefoni, *tablet* o vari altri apparecchi tecnologici per capire quanto i nostri dati passino da un continente all'altro alla velocità di un *click*.

Le esigenze di velocità delle informazioni vanno però bilanciate per tutelare da abusi ed anarchie i dati personali coinvolti[79].

Infatti, proteggere i dati personali nei trasferimenti transfrontalieri e non significa non solo tutelare le persone ma, anche, la concorrenza leale dei mercati nazionali ed internazionali, la sicurezza privata (del cittadino come dell'impresa) e quella pubblica.

Tali valutazioni non sono sfuggite né al Legislatore europeo della Direttiva 95/46/CE, né a quello del recente Regolamento (UE) 2016/679 (c.d. GDPR), che, da un lato, prevede e stimola la libera circolazione dei dati all'interno dell'Unione, in conformità ai propri principi e garanzie dell'interessato, e dall'altro, vieta i trasferimenti dei dati in assenza delle tutele in esso previste.

Il Regolamento, infatti, prevede che i dati personali possano uscire dai confini UE solo a condizione che sussistano i requisiti presenti negli artt. 44 e ss.

3.2 Trasferimento in base ad una decisione di adeguatezza ex articolo 45

I dati personali possono essere trasferiti verso un Paese extra UE o un'organizzazione internazionale se per il Paese di destinazione o l'organizzazione internazionale sia stata adottata una decisione di adeguatezza, cioè un atto formale (c.d.

[79] Come ricorda espressamente il Cons. 2 del Regolamento UE n. 2016/679: "[…] *il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza di economie nel mercato interno e al benessere delle persone fisiche"*.

atto di esecuzione) della Commissione Europea che decide se in essi si garantisce un livello di protezione adeguato alla tutela dei dati personali.

Il passaggio di dati può derivare sia direttamente dall'interessato sia da altro titolare o responsabile del trattamento.

Tale provvedimento è reso dalla Commissione dopo aver valutato lo stato di diritto del Paese, il rispetto dei diritti e libertà fondamentali eventualmente garantiti, la legislazione generale e settoriale (in tema di sicurezza, difesa, diritto penale ed accesso delle autorità ai dati personali), la regolamentazione di eventuali successivi trasferimenti dei dati verso ulteriori Paesi terzi o organizzazioni internazionali e l'esercizio della giurisdizione[80].

Altri requisiti essenziali sono la presenza di un'Autorità di controllo indipendente a garanzia della protezione dei dati e l'assunzione di impegni internazionali con convenzioni o altri atti giuridicamente vincolanti ai fini della protezione dei dati.

La decisione di adeguatezza è, quindi, il frutto di attenta valutazione del livello di "cultura" giuridica della protezione del dato presente nel Paese terzo o nell'organizzazione internazionale, prevedendosi anche un riesame periodico di almeno ogni 4 anno della permanenza dei requisiti nonché la possibilità di revoca, la modifica o sospensione della decisione, senza effetto retroattivo.

La Direttiva 95/46/CE, prevedeva anch'essa il presupposto della decisione di adeguatezza e ne sono state emesse molteplici, che resteranno in vigore sino alla modifica, sostituzione o abrogazione della Commissione; ad oggi la Commissione ha riconosciuti solamente ad 11 nazioni un adeguato livello di protezione, tra queste Andorra, Argentina, Australia, Canada, Israele, Nuova Zelanda, Svizzera, Uruguay[81].

Gli atti di esecuzione in esame sono pubblicati in Gazzetta Ufficiale dell'Unione Europea e sul sito del Paese terzo, suo territorio o settore o dell'organizzazione internazionale cui si riferiscono.

Percorso diverso ha avuto, invece, il c.d. Privacy Shield, ossia l'accordo internazionale approvato dalla Commissione Europea ed U.S.A., del quale ci occuperemo nei capitoli successivi

---

[80] https://www.altalex.com/documents/codici-altalex/2018/03/05/regolamento-generale-sulla-protezione-dei-dati-gdpr

[81] Decisione della commissione sul livello di adeguatezza della tutela dei dati personali dei paesi terzi, Consultabile su: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

3.3 Trasferimento soggetto a garanzie adeguate ex articolo 46

Se il trasferimento non è fatto direttamente dall'interessato, bensì dal titolare o responsabile del trattamento UE, esso può avvenire anche in assenza di decisione di adeguatezza del Paese non UE o dell'organizzazione internazionale in soli 2 casi:

1. Se essi prevedono nel proprio ordinamento a favore degli interessati sia diritti azionabili sia mezzi di ricorso effettivi ad autorità giudiziaria e di controllo e;
2. Se sussistono garanzie, da distinguersi in
    a. Garanzie che non necessitano di autorizzazione dell'Autorità di controllo competente, quali potrebbero essere strumenti giuridici vincolanti e con efficacia esecutiva tra autorità o organismi pubblici, norme vincolanti d'impresa ex articolo 47 GDPR, clausole di protezione dati adottate dalla Commissione europea, codici di condotta ex articolo 40 GDPR e contestuale impegno vincolante ed esecutivo del titolare e responsabile del trattamento nel paese terzo di applicare le garanzie adeguate);
    b. Garanzie che necessitano di preventiva autorizzazione dell'Autorità di controllo competente, clausole contrattuali fra titolare o responsabile del trattamento UE e quelli del paese terzo o organizzazione internazionale, oppure disposizioni da inserire in accordi amministrativi fra enti pubblici che prevedano diritti effettivi ed azionabili per gli interessati.

In concreto, l'assenza di decisione di adeguatezza è compensata dal fatto che i soggetti coinvolti ne trasferimento dei dati adottino nel contratto che ne regola i rapporti strumenti di garanzia già approvati dalla Commissione europea o dei Garanti nazionali, e pertanto non soggetti ad ulteriore autorizzazione, oppure se le singole disposizioni contrattuali o dell'accordo siano approvate dall'Autorità di controllo.

Ne consegue che l'adeguatezza della garanzia sarà data dalla conformità a quanto già vagliato dall'Autorità, oppure espressamente dichiarato da questa, rispetto al singolo caso.

3.4 Trasferimento in base a norme vincolanti d'impresa ex articolo 47

In assenza di decisione di adeguatezza il trasferimento di dati personali è lecito se, fra società dello stesso gruppo diffuse anche in Paesi terzi, sussistono norme vincolanti di impresa approvate dall'Autorità di controllo nazionale.

È quindi necessario che il gruppo imprenditoriale o di imprese coinvolte nel trasferimento dati, adotti una propria regolamentazione che, oltre a prevedere espressamente diritti agli interessati da azionare per il trattamento dei loro dati, rispetti almeno i seguenti principi:

- Indicazione della struttura e coordinate di contatto del gruppo;
- Specificazione dei trasferimenti dei dati, delle categorie di dati personali coinvolte, del tipo di trattamento e finalità, della tipologia di interessati cui i dati si riferiscono ed individuazione del Paese non UE di destinazione dei dati;
- Natura vincolante, esterna ed interna delle norme;
- Applicazione al trattamento dei principi generali di protezione dei dati, dei diritti all'interessato ivi previsti e della possibilità di proporre reclamo all'Autorità di controllo e giurisdizionale, previsti dal GDPR;
- Responsabilità del titolare o responsabile del trattamento stabilito in UE per a violazione delle norme vincolanti da parte della società del gruppo del Paese terzo, salvo dimostri che l'evento dannoso non è ad essa imputabile;
- Specificazione delle modalità con cui è fornita l'informativa ex artt. 13 e 14 GDPR agli interessati:
- Individuazione dei compiti del DPO nominato o di altro soggetto incaricato del controllo sull'osservanza delle norme vincolanti e le modalità di gestione dei reclami;
- Previsione di procedure di reclamo;
- Cooperazione e meccanismi di segnalazione all'Autorità di controllo;
- Formazione del personale che accede ai dati personali in materia di protezione dei dati

Fuori dalle ipotesi sopra indicate il trasferimento è comunque ammissibile se sussistono le situazioni di deroga specificate dall'art. 49 GDPR, e cioè:

- Se l'interessato, previa informativa inerente anche i rischi di trasferimento attuato in mancanza di decisione di adeguatezza o garanzie adeguate, presta espresso consenso;
- Se il trasferimento è necessario per l'esecuzione di un contratto o misure precontrattuali adottate su richiesta dell'interessato, ad esempio, un'attività di intermediazione per l'acquisto di beni o servizi fuori UE;
- Se il trasferimento è necessario per importanti motivi di interesse pubblico o per accertare o difendere un diritto in sede giudiziaria, si pensi ai dati personali, ad esempio, del cliente che l'avvocato deve trasferire da in un Paese non UE ove instaurare la causa; in tal caso i dati saranno conosciuti dall'Autorità Giudiziaria straniera e dalle controparti e rispettivi legali coinvolti nella controversia;
- Se il trasferimento è necessario per la tutela di interessi vitali dell'interessato o di altre persone, qualora l'interessato sia nell'incapacità fisica o giuridica di dare il proprio consenso; ad esempio, nel caso del trasferimento di un malato per ragioni di cura;
- Se i trasferimenti siano indicati in un registro che, secondo il diritto dell'Unione o dello Stato membro, fornisca informazioni al pubblico e sia consultabile dal pubblico o da chi dimostri un legittimo interesse in base ai requisiti della consultazione previsti dall'Unione o dagli Stati membri.

In mancanza delle citate ipotesi di deroga, il trasferimento è lecito solo se non ripetitivo e non massivo, se necessario ad interessi legittimi inderogabili del titolare del trattamento e purché il titolare, secondo il principio di *accountability*, abbia valutato ogni aspetto del trasferimento e fornito le corrispondenti garanzie adeguate ai fini della protezione dei dati.

Infine, l'ultimo requisito di conformità al Regolamento (UE) 2016/679 è che l'interessato sia informato che i suoi dati personali sono soggetti al trasferimento ad un paese fuori UE o ad un'organizzazione internazionale.

Sul punto il GDPR prevede, infatti, espresso obbligo a carico del titolare del trattamento di informativa non solo sulla migrazione ma, anche, su quali presupposti essa avviene e cioè se si basa su una decisione di adeguatezza, garanzie adeguate, norme vincolanti di impresa o altre ipotesi di deroga ex art. 49 GDPR.

L'informativa è, quindi, lo strumento principale per consentire all'interessato l'effettiva conoscenza del trasferimento dei dati che lo riguardano al fine di esercitare i diritti previsti dal GDPR e di assicurarsi che gli stessi, una volta trasmessi, siano soggetti alle medesime garanzie e tutele godute in UE.

4. Gli accordi sui trattamenti dei dati tra UE e U.S.A.

Quanto analizzato in precedenza, ci permette di comprendere come i nostri dati circolano all'interno del panorama europeo, soprattutto alla luce del nuovo Regolamento UE 2016/679.

Tuttavia, può capitare che i nostri dati vengano trasferiti anche all'esterno dell'Unione, e per far si che circolino liberamente, è necessario che questi garantiscano un elevato livello di protezione dei dati.

Un problema sorse con gli Stati Uniti; il sistema statunitense sulla protezione dei dati era sviluppato in modo molto diverso da quello europeo e non si sarebbe qualificato come sistema in grado di garantire la sicurezza dei dati personali secondo gli standard comunitari.

Per riuscire a superare l'impasse ed evitare una situazione che avrebbe avuto effetti molto negativi sugli scambi tra l'UE e gli Stati Uniti, il dipartimento del commercio statunitense mise appunto dei principi.

Si trattava di uno strumento su base volontaria rivolto alle imprese ed organizzazione americane per adeguarsi al livello di protezione richiesto dalla Direttiva

95/46/CE ed essere così dichiarate “approdo sicuro”, letteralmente in inglese “Safe Harbour”, con annessa dichiarazione di “adeguatezza”.

Il 26 luglio 2000 la Commissione approvò una decisione di adeguatezza offerta dai principi di approdo sicuro e dalle relative “FAQ”, domande più frequenti, in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti.

I principi del “Safe Harbour” erano costruiti da sette punti fondamentali (notifica, scelta, trasferimento successivo, sicurezza, integrità dei dati, accesso e garanzie di applicazione).

1. Per quanto concerne il primo dei punti, la notifica, le persone devono essere informate sulle finalità della raccolta dei dati che le riguarda, i modi per contattare l’organizzazione per avere ulteriori informazioni in merito o per effettuare reclami e all’eventuale utilizzo da parte di terzi[82];
2. Il secondo punto, la scelta, è la possibilità offerta alla persona di consentire o rifiutare che le informazioni personali siano rivelate a terzi, o che le informazioni siano utilizzate per fini diversi da quelli per cui erano state raccolte in origine;
3. Il terzo punto, quello del trasferimento successivo, entra in gioco qualora l’organizzazione abbia intenzione di trasferire i dati a terzi. Prima di farlo, però, dovrà prima verificare che quest’ultimo aderisca anch’esso ai principi dell’approdo sicuro o che comunque risulti essere coperto da garanzie di adeguatezza agli standard richiesti;
4. Il quarto punto riguarda la sicurezza: chi conserva dati personali deve prendere ogni possibile precauzione per evitare che quelle informazioni non vengano trafugate o che ve ne sia fatto un uso non conforme;
5. Il quinto punto riguarda l’integrità dei dati, le informazioni raccolte devono essere pertinenti allo scopo per il quale sono raccolte;

[82] 2000/520/CE: Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti. Allegato 1. Dichiarata invalida il 6 Ottobre 2015 in seguito alla sentenza nella causa C-362/14 della Corte di giustizia dell’Unione europea

6. L'accesso è il sesto punto previsto dal "Safe Harbour" e stabilisce il diritto per gli individui di accedere alle informazioni personali raccolte su di essi da un'organizzazione e che possano correggerle o cancellarle se inesatte;
7. Il settimo ed ultimo punto, invece, riguarda le garanzie di applicazione; devono essere previsti dei meccanismi che permettano di risolvere eventuali contenziosi sulla base dei principi istituiti. Vi deve essere l'obbligo di rimediare a problemi causati dalla mancata applicazione dei principi e sanzioni sufficientemente pesanti da garantire il rispetto dell'applicazione dei principi.

Per più di 10 anni il "Safe Harbour" ha garantito e regolato il trasferimento dei dati personali dall'Europa alle aziende ed organizzazioni americane, fino a quando uno studente austriaco, Max Schrems, avanza la sua battaglia contro *Facebook*, per la protezione dei propri dati personali.

I dati personali degli utenti europei vengono trasferiti dalla filiale irlandese di *Facebook*, sede europea del *social network*, ai server situati sul suolo americano, dove il diritto e la prassi americana offrono una sicurezza adeguata contro la sorveglianza svolta da autorità pubbliche.

Nel 2011, Schrems chiede a *Facebook* di vedere i propri dati personali conservati sui server americani.

Da *Facebook* riceve i suoi dati dei tre anni precedenti, a partire dall'iscrizione al sito, tra i quali erano compresi anche dati da lui cancellati ma che venivano invece ancora trattati dal *social* stesso.

Preso atto della scarsa tutela della privacy garantita da *Facebook*, Schrems denuncia varie volte quest'ultimo al Data Protection Commissioner, l'autorità garante della privacy irlandese, richiedendo un blocco al trasferimento dei dati dalla filiale irlandese ai server americani.

Nel 2012, a seguito di un'indagine, l'Autorità irlandese predispone delle raccomandazioni a Facebook, affinché si adegui alla normativa europea e garantisca la cancellazione definitiva dei dati, qualora richiesto[83].

Poi, nel 2013, a seguito di un'intervista, l'informatico Edward Snowden, rivela la sorveglianza di massa effettuata dalle agenzie di intelligence americane, quali in

[83] Europe-v-Facebook, http://www.europe-v-facebook.org/CJEU_IR.pdf

particolare la NSA, National Security Agency, a scapito di tutti i dati presenti sul suolo americano, a prescindere dalla loro provenienza.

In seguito a tali rivelazioni, Schrems si rivolge nuovamente all'Autorità irlandese denunciando la scarsa sicurezza dei dati trasferiti nei server americani di *Facebook.*

Questa volta, però, la richiesta viene respinta dall'Autorità irlandese rimandando alla decisione della Commissione del 26 luglio 2000 in base alla quale il regime di "approdo sicuro" degli Stati Uniti veniva dichiarato avere un livello adeguato di protezione dei dati personali trasferiti.

Schrems, a quel punto, decide di fare ricorso alla High Court of Ireland (l'Alta Corte di Giustizia irlandese), la quale per poter valutare la questione si rivolge a sua volta, mediante rinvio pregiudiziale, alla Corte di Giustizia dell'Unione Europea[84].

Alla Corte viene chiesto se la decisione della Commissione del 26 luglio 2000 abbia tra i suoi effetti quello di impedire ad un'autorità nazionale di controllo di poter aprire un'indagine in seguito ad una denuncia contro un paese terzo che dia motivo di preoccupazione in quanto ad una non adeguata protezione dei dati personali, e se sia tra i suoi poteri quello di sospendere il trasferimento di dati in oggetto.

La Corte nella sua sentenza del 6 ottobre 2015, reputa che l'esistenza di una decisione della Commissione che dichiara che un paese terzo garantisce un livello di protezione adeguato dei dati personali trasferiti non può sopprimere e neppure ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza della Carta dei Diritti Fondamentali dell'Unione Europea e della Direttiva[85].

Infatti, la Direttiva 95/46/CE concede alle autorità nazionali il potere di valutare se il trasferimento dei dati personali 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, passando poi a valutare la validità della decisione della Commissione, dichiara che quest'ultima si è limitata ad esaminare il regime del "Safe Harbour", senza prendere in considerazione anche altri aspetti come la legislazione nazionale o gli impegni assunti in campo internazionale[86], osserva inoltre che al regime "Safe Harbour"

[84] Sentenza Schrems vs Data Protection Commissioner della High Court of Ireland del 18 Giugno 2014
[85] Sentenza della Corte di giustizia nella causa Maximilian Schrems contro Data Protection Commissioner (Schrems), C-362/14, ECLI:EU: C:2015:650 del 6 ottobre 2015, punto 66
[86] Schrems, nota 165, punto 78

prevalgono le esigenze di sicurezza nazionale e della legislazione americana, obbligando le imprese americane a disapplicare senza alcun limite le norme dell'"approdo sicuro" qualora siano in contrasto con tali esigenze[87].

Sono possibili, dunque, ingerenze da parte delle autorità pubbliche americane che possono accedere in maniera generalizzata ai dati personali delle persone ledendo così al diritto fondamentale del rispetto della vita privata.

Infine, la Corte giunge ad invalidare la decisione della Commissione del 26 luglio 2000, che fino a quel momento era stata adottata da oltre 4500 imprese americane per trattare i dati dei cittadini europei[88].

4.1 L'Accordo EU-USA "Privacy Shield", lo scudo della privacy

In seguito all'annullamento dell'Accordo[89], gli Stati membri hanno concesso un breve periodo di grazia per consentire di attuare delle contromisure.

Il Garante italiano della privacy, Antonello Soro, a inizio gennaio 2016 in una lettera parlava di "rischi di pesanti conseguenze dal punto di vista economico", nel caso in cui non si fosse giunti rapidamente ad un nuovo accordo che rimpiazzasse il regime instaurato dal "Safe Harbour"[90].

Così il 2 febbraio 2016 la Commissione europea raggiunge un accordo su un nuovo regime che regoli gli scambi transatlantici di dati personali a fini commerciali con il governo degli Stati Uniti[91].

Il nuovo accordo prende il nome di "Scudo UE-USA per la privacy" adottato il 12 luglio 2016[92].

---

[87] Schrems, nota 165, punti 79-98. Per esempio, in base all'articolo 702 della legge relativa alla vigilanza sull'intelligence esterna (FISA) ai servizi della comunità dell'intelligence statunitense viene consentito di poter richiedere l'accesso a informazioni, tra le quali anche i contenuti delle comunicazioni via Internet, che, sebbene siano conservate all'interno degli Stati Uniti, riguardano tuttavia cittadini stranieri che sono situati al di fuori degli USA.

[88] Schrems, nota 165, punto 106

[89] Trasferimento dati negli U.S.A.: il Garante dispone la caducazione della autorizzazione "Safe Harbor"**;** per maggiori approfondimenti **"**https://www.rplt.it/privacy-data-protection-d100/trasferimento-dati-negli-u-s-a-il-garante-dispone-la-caducazione-della-autorizzazione-safe-harbor/**"**

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

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

[92] Pubblicato nella Gazzetta Ufficiale dell'Unione Europea con decisione di esecuzione (UE) 2016/1250 della Commissione del 12 luglio 2016 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy

L'accordo si presenta come una forma rivisitata del "Safe Harbour" che richiede alle aziende americane maggiori controlli ed offre maggiori garanzie ai cittadini europei.

I principi su cui si basa sono i seguenti: in primis, degli obblighi rigorosi per le imprese che trattano dati personali di cittadini europei.

Al Dipartimento del Commercio degli Stati Uniti sono assegnati maggiori poteri e tra di essi vi è quello di sottoporre le imprese a verifiche e aggiornamenti periodici per controllare il rispetto dei diritti individuali.

Lo stesso livello di protezione deve essere garantito anche quando avviene un trasferimento successivo a terze parti.

Il secondo punto riguarda gli obblighi di trasparenza per l'accesso da parte del governo degli Stati Uniti.

Gli USA hanno offerto una garanzia scritta all'UE che l'accesso delle autorità pubbliche saranno soggetto a limitazioni ed eccezioni.

Viene inoltre aggiunto un meccanismo di ricorso all'interno del Dipartimento di Stato accessibile a qualunque cittadino dell'UE, un meccanismo c.d. di "mediazione".

Il terzo punto riguarda la tutela effettiva dei diritti che viene garantita con la creazione di meccanismi di risoluzione delle controversie.

Le imprese devono rispondere entro tempi precisi alle denunce.

Le persone potranno anche rivolgersi presso le autorità nazionali di protezione dei dati, che potranno portare le loro denunce dinnanzi al Dipartimento del commercio e alla FTC, Federal Trade Commission.

Nel caso in cui non venga trovata una soluzione è possibile, come *extrema ratio*, sottoporre il caso ad arbitrato.

L'ultimo punto riguarda un'analisi annuale comune, ovvero un'analisi congiunta della Commissione europea e del Dipartimento del Commercio degli Stati Uniti in modo da controllare il corretto funzionamento dello "*Shield*", combattere la criminalità e garantire la sicurezza nazionale[93].

Ad aprile la bozza della proposta di accordo "Privacy Shield" presentata dalla Commissione era stata accolta positivamente dal Gruppo di lavoro ex Articolo 29, il quale riconosceva agli Stati Uniti i progressi fatti nei cinque mesi precedenti, per adeguarsi alle

[93] Comunicato stampa della Commissione europea del 12 Luglio 2016, Consultabile su: http://europa.eu/rapid/press-release_IP-16-2461_it.htm

richieste europee, in particolare elogia la maggior trasparenza offerta da parte degli Stati Uniti.

Il gruppo di lavoro valutava positivamente l'introduzione di un meccanismo indipendente di controllo e la possibilità dei cittadini europei di accedere a strumenti giudiziari[94].

A maggio del 2016 il Garante europeo della Protezione dei Dati emette il suo parere sull'Accordo che, però, non risulta altrettanto positivo, ritenendo necessari numerosi miglioramenti.

In particolare, il Garante si sofferma sui nuovi requisiti che verranno richiesti dall'articolo 45 del Regolamento UE 2016/679.

Per la valutazione sull'adeguatezza va anche tenuto conto che la soglia affermata dalla Corte di Giustizia europea nella sentenza "Schrems" è quella della "sostanziale equivalenza"[95].

Gli Stati Uniti dovrebbero dunque garantire tutti gli elementi chiave previsti in materia di protezione dei dati europea.

Il Garante ritiene dunque probabile un'ulteriore invalidazione dell'accordo da parte della Corte di Giustizia dell'Unione Europea, e critica la scarsa lungimiranza dell'accordo, che potrebbe presto portare ad una nuova situazione di incertezza per le imprese.

Un'ulteriore critica del Garante è rivolta alla necessità di controlli più mirati nelle operazioni di *signal intelligence*[96], con le quali una quantità molto elevata di dati potrebbe essere oggetto di raccolta e utilizzo.

In conclusione il Garante dichiara che il "Privacy Shield" può essere un passo nella giusta direzione, ma richiede ancora miglioramenti che lo portino a tutelare maggiormente i diritti dell'individuo e alla protezione dei dati personali previsti dall'UE, suggerendo l'adozione di regole più specifiche per regolare l'accesso alle autorità americane ai dati personali e la necessità di adeguare l'accordo ai principi di "privacy by

[94] Parere 01/2016 WP238 sulla decisione di adeguatezza della bozza di accordo "Privacy Shield EU-US", Consultabile su: http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
[95] Schrems, nota 165, punti 71, 73, 74 e 96
[96] Attività d'intelligence attraverso captazione di segnali

design" e "privacy by default", previsti dal nuovo Regolamento sulla Protezione dei Dati[97].

4.2 La caducazione dell'Accordo "Privacy Shield"

A pochi anni dall'Accordo tra UE-USA "Privacy Shield", e dalla nota sentenza "Schrems", la Corte di Giustizia dell'Unione europea il 16 luglio 2020 si è pronunciata in merito al regime di trasferimento dei dati tra l'Unione europea e gli Stati Uniti, invalidando l'adeguatezza del "Privacy Shield", adottata nel 2016 dalla Commissione europea in seguito alla decadenza dell'Accordo "Safe Harbour"[98].

Nella stessa sentenza la Corte ha ritenuta valida la decisione 2010/87 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in Paesi terzi.

Nell'attuale contesto normativo, in particolare quello imposto dal Regolamento (UE) 2016/679, la sentenza è destinata ad avere un impatto profondo per tutti gli operatori coinvolti, non solo i grandi player dell'economia digitale (Facebook & Co.) ed i fornitori più piccoli di servizi digitali, ma anche per le imprese europee che di tali fornitori tecnologici si avvalgono nell'ambito della propria attività economica.

Come dicevamo nei capitoli precedenti, qualche mese dopo la prima sentenza Schrems, il 12 luglio 2016, la Commissione, per superare le conseguenze dell'invalidità della Decisione relativa al Safe Harbor, aveva adottato la Decisione di esecuzione (UE) 2016/1250 sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy ("Decisione Privacy Shield")[99].

La CGUE ha quindi dovuto giocoforza prendere posizione anche su alcune questioni pregiudiziali relative alla Decisione Privacy Shield ed alla validità.

---

[97] Sintesi del parere del Garante europeo della protezione dei dati sul progetto di decisione in merito all'adeguatezza dello scudo UE–USA per la privacy

[98] La Corte dichiara invalida la decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy; per approfondimenti: "https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091it.pdf"

[99]Decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy [notificata con il numero C(2016) 4176]: per maggiori approfondimenti: "https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016D1250"

Al termine del complesso procedimento che si è cercato di descrivere sopra in modo sintetico, lo scorso 16 luglio 2020, la CGUE ha finalmente emanato la sentenza in commento.

La sentenza in commento, oltre a decidere in merito alla validità della Decisione SCC e della Decisione Privacy Shield, si è anche occupata di fornire alcuni importanti chiarimenti.

In primo luogo, la CGUE ha chiarito che l'art. 2, paragrafi 1 e 2, del GDPR (che ne disciplina l'ambito di applicazione materiale) va interpretato nel senso che rientra nell'ambito di applicazione del GDPR un trasferimento di dati a fini commerciali da un operatore stabilito all'interno di uno stato membro verso uno stabilito in un paese terzo, nonostante, durante o dopo tale trasferimento, i suddetti dati possano essere sottoposti a trattamento da parte delle autorità del paese terzo.

La CGUE prosegue chiarendo che l'art. 46 va interpretato nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti dal paragrafo 1 devono garantire che i diritti degli interessati i cui dati personali sono trasferiti verso un paese terzo sulla base di clausole tipo di protezione adottate dalla Commissione ai sensi del paragrafo 2, lettera c), godano di un livello di protezione non necessariamente identico, ma quantomeno sostanzialmente equivalente a quello garantito all'interno dell'Unione dal GDPR, interpretato alla luce della Carta.

Per valutare il livello di protezione, si devono considerare sia le clausole contrattuali convenute tra titolare o responsabile del trattamento stabilito nell'Unione ed il destinatario stabilito nel paese terzo interessato, sia gli elementi rilevanti del sistema giuridico di tale paese terzo relativamente all'accesso delle autorità di tale paese ai dati personali trasferiti.

Nella sentenza in commento, la CGUE si occupa anche di chiarire la portata dell'art. 58, paragrafo 2, lettere f) e j), che, in relazione alle autorità di controllo, prevede che queste hanno, tra gli altri, il potere di imporre una limitazione provvisoria o definitiva al trattamento, compreso il divieto, e di ordinare la sospensione dei flussi di dati verso un paese terzo.

Al riguardo, la CGUE ha chiarito che tale norma deve essere interpretata nel senso che – a meno che non esista una decisione di adeguatezza adottata dalla Commissione ai sensi dell'art. 45 del GDPR (come la Decisione Privacy Shield) – l'autorità di controllo

competente è tenuta a sospendere o a vietare il trasferimento verso un paese terzo effettuato sulla base di clausole tipo di protezione adottate dalla Commissione (come nel caso della Decisione SCC)[100], qualora tale autorità ritenesse, alla luce delle circostanze proprie di tale trasferimento, che tali clausole non siano o non possano essere rispettate in tale paese e che la protezione richiesta dal diritto dell'Unione non possa essere garantita con altri mezzi, nel caso in cui il titolare o il responsabile stabiliti nell'Unione non abbiano loro stessi sospeso o cessato il trasferimento.

L'*High Court* irlandese aveva posto al riguardo alcune questioni pregiudiziali, ed in particolare:

se l'autorità di controllo di uno stato membro sia o meno vincolata dalle constatazioni contenute nella Decisione Privacy Shield;

se, considerando le constatazioni fatte dalla stessa *High Court* in merito al diritto USA, il trasferimento verso tale paese sul fondamento delle clausole tipo di protezione di cui alla Decisione SCC violi i diritti di cui agli 7, 8 e 47 della Carta, che sanciscono rispettivamente il diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali ed il diritto ad un ricorso effettivo e a un giudice imparziale;

se l'istituzione della figura del "mediatore" menzionato nell'allegato III alla Decisione Privacy Shield sia compatibile con l'art. 47 della Carta.

Come chiarito all'interno della sentenza, per poter dare una risposta completa al giudice del rinvio (l'*High Court* irlandese), la CGUE ha dovuto esaminare la conformità della Decisione Privacy Shield al GDPR, letto alla luce della Carta.

La sentenza, quindi, analizza in dettaglio il contenuto della Decisione Privacy Shield, evidenziandone, tra l'altro, i seguenti elementi:

come nel caso della decisione 2000/520/CE (*Safe Harbor*), anche la Decisione Privacy Shield sancisce il primato delle esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia rispetto ai principi relativi alla protezione dei dati sanciti nella stessa Decisione Privacy Shield, il che rende possibili ingerenze sui

[100] DECISIONE DELLA COMMISSIONE del 5 febbraio 2010 relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio; https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32010D0087&from=IT

diritti fondamentali delle persone, derivanti dall'accesso da parte delle autorità USA ai dati personali trasferiti dall'Unione agli Stati Uniti;

la Commissione, nella Decisione Privacy Shield, ha quindi valutato le limitazioni e le garanzie previste dalla normativa statunitense, in particolare l'art. 702 del *Foreign Intelligence Surveillance Act* (FISA), che autorizza programmi sorveglianza PRISM e UPSTREAM, l'*Executive Order* (EO) 12333 e il *Presidential Policy Directive* (PPD) 28, in relazione all'accesso ai dati trasferiti negli USA e l'utilizzo degli stessi da parte delle pubbliche autorità statunitensi, constatando, all'esito di tale valutazione, che gli Stati Uniti si limitano a quanto strettamente necessario per conseguire l'obbiettivo legittimo ricercato, e che contro tali ingerenze esiste comunque una tutela giuridica efficace.

Tuttavia, la CGUE evidenzia che, in merito agli aspetti sopra menzionati, il giudice di rinvio invece ha dei dubbi rispetto alle conclusioni della Commissione, in quanto secondo l'*High Court* il diritto degli Stati Uniti non prevedrebbe garanzie e limitazioni rispetto alle ingerenze autorizzate dalla sua normativa nazionale né una tutela giurisdizionale effettiva, in quanto l'instaurazione del mediatore non rimedierebbe alle lacune dell'ordinamento USA.

La sentenza prosegue descrivendo i diritti fondamentali i cui agli art. 7 e 8 della Carta, precisando altresì che, ai sensi dell'art. 52, paragrafo 1, della Carta stessa, "eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà" e che *"*nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

La CGUE ha quindi esaminato la normativa statunitense sopra citata ed i relativi programmi di sorveglianza, alla luce di quanto previsto nella Carta, e nell'ambito di tali analisi ha rilevato che:

l'*United States Foreign Intelligence Surveillance Court* non autorizza singole misure di sorveglianza ma programmi di sorveglianza (ad esempio, PRISM e UPSTREAM) basati sull'art. 702 del FISA: il controllo di tale corte, quindi, non riguarda il fatto se la persona è un obbiettivo adatto a fornire informazioni di intelligence, ma solo se i programmi sono in linea con gli obbiettivi di intelligence;

conseguentemente, dall'art. 702 del FISA non risulta alcuna limitazione all'autorizzazione, né l'esistenza di garanzie per i cittadini stranieri e, conseguentemente, l'art. 702 del FISA "non è idoneo a garantire un livello di tutela sostanzialmente equivalente a quello garantito dalla Carta";

sebbene la PPD-28 imponga alcuni limiti e requisiti ai programmi di sorveglianza fondati sull'art. 702 del FISA, che sarebbero vincolanti per i servizi di intelligence USA, lo stesso governo degli Stati Uniti ha ammesso, in risposta ad un quesito della Corte, che in realtà la PPD-28 non conferisce agli interessati diritti azionabili davanti ai giudici, con la conseguenza che la PPD-28 non è idonea a garantire un livello di protezione sostanzialmente equivalente a quello risultante dalla Carta, contrariamente a quanto previsto dall'art. 45, paragrafo 2, lett. a), del GDPR, che fa dipendere il livello di protezione anche dall'esistenza di "diritti effettivi e azionabili dagli interessati";

in merito ai programmi di sorveglianza basati sull'EO 12333, nemmeno essi conferiscono diritti nei confronti della autorità azionabili davanti ai giudici;

La CGUE conclude quindi la sua analisi affermando in modo perentorio che nessuna delle norme sopra citate corrispondono ai requisiti minimi connessi, in base al diritto dell'Unione, al principio di proporzionalità, quindi i programmi di sorveglianza che si fondano su tali norme non si possono considerare limitati allo stretto necessario.

Conseguentemente, le limitazioni alla protezione dei dati personali derivanti dalla normativa interna USA, non corrispondono ai requisiti previsti dall'art. 52, paragrafo 1, della Carta.

La sentenza prosegue analizzando la figura del mediatore in relazione all'art. 47 della Carta.

A tal proposito, la CGUE contesta quanto sostenuto dalla Commissione nella Decisione Privacy Shield, secondo cui con l'istituzione del mediatore si poteva ritenere che gli Stati Uniti assicurassero un livello di protezione sostanzialmente equivalente a quello di cui all'art. 47 della Carta, con le seguenti convincenti argomentazioni:

il mediatore riferisce direttamente al Segretario di Stato, che lo nomina;

la Decisione Privacy Shield non contiene indicazioni in merito al fatto che il mediatore è autorizzato o meno a prendere decisioni vincolanti per i servizi di intelligence;

il meccanismo di mediazione non fornisce quindi mezzi di ricorso che offra garanzie sostanzialmente equivalenti a quelle di cui all'art. 47 della Carta.

Secondo la CGUE, dunque, nel sostenere, all'art. 1, paragrafo 1, della Decisione Privacy Shield, che gli USA assicurano un livello adeguato di protezione dei dati personali trasferiti dall'Unione verso organizzazione stabilite negli USA nell'ambito dello scudo Unione europea/USA, la Commissione ha disatteso i requisiti previsti dall'art. 45, paragrafo 1, del GDPR, letti alla luce degli articoli 7, 8 e 47 della Carta.

La conseguenza di quanto precede è che l'art. 1 della Decisione Privacy Shield, e quindi tutta la Decisione Privacy Shield che si fonda su tale art. 1, deve essere considerata invalida.

Infine, la CGUE rileva che l'annullamento della Decisione Privacy Shield non comporta alcuna lacuna normativa, visto che l'art. 49 del GDPR stabilisce a quali condizioni possono avvenire trasferimenti di dati personali verso paesi terzi quando manca una decisione di adeguatezza ai sensi dell'art. 45 del GDPR oppure mancano garanzie appropriate ai sensi dell'art. 46 del GDPR.

CAPITOLO TERZO

L'impatto del GDPR sulle società multinazionali alla luce del caso "Cambridge Analytica"

1. GDPR 3 ANNI DOPO: QUAL È IL LIVELLO DI MATURITÀ DELLE AZIENDE

1.1 Adeguamento del GDPR: lo stato delle imprese italiane

A poco meno di tre anni dall'entrata in vigore del nuovo Regolamento (UE) 2016/679 la situazione delle imprese italiane in merito alla sua applicazione è cambiata positivamente.

Abbiamo già visto nei paragrafi precedenti come le *Big Tech* quali *Facebook, Google, Amazon* e non solo, soprattutto dopo lo scandalo "*Cambridge Analytica*", abbiano adeguato le *policy* interne.

In Italia si registrano progressi significativi in tema di adeguamento alla normativa, con aumenti nel budget a disposizione delle organizzazioni e crescita di maturità, in termini di concretezza dei progetti e di cambiamenti organizzativi mirati.

La complessità e l'importanza della materia richiedono comunque continui sforzi da parte delle imprese, necessari per adeguarsi ai principi imposti dalla normativa in materia di protezione dei dati personali e per rispondere alle richieste delle Autorità.

A tal proposito in diversi Stati europei sono state irrogate le prime sanzioni pecuniarie per violazione del Regolamento.

In Italia, al contrario, l'atteggiamento dell'Autorità Garante è stato inizialmente accomodante, complici anche i ritardi nell'elezione del nuovo collegio dell'Autorità Garante.

Tuttavia, nel periodo più recente si è assistito a un'intensificazione dei controlli e delle ispezioni e all'applicazione delle prime sanzioni previste dalla normativa locale e sovranazionale in materia di protezione dei dati.

Grazie alla Ricerca condotta dall'Osservatorio *Cyber Security & Data Protection*[101], possiamo osservare come è cambiato il contesto italiano.

Per esplorare i cambiamenti in corso nelle imprese italiane relativi alla Data Protection, l'Osservatorio ha considerato quattro aspetti:

- Stato dei progetti di adeguamento
- Budget dedicato
- Azioni implementate
- Criticità riscontrate

Dallo studio si evince che quasi la totalità delle aziende italiane ha messo in atto o perfezionato progetti di adeguamento al GDPR.

È opportuno anche ricordare che un progetto di adeguamento al GDPR deve comprendere le seguenti fasi:

1. La creazione del registro dei trattamenti: il registro dei trattamenti, disciplinato dall'articolo 30 del Regolamento, è un documento volto a tenere traccia di tutte le operazioni di trattamento effettuate:
2. Stesura/ modifica della modulistica: un esempio è dato dall'informativa, che deve essere completa ed aggiornata secondo le prescrizioni del GDPR;
3. Individuazione dei ruoli e delle responsabilità: è tassativamente necessario, sulla base della nuova normativa, individuare e contrattualizzare tutti i responsabili del trattamento
4. Definizione delle politiche di sicurezza e valutazione dei rischi: tenuto conto della natura, dell'ambito di applicazione e delle finalità del trattamento, nonché dei diversi rischi per i diritti e le libertà delle persone fisiche, ogni titolare deve mettere in atto misure tecniche e organizzative adeguate al fine di garantire la conformità del trattamento stesso al Regolamento
5. Processo di data *breach:* con il termine "*data breach*" si intende il complesso di azioni che deve svolgere il titolare del trattamento in caso di distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trattati. Pertanto, ai sensi dell'articolo 33 del Regolamento ne deve dare

[101] https://www.osservatori.net/it/ricerche/osservatori-attivi/cybersecurity-data-protection

comunicazione all'Autorità di Controllo (entro 72 ore dall'avvenuta conoscenza della violazione) e, nei casi più gravi, anche agli interessati;

6. Valutazione d'impatto sulla protezione dei dati personali: quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate, il GDPR obbliga i titolari a svolgere una valutazione di impatto (c.d. Data Protection Impact Assessment – DPIA) prima di dare inizio al trattamento stesso;
7. Implementazione dei processi per l'esercizio dei diritti dell'interessato: il GDPR ha ampliato il novero dei diritti concessi agli interessati, in particolare introducendo in modo puntale il diritto alla portabilità dei dati e il diritto all'oblio;
8. Data Protection Officer (DPO): il GDPR prevede la nuova figura del Data Protection Officer, la cui nomina è obbligatoria in una serie di ipotesi previste dall'articolo 37 del Regolamento[102]

Con riferimento alle suddette fasi, dalla rilevazione è emerso che le principali azioni che sono state già compiute dalle organizzazioni riguardano la creazione del registro dei trattamenti (85%), l'individuazione dei ruoli e delle responsabilità (81%), la modifica della modulistica (76%), la procedura di *data breach notification* (68%), la definizione delle politiche di sicurezza e di valutazione dei rischi (66%), la valutazione d'impatto sulla protezione dei dati personali (56%) e l'implementazione dei processi per l'esercizio dei diritti dell'interessato (54%)[103].

Il dato più interessante, tuttavia si riscontra con riferimento alla figura del DPO all'interno delle aziende.

Il Data Protection Officer è presente formalmente nel 65% delle organizzazioni, mentre nel 6% dei casi si tratta di una presenza di tipo informale.

Rispetto alla rilevazione dell'osservatorio condotta l'anno precedente si è registrato un incremento del 46 % di aziende che hanno introdotto la figura in esame nel proprio organico: nel 2017 infatti, le percentuali si attestavano rispettivamente al 15% e al 10%.

[102] Vedi cap. III, Par. 2
[103] https://www.osservatori.net/it/ricerche/osservatori-attivi/cybersecurity-data-protection

1.2 Il Decreto 101/2018 di adeguamento della normativa italiana al GDPR

Il 4 settembre 2018 è stato pubblicato in Gazzetta Ufficiale n. 205 il Decreto Legislativo 10 agosto 2018, n. 101 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati*"

Come abbiamo avuto modo di affrontare, il Decreto Legislativo 196/2003 (vecchio "Codice privacy") non è stato abrogato, bensì modificato ed integrato dal nuovo decreto che ne realizza l'adeguamento alle disposizioni del GDPR.

La normativa italiana, come è bene sottolineare, va interpretata e applicata conformemente a quella europea, in quanto integra, ma non sostituisce il GDPR.

Infatti, ai sensi dell'articolo 288 TFUE, si ricorda che "ciascun regolamento europeo, e pertanto anche il Regolamento 679/2016 (GDPR), ha portata generale (..) è obbligatorio in tutti i suoi stati membri e direttamente applicabile in ciascuno degli stati membri.

Passiamo ad analizzare la struttura e le principali novità apportate dal nuovo Decreto Legislativo 101/2018.

Il Decreto è suddiviso in 6 capi:

- Il Capo I e il Capo II sono innovativi e sostitutivi di tutta la Parte I del vecchio Codice Privacy e riguardano sostanzialmente principi e disposizioni generali, disposizioni in materia di diritti degli interessati, titolare e responsabile del trattamento.

In base all'articolo 2-quater, i codici di condotta (ora rinominati "Regole deontologiche), contenuti nell'allegato A del vecchio Codice Privacy dovranno essere riveduti e corretti alla luce delle norme europee e riproposti all'esame del garante che , se ritenuti conformi al Regolamento, li approverà: gli stessi Allegati B (misure minime di sicurezza) e C (trattamento dei dati in ambito giudiziario o per fini di polizia), invece, sono stati abrogati.

Si segnala, inoltre, l'articolo 2-quinquies in tema di consenso del minore in relazione ai servizi della società dell'informazione; con riguardo a tali servizi il trattamento dei dati del minore di età inferiore ai 14 anni è lecito a condizione che il consenso sia prestato da chi esercita la responsabilità genitoriale.

Invece, l'articolo 2-ter evidenzia la base giuridica del trattamento dei dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri (base giuridica diversa dal consenso e prevista all'articolo 6, paragrafo 3, lettera b) del GDPR) è costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.

L'articolo 2-sexies, invece, pone l'accento sul trattamento di categorie particolari di dati personali (di cui all'articolo 9 GDPR) necessario per motivi di interesse pubblico rilevante, ed elenca una serie di materie in cui l'interesse pubblico si considera rilevante (ad esempio, l'accesso a documenti amministrativi e accesso civico; cittadinanza, immigrazione, asilo; controlli e ispezioni; obiezione di coscienza; gestione rapporti di lavoro ecc..).

L'articolo 2-septies disciplina dettagliatamente il trattamento di dati genetici, biometrici e relativi alla salute; tali dati possono essere trattati solo in presenza di una delle condizioni elencate al paragrafo 2 del suddetto articolo e solo in conformità alle misure di garanzia stabilite dal Garante all'interno di un provvedimento adottato con cadenza almeno biennale.

L'articolo 2-octies riguarda invece i dati relativi a condanne penali (di cui all'articolo 10 GDPR).

Fatto salvo a quanto previsto dal d.lgs. 51/2018 (in tema di trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali), il loro trattamento, quando non avviene sotto il controllo dell'autorità pubblica, non può essere autorizzato solo da una norma di legge o, nei casi pervisti dalla legge, di regolamento, riguardanti in particolare (a titolo esemplificativo e non esaustivo): adempimento di obblighi e esercizio di diritti da parte di interessato o titolare in materia di diritto del lavoro; accertamento, esercizio o difesa di un diritto in sede giudiziaria, esercizio del diritto di accesso ai dati e ai documenti amministrativi, accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto ecc..).

Particolarmente interessante è l'articolo 2-undecies, rubricato "limitazione ai diritti dell'interessato", il quale elenca una serie di situazioni in cui l'esercizio dei diritti dell'interessato di cui agli articoli dal 15 al 22 del GDPR, e il reclamo di cui all'articolo 77 GDPR, subiscono delle limitazioni, in quanto possono comportare un pregiudizio effettivo e concreto, agli interessati tutelati in base alle disposizioni in materia di riciclaggio, allo svolgimento di investigazioni difensive o all'esercizio di un diritto in sede giudiziaria, alla riservatezza dell'identità del dipendente che segnala, ai sensi della legge 30 novembre 2017 n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio (c.d. Whistleblowing)[104].

Un'ulteriore novità è rappresentata dall'articolo 2-terdecies che disciplina l'esercizio dei diritti di cui agli articoli da 15 a 22 del GDPR, qualora l'interessato sia una persona deceduta; tali diritti possono essere esercitati da chi ha un interesse proprio o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari e meritevoli di protezione.

Infine, l'articolo 2-quaterdecies in tema di attribuzioni e compiti a soggetti designati disciplina che il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità. E nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento dei dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

Il titolare o il responsabile individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta (è questo al riferimento alle c.d." persone autorizzate", ex incaricati del trattamento in base al vecchio Codice Privacy).

- Il Capo III contiene numerose modifiche alla Parte II del Codice privacy e riguarda sostanzialmente disposizioni in materia di trattamento dei dati personali relativi a specifici settori: trattamento da parte di forze di polizia e per fini di sicurezza nazionale o difesa; trattamento in ambito pubblico; trattamento di dati personali in ambito sanitario; trattamento di dati relativi a studenti; trattamenti ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici; altri trattamenti in ambito pubblico o di

[104] Whistleblowing, la nuova Direttiva europea e la protezione dei dati: https://www.altalex.com/documents/news/2020/02/13/whistleblowing-nuova-direttiva-europea-protezione-dati

interesse pubblico; trattamenti nell'ambito del rapporto di lavoro; servizi di comunicazione elettronica; attività giornalistiche.

Nell'ambito di trattamenti di dati personali relativi al rapporto di lavoro, l'articolo 9 del decreto di adeguamento prevede l'inserimento nel Codice privacy dell'articolo 111-bis che stabilisce che le informazioni di cui all'articolo 13 GDPR, in caso di candidature spontanee, vengano fornite al primo contatto utile, successivo all'invio del curriculum.

Inoltre, nei limiti di cui all'articolo 6, paragrafo 1 lettera b del GDPR (trattamento necessario per l'esecuzione di un contratto o di misure precontrattuali adottate su richiesta dell'interessato), il consenso al trattamento dei dati personali presenti nei curricula non è dovuto.

Sono innovativi anche i riferimenti al telelavoro, lavoro agile e domestico e al controllo a distanza, in riferimento al quale viene ribadito il divieto di controllo a distanza dei lavoratori previsto dall'articolo 4 dello Statuto dei Lavoratori.

- Il Capo IV apporta modifiche alla Parte III del Codice privacy e riguarda principalmente organizzazione, compiti e poteri del Garante, nonché sanzioni e illeciti penali

Per quanto concerne gli strumenti attraverso cui rivolgersi all'autorità di controllo, si evidenzia che l'articolo 13 del decreto 101/2018 ha innovato l'articolo 144 del Codice privacy prevedendo adesso che "chiunque può rivolgere una segnalazione che il Garante può valutare può valutare anche ai fini dell'emanazione dei provvedimenti di cui all'articolo 58 del Regolamento", articolo che elenca tutti i poteri dell'autorità di controllo; si ricorda a tal proposito, che in precedenza solo l'interessato poteva inviare segnalazioni.

Anche l'articolo 141 è stato modificato dall'articolo 13 lettera c) del decreto in esame e, a seguito di tale modifica, adesso cita: "L'interessato può rivolgersi al Garante mediante reclamo ai sensi dell'articolo 77 del Regolamento".

Il reclamo resta l'unico strumento di tutela amministrativa per l'interessato.

Non è infatti più possibile presentare il ricorso dinnanzi al Garante, come strumento di tutela alternativa a quella giurisdizionale.

La nuova normativa conferisce al Garante compiti e poteri ulteriori, in particolare l'articolo 154-ter attribuisce all'autorità la legittimazione ad agire in giudizio nei

confronti del titolare o del responsabile del trattamento, in caso di violazione delle disposizioni in materia di protezione dei dati personali.

L'articolo 166 del Codice privacy è completamente novellato dal decreto 101/2018 e definisce in modo dettagliato i criteri di applicazione delle sanzioni amministrative pecuniarie di cui all'articolo 83 GDPR, nonché i provvedimenti correttivi di cui all'articolo 58 GDPR.

Il Garante è l'organo deputato ad irrogare tali sanzioni e adottare tali provvedimenti.

Per quanto riguarda gli illeciti penali, è stato novellato l'articolo 167 del vecchio Codice privacy e sono state aggiunte due nuove fattispecie di reato.

È stata ampliata la casistica riconducibile a ipotesi di trattamento illecito di dati personali e previsto che il pubblico ministero informi senza ritardo il Garante, non appena abbia ricevuto la notizia di reato.

L'articolo 167-bis introduce il reato di comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala.

L'articolo 167-ter introduce il reato di acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala.

- Il Capo V contiene disposizioni processuali e non ha subito sostanziali modifiche
- Il Capo VI, invece, è del tutto nuovo e contiene disposizioni transitorie e finali (articoli da 18 a 27 del decreto 101/2018)

In particolare, si segnala l'articolo 21 in tema di autorizzazioni generali del Garante per la protezione dei dati personali: le cui autorizzazioni generali relative alle situazioni di trattamento di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché al Capo IX del GDPR saranno sottoposte a revisione ed approvazione del Garante, qualora siano conformi alla normativa europea.

Invece, le autorizzazioni del Garante adottate prima della data di entrata in vigore del decreto 101/2018 e relative a trattamenti diversi da quelli precedentemente elencati, cessano di produrre effetti.

Discorso diverso per i provvedimenti del Garante antecedenti al 25 maggio 2018 (come, ad esempio, quelli in materia di video sorveglianza, amministratori di sistema, marketing, ecc..): tali provvedimenti continuano ad applicarsi, in quanto compatibili con il GDPR e con le disposizioni del nuovo Codice privacy.

Infine, l'articolo 24, sempre con riferimento al regime sanzionatorio, per il principio penalistico del *favor rei,* prevede che il decreto in esame sostituisce le sanzioni penali previste dal Codice privacy con le sanzioni amministrative previste dal Regolamento europeo, anche riguardo a violazioni commesse anteriormente alla data di entrata in vigore del decreto stesso e sempre che il procedimento penale non sia stato definito con sentenza o con decreto divenuti irrevocabili.

2. LE AZIONI COMPIUTE

2.1 Il DPO (Data Protection Officer)

Come abbiamo avuto modo ampliamente di affrontare nei capitoli precedenti, le aziende, dall'entrata in vigore del Regolamento (UE) 679/2916, hanno dovuto adeguarsi ad una maggiore tutela richiesta dall'Unione Europea verso i dati particolari di tutti gli utenti del web e no.

Per far si che ciò accada, all'interno della quarta sezione del Capo IV del Regolamento è stata introdotta una nuova figura, quella del *Data Protection Officer* (DPO).

Il DPO, ovvero il Responsabile della protezione dei dati, è un istituto già noto all'interno delle multinazionali americane[105], nonché in alcuni ordinamenti europei dove già sono state introdotte figure similari[106] come Germania, Austria e Repubblica Ceca.

Dunque, tramite l'emanazione del Regolamento, data la sua generale applicabilità e la sua efficacia diretta esplicata verso ogni ordinamento nazionale degli Stati membri, per la prima volta entra in pianta stabile nell'ordinamento comunitario la figura del Data Protection Officer, che diventerà una figura di riferimento per la protezione dati degli individui, e che si aggiungerà al novero dei soggetti che operano all'interno del procedimento di trattamento dei dati personali, insieme al titolare e al responsabile.

L'articolo 37 espone al primo paragrafo i casi in cui sistematicamente si rende necessaria la nomina da parte del titolare e del responsabile del trattamento del DPO e cioè quando:

a. Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b. Le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità,

[105] Cfr. F. PIZZETTI, Privacy e il Diritto Europeo alla Protezione dei Dati Personali, Torino, 2016, p. 155.
[106] Il riferimento è al datenschutzbeauftragter introdotto con il Bundesdatenschutzgesetz del 2003 e con il quale il responsabile della protezione dei dati sembra presentare svariate analogie come: l'obbligo di nomina in base ad un numero minimo di dipendenti (secondo l'originaria formulazione dell'art. 37che sembra essere stata espunta dal dettato normativo), la possibilità per il DSB di avere accesso a tutte le informazioni relative ai trattamenti, il divieto di penalizzare il DSB per le funzioni esplicate in base al ruolo che riveste e l'approccio, derivante dal modello tedesco, di corporate self-monitoring dove sono le società che direttamente si fanno carico di un adeguamento e di uno scrupoloso controllo nella gestione dei dati personali. G. M. RICCIO, Data Protection Officer e altre figure, cit., pag. 50-51.

richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c. Le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie di dati personali di cui all'articolo 9 (si fa riferimento alla categoria dei c.d. dati particolari) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il *Data Protection Officer* si configura dunque come una figura estremamente garantista a tutela degli interessi e diritti delle persone fisiche, la cui necessità di nomina (intesa come un vero obbligo gravante sul titolare del trattamento) è prevista in quei particolari settori, a carattere prevalentemente pubblicistico o dove categorie di dati più o meno sensibili vengono trattati, ma non solo: infatti la nomina può essere necessaria anche qualora le attività del titolare trattino dati personali su larga scala[107], richiedendo altresì il monitoraggio[108] costante e sistematico degli interessati.

[107] Il Regolamento non dà una definizione del termine "larga scala". A tal proposito di grande utilità sono state le Linee-guida sui responsabili della protezione dei dati (RPD) adottate il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017), dove il Gruppo Articolo 29 ha fornito ampie delucidazioni interpretative e chiari esempi a supporto. Il gruppo fornisce dei criteri per capire quanto un trattamento sia applicato su larga scala e sono: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; 1) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; 2) la durata, ovvero la persistenza, dell'attività di trattamento; 3) la portata geografica dell'attività di trattamento. Gli esempi di trattamenti su larga scala che il Gruppo riporta sono:1) trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività; 2) trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio); 3) trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food; 4) trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività; 5) trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale; 6) trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici. GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, le Linee-guida sui responsabili della protezione dei dati (RPD) adottate il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017), WP 243, 2016. Bisogna sottolineare comunque come il Considerando n. 91 del Regolamento in realtà fornisca un abbozzo dei criteri per definire il concetto di trattamenti su larga scala identificandoli come quelli che "mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato". Continua poi prevedendo che "Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato".

[108] Come per il concetto di larga scala anche quello di monitoraggio regolare e sistematico non trova un'esplicita spiegazione all'interno della disposizione regolamentare. Sempre all'interno delle linee guida predisposte dal Gruppo di lavoro art. 29 sono forniti esempi riguardo ciò che il Gruppo intende per "regolare" e "sistematico". L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del WP29: 1) che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito; 2) ricorrente o ripetuto a intervalli costanti; 3) che avviene in modo costante o a intervalli periodici. L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29: 1) che avviene per sistema; 2) predeterminato, organizzato o metodico; 3) che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; 4) svolto nell'ambito di una strategia. Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc. GRUPPO DI LAVORO ARTICOLO 29 IN

Oppure, come specificato al paragrafo 4, qualora sia previsto dal diritto dell'Unione o da una previsione normativa di uno Stato membro, nel caso in cui il titolare e il responsabile del trattamento, nei casi diversi dal paragrafo 1, volontariamente possono designare un responsabile della protezione dei dati personali.

Il responsabile dei dati personali è una figura altamente tecnica e professionale che è scelta in base alla conoscenza specifica della normativa e della prassi in tema di protezione dei dati personali e in base alla capacità di assolvere ai compiti previsti dall'articolo 39 del Regolamento.

È previsto inoltre che il DPO possa essere anche un dipendente del titolare o del responsabile del trattamento, o in alternativa essere assunto in base ad un contratto di servizi; ad ogni modo incombe sul titolare l'obbligo di pubblicare i dati di contatto del *privacy officer* e di comunicarli all'autorità di controllo (par. 6 e 7, arti.37).

Ulteriori importanti disposizioni in merito al soggetto del responsabile della protezione dati sono contenute all'articolo 38 denominato "Posizione del responsabile della protezione dei dati".

Innanzitutto, è previsto che il *Data Protection Officer* sia coinvolto tempestivamente e adeguatamente in tutte le questioni riguardante la protezione dei dati durante il trattamento e, al fine di garantirne l'autonomia e l'indipendenza, che sia sostenuto direttamente dal titolare e dal responsabile che hanno il compito di fornire le risorse necessarie al responsabile della protezione dati per assolvere i suoi compiti e mantenere la propria conoscenza specialistica.

Inoltre, è previsto che il *Data Protection officer* mantenga rapporti direttamente con il vertice gerarchico del trattamento (titolare o al posto suo il responsabile) in modo tale da evitare rapporti diretti con altri soggetti ed evitare che così aumentino gli eventuali centri di imputazione della responsabilità nel caso in cui si verifichi un illecito riferibile al trattamento e infine che il DPO non sia rimosso o penalizzato per aver adempiuto ai propri compiti.

Il responsabile ella protezione dati si configura poi come un soggetto intermedio tra titolare e interessato e tra titolare e autorità di controllo.

Infatti, una funzione molto importante del *Data Officer*, data anche l'autonomia e l'indipendenza di cui gode, è quella di essere un utile referente per le autorità garanti, ma soprattutto per gli interessati, che finalmente trovano un diretto riscontro alle proprie istanze nella persona del *Data Protection Officer*.

Ciò è ricavabile direttamente dal dettato normativo quando al paragrafo 4 dell'articolo 38 il Regolamento prevede che "Gli interessati possono contattare il responsabile della protezione

MATERIA DI PROTEZIONE DEI DATI PERSONALI, le Linee-guida sui responsabili della protezione dei dati (RPD) adottate il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017), WP 243, 2016.

dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento".

Per quanto riguarda, invece, la figura di cooperazione del DPO con le autorità di controllo, l'articolo 39 rubricato "Compiti del responsabile della protezione dei dati", prevede alla lettera d) che il responsabile è incaricato in linea generale di "cooperare con l'autorità di controllo", mentre alla successiva lettera e) di "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.".

Ulteriori compiti previsti dall'articolo 39, oltre al generale obbligo di considerare ai fini del trattamento, i rischi inerenti, la natura, l'ambito d'applicazione, il contesto e le finalità, il responsabile della protezione dati è incaricato inoltre di:

a) Informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) Sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) Fornire, se richiesto, un parare in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35.

Per il Gruppo di Lavoro ex. Articolo 29 la nomina di un *Data Protection Officer* è importante in quanto questa figura rappresenta un elemento fondante ai fini della responsabilizzazione.

La stessa presenza del DPO può facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese, nel rispetto del principio di *accountability*.

Il Gruppo ricorda, inoltre, che il responsabile della protezione dati svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del Regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e pre impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.

Pertanto, i Garanti europei consigliano che la presenza del *Data Protection Officer* sia l'approccio standard all'interno della struttura del titolare e del responsabile, prevedendo inoltre, la necessità che il DPO partecipi ai gruppi di lavoro che si occupano delle attività di trattamento, all'interno della struttura suddetta[109].

2.2 Il registro del Trattamento dati

Il Regolamento (UE) 2016/679 prevede, all'articolo 30, una delle necessarie attività di *compliance* aziendale, in materia di dati personali, da definirsi quale parte necessaria di un sistema di corretta gestione dei dati[110]: il "Registro delle attività del trattamento dei dati personali".

Rientra tra gli obblighi del titolare e del responsabile del trattamento definiti nella Sezione I del Capo IV e si tratta di un adempimento nuovo anche se ha delle affinità con l'elenco dei trattamenti contenuto nel Documento Programmatico sulla Sicurezza previsto dal Codice *privacy* fino al 2012 in caso di trattamento di dati particolari e giudiziari.

La funzione del registro è duplice, difatti esso:

a) Rappresenta una misura di responsabilizzazione per il titolare ed il responsabile del trattamento
b) Permetta la verifica successiva da parte dell'Autorità di controllo del rispetto della normativa da parte dei soggetti obbligati (articolo 30)[111]

Il registro è un documento che raccoglie le principali informazioni sulle attività di trattamento compiute dal titolare e, se nominato, dal responsabile del trattamento; è altresì uno strumento fondamentale per tracciare l'esistente; verificare la conformità al regolamento; divulgare informazioni, consapevolezza e condivisione interna; ancorché misure per la pianificazione e controllo della politica della sicurezza di dati e banche di dati.

[109] M. Iaselli, I compiti del Data Protection Officer: chiariamo tutti i dubbi, 21 aprile 2017, in www.agendadigitale.eu.
[110] Sull'utilità della tenuta del registro per qualsiasi organizzazione, anche se con meno di 250 dipendenti, si veda M. GaGliarDi, *Il nuovo obbligo di tenuta del Registro delle attività di trattamento di dati personali*, in G. coManDè e G. MalGieri, *Manuale per il trattamento dei dati personali*, Milano, 2018, p. 66.
[111] Così, Gea arcella, *GDPR: il Registro delle attività di trattamento e le misure di accountability*, in *Rivista Notariato*, 4/2018.

I registri (al plurale in quanto sono tenuti sia dal titolare che dal responsabile del trattamento), rappresentano uno dei basilari elementi di accountability del titolare, ossia uno degli adempimenti più importanti concernenti le attività di trattamento, in quanto sono in grado di fornire un quadro aggiornato delle operazioni e dei trattamenti in essere all'interno della propria organizzazione, indispensabile per ogni attività di valutazione o analisi del rischio e preventivo rispetto a tale attività.

In quanto alla forma che deve assumere il registro, ovviamente deve essere scritto, e preferibilmente in formato elettronico; tali registri non vanno notificati ma dovranno essere messi a disposizione, e/o esibiti, all'Autorità Garante, qualora li richieda, così come previsto dal paragrafo 4 dell'articolo 30: "su richiesta, il titolare del trattamento il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo".

In ogni caso risulta opportuno indicare, oltre alla tipologia di forma del trattamento, per esempio se scritta, anche il luogo ed i mezzi di conservazione atti a prevenire accessi non autorizzati o la perdita accidentale.

Per il formato elettronico, sarà utile indicare gli strumenti elettronici (ai sensi dell'articolo 4, comma 3, lettera b) del d.lgs. 196/2003) adottati da ciascun trattamento, in quanto sono queste informazioni essenziali per individuare, successivamente, i rischi di sicurezza a cui possono essere esposti i dati personali, nonché le responsabilità riguardo la loro gestione e manutenzione.

Va detto anche che nei casi in cui l'utilizzo e la conservazione dei documenti siano in carico presso la struttura organizzativa responsabile del trattamento, gli strumenti informatici sono in genere centralizzati e di competenza di strutture dedicate, come la Gestione dei Sistemi Informativi, o esterne all'organizzazione e riguardanti fornitori di servizi tecnologici.

L'utilità di specificare nel registro, gli strumenti elettronici utilizzati si ritrova anche nella gestione del ciclo di vita del trattamento, perché possono mutare i fornitori di servizi o le tecnologie utilizzate (ad esempio, nuove applicazioni, servizi cloud, ecc..), che possono produrre impatti sulla sicurezza dei dati trattati.

Segnatamente, nelle attività periodiche di aggiornamento del registro e delle misure adottate (articolo 24, comma 1) diventerà più agevole individuare quei

cambiamenti che richiedono di rivedere gli adeguamenti effettuati in precedenza per rispondere agli obblighi previsti dal Regolamento, tra cui la valutazione di impatto per i diritti e le libertà degli interessati in ragione dell'adozione di nuove tecnologie[112].

Il registro del titolare del trattamento contiene le seguenti informazioni:

- Il nome e i dati di contatto del titolare del trattamento e, se presente, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- Le finalità del trattamento;
- La descrizione delle categorie di interessati e delle categorie di dati personali;
- Le categorie di destinatari a cui i dati personali siano stati o saranno comunicati, compresi i destinatari di paesi terzi;
- Se presenti, i trasferimenti di dati personali verso paesi terzi e la loro identificazione;
- I termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.

Quali informazioni devono contenere i registri delle attività del trattamento?[113]

Il Regolamento individua dettagliatamente le informazioni che devono essere contenute nel Registro delle attività di trattamento del titolare (articolo 30, paragrafo 1 del GDPR) e in quello del responsabile (articolo 30, paragrafo 2 del GDPR).

Con riferimento ai contenuti si rappresenta quanto segue:

a) Nel campo "finalità del trattamento" oltre alla precipua indicazione delle stesse, distinta per tipologie di trattamento (es. trattamento dei dati dei dipendenti per la gestione del rapporto di lavoro: trattamento dei dati di contatto dei fornitori per la gestione degli ordini), sarebbe opportuno indicare anche la base giuridica dello stesso (v. articolo 6 del GDPR; in merito, con particolare riferimento al "legittimo interesse", si rappresenta che il registro potrebbe riportare la descrizione del legittimo interesse concretamente perseguito, le "garanzie adeguate" eventualmente approntate, nonché, ove effettuata, la preventiva valutazione d'impatto posta in essere dal titolare.

   Sempre con riferimento alla base giuridica, sarebbe parimenti opportuno: in caso di trattamenti di "categorie particolari di dati", indicare una delle condizioni di cui all'articolo 9, paragrafo 2 del GDPR; in caso di trattamenti di dati relativi a condanne penali e reati, riportare la specifica normativa (nazionale o dell'Unione europea) che ne autorizza il trattamento ai sensi dell'articolo 10 del GDPR;

[112] Linee-guida *Working Part 29, wp248*.
[113] Le spiegazioni del Garante. FAQ sul Registro delle attività di trattamento.

b) Nel campo “descrizione delle categorie di interessati e delle categorie di dati personali” andranno specificate sia le tipologie di interessati (es. clienti, fornitori, dipendenti) sia quelle di dati personali oggetto di trattamento (es. dati anagrafici, dati sanitari, ecc..)

c) Nel campo “categorie di destinatari a cui i dati sono stati o saranno comunicati” andranno riportati, anche semplicemente per categoria di appartenenza, gli altri titolari cui siano comunicati i dati (es. enti previdenziali cui debbano essere trasmessi i dati dei dipendenti per adempiere agli obblighi contributivi). Inoltre, si ritiene opportuno che siano indicati anche gli eventuali altri soggetti ai quali – in qualità di responsabili e sub responsabili del trattamento – siano trasmessi i dati da parte del titolare. Ciò al fine di consentire al medesimo titolare di avere effettiva contezza del novero e della tipologia dei soggetti esterni cui sono affidate le operazioni di trattamento dei dati personali;

d) Nel campo “trasferimenti di dati personali verso un paese terzo o un’organizzazione internazionale” andrà riportata l’informazione relativa ai suddetti trasferimenti unitamente all’indicazione relativa al Paese/i terzo/i cui i dati sono trasferiti e alle “garanzie” adottate ai sensi del Capo V del GDPR;

e) Nel campo “termini ultimi previsti per la cancellazione delle diverse categorie di dati” dovranno essere individuati i tempi di cancellazione per tipologia e finalità di trattamento. Ad ogni modo, ove non sia possibile stabilire a priori un termine massimo, i tempi di conservazione potranno essere specificati mediante il riferimento a criteri indicativi degli stessi;

f) Nel campo “descrizione generale delle misure di sicurezza” andranno indicate le misure tecnico-organizzative adottate dal titolare ai sensi dell’articolo 32 del GDPR tenendo presente che l’elenco ivi riportato costituisce una lista aperta e non esaustiva, essendo rimasta al titolare la valutazione finale relativa al livello di sicurezza adeguato, caso per caso, ai rischi presentati dalle attività di trattamento concretamente poste in essere. Tale lista ha carattere dinamico (e non più statico come è stato per l’Allegato B del d.lgs. 196/2003) dovendosi continuamente confrontare con gli sviluppi della tecnologia e l’insorgere di nuovi rischi. Le misure di sicurezza possono essere descritte in forma riassuntiva e sintetica, o comunque idonea a dare un quadro generale e complessivo di tali misure in relazione alle attività di trattamento svolte, con possibilità di fare rinvio per una valutazione più dettagliata a documenti esterni di carattere generale.

2.3 Il processo di Data Breach notification

Il Regolamento Europeo GDPR individua, tra le "figure soggettive", coloro che stabiliscono finalità e modalità di gestione dei dati personali (i c.d. "titolari del trattamento"), ai quali viene attribuito l'onere di adottare misure tecnico/organizzative atte a minimizzare la probabilità di violazione degli stessi dati (o "personal data breach") con conseguente possibile impatto sulle persone fisiche (gli "interessati al trattamento" o "interessati").

Tali misure, per quanto incisive, non azzerano mai la possibilità di un incidente e dunque il titolare è tenuto a mettere in atto un processo di gestione del personal data breach che gli consenta di rendere minimo l'impatto sugli interessati dovuto ad una compromissione dei dati personali, ottemperando nel contempo agli obblighi normativi previsti dallo stesso GDPR e da altre normative di settore.

Per descrivere cosa si intenda per personal data breach si può ricorrere dapprima alle definizioni riportate nella normativa vigente e, successivamente, si può cercare di contestualizzare questo fenomeno nell'ambito delle "*best practice*" con l'obiettivo di strutturare un processo di gestione.

La definizione di personal data breach (in italiano "violazione dei dati personali") è riportata al Capo I – Disposizioni Generali articolo 4 del GDPR nel quale si definisce come: "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati".

Tuttavia, una definizione più dettagliata e pragmatica viene fornita nel documento "linee guida sulla notifica delle violazioni dei dati personali ai sensi del regolamento (UE) 2016/679" pubblicato in ultima versione il 6 febbraio 2018 dal Gruppo di Lavoro Articolo 29 per la Protezione dei Dati Personali.

In questo documento si afferma in modo chiaro ed esplicito che un personal data breach "è un tipo di incidente di sicurezza" la cui conseguenza "è che il titolare del trattamento non è più in grado di garantire l'osservanza dei principi relativi al trattamento dei dati personali di cui all'articolo 5 del Regolamento".

Questo passaggio è di estrema importanza dal momento che mette in relazione il concetto di violazione di dati personali con quello dell'incidente di sicurezza e quindi ci

fornisce tutta una serie di strumenti e "best Practice" per poter definire i processi operativi per la gestione del *personal data breach*.

Ancora il documento del Gruppo di Lavoro Articolo 29 definisce quali siano le tipologie di data breach, riprendendo anche quanto riportato nel parere 3/2014 e contestualizzando rispetto ai tre principi ben noti della sicurezza delle informazioni ossia riservatezza, integrità e disponibilità:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

Si evidenzia che la "violazione di disponibilità" viene determinata sicuramente dalla perdita o distruzione dei dati, ma anche dall'accesso, cioè dall'impossibilità da parte del titolare e dell'interessato di accedere ai dati ed ai servizi ad essi correlati.

Questo aspetto viene spesso trascurato nella gestione dei data breach ma è di assoluta importanza, dal momento che l'impossibilità ad accedere ai dati può senza dubbio causare danni agli interessati.

Si pensi ad esempio all'impossibilità di accedere ai dati sanitari in occasione di un importante intervento medico o al mancato accesso ai propri dati bancari con conseguente impossibilità a procedere con operazioni di pagamento o di fido.

Altro aspetto importante introdotto dal GDPR è l'obbligo di notifica del data breach all'Autorità Garante entro il termine di 72 ore.

Tale obbligo viene sancito al Capo IV – Titolare del trattamento e responsabile del trattamento – Sezione 2 – Sicurezza dei dati personali – articolo 33 ed è in capo al titolare del trattamento che: "notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".

Il Gruppo di Lavoro Articolo 29, sempre nel documento "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" chiarisce che: "il momento esatto in cui il titolare del trattamento può considerarsi "a conoscenza" di una particolare violazione dipenderà dalle circostanze della violazione.

In alcuni casi sarà relativamente evidente fin dall'inizio che c'è stata una violazione, mentre in altri potrebbe occorrere del tempo per stabilire se i dati personali sono stati compromessi.

Tuttavia, l'accento dovrebbe essere posto sulla tempestività dell'azione per indagare su un incidente per stabilire se i dati personali sono stati effettivamente violati e, in caso affermativo, prendere misure correttive ed effettuare la notifica, se necessario".

Nella gestione del *personal data breach* è necessario far precedere le eventuali azioni di notifica con l'analisi e la contestualizzazione dell'incidente occorso.

Le comunicazioni previste dal GDPR non si esauriscono alla sola Autorità Garante ma si estendono anche agli interessati, ai sensi dell'articolo 34 paragrafo 1:

"Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche."

Si tratta di un altro adempimento a carico del titolare del trattamento che agisce sempre in coordinamento con l'eventuale responsabile del trattamento.

L'obbligo di notifica di un personal data breach, dunque, potrebbe non esaurirsi con una comunicazione dell'Autorità Garante ed agli interessati al trattamento.

È infatti necessario far riferimento alle normative vigenti nel proprio settore di attività, che potrebbero indicare ulteriori incombenze di questo tipo a carico dei soggetti coinvolti nel trattamento di dati personali, e del titolare del trattamento in primis[114].

[114] Solo per rimanere in ambito europeo si possono considerare, ad esempio, le seguenti normative:

- *Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS).* L'articolo 19, paragrafo 2, del regolamento eIDAS fa obbligo ai prestatori di servizi fiduciari di comunicare all'organismo di vigilanza qualsiasi evento che comporti un impatto sul servizio offerto o sui relativi dati; qualora tali dati siano personali, il prestatore di servizi fiduciari deve comunicare anche all'Autorità Garante per la Protezione dei Dati Personali.
- *Direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (direttiva NIS).* Gli operatori di servizi essenziali ed i fornitori di servizi digitali sono obbligati a notificare gli incidenti di sicurezza alle rispettive autorità competenti ai sensi degli articoli 14 e 16. Tali incidenti possono interessare anche dati personali ed, in caso di compromissioni degli stessi, si rende necessaria una comunicazione all'Autorità Garante da parte degli stessi soggetti ai sensi del GDPR ed in maniera distinta rispetto a quanto previsto dalla direttiva NIS.

L'articolo 33 del GDPR, al paragrafo d) obbliga il titolare del trattamento dei dati personali a comunicare all'Autorità Garante:

"le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi".

Il GDPR non indica specifiche misure di sicurezza da adottare, ma lascia al titolare del trattamento la scelta e le modalità di applicazione delle stesse secondo un approccio pragmatico, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, secondo quanto descritto all'articolo 32 paragrafo 1 – Sicurezza del trattamento.

2.4 La valutazione di impatto sulla protezione dei dati personali e la consultazione preventiva

L'obiettivo del legislatore europeo di alzare l'asticella della protezione dei dati personali compie un ulteriore passo in avanti grazie all'introduzione di due istituti molto importanti, che sottolineano ancor di più l'importanza di una tutela preventiva e di tipo precauzionale piuttosto che successiva-riparatoria.

La valutazione d'impatto e la consultazione preventiva configurano una protezione dei dati personali votata alla pragmaticità, in quanto diventa obbligo cogente compiere tali attività al fine di ottemperare ai principi del trattamento, e votata alla dinamicità, in quanto si tratta di adempimenti che, per la loro stessa natura, devono aggiornarsi, ogniqualvolta le operazioni di trattamento si sviluppano[115].

La valutazione d'impatto e la consultazione preventiva rappresentano due ulteriori corollari del principio generale di trattamento dei dati personali in modo non rischioso e, in tal senso, questi due strumenti risultano essere presupposti procedurali rispetto alla

- *Direttiva 2009/136/CE (direttiva sui diritti dei cittadini) e regolamento (UE) n. 611/2013 (regolamento sulla notifica delle violazioni).* I fornitori di servizi di comunicazione elettronica accessibili al pubblico devono notificare le violazioni alle autorità nazionali competenti nel contesto della direttiva 2002/58/CE52.

[115] F. PIZZETTI, PRIVACY E IL DIRITTO EUROPEO ALLA PROTEZIONE DEI DATI PERSONALI, cit. p. 295.

determinazione e all'adozione delle misure tecnico-organizzative di sicurezza del trattamento.

Qui risiede senza dubbi uno dei principali aspetti di importanza dei nuovi istituti: con la previsione obbligatoria e l'applicazione costante da parte dei titolari del trattamento, si anticipa la tutela ad un momento anteriore al trattamento dei dati, non si attende una violazione per poter analizzare i punti deboli del trattamento per poi attuare le corrispondenti misure di sicurezza, ma tramite l'analisi del rischio si individuano in anticipo i rischi verificabili, in base alla tipologia di dati e di operazioni da porre in essere, e potendo così predisporre tutte le misure necessarie e adeguate affinché dal trattamento non derivino lesioni gravi ai diritti e alle libertà delle persone fisiche.

Ai sensi dell'articolo 35 del Regolamento, il titolare effettua una valutazione d'impatto prima di procedere al trattamento, qualora una particolare tipologia di trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche tenuto conto del fatto che all'interno del procedimento si prevedano l'uso di particolari nuove tecnologie e considerati inoltre il contesto, la natura, l'oggetto e le finalità.

È previsto che durante lo svolgimento della valutazione, qualora sia designato dall'organigramma della struttura del titolare, venga coinvolto quale soggetto professionale il responsabile della protezione dati, che svolge funzione di consulente tecnico.

La valutazione d'impatto si configura come tappa fondamentale e imprescindibile di tutte quelle forme molto rischiose di trattamento, tra le quali a titolo esemplificativo l'articolo 35 paragrafo 3, individua la valutazione sistematica e globale di aspetti personali delle persone fisiche tramite trattamenti automatizzati, compresi la profilazione, e sulle quali si fondano decisioni che esplicano effetti giuridici su dette persone; oppure il trattamento su larga scala di categorie di dati personali c.d. sensibili (dati personali che rilevino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona); e infine la sorveglianza su larga scala di una zona accessibile al pubblico.

Inoltre, al fine di facilitare il compito del titolare tanto in sede di valutazione quanto nelle fasi successive, le autorità di controllo possono redigere degli elenchi nei

quali sono racchiuse ed esplicate le tipologie di trattamenti per cui si rende necessaria, o non necessaria, una valutazione pre-impatto dei rischi.

Per quanto riguarda infine il contenuto essenziale minimo della valutazione, questo è disciplinato al paragrafo 7, che prevede la presenza necessaria di almeno:

a) Una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) Una valutazione delle necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) Una valutazione dei rischi per i diritti e le libertà degli interessati
d) Le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Alla disposizione subito successiva è previsto invece che ogniqualvolta la valutazione d'impatto rilevi un reale rischio elevato, in assenza di misure adeguate per attenuarne la pericolosità, il titolare prima di procedere al trattamento, debba consultare obbligatoriamente l'autorità di controllo.

Quest'ultima, qualora il trattamento risulti illecito o carente sotto il profilo dell'adeguatezza per la prevenzione del rischio, ha l'onere di fornire un parere scritto entro otto settimane dalla richiesta di consultazione (prorogabile di ulteriori sei settimane, con il rispettivo obbligo di informativa nei confronti del titolare) con facoltà di esercitare i poteri investigativi, correttivi, autorizzativi e consultivi previsti all'articolo 58 del Regolamento.

Al fine della redazione del parere scritto, il titolare per rendere completo all'Autorità di controllo il quadro generale della situazione le comunica:

a) Le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
b) Le finalità e i mezzi del trattamento;

c) Le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati;
d) I dati di contatto del titolare della protezione dei dati;
e) Le risultanze della valutazione d'impatto di cui all'articolo 55;
f) Ogni altra informazione richiesta dall'autorità di controllo.

Infine, tanto la valutazione d'impatto quanto l'autorizzazione preventiva subiscono una deroga nel caso in cui gli Stati membri abbiano previsto un'autonoma base giuridica per delle particolari ipotesi di trattamento come disciplinato dall'articolo 6 lett.c) ed e), cioè quando il trattamento risulti necessario ad adempiere un obbligo legale in capo al titolare o generalmente sia funzionale all'esecuzione di compiti di interesse pubblico.

CONCLUSIONI

Durante tutto il corso dell'elaborato abbiamo spaziato dall'analisi del funzionamento del *social network Facebook* alla connessa vicenda "*Cambridge Analytica*" effettuata alla luce delle regole introdotte dal Regolamento (UE) 2016/679, e questo ci consente di risaltare tutta la complessità che caratterizza attualmente la tutela dei dati personali all'interno del nuovo e dinamico panorama digitale.

È evidente, infatti, che la velocità con cui tale settore si è evoluto, e si sta evolvendo, connessa all'intrecciarsi di una molteplicità di interessi di tipo economico, sociale, giuridico e culturale, renda la materia oggetto di regolamentazione estremamente "insidiosa", anche a causa dell'imprevedibilità degli ulteriori sviluppi che si realizzeranno anche solo nel breve-medio termine.

Al contempo, poiché il progresso tecnologico non può e non deve essere arrestato, diviene necessario incanalare tale forza innovativa verso un utilizzo consapevole e proficuo, che si ponga a vantaggio e non a detrimento dell'evoluzione delle moderne società.

È proprio alla luce di tale complessità e alla necessità di offrire adeguati strumenti regolativi che deve leggersi il nuovo quadro normativo di tutela dei dati personali.

Se, infatti, la Direttiva europea 95/46/CE focalizzava l'attenzione quasi esclusivamente sulla tipologia dei dati raccolti e sugli strumenti di garanzia messi a disposizione degli interessati, il GDPR pone, invece, il proprio accento sulla responsabilizzazione del titolare del trattamento, in base alla convinzione che la tutela non possa che partire *ab origine* dal soggetto che decide di intraprendere, dettandone le relative condizioni e finalità, un'attività di sfruttamento di tali preziose informazioni.

Come è stato ampiamento evidenziato nel corso dell'analisi, *l'accountability* del titolare del trattamento costituisce la "spina dorsale" dell'intero Regolamento europeo: è da questo principio cardine, infatti, che si dipanano tutte le novità normative in materia ed è dall'atteggiamento proattivo del titolare, sorretto ed incentivato dalle autorità competenti, che si avvia il peculiare percorso di tutela tracciato dal legislatore.

Un processo di responsabilizzazione che trova, inoltre, piena estrinsecazione con la rilevante decisione, come evidenziato, di far gravare su tale soggetto l'onere della prova: ai sensi del Regolamento, infatti, il titolare è tenuto non solo ad esaminare

attentamente la propria attività al fine di individuare le misure tecniche ed organizzative più idonee a limitare al minimo situazioni lesive della sfera d'identità dei soggetti interessati, ma al contempo a dimostrare, a seconda della tipologia del trattamento implementato, di aver fatto tutto il possibile per tutelare i propri utenti.

Ne consegue, quindi, che il legislatore europeo con tale atto ha deciso di modificare completamente il tradizionale punto di osservazione della protezione dei dati personali, spostandolo dal destinatario della tutela al soggetto che attivamente utilizza tali informazioni. Ed è proprio su tale riorganizzazione che gli elementi essenziali dell'intero impianto normativo sono stati ridefiniti.

Ebbene, se l'accountability costituisce il principio cardine del nuovo quadro regolativo europeo, proprio la limitata accuratezza nella determinazione delle misure di protezione dei propri utenti ha rappresentato, invece, il più rilevante elemento di criticità del sistema di trattamento implementato da Facebook e, conseguentemente, causa scatenante la vicenda "*Cambridge Analytica*".

Come evidenziato nel corso dell'analisi, per anni il social network ha perseguito le proprie finalità commerciali delineando un duplice livello di sfruttamento dei dati personali dei propri clienti: una dimensione più superficiale e palese, costituita dall'esplicita attività di condivisione di immagini, di foto personali, di pensieri e di commenti realizzata direttamente dagli interessati; ed un'altra sottesa, a tratti intenzionalmente e maliziosamente nascosta, contraddistinta dall'analisi delle azioni, non tutte consapevolmente realizzate, degli utilizzatori del social network.

Si tratta di un vero e proprio sistema multilivello di raccolta di preziose informazioni personali che è stato reso possibile sviluppare grazie all'immagine di piattaforma di condivisione gratuita e ad un sistema di condizioni d'uso poco trasparenti, che ha trasmesso agli utenti l'ingannevole percezione di disporre, sempre e comunque, del pieno controllo dei propri dati personali.

Una volta individuata la duplice struttura alla base del funzionamento del social network, diventa ovviamente rilevante valutare se il nuovo quadro normativo avrebbe potuto effettivamente limitare ovvero impedire le conseguenze dannose derivate dall'indebita sottrazione di informazioni di milioni di profili personali.

Con riferimento al primo e più superficiale livello di raccolta dei dati summenzionato, in conformità a quanto è stato evidenziato, è possibile affermare che

l'applicazione delle nuove regole avrebbe sicuramente inciso, incrementando, perlomeno, il grado di sicurezza della piattaforma.

L'articolato sistema di obblighi posti a carico dei titolari che effettuano trattamenti a così elevato rischio per la privacy, prevedendo un'analisi d'impatto *ex ante* (DPIA), nonché consultazioni obbligatorie con le autorità competenti (art.36) e comunicazioni imposte in caso di violazioni (artt. 33 e 34), avrebbe, infatti, agevolato l'individuazione di comportamenti dolosamente o colposamente lesivi dell'identità personale degli utenti.

La piattaforma sarebbe stata, inoltre, incentivata in maniera naturale verso la predisposizione di più adeguate misure tecniche ed organizzative di tutela e ad un loro dinamico rinnovamento in vista dell'impiego di nuove tecniche digitali.

Un ripensamento del proprio modello di attività imperniato sui principi della privacy by design e by default che sarebbe stato incoraggiato, d'altra parte, non solo dal carattere deterrente del più incisivo sistema sanzionatorio previsto[116], ma soprattutto dall'effettiva impossibilità attuale di svolgere una simile attività all'interno del panorama europeo in violazione degli elementi fondamentali che legittimano il trattamento nel nuovo quadro normativo.

In particolare, *Facebook* sarebbe stata costretta ad indicare in maniera esplicita e trasparente l'esistenza di finalità qualitativamente diverse, a richiedere forme di consensi assolutamente differenziati a causa della granularità dei dati raccolti e, con riferimento alle attività di profilazione compiute dalla stessa piattaforma, a mettere a disposizione tecniche specifiche di acquisizione del consenso ovvero di opposizione al trattamento automatizzato nel rispetto di quanto stabilito dall'art. 22.

Simili considerazioni valgono anche per quanto riguarda la determinazione dei tempi di archiviazione dei dati personali, che ad oggi non vengono specificati nelle condizioni d'uso in violazione dell'art. 5, paragrafo 1, lett. e), nonché per la

[116] Il rafforzamento della responsabilizzazione della figura del titolare del trattamento si riflette anche nell'inasprimento delle pene in caso di mancato rispetto della nuova normativa. Il Regolamento, infatti, riconosce alle autorità nazionali di controllo la possibilità di irrogare sanzioni pecuniarie ed amministrative, previa valutazione caso per caso della natura, della gravità e della durata della violazione e del grado di responsabilità del soggetto di cui sopra, tenuto conto delle misure di sicurezza che ha o che avrebbe dovuto implementare. Per peculiari categorie di violazioni il Regolamento all'art. 83, comma 6, riconosce, in particolare, la possibilità di infliggere sanzioni amministrative pecuniarie fino a 20.000.000 EUR, o per le imprese, fino al4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore. Spetta, invece, ai singoli Stati membri la determinazione delle norme relative alle sanzioni per le violazioni non esplicitamente regolate dall'attuale normativa in materia di tutela dei dati personali.

realizzazione dell'esercizio del diritto all'oblio, disciplinato per la prima volta ad opera dell'art 17.

In altri termini, l'applicazione delle nuove regole nell'ambito del primo livello di trattamento dei dati avrebbe garantito una "rete di sicurezza" a favore degli utenti che quotidianamente utilizzano la piattaforma, offrendo loro una maggiore tracciabilità dei dati ceduti e parallelamente più ampi strumenti di azione a propria difesa, rafforzata da un dialogo di tipo continuato tra il *social network* e le autorità competenti.

Limiti in termini di applicabilità e di efficacia del Regolamento europeo rispetto alla struttura multilivello realizzata da *Facebook* si riscontrano, invece, con riferimento al secondo e più nascosto livello di trattamento dei dati.

La condivisione delle informazioni personali dei propri utenti da parte della piattaforma con imprese del gruppo, clienti, partner tecnici e sviluppatori di applicazioni esterne, come previste dalle condizioni d'uso, mette completamente in crisi il modello del consenso consapevole e, di conseguenza, la piena efficacia del Regolamento.

L'allungamento tendenzialmente illimitato della catena di valore delle informazioni personali a causa dei successivi ritrasferimenti basati su superficiali approvazioni da parte degli utenti, così come è avvenuto nella vicenda "*Cambridge Analytica*", determina inevitabilmente la separazione del dato dalla persona, trascinandolo lungo una spirale indeterminata di continue utilizzazioni, che impediscono un effettivo controllo sullo stesso.

Tale pericoloso e nebuloso percorso connesso ad un modello di business che si fonda quasi esclusivamente sulla continua condivisione delle informazioni sembra ad oggi sfuggire, almeno in parte, all'applicazione delle nuove regole europee.

Come è noto, la disciplina dedicata alla ritrasmissione dei dati personali è racchiusa nel Capo V e fa riferimento a trasferimenti verso paesi extraeuropei o organizzazioni internazionali, limitandone la realizzazione a soli tre casi specifici[117].

[117] Il Regolamento 2016/679 prevede che il trasferimento possa considerarsi legittimo in tre situazioni specifiche. In primo luogo, quando venga autorizzato dalla Commissione europea in base ad una decisione di adeguatezza ex art. 45. Al fine di garantire che il trasferimento di dati personali sia effettuato nel rispetto di specifiche condizioni che consentono di non pregiudicare il livello di protezione garantito dal nuovo quadro normativo, il Regolamento affida alla Commissione europea il compito di stilare una lista di Stati terzi e di organizzazioni internazionali in grado di offrire un sistema di tutele adeguato. In base a tale decisione, che deve effettuarsi in conformità a specifici indicatori stabiliti all'art. 45, i titolari avranno la possibilità di trasmettere informazioni personali ai paesi presenti in tale elenco senza dover richiedere autorizzazioni specifiche da parte di un'autorità di controllo. Il secondo caso riguarda quelle situazioni in cui in cui il titolare o il responsabile del trattamento abbiano fornito garanzie adeguate a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi ex art. 46. Infine, il Regolamento consente il trasferimento nel caso in cui vi siano norme vincolanti d'impresa72exart. 47. Ai sensi dell'art. 4, n 20 del Regolamento

Il fine è ovviamente quello di evitare che i soggetti interessati siano esposti a forme di tutela e di sicurezza diverse e, soprattutto, non qualitativamente all'altezza del nuovo quadro europeo.

Tale previsione, di assoluta importanza nell'attuale mondo digitale privo di barriere territoriali, è in grado però di ovviare solo in parte a situazioni simili a quella accaduta con il caso "*Cambridge Analytica*".

In un'era dominata da piattaforme che operano in condivisione e raccolgono in maniera sempre più invasiva informazioni con la collaborazione di soggetti terzi, sarebbe stato auspicabile, infatti, un intervento del legislatore europeo direttamente e specificamente orientato a disciplinare il sempre più vasto ed eterogeno fenomeno dei trasferimenti dei dati personali per motivi di profilazione od utilizzo condiviso, come ad esempio accade con i "*social media plug-in*"[118], che permettono di usufruire dei servizi di un sito utilizzando come meccanismo di accesso e di riconoscimento il profilo personale (ed in particolare le credenziali) creato su un *social network* più noto, come *Facebook, Google o Twitter*.

Tali particolari modalità di trattamento, prevedendo il coinvolgimento di molteplici titolari diversi e l'intersecarsi di finalità eterogenee, dovrebbero, infatti, essere sottoposte a regole ancor più rigide, imperniate su istruzioni complete ed esaurienti a favore dei soggetti interessati e legittimate solo in base a consensi espliciti e dettagliati.

Il livello di rischio sotteso dovrebbe, infatti, spingere verso la previsione legislativa di specifiche ed autonome modalità di approvazione di tali pratiche, mediante l'individuazione di tecniche idonee a suscitare l'attenzione degli utenti, non essendo ormai sufficienti le tradizionali modalità di raccolta dei consensi.

In assenza di tali elementi, il rischio di una perdita definitiva dei dati personali all'interno dell'articolato e complesso panorama della Rete risulta ancora presente e

---

europeo per norme vincolanti d'impresa debbono intendersi: "le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune".

[118] In campo informatico, il plug-in è un programma che interagisce con un altro programma per ampliarne o estenderne le funzionalità originarie. Tali strumenti, quindi, possono avere molteplici applicazioni a seconda delle specifiche finalità che si vogliono perseguire. I più diffusi sono quelli che, come indicato nel testo, consentono di utilizzare un'applicazione sfruttando le stesse credenziali di accesso di un social network a cui si è già iscritti non dovendone quindi creare altre. In altri casi i plug-in consentono di condividere le informazioni presenti su un sito terzo (notizie, frasi, foto) sul profilo personale creato sul social network.

sempre più rilevante, nonostante le pur incisive regole previste dal nuovo quadro normativo.

Da quanto evidenziato, quindi, è indubbio che in un panorama estremamente dinamico in cui il dato rappresenta ormai l'elemento cardine delle società dato-centriche, ma che al contempo rischia di diventarne facile preda, il nuovo impianto normativo introdotto dal Regolamento 2016/679 rappresenta oggi un fondamentale e solido strumento di tutela.

Tuttavia, le sfide da affrontare lungo l'orizzonte della digitalizzazione sembrano essere ancora molteplici e rilevanti.

Risulta necessario continuare sulla via della regolazione delle complesse e sempre più sofisticate forme di raccolta e di profilazione dei dati personali, che quotidianamente minacciano la normale evoluzione dell'identità dei soggetti coinvolti, sanzionando le indebite strumentalizzazioni esterne per finalità che esulano la sfera di determinazione dei singoli.

Questo implica interventi normativi esplicitamente mirati alle eventuali fasi successive ed ulteriori rispetto alla raccolta e al trattamento dei dati personali, con la previsione di peculiari regole e limitazioni nel caso in cui il titolare intenda procedere ad una successiva trasmissione delle informazioni in proprio possesso ovvero avvalersi della collaborazione di soggetti terzi.

In particolare, risulta essenziale prevedere forme di consenso specifico e soprattutto separato, diverse da quelle previste per il trattamento "originario", che siano in grado di allertare l'utente circa le potenziali implicazioni derivanti dall'utilizzo di tali applicazioni esterne e di consentirgli di controllare il percorso intrapreso dai propri dati personali.

È evidente che proseguire per tale strada significa continuare a monitorare e studiare, a livello nazionale e sovranazionale, il fenomeno della digitalizzazione, evitando di rifuggire dall'evoluzione tecnologica, ma comprendendone a fondo le dinamiche, in modo che l'intervento regolativo non sia mai avulso dal contesto reale, ma al contrario sia in grado di esaltarne i punti di forza in vista del progresso delle società digitali e di scongiurarne gli eventuali rischi.

Quindi, come è stato efficacemente evidenziato: "è necessario accettare la sfida e difendere le ragioni delle regole, che sono poi anche quelle della libertà e della democrazia"[119].

Al contempo, parallelamente al percorso di rafforzamento *dell'accountability* dei titolari e di moltiplicazione dei momenti di collaborazione tra questi soggetti e le autorità competenti, risulterà fondamentale l'avvio di un processo di responsabilizzazione dell'utente digitale, in modo che si arrivi alla piena consapevolezza che nel mondo delle piattaforme ad accesso gratuito il bene di scambio non è rappresentato da un valore monetario, bensì è costituito dal soggetto stesso e dal relativo bagaglio di informazioni personali.

Laddove il dato normativo non è in grado di arrivare ed esperito il controllo delle autorità a tale ambito preposte, è il comportamento prudente e cosciente dell'utente che deve intervenire, nella convinzione che i dati personali rappresentano sempre più un bene prezioso da preservare e, soprattutto, da non lasciar inconsapevolmente fluire nello spazio senza confini della Rete.

Ne consegue che il proficuo intrecciarsi tra intervento regolativo consapevole e tempestivo, atteggiamento proattivo dei titolari del trattamento e responsabilizzazione degli utenti digitali costituirà sempre più un fattore imprescindibile per la crescita sostenibile ed intelligente, soprattutto con riferimento ai sempre più ampi ambiti di applicazione e di utilizzo dei dati personali.

In assenza di tale combinato agire, al contrario, è ragionevole attendersi il perpetuarsi del rischio che l'impiego sempre più invasivo delle nuove tecnologie, da strumento di crescita e di sviluppo della collettività basato sulla fertile condivisione di informazioni e conoscenza, si tramuti in veicolo di limitazione di libertà personali e di diritti fondamentali, trasformando la tanto desiderata società digitale in una società fortemente distopica.

[119] Così F. PIZZETTI, Privacy e il diritto europeo alla protezione dei dati personali –dalla Direttiva 95/46 al nuovo Regolamento europeo, op. cit., p. 306.

BIBLIOGRAFIA

A. BARBERA, Art. 2 della Costituzione, in Commentario della Costituzione (a cura di) G. BRANCA, Bologna, 1975

A. CERRI, voce Riservatezza (diritto alla), in Dig. disc. pubbl., vol. IV, Torino, 1989

A. PAPA, Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico, Torino, 2009

A. VALASTRO, Libertà di comunicazione e nuove tecnologie, Milano, 2001

B. VAN DER SLOOT - S.VAN SCHENDEL, Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study in Jipitec, Journal of Intellectual Property, Information Technology and E-Commerce Law, n.7 (2)/2016

BARBARANELLI, C., CAPRARA, G. V., VECCHIONE, M., & FRALEY, C. R. (2007). Voters' personality traits in presidential elections. Personality and Individual Differences, 42(7), 1199-1208

BERELSON, B. R., LAZARSFELD, P. F. & MCPHEE, W. N. (1954). Voting: a study of opinion formation in a presidential campaign, Chicago, University of Chicago Press

BRITTANY KAISER, La dittatura dei dati, HarperCollins Italia, 2019

C. MARKOU, The 'Right to be Forgotten': Ten Reasons Why It Should Be Forgotten, in S. GUTWIRTH, R. LEENES e P. DE HERT (a cura di), Reforming European Data Protection Law, Springer, Dordrecht, 2015, p. 203 ss., spec. p. 208.

CAMPBELL, A., CONVERSE, P. E., MILLER, W. E. & STOKES, D. (1960). The American voter, New York, Wiley.

CAPRARA, G.V., BARBARANELLI, C. E BORGOGNI, L. (1993). Big Five Questionnaire. O.S. Organizzazioni Speciali, Firenze

CATTELL, R. B. (1943). The description of personality: Basic traits resolved into clusters. Journal of Abnormal and Social Psychology, 38, 476-506

CATTELL, R. B. (1945a). The description of personality: Principles and findings in a factor analysis. American Journal of Psychology, 58, 69-90.

CATTELL, R. B. (1945b); The principle trait clusters for describing personality. Psychological Bulletin, 42, 129-161

CHRISTOPHER WYLIE, Come ho creato e poi distrutto Cambridge Analyitica, Longanesi, 2020

F. BARTOLOMEI, La dignità umana come concetto e valore costituzionale, Torino, 1987

F. PIZZETTI, Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo, Giappichelli Editore, 2016

G. - NALDI M., Big data e privacy by design, Torino, 2017

G. ALPA, Diritti della personalità emergenti, diritto all'identità personale, in Giurisprudenza di merito, 1989, IV, pp. 464 e ss

G. ARMSTRONG – P. KOTLER, Marketing an introduction, Pearson education, 2016

G. BUSIA - L. LIGUORI - O. POLLICINO (a cura di), Le nuove frontiere della privacy nelle tecnologie digitali, Roma, 2016

G. BUTTI e A. PIAMONTE, GDPR: nuova privacy. La conformità su misura, Iter Edizioni, 2017.

G. D'ACQUISTO e M. NALDI, Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza, Giappichelli Editore, 2017

G. DI GENIO,Trasparenza e Accesso ai dati personali, Cap VIII, in La Nuova Disciplina Europea della Privacy, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 164.

G. OLIVIERI – V. FALCE, Smart cities e diritto dell'innovazione, in Quaderni di giurisprudenza, Milano, 2016.

GERBER, A., HUBER, G., DOHERTY, D., DOWLING, C. & PANAGOPOULOS, C. (2013). Big Five Personality Traits and Responses to Persuasive Appeals: Results from Voter Turnout Experiments. Political Behavior, Vol. 35, No. 4 (December 2013), pp. 687-728

I. S. RUBINSTEIN, Big Data: The End of Privacy or a New Beginning?, in International Data Privacy Law, n. 2/2013

M. CUNIBERTI (a cura di), Nuove tecnologie e libertà della comunicazione, Milano, 2008

M. J. BAKER, Marketing Strategy and Management; 3rd Revised edition, Londra, 2000

M. KRZYSZTOFEK, Post-Reform Personal Data Protection in the European Union: General Data Protection Regulation (EU) 2016/679, Kluwer Law International, Alphen aan den Rijn, 2017, p. 120,122.

M. OREFICE, I Big Data e gli effetti su privacy, trasparenza e iniziativa economica, Roma, 2018

M. R. ALLEGRI - G. D'IPPOLITO (a cura di), Accesso a internet e neutralità della rete, tra principi costituzionali e regole europee, Roma, 2017

O. POLLICINO – T. E. FROSINI – E. APA, Diritti e libertà in Internet, Milano, 2017

P. CARETTI, Diritto dell'informazione e della comunicazione. Stampa, radiotelevisione, telecomunicazioni, teatro e cinema, Bologna, 2005

P. KOTLER, Marketing management,15th edition, Londra, 2017

R. BIFULCO - O. POLLICINO - G. D'ACQUISTO - M. NALDI - M. BASSANI - F. PIZZETTI (a cura di), Intelligenza artificiale, protezione dati personali e regolazione, Milano, 2018

RUBINSTEIN IRA S., Big Data: The End of Privacy or a New Beginning? in International Data Privacy Law, 2013, Vol. 3, No. 2

S. RODOTÀ, Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione., Roma, 1997

S. SABRAUTZKI, Strategies, Mission, Vision, Goals, Monaco, 2010

S. WACHTER, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR, in Computer law & security Review, n. 34/2018, pp. 436–449

T.A. AULETTA., Riservatezza e tutela della personalità, Milano, 1978

V. MAYER - SCHÖNBERGER - K. N. CUKIER, Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà, Milano, 2013

V.P. PATRONO, voce Privacy e vita privata (dir. pen.), in Enc. Dir., XXXV, Milano, 1972

ZACCARIA R., I tre codici della Società dell'informazione, Torino, 2006

SITOGRAFIA

5 Chang, A. (2 maggio 2018) The Facebook and Cambridge Analytica scandal, explained with a simple diagram. Vox. https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridgeanalytica-trump-diagram (consultato il 4 dicembre 2020)

AGI. (26 marzo 2018) Perché non salta fuori il nome del partito italiano per cui lavorò Cambridge Analytica? https://www.agi.it/politica/partito_italiano_cambridge_analytica_intervista_wylie-3684939/news/2018- 03-26/ (consultato il 2 dicembre 2020)

Ballahus, R. (25 ottobre 2017). Trump-liked company reached out to Wikileaks on hacked emails. The Wall Street Journal. https://www.wsj.com/articles/wikileaks-assange-says-he-rejected-overture-fromtrump-linked-group-1508961298 (consultato il 3 dicembre 2020)

BBC News. (22 marzo 2018). Cambridge Analytica: The data firm's global influence. https://www.bbc.com/news/world-43476762 (consultato il 1 dicembre 2020)

BRUGIOTTI E., La privacy attraverso la "generazione dei diritti", da www.dirittifondamentali.it, Università degli studi di Cassino e del Lazio Meridionale, pdf, 2013; (consultato il 19 novembre 2020)

Channel 4 News. (20 marzo 2018). Cambridge Analytica: Undercover Secrets of Trump's Data Firm. https://www.youtube.com/watch?v=cy-9iciNF1A (consultato il 3 dicembre 2020)

Confessore, N. & Hakim, D. (6 marzo 2017). Data Firm Says 'Secret Sauce' Aided Trump; Many Scoff. The New York Times. https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html?_r=1. (consultato il 3 dicembre 2020)

Doward, J. & Gibbs A. (4 marzo 2017). Did Cambridge Analytica influence the Brexit vote and the US elections? The Guardian. https://www.theguardian.com/politics/2017/mar/04/nigel-oakes-cambridgeanalytica-what-role-brexit-trump (consultato il 2 dicembre 2020)

Fonti stampa inizialmente avevano calcolato che il numero di utenti coinvolti fosse inferiore, intorno ai 50 milioni, ma una nota pubblicata da Facebook ha precisato

che gli utenti esposti sono stati 87 milioni. Si veda Schroepfer, M. (4 aprile 2018). Facebook Newsroom. An update on our plans to restrict data access on Facebook. https://newsroom.fb.com/news/2018/04/restricting-data-access (consultato il 4 dicembre 2020)

FRA (European Union Agency for Fundamental Rights) – CONSIGLIO D'EUROPA, Manuale sul diritto europeo in materia di protezione dei dati, da www.fra-europa.eu, pdf, 2014; (consultato il 20 novembre 2020)

GALGANI F., La nascita del diritto alla privacy negli Stati Uniti e in Europa, da www.informatica-libera.net, 2014; (consultato il 22 novembre 2020)

GHIRIBELLI A., Il diritto alla privacy nella Costituzione italiana, da www.teutas.it, 2007; (consultato il 29 novembre 2020)

GUZZO A., Il concetto di privacy enhancing technologies, pubb. in Sicurezza informatica e tutela della privacy, 26 febbraio 2009, reperibile all'indirizzo www.diritto.it., 2009; (consultato il 19 novembre 2020)

Hamburger, T. (13 dicembre 2015). Cruz campaign credits psychological data and analytics for its rising success. The Washington Post. https://www.washingtonpost.com/politics/cruz-campaign-creditspsychological-data-and-analytics-for-its-rising-success/2015/12/13/4cb0baf8-9dc5-11e5-bce4-708fe33e3288_story.html?utm_term=.d88e13292410. (consultato il 3 dicembre 2020)

https://www.coine.it/social-media-marketing/facebook-lookalike-audience/ (consultato il 5 dicembre 2020)

https://www.newscientist.com/article/2166435-how-facebook-let-a-friend-pass-my-data-to-cambridge-analytica/#ixzz6i7bJSc5U (consultato il 6 dicembre 2020)

https://www.osservatori.net/it/ricerche/osservatori-attivi/cybersecurity-data-protection (consultato il 10 dicembre 2020)

https://www.rplt.it/privacy-data-protection-d100/trasferimento-dati-negli-u-s-a-il-garante-dispone-la-caducazione-della-autorizzazione-safe-harbor/ (consultato il 6 dicembre 2020)

IASELLI M., I compiti del Data Protection Officer: chiariamo tutti i dubbi, 21 aprile 2017, in www.agendadigitale.eu.; (consultato il 23 novembre 2020)

Il Post. (14 agosto 2017). Breve storia della “alt-right”. https://www.ilpost.it/2017/08/14/breve-storiadella-alt-right/ (consultato il 1 dicembre 2020)

Kroll, A. (Giugno-Luglio 2018). Cloak and Data: The real story behind Cambridge Analytica’s Rise and Fall. Mother Jones. https://www.motherjones.com/politics/2018/03/cloak-and-data-cambridge-analyticarobert-mercer/ (consultato il 3 dicembre 2020)

LATTANZI R., «Diritto alla protezione dei dati di carattere personale»: appunti di viaggio, in DIRITTO ALLA PRIVACY E TRATTAMENTO AUTOMATIZZATO DEI DATI FRA DIRITTO CIVILE, DIRITTO PENALE E DIRITTO INTERNAZIONALE ED EUROPEO, da www.cde.unict.it/quadernieuropei/giuridiche/63_2014.pdf, pdf, 2014; (consultato il 24 novembre 2020)

PROKOP, A. (2 maggio 2018). Cambridge Analytica shutting down: the firm’s many scandals, explained. (consultato il 29 novembre 2020)

REMOTTI R., Il diritto alla privacy e ricerca scientifica, Qual è il bene giuridico tutelato, par.2, da www.web.tiscalinet.it, pdf, 2002; (consultato il 24 novembre 2020)

Reuters. (21 marzo 2018) What are the links between Cambridge Analytica and a Brexit campaign group? https://www.reuters.com/article/us-facebook-cambridge-analytica-leave-eu/what-are-the-linksbetween-cambridge-analytica-and-a-brexit-campaign-group-idUSKBN1GX2IO (consultato il 2 dicembre 2020)

Simonetta, B. (5 maggio 2018). Cambridge Analytica fallisce, ma i personaggi chiave si spostano in Emerdata. Il Sole 24 Ore. https://www.ilsole24ore.com/art/tecnologie/2018-05-05/cambridge-analyticafallisce-ma-personaggi-chiave-si-spostano-emerdata-192526.shtml?uuid=AEXw0ijE&refresh_ce=1. (consultato il 3 dicembre 2020)

Sterling, J. (17 novembre 2016). White nationalism, a term once on the fringes, now front and center. CNN. https://edition.cnn.com/2016/11/16/politics/what-is-white-nationalism-trnd/. (consultato il 1 dicembre 2020)

Vox https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-analytica-trump-russiamueller. (consultato il 29 novembre 2020)

Wagner, K. (17 marzo 2018). Here's how Facebook allowed Cambridge Analytica to get data for 50 million users. Recode. https://www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trumpexplained-user-data. (consultato il 3 dicembre 2020)

Whistleblowing, la nuova Direttiva europea e la protezione dei dati: https://www.altalex.com/documents/news/2020/02/13/whistleblowing-nuova-direttiva-europea-protezione-dati (consultato il 9 dicembre 2020)

LEGISLAZIONE

CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA, 2000

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, Decreto legislativo 30 giugno 2003, n. 196

COM (2014) 442 Final, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Verso una florida economia basata sui dati, 2014

CONSIGLIO D'EUROPA, Comitato dei ministri (1987), Raccomandazione n. R (87) 15 agli Stati membri che disciplina l'uso dei dati personali nell'ambito della pubblica sicurezza, 17 settembre 1987

CONSIGLIO D'EUROPA, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data; Strasburgo, 2017

CONVENZIONE EUROPEA DEI DIRITTI DELL'UOMO E DELLE LIBERTA' FONDAMENTALI, 1950

DECISIONE QUADRO 2002/187/GAI, Consiglio del 28 febbraio 2002 che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità, 2002 e successive modificazioni: DECISIONE QUADRO 2003/659/GAI, Consiglio del 18 giugno 2003 e DECISIONE QUADRO 2009/426/GAI, Consiglio del 16 dicembre 2008 (decisioni Eurojust)

DECISIONE QUADRO 2008/615/GAI, Consiglio del 23 giugno 2008, sul "potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera", 2008

DECISIONE QUADRO 2008/977/GAI, Consiglio del 27 novembre 2008, sulla "protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale",2008

DIRETTIVA (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo 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 e che abroga la decisione quadro 2008/977/GAI del Consiglio

DIRETTIVA 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro)

DIRETTIVA 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

DIRETTIVA 2006/24/CE, Riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, 15 marzo 2006

DIRETTIVA 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

DIRETTIVA UE 2016/681 del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) dei passeggeri dei voli in arrivo o in partenza dal territorio degli Stati membri, a fini di prevenzione, accertamento, indagine e azione penale per i reati di terrorismo e altri gravi reati

DOCUMENTO COM (2012) 529 final, Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, Sfruttare il potenziale del cloud computing in Europa, 2012

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI nel Parere 2012/ C192/ 05, del 7 marzo 2012 sul pacchetto di riforma della protezione dati;

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI PERSONALI, Parere del 4 aprile 2007, cit. punti 61-73, e il Terzo Parere del 27 aprile 2007;

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, relativo alla proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, 27 aprile 2007;

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Decisione Commissione, clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento in paesi terzi, dir. 95-46-CE - 5 febbraio 2010;

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Guida al nuovo regolamento europeo in materia di protezione dati, 2016;

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookies, doc. web n. 311884, 8 maggio 2014;

GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, Parere 1/2008 (WP 148) "sugli aspetti della protezione dei dati connessi ai motori di ricerca", 2008;

GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, il Parere 8/2010 (WP 179) "sul diritto applicabile", 2010;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI Dichiarazione sul Rafforzamento dell'ottemperanza dei responsabili del trattamento alla normativa sulla tutela dei dati – (WP101), Bruxelles, 2004;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, le Linee-guida sui responsabili della protezione dei dati (RPD) adottate il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017), (WP 243), 2017.

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Lettera a Facebook sul caso Whatsapp – 27/10/2016;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Linee-guida sul diritto alla "portabilità dei dati", 13 dicembre 2016 Versione emendata e adottata il 5 aprile 2017, (WP 242), 2017;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 05/2012 sul Cloud computing, (WP196), 1 luglio 2012;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 03/2014 “sulla notifica delle violazioni dei dati personali (WP213), 25 marzo 2014;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 05/2014 “sulle tecniche di anonimizzazione” (WP 216), 10 aprile 2014;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 13/2011 sui servizi di geo-localizzazione su dispositivi mobili intelligenti, (WP185), 16 maggio 2011;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Statement on the role of a risk-based approach in data protection legal frameworks (WP 218), 30 maggio 2014;

REGOLAMENTO (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

SENTENZA DELLA CORTE (GRANDE SEZIONE) del 13 maggio 2014. Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.

SENTENZA DELLA CORTE DI GIUSTIZIA NELLA CAUSA MAXIMILIAN SCHREMS CONTRO DATA PROTECTION COMMISSIONER (Schrems), C-362/14, ECLI:EU: C:2015:650 del 6 ottobre 2015, punto 66

SENTENZA SCHREMS VS DATA PROTECTION COMMISSIONER DELLA HIGH COURT OF IRELAND del 18 Giugno 2014