UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE POLITICHE, GIURIDICHE
E STUDI INTERNAZIONALI

Corso di laurea *Triennale* in Diritto dell'Economia

LA TUTELA DEI DATI PERSONALI COME DIRITTO FONDAMENTALE DELL'UNIONE EUROPEA: IL CASO *CAMBRIDGE ANALYTICA*

Relatore: Prof. Daniele Ruggiu

Laureando: MICHELE DE ZEN
matricola N. 2010120

A.A. 2021/2022

RINGRAZIAMENTI

"*Ma non sei ancora stanco di studiare? Giurisprudenza non ti è bastata?*"

Quante volte mi sono sentito fare queste domande quando dicevo di essermi iscritto un'altra volta all'università ("*Ah, online allora? Pegaso?*"), dopo la mia prima laurea in Giurisprudenza a Padova nel 2014.

Ed ecco perché il primo e più importante ringraziamento lo faccio a me stesso, per non essermi accontentato. Per aver assecondato la mia curiosità, la mia voglia di imparare sempre cose nuove, la mia necessità di mettermi continuamente alla prova. La mia voglia di scoprire, la mia voglia di migliorarmi continuamente.

Grazie ai miei genitori e a mio fratello, la mia famiglia, i miei primi tifosi, il mio porto sicuro, so che siete sempre orgogliosi di me, e che sarete sempre dalla mia parte. Altre nuove fantastiche avventure ci aspettano!

Grazie a Beatrice, la mia soulmate, l'ultima persona che saluto prima di un esame, e la prima a cui scrivo dopo averlo finito, il mio esempio di costanza ed impegno nello studio, la mia compagna di vita!

Grazie a Diana per alimentare ogni giorno in me la passione verso questa materia: ne abbiamo passate tante insieme, e chissà quante ancora ne passeremo. Sei l'amica che pochi meriterebbero, ma di cui tutti avremmo bisogno.

Grazie al mio amico Clay: c'eri 8 anni fa, ci sei oggi. E non è poco. Grazie per avermi aiutato a portare avanti il mio impegno sportivo, grazie per avermi sempre difeso, grazie per aver giocato sempre nella mia stessa squadra.

Infine, *last but not least*, grazie al Prof. Daniele Ruggiu, che ha portato infinita pazienza, che mi ha accompagnato e indirizzato in questo percorso. Prometto che imparerò a scrivere bene le note!

Ci sono tanti modi per viaggiare, e questa mia seconda laurea non è che un altro dei miei viaggi, ai quali non saprei rinunciare per nulla al mondo: così come non rinuncerei mai ad imparare qualcosa di nuovo, qualcosa che (ancora) non so.

Non lo so dove mi porterà il mio prossimo viaggio, ma è certo che: la lista è lunga, il tempo è poco, fermarsi non è un'opzione. Mai.

On to the next!

Michele

LA TUTELA DEI DATI PERSONALI COME DIRITTO FONDAMENTALE DELL'UNIONE EUROPEA:
IL CASO *CAMBRIDGE ANALYTICA*

ABSTRACT 7
INTRODUZIONE 9
CAPITOLO 1 - IL CASO *CAMBRIDGE ANALYTICA* 17
1.1 RICOSTRUZIONE DEI FATTI 17
1.2 IL RUOLO DI FACEBOOK 19
1.3 BREXIT E ELEZIONI PRESIDENZIALI AMERICANE DEL 2016 24
1.4 NON CONTA IL CHI, CONTA IL COME 26
CAPITOLO 2 - DEFINIZIONI E CONCETTI 29
2.1 IL CONCETTO DI PROFILAZIONE 29
2.2 IL CONCETTO DI MICROTARGETING 32
2.3 IL CONCETTO DI CONSENSO 34
CAPITOLO 3 - IL QUADRO NORMATIVO DI RIFERIMENTO 37
3.1 IL REGOLAMENTO UE 2016/679 – IN PARTICOLARE SULL'APPLICABILITÁ ALL'ABUSO DI DATI SOCIAL 37
3.2. LA RISOLUZIONE DEL PARLAMENTO EUROPEO N. 2018/2855 43
3.3 IL RUOLO DELLE DATA PROTECTION AUTHORITIES 45
3.3.1 IL GARANTE ITALIANO PER LA PROTEZIONE DEI DATI PERSONALI 45
3.3.2 L'INFORMATION COMMISIONER'S OFFICE 52
3.3.3 LA FEDERAL TRADE COMMISSION 53
3.3.4 L'ATTORNEY GENERAL OF MASSACHUSETTS 56
CAPITOLO 4 – SVILUPPI FUTURI 61
4.1 INTELLIGENZA ARTIFICIALE E GDPR 61
4.2 CONSENSO CONSAPEVOLE 63
4.3 CULTURA, DEMOCRAZIA, LIBERTÀ 67
4.4 BUONI PROPOSITI 71
CONCLUSIONI 73
BIBLIOGRAFIA 79
SITOGRAFIA 83
PROCEDIMENTI GIUDIZIARI 93

Leggete, studiate, e lavorate sempre con etica e passione;
ragionate con la vostra testa e imparate a dire di no;
siate ribelli per giusta causa, difendete la natura e i più deboli;
non siate conformisti e non accodatevi al carro del vincitore;
siate forti e siate liberi, altrimenti quando sarete vecchi e deboli
rimpiangierete le montagne che non avete salito
e le battaglie che non avete combattuto.

Mario Rigoni Stern

ABSTRACT

L'elaborato si propone di svolgere un approfondimento sulla tutela dei dati personali come diritto fondamentale dell'Unione Europea, alla luce del caso socio–politico–giudiziario che ha visto coinvolta la società di diritto inglese *Cambridge Analytica* negli anni dal 2013 al 2018.

Analizzando la vicenda da un punto di vista sociale, etico e giuridico, l'elaborato, attraverso un metodo di ricerca basato non solo su fonti giornalistiche, ma anche fonti legislative e giudiziarie, si propone di vedere come la tutela dei dati personali sia divenuta oggi un diritto fondamentale la cui protezione, visti i valori e i dgli altri diritti coinvolti è divenuta oggi strategica.

In questo senso, l'analisi del Regolamento Generale sulla protezione dei dati personali n. 2016/679 (cd. GDPR) risulta anche funzionale ad una riflessione sugli sviluppi futuri che la regolamentazione in materia deve affrontare per stare al passo con lo sviluppo tecnologico.

INTRODUZIONE

È il 2014 quando Aleksandr Kogan[1], un ricercatore dell'Università di Cambridge, e la sua azienda, la *Global Science Research*, creano un app nell'ecosistema della piattaforma social Facebook: è "*thisisyourdigitallife*"[2]. Come tante altre app presenti sullo store del social, l'app, in cambio di risposte ad alcune domande che vertono su svariati argomenti che riguardano genericamente la vita privata dell'utente, consente di elaborare in maniera piuttosto precisa il profilo psicologico dell'intervistato. Circa 270.000 utenti utilizzeranno quell'app, immettendo dati personali per avere in cambio una sorta di consulenza psicologica sul proprio carattere e le proprie caratteristiche attitudinali. A partire da questi dati però, *thisisyourdigitallife* avvia una profilazione di massa di proporzioni mai viste: non si limita infatti ad analizzare i profili degli utenti che volontariamente si erano sottoposti al questionario, ma incomincia a raccogliere dati personali di tutti i loro contatti, e a loro volta di tutti contatti di questi e oltre,venendo a costruire una rete in grado di coprire milioni di persone in tutto il mondo[3].

L'esito di questa profilazione di massa sono più di 87 milioni di persone profilate con una accuratezza allora inimmaginabile, un'accuratezza tale da rivelare le loro preferenze non solo in ambito commerciale, ma anche sociale, culturale e presino politico e religioso: mostrando sia ciò che queste persone preferiscono, vogliono e desiderano, ma anche ciò che potrebbero prefererire, volere, desiderare e, alla fine,

---

[1] Aleksandr Kogan lavorò presso l'Università di Cambridge dal 2012 al 2018 in qualità di *Senior Research Associate*. Dopo aver patteggiato con la *Federal Trade Commission* nell'ambito dello scandalo *Cambridge Analytica*, divenne *Chief Operating Officer* dell'azienda HiOperator.

[2] *Thisisyourdigitallife* fu creata inizialmente con lo scopo dichiarato di svolgere una ricerca accademica. Per ulteriori informazioni si veda Tufekci (2018).

[3] Fino al 2015, infatti, Facebook consentiva a queste app di ottenere, con il semplice consenso dell'utente che decideva di utilizzarla, non solo le informazioni presenti sul profilo dell'utilizzatore, ma anche quelle ricavabili direttamente e indirettamente dai profili collegati. Solo in concomitanza con l'emerge dello scandalo e con l'entrata in vigore del nuovo Regolamento Europeo 2016/679 Facebook modificò in senso migliorativo le condizioni d'uso della piattaforma e le informative sull'utilizzo dei dati personali. L'ultima revisione è datata 4 gennaio 2022, in concomitanza con il cambio di ragione sociale in Meta Platforms, Inc.. Per ulteriori informazioni si veda Facebook, Normativa sui Dati.

scegliere in certe condizioni. Tramite l'app di terza parte, e tramite quella che viene chiamata in gergo tecnico API v.1.0 (*application programming interface*)[4], Kogan riuscì a creare il profilo psicologico degli utenti utilizzando una grande varietà di caratteristiche e tratti della personalità, tra cui il genere, il QI, l'età, la data di nascita, il percorso formativo, il percorso professionale, i mi piace, le interazioni online, dettagli sulle relazioni affettive e molti altri fattori[5], sebbene non sia tuttora possibile stabilire con esattezza e con certezza effettivamente quali e quanti dati siano stati prelevati dall'app.

Una volta raccolti e analizzati i profili di queste 87 milioni di persone, Kogan non li tenne per sé per studiarli come aveva dichiarato, ma li cedette alla società inglese *Cambridge Analytica*, fondata nel 2013 dal pubblicitario Nigel Oakes quale branca della società *Strategic Communication Laboratories* che si occupava di analisi di dati (non solo a carattere statistico) nell'ambito di campagne elettorali[6]. La miniera di informazioni raccolte fu poi messa a frutto da *Cambridge Analytica* nell'ambito di diverse campagne politiche al fine di indirizzare, come si vedrà nel corso del capitolo 2, le scelte politiche di ignari elettori sparsi per il mondo.

Le campagne politiche più importanti nelle quali furono messi a frutto i dati ottenuti furono di sicuro le elezioni presidenziali statunitensi, che videro fronteggiarsi Donald Trump e Hillary Clinton nel 2016, e il referendum per la Brexit (ovvero l'uscita del Regno Unito dall'Unione Europea).

Quello che ha coinvolto *Cambridge Analytica* è stato senza dubbio il più grande scandalo mondiale legato all'utilizzo dei dati personali. Ed è proprio dalla definizione di dato personale che bisogna prendere le mosse.

L'articolo 4 del Regolamento Generale sulla Protezione dei Dati 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016[7] (d'ora in avanti anche solo il

---

[4] Per il funzionamento tecnico delle app di terze parti su Facebook e dell'API v. 1.0, oggi sostituita dall'API v.2.0, si veda Hartmans (2018) e Symeonidis e al. (2018).

[5] Per la lista completa, si veda Hartmans (2018) e Weiss (2018).

[6] *Cambridge Analytica*, in seguito alle accuse di aver utilizzato illegittimamente i dati di milioni di persone, ha cessato la propria attività, avviando le procedure di insolvenza nel Regno Unito e di bancarotta negli Stati Uniti. Sul punto, si veda BBC (2018) e Vengattil (2018).

[7] 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

"GDPR") fornisce la seguente definizione di "*dato personale*": "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*"*.

Emerge di tutta evidenza come quindi il GDPR, legislazione di recente produzione adottata dall'Unione Europea proprio per far fronte alle crescenti minacce che l'avanzamento tecnologico e digitale pongono all'integrità e alla protezione dei dati personali, come si vedrà meglio *infra*, adotti una definizione molto ampia e comprensiva di dato personale, che va ad abbracciare una moltitudine di possibili informazioni (passate, presenti, e future o ancora non esistenti) che possano identificare con precisione una persona fisica[8].

Nella società dell'informazione (*rectius* dell'*over – informazione*[9]) e della comunicazione (*rectius* dell'*over – comunicazione*) in cui viviamo, la conoscenza e la condivisione volontaria di qualsiasi tipo di informazione sembrano essere diventati il motore del vivere quotidiano, sia da un punto di vista strettamente personale, sia da un punto di vista micro e macroeconomico. La digitalizzazione e le sempre crescenti possibilità offerte dalle nuove tecnologie hanno infatti ridefinito le modalità tradizionali di intendere la vita economica, le interazioni tra i consociati, i rapporti tra il pubblico e il privato (si pensi ad esempio alle novità introdotte a seguito dell'avvento della pandemia da SARS CoV - 2, che fino a poco prima sembravano appartenere ad un altro mondo o sembravano irrealizzabili[10]).

---

circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento Generale sulla Protezione dei dati).

[8] Le persone giuridiche sono infatti escluse dal campo di applicazione del GDPR.

[9] Sul concetto di società dell'informazione e della comunicazione si veda., tra gli altri, Papa (2009); Olivieri e Falce (2016); Berlocco (2019).

[10] Si pensi ad esempio al Sistema Pubblico di Identità Digitale (cd. SPID) con le quali è possibile accedere ai servizi online della pubblica amministrazione e dei privati aderenti.

Ma se fino al ventennio scorso l'avanzamento tecnologico si misurava in megabyte, in velocità al secondo, e nella riduzione delle dimensioni (si pensi all'avvento del personal computer, dei tablet, degli smartphone), oggi l'avanzamento tecnologico si basa principalmente sulla capacità di elaborare informazioni che l'utente stesso volontariamente (dall'esigenza che alcuni sentono di condividere il piatto della cena nel ristorante stellato, alla condivisione di foto di figli (magari non ancora nati, tanto da arrivare al paradosso che un essere umano, prima ancora di acquisire capacità giuridica, acquisisce un profilo social, ai video in cui raccontiamo di come siamo soliti preparare la pasta alla carbonara, convinti che a qualcuno interessi veramente) o involontariamente rilascia (si pensi a dispositivi come Amazon Alexa o Google Home, che sono in grado di captare, tramite messaggi vocali, molte informazioni ulteriori rispetto a quelle che vogliamo comunicare), o sulla capacità di creare nuovi strumenti in grado di elaborare informazioni e restituire vantaggi concreti sotto le forme più disparate.

Un'inchiesta del New York Times del 2017[11] ha stimato che ogni anno l'industria dell'elaborazione dei dati personali (ivi inclusa la rivendita degli stessi, cd. *data brokerage*) generi trilioni di dollari, con ricavi che, nel 2018, superavano i 250 miliardi di dollari.

Si pensi anche all'*Internet of things*[12], che consente di trasformare beni che fino a poco tempo fa consideravamo avere una sola specifica finalità (la macchina serve per spostarsi, la televisione a guardare i canali tradizionali…) in beni capaci di elaborare migliaia di informazioni, connettersi con altri dispositivi simili, immagazzinare informazioni, così da rendere da un lato l'esperienza di utilizzo sempre più avanzata e personalizzata sui bisogni dell'utente, ma dall'altro lo rendono anche più tracciato e tracciabile.

E se fino a poco fa queste risorse tecnologiche erano riservate alle grandi aziende, o a pochi ricchi che se le potevano permettere, oggi, secondo un recente studio di Strategy

[11] Madsbjerg (2017).

[12] Si veda lo studio realizzato per la Commissione Europea nell'ambito dell'Agenda Digitale, "Communications Networks, Content & Technology, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination", in publications.europa.eu, Aguzzi (2014).

Analytics[13], almeno il 50% della popolazione possiede uno smartphone (quindi circa 4 miliardi di persone), mentre nel 1994 solo 30.000 persone in tutto il mondo ne possedevano uno. Ecco quindi che, con la democratizzazione dell'accesso alla tecnologia, anche il numero di informazioni che ogni giorno circolano su questa rete globale è esponenzialmente aumentato, dando luogo ai cd. *big data*, enormi quantità di dati e informazioni di vario tipo che, elaborati nella maniera corretta, possono contribuire ad una *user experience* calibrata quasi su misura sull'utente, una sorta di *tailored made customer experience*.

In una società di questo tipo, dove appunto il *craving for information* e la individualizzazione dei servizi offerti dalla tecnologia la fanno da padrone, è evidente come il valore dei dati personali, come sopra definito, sia inestimabile. Tutto ruota intorno alla persona (utente per meglio dire) e al relativo bagaglio di informazioni personali che si porta dietro, che gli appartiene. Ma se i dati personali sono un asset della persona, allora come tali vanno tutelati, alla stessa stregua di come sono tutelate, ad esempio, l'integrità fisica o la proprietà. Come si vedrà nell'analisi sul caso *Cambridge Analytica*, anche i dati personali si possono sottrarre illegittimamente, e questo anche a partire da informazioni anonime, possono essere oggetto di trasferimento, possono essere venduti senza titolo, possono essere manipolati da terzi per finalità indebite sconosciute ai diretti interessati.

Anche la tutela dei dati personali va quindi ricompresa nella tutela dei diritti fondamentali dell'individuo, onde evitare che gli indubbi vantaggi portati dalle nuove tecnologie, come fagocitatori di dati personali e informazioni, collidano irrimediabilmente con un'eccessiva compressione dei diritti fondamentali del singolo, che si trova molto spesso sovraesposto, scandagliato e sminuzzato negli aspetti più intimi della propria sfera personale. Utilizzare i dati personali come merce di scambio per l'utilizzo di servizi, se da un lato può apparire apparentemente poco o per nulla dispendioso da un punto di vista economico (si pensi allo slogan, ora rimosso, della piattaforma online Facebook: "It's free and always will be"[14]), dall'altro lato rischia

[13] Mawston (2021).

[14] Con un deciso cambio di prospettiva, lo slogan attuale (alla data del 2 aprile 2022) risulta essere "Facebook ti aiuta a connetterti e rimanere in contatto con le persone della tua vita."

di condurre a fenomeni di "penalizzazione della propensioni"[15], limitando e comprimendo le possibilità di scelta del singolo. Ad esempio, come si vedrà in seguito, tramite la profilazione e processi decisionali automatizzati (come, ad esempio, l'utilizzo di cookie di profilazione), l'utente di un sito web potrebbe essere portato a visualizzare sempre e soltanto un certo tipo di pubblicità, escludendone altra, limitando di fatto drasticamente la sua possibilità di scelta di visualizzare prodotti diversi, anche magari non affini alle sue esigenze e preferenze[16].

Ma se appare pressoché anacronistico il principio del *right to be let alone* teorizzato da Warren e Brandeis nel diritto alla privacy del 1890[17], è altrettanto vero che la tutela dell'individuo in questa società dato – centrica, che si riverbera nella necessità che la costruzione del suo profilo digitale sia compiuta nella maniera più etica possibile da parte delle istituzioni digitali, debba passare attraverso i binari della protezione dei dati personali come diritto fondamentale.

E di ciò sembra esserne pienamente consapevole il legislatore europeo che, al considerando numero 1 del GDPR, quindi proprio in estrema apertura del Regolamento, rende subito estremamente chiaro il concetto che "La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano." Ribadisce poi lo stesso concetto all'articolo 1, stabilendo che il Regolamento "protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali […]".

Sebbene non sia un diritto di carattere assoluto, come espressamente previsto dal considerando 4 e come si vedrà meglio *infra*, il GDPR fissa dei paletti, dei confini, oltre i quali chi utilizza informazioni personali altrui non può andare, dovendo quindi

[15] Mayer – Schonberger e Cukier (2013).

[16] Sul punto si veda Article 29 Working Party (2018).

[17] Warren e Brandeis (1890), 193-220.

assumere un comportamento in linea con la delicatezza sia della materia che del materiale trattato, attraverso un sistema *risk based* che si vedrà meglio più avanti[18].
Non adottare questo tipo di approccio significherebbe rendere uno strumento come Internet, dove sono immagazzinati la stragrande maggioranza dei nostri dati personali, un'arma di controllo di massa, al posto che uno straordinario strumento di libertà, democratizzazione e uguaglianza.
"Privacy is no longer a social norm", dirà Mark Zuckerberg nel 2010 ai Crunchie Awards a San Francisco, USA[19], salvo poi acquistare nel 2013 non solo la sua villa a Palo Alto, California, ma anche le quattro attorno proprio per salvaguardare la sua privacy, è un'affermazione che, se riproposta nel 2022, farebbe rabbrividire molti, se non tutti. Purtroppo, però ci sono state anche istituzioni e aziende che, beneficiando di una legislazione troppo lassiva, che si è occupata solo recentemente di una vera tutela della ricchezza e del valore insiti nel concetto di dati personali, in quanto afferenti alla persona inteso come singolo, hanno fatto di quella affermazione il loro cavallo di battaglia, trovando terreno fertile sul quale arricchirsi e speculare.
Come *Cambridge Analytica*.

[18] Nel diritto italiano, il diritto alla protezione dei dati personali trova il suo primo riconoscimento nella sentenza della Corte di Cassazione n. 2129 del 1975, che portò, unitamente all'influenza esercitata dalle Direttive Europee n. 97/66/CE, 95/46/CE e 2002/58/CE, all'adozione della cd. legge sulla privacy (legge 31 dicembre 1996 n. 675), in seguito assorbita nel Codice in materia di protezione dei dati personali, adottato con decreto legislativo 30 giugno 2003 n. 196. Il GDPR in Italia fu recepito con l'adozione del decreto legislativo 10 agosto 2018 n. 101, recante "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)" in G.U. 4 settembre 2018 n. 205.
[19] Johnson (2010).

CAPITOLO 1 - IL CASO *CAMBRIDGE ANALYTICA*

1.1 RICOSTRUZIONE DEI FATTI

È difficile negare che il 2018 sia stato un anno spartiacque, un *turning point*, per quanto riguarda la materia della tutela dei dati personali. E non solo per l'entrata in vigore del GDPR, ma anche perché, con tempismo perfetto, venne a galla uno dei più grandi scandali legati alla violazione dei dati personali nell'era moderna.

Grazie a due inchieste parallele del *The New York Times*[20] e del *The Guardian*[21], si iniziò a far luce sui collegamenti tra la società di profilazione *Cambridge Analytica*, la piattaforma social Facebook e l'applicazione "*thisisyourdigitallife*".

Cambridge Analytica, fondata nel 2013 da Nigel Oakes come branca della società *Strategic Communication Laboratories* (d'ora in avanti anche solo "*SCL*"), fu una società con sede a Londra specializzata nella raccolta di dati personali ricavati dall'utilizzo di social network per la successiva realizzazione di profili di carattere politico attraverso l'impiego e lo sfruttamento di tecniche di *microtargeting*[22] comportamentale. Trattando queste informazioni, la società riusciva a creare modelli predittivi basati sulla combinazione dei dati raccolti da poter utilizzare durante le campagne politiche. Si stima che tra il 2013 e il 2018 *Cambridge Analytica* lavorò a più di 200 campagne elettorali in tutto il mondo[23]. Tra le più importanti, si ricordano quella del presidente kenyota Uhuru Kenyatta nel 2013, quella per la Brexit tra il 2015 e il 2016, e quella per l'elezione del Presidente degli Stati Uniti del 2016. Lavorò anche per un non meglio precisato partito italiano nelle elezioni del 2013[24].

[20] Rosenberg, Confessore e Cadwalladr (2018).

[21] Cadwalladr e Graham-Harrison (2018).

[22] Cfr. capitolo 2, paragrafo 2, p. 27.

[23] BBC News (2018).

[24] AGI (2018). Secondo un reportage di Presa Diretta del 10/02/2020, visibile al link https://www.youtube.com/watch?v=cckZ6Eom2bU, emergerebbe una richiesta di informazioni inviata ad Alexander Nix da parte di Corrado Passera (al tempo iscritto al partito Italia Unica) con una mail del 01/07/2016.

Come ebbe modo di dire Alexander Nix, CEO di *Cambridge Analytica* tra il 2013 e il 2018, la società si occupava di gestire il lato social delle compagne, assicurandosi che "i messaggi giusti arrivassero agli elettori giusti"[25].

Per quello che qui attiene, la vicenda cominciò ad assumere contorni illegittimi nel 2015 in seguito all'avvio di una collaborazione tra l'applicazione *thisisyourdigitallife* e Facebook. *Thisisyourdigitallife* fu realizzata nel 2015 da Aleksandr Kogan, ricercatore presso l'Università di Cambridge e titolare della società *Global Science Research,* con lo scopo – dichiarato – di svolgere una ricerca accademica, permettendo alle persone, in cambio di un consenso spesso rilasciato in maniera molto superficiale, di scoprire il loro profilo psicometrico dopo aver risposto ad alcune domande su un questionario basato su cinque tratti della personalità (cd. *Big Five*)[26]. Kogan si basò sul modello di profilazione psicometrica elaborato da Michal Kosinski e basato sul metodo OCEAN[27]. Così come migliaia altre applicazioni presenti su Facebook, anche questa applicazione consentiva di svolgere il questionario semplicemente utilizzando le stesse credenziali di accesso al social network. Sfruttando una policy di Facebook ora non più in vigore, l'app aveva inoltre accesso anche alle bacheche dei cosiddetti "amici" dell'utente, i quali pertanto venivano illegittimamente e inconsapevolmente spiati, senza aver rilasciato alcun consenso.

Con tale meccanismo, fu sufficiente che appena 270.000 utenti utilizzassero l'app per raccogliere informazioni personali relative a più di 50 milioni di profili in tutto il mondo[28]. Tale enorme mole di dati consentì allo sviluppatore di vendere quei dati a *Cambridge Analytica*, così da poterne estrapolare il profilo politico, violando così i termini e le condizioni del social network, che sebbene non proibissero la raccolta dei dati, ne vietavano invece espressamente la condivisione con terze parti non autorizzate. Con quei 50 milioni di profili[29], *Cambridge Analytica* riuscì ad elaborare il profilo di

[25] Reuters (2018).

[26] Costa e McCrae (1988 – 1996).

[27] Per ulteriori informazioni si veda NaturPhilosophie (2017).

[28] Fonti legate alla 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 circa *87 milioni*. Sul punto, si veda D'Alessandro (2018).

[29] Wagner (2018).

oltre 240 milioni di cittadini americani. Solo grazie all'utilizzo di un app dal carattere prettamente ludico, si è arrivati quindi ad una delle più gravi violazioni dei dati personali dall'avvento delle nuove tecnologie, portando quindi alla luce le molteplici fragilità di un sistema troppo permissivo e forse ancora legislativamente embrionale e poco regolamentato.

Il lavoro di questa società, passato in sordina per molto tempo, sarebbe diventato di interesse pubblico solamente a seguito dell'inaspettata vittoria di Donald Trump alle elezioni presidenziali statunitensi, anche su impulso del *whistleblower* Christopher Wiley, ex dipendente di *Cambridge Analytica*, il quale, pentitosi raccontò alla stampa quanto stava accadendo[30].

Nel capitolo 3 si analizzerà la legislazione applicabile al caso *Cambridge Analytica*, le sanzioni comminate, nonché il ruolo delle *Data Protection Authorities* nella vicenda.

1.2 IL RUOLO DI FACEBOOK

Come si è avuto modo di dire poc'anzi, il ruolo della piattaforma social Facebook (oggi Meta, Inc.) è stato cruciale nella vicenda. Sebbene questo sia vero, è altrettanto vero però che è necessario fare una premessa: Facebook non ha nulla a che vedere con la nascita di *Cambridge Analytica*. Infatti, il modello di impresa che aveva in mente Alexander Nix prese piede dall'amicizia con Sophie Schmidt, figlia di Eric Schmidt, CEO di Google[31]. Durante un tirocinio presso la *SCL*, Nix era interessatissimo dagli sviluppi legati alla piattaforma di *Google Analytics*, che aveva iniziato a raccogliere e analizzare i dati dei visitatori di quasi la metà dei maggiori siti al mondo: tramite l'installazione dei *cookie* nei dispositivi degli utenti, i clienti di Google erano in grado di sapere qual era il tasso dei *clic*, cosa stessero scaricando gli utenti, a quali contenuti fossero più interessati e anche il tempo medio di navigazione. Ecco che quindi successivamente Nix si mise al lavoro per fondare una società che avrebbe sfruttato le tecniche predittive ideate da Google, adattandole al business delle campagne elettorali. Per fare ciò, aveva bisogno di accumulare più dati possibili da una grande varietà di fonti eterogenee tra loro, per poi pulire i dati incrociando i patrimoni informatici con un metodo scientifico e granulare, basato su algoritmi.

[30] Wiley (2020).

[31] Kaiser (2019).

Facebook, quindi, entrò in gioco solo successivamente, come terreno fertile nel quale sviluppare e mettere in moto quella macchina affamata di dati quale fu *thisisyourdigitallife*.

Come si diceva nel paragrafo 1, agli utenti era richiesto di fornire un consenso molto poco informato all'utilizzo dell'app.

L'architettura privacy di Facebook vigente al momento in cui si è verificato il caso *Cambridge Analytica*, oggi oggetto di revisione, si fondava su due documenti, la "Dichiarazione dei diritti e delle responsabilità", aggiornata al 31 gennaio 2018, e la "Normativa sui dati", aggiornata al 29 settembre 2016. Ciò prima dell'entrata in vigore del GDPR[32]. Dalla lettura combinata dei due documenti emergevano una serie di regole poco trasparenti e molto complicate.

Senza scendere nel dettaglio del contenuto della documentazione proposta, è indubbio che una delle più grandi criticità era rappresentata dalla finalità per la quale la piattaforma dichiarava di raccogliere ed utilizzare i dati personali, nonché il livello di trasparenza insito in essa. Quando l'utente medio si approccia all'iscrizione al social network, si aspetta infatti di rilasciare i suoi dati per permettere a Facebook di dargli accesso ad una piattaforma digitale in grado di mettere in contatto le persone attraverso la condivisione istantanea di immagini, pensieri, opinioni, video, notizie di vario genere. Tale obiettivo era ribadito anche nella sezione dedicata alla normativa sui dati, laddove si specificava che la *mission* di Facebook consisteva nel "rendere il mondo più aperto e connesso" consentendo alle "persone di condividere contenuti". Tali diciture sono ora sparite dal documento.

[32] La nuova architettura prevede invece delle Condizioni d'uso rinvenibili al seguente link: https://www.facebook.com/legal/terms/update e una Normativa sui Dati rinvenibile qui: https://www.facebook.com/about/privacy/update. È interessante il fatto che negli ultimi 4 anni, a seguito dello scandalo Cambridge Analytica, non sia cambiata la nota di chiusura del paragrafo "Come vengono condivise queste informazioni?", laddove recita "Nota: 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 dati di Facebook e Instagram se l'utente non ha usato la loro app per tre mesi. Inoltre, stiamo apportando modifiche a 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."

Da un punto di vista più asettico, tuttavia, senza farsi trarre in inganno da dichiarazioni d'intenti più emotive che altro, si osserva che quanto sopra attiene più alla *vision* di Facebook, più che alla sua *mission*: meno attraente della *vision* aziendale, la *mission* vera e propria nasconde un aspetto molto meno appetibile per i potenziali clienti – iscritti alla piattaforma: e cioè che l'iscrizione è solo *prima facie* gratuita. A confermare questa tesi era proprio l'art. 9 della Dichiarazione dei diritti e delle responsabilità di Facebook (ora trasposta, con alcune modifiche, ma sostanzialmente in maniera identica nel contenuto, nel paragrafo "Autorizzazioni concesse dall'utente a Facebook", con un ribaltamento evidente dell'*accountability* sull'utente), laddove si manifestava esplicitamente la possibilità di offrire pubblicità e altri contenuti commerciali o contenuti di inserzionisti sponsorizzati e quindi si dichiarava che l'utente, utilizzando la piattaforma, di fatto prestava il consenso all'utilizzo del loro nome, immagine del profilo e delle informazioni condivise[33]. Tale consapevole omissione, cioè il fatto di non aver specificato chiaramente che il controvalore del servizio, il prezzo del servizio, è rappresentato dalla cessione di proprie informazioni, spesso anche di categorie particolari di dati (art. 9 GDPR), in quanto in grado di rilevare dati particolarmente sensibili dell'utente (si pensi a condizioni di salute o convinzioni politiche), ha significato la creazione di una crepa nella sicurezza della piattaforma, con il risultato di consentirne un uso particolarmente disinvolto e disinibito da parte degli utenti ignari. Ciò in pieno contrasto con quanto previsto dall'art. 5 del GDPR, secondo cui le informazioni per essere raccolte richiedono finalità determinate, esplicite e legittime. In questo senso, un'informativa chiara e

[33] In particolare, nel documento "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 utilizzare 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 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".

trasparente sulle finalità di utilizzo dei dati avrebbe potuto permettere agli utenti di essere liberi di decidere se conferire o meno tali dati[34].

Facebook inizialmente tentò di giustificare lo scandalo spiegando che il permesso all'uso dei dati a favore di *Cambridge Analytica* era stato concesso solamente per fini scientifico – accademici, ma il CEO di *Cambridge Analytica*, Nix, smentì immediatamente questa circostanza, quasi pavoneggiandosi dell'essere riuscito a fare un utilizzo commerciale dei dati. Facebook, infatti, secondo i meglio informati, sarebbe stata a conoscenza dell'utilizzo illecito dei dati già dal 2015[35], tanto che si sarebbe attivata per chiedere a *Cambridge Analytica* l'immediata cancellazione degli stessi, senza tuttavia informare gli utenti del *data breach* in corso e senza mai rilasciare alcuna dichiarazione pubblica. Secondo quanto dichiarato da Christopher Wiley, la società di Menlo Park non si impegnò particolarmente per ottenere la distruzione dei dati, fino a quando nel 2018 ingaggiò la società di indagini digitali forensi Stroz Friedberg e contemporaneamente, il 16 marzo 2018, sospese dal social network gli account degli individui legati a *Cambridge Analytica*, alla società madre *SCL*, il Dottor Kogan e Christopher Wiley stesso[36]. Stando a Facebook, infatti, questi avevano garantito di non essere in possesso di dati raccolti in modo illecito. Tale rassicurazione era basata sulla conferma – poi smentita – di Alex Tayler, ex dipendente di *Cambridge Analytica*, il quale aveva garantito, mentendo, a Facebook, di aver cancellato i dati e tutte le sue copie dai server di *Cambridge Analytica*. Tale rassicurazione era avvenuta semplicemente tramite scambio di mail (dall'oggetto "Dichiarazione di innocenza" …) tra Tayler e Allison Hendrick di Facebook. Quel giorno *Cambridge Analytica* rilasciò una dichiarazione in risposta alla sospensione, sostenendo di aver sempre agito nel rispetto delle norme della piattaforma e che si era resa proattiva nel risolvere la questione, collaborando[37]. Contemporaneamente, tuttavia, la giornalista Carole Cadwalladr e il The New York Times pubblicarono degli articoli di inchiesta su *Cambridge Analytica* e Facebook, imboccati da Christopher Wiley[38].

[34] Per un approfondimento si veda Article 29 Working Party (2018).

[35] Hamilton (2019).

[36] Wiley (2020).

[37] Kaiser (2019).

[38] Rosenberg, Confessore e Cadwalladr (2018).

Wiley sarebbe stato in possesso anche di prove secondo cui fu Aleksandr Kogan a svolgere tutto il lavoro di raccolta dati, e che *Cambridge Analytica* non verificò mai se fossero stato raccolti nel rispetto delle norme del social network. Secondo la copia dell'accordo tra Kogan e *Cambridge Analytica*, i fini del lavoro non avevano nulla di accademico, ma avevano solamente risvolti commerciali: *Cambridge Analytica* avrebbe pagato un milione di dollari a Kogan per la raccolta dei dati su Facebook, mentre altri dati confermavano che *Cambridge Analytica*, complessivamente parlando, aveva speso oltre 7 milioni di dollari per l'intero progetto di acquisizione e modellazione dei dati degli utenti. Wiley era perfettamente a conoscenza che l'operazione intrapresa da Kogan aveva messo in allarme Facebook, ma questa aveva deciso di non occuparsi del problema, negligentemente[39].

I dati non cancellati nel 2015 sarebbero infatti serviti a condurre in porto con successo la campagna elettorale di Trump nel 2016, cambiando di fatto il corso della storia. Ecco perché, molto semplicemente, *Cambridge Analytica* non poteva sbarazzarsi di quei dati: perché erano alla base del suo intero business multimilionario.

Cambridge Analytica aveva mentito a Facebook, e Facebook si era limitata a ricevere delle rassicurazioni all'acqua di rose. Tutto ciò fu alla base dello scoppio del più grande *data breach* della storia della tecnologia, così da essere definito *Datagate*[40].

In seguito alla diffusione della vicenda, Mark Zuckerberg, socio fondatore e CEO di Facebook, fu udito in udienza presso le commissioni riunite di Camera e Senato degli Stati Uniti d'America il 10[41] e l'11[42] aprile 2018 per illustrare il funzionamento della piattaforma e dare spiegazioni in merito alla fuga di dati. Fu udito anche il mese successivo dal Parlamento Europeo[43].

Ruppe il silenzio il 21 marzo 2018, con un lungo post dal seguente contenuto: "We have a responsibility to protect your data, and if we can't then we don't deserve to serve you. I've been working to understand exactly what happened and how to make sure this doesn't happen again. The good news is that the most important actions to prevent

[39] Wiley (2020).

[40] Valsania (2018).

[41] Per l'intera trascrizione dell'audizione del 10 aprile 2018 si veda Bloomberg Government (2018).

[42] Per l'intera trascrizione dell'audizione dell'11 aprile 2018 si veda Bloomberg Government (2018).

[43] Anderson (2018).

this from happening again today we have already taken years ago. But we also made mistakes, there's more to do, and we need to step up and do it. […] I started Facebook, and at the end of the day I'm responsible for what happens on our platform. I'm serious about doing what it takes to protect our community. While this specific issue involving *Cambridge Analytica* should no longer happen with new apps today, that doesn't change what happened in the past. We will learn from this experience to secure our platform further and make our community safer for everyone going forward"[44].

Gli investitori si vendicarono, tanto che sul Nasdaq il titolo perse quasi 20 miliardi di dollari in pochi minuti e un gruppo di azionisti fece causa contro la società per aver rilasciato dichiarazioni false e ingannevoli[45]. Nel frattempo, gli utenti di tutto il mondo si mobilitarono per porre fine alla dipendenza da social network: lo fecero però attraverso un altro social network, Twitter, utilizzando l'hashtag *#DeleteFacebook*. A riprova che, pur senza dirlo, Facebook deteneva ormai il monopolio del mercato.

Come sostenuto dal quotidiano online Vox, si potrebbe quasi affermare che fu quasi di più uno scandalo di Facebook, che uno scandalo di *Cambridge Analytica*[46].

Edward Snowden, con un post su Twitter, invece disse che "Facebook makes their money by exploiting and selling intimate details about the private lives of millions, far beyond the scant details you voluntarily post. They are not victims. They are accomplices"[47].

1.3 BREXIT E ELEZIONI PRESIDENZIALI AMERICANE DEL 2016

Come evidenziato in precedenza, i dati raccolti tramite Facebook furono indispensabili per *Cambridge Analytica* al fine di costruire profili politici[48] degli utenti, da poter poi riutilizzare durante svariate campagne presidenziali tra il 2013 e il 2018 tramite *microtargeting*. Come sostenuto da Alexander Nix in un video trasmesso

[44] Salinas (2018).

[45] Ryskamp (2020).

[46] Chang (2018).

[47] Snowden, tweet del 17 marzo 2018.

[48] Ai sensi dell'art. 9 del GDPR, le opinioni politiche sono considerate particolari categorie di dati (cd. dati sensibili) per il cui trattamento devono necessariamente verificarsi le condizioni di cui all'art. 9 co. 2, imponendo così particolari cautele ulteriori rispetto a quelle standard.

dall'emittente Channel 4, "Non si vincono le campagne con i fatti, ma con le emozioni"[49].

Che *Cambridge Analytica* abbia avuto un ruolo importante nella campagna di Trump sono gli stessi Nix e Tayler ad ammetterlo, in un video sotto copertura diffuso da Channel 4, che attraverso dei giornalisti fintisi politici dello Sri Lanka interessati ai servizi di *Cambridge Analytica* nell'ambito delle elezioni del proprio paese, avevano ottenuto informazioni riservate dai due. Nix affermò che *Cambridge Analytica* aveva curato ogni minimo aspetto, al contrario di quanto invece sostennero Donald Trump stesso e Brad Parscale fin dal 2016[50]. Le due direttrici della campagna furono la mobilitazione di massa e la propaganda denigratoria, come in effetti si rivelò essere.

Non di minor importanza per il corso della storia politica recente fu il voto sull'uscita dall'Unione Europea della Gran Bretagna, cd. Brexit.

Cambridge Analytica, infatti, attraverso i due ex dipendenti Brittany Kaiser e David Wilkinson (*Chief Data Scientist*) affiancò il partito *Leave.eu*, a favore dell'uscita del Paese dall'UE. Il contributo fondamentale che diedero fu legato ai metodi di profilazione dell'elettorato, replicando quelli già conosciuti per le campagne politiche in cui era stata coinvolta *Cambridge Analytica*.

Nonostante una prima fase di negazione della sussistenza di rapporti tra *Leave.eu* e *Cambridge Analytica*, successivamente, dopo aver vinto il referendum, il politico Arron Banks dichiarò che il risultato raggiunto fu merito dell'impiego scientifico dei dati, citando molto spesso l'attività di consulenza messa in piedi da *Cambridge Analytica*. Lo stesso Banks disse che la campagna Leave.eu fu quella più virale del Regno Unito, intercettando, in una sola settimana, quasi 4 milioni di utenti su Facebook[51].

Queste due campagne rappresentano l'emblema di come, a partire dalla campagna elettorale di Obama, il *microtargeting* emozionale profilato sul singolo sia diventato la *conditio sine qua non* nell'architettura di una campagna elettorale politica. Wiley, ad esempio, aveva sostenuto quanto segue all'Observer: "Trump is like a pair of Uggs, or Crocs, basically. So how do you get from people thinking 'Ugh. Totally ugly' to the

[49] Rociola (2018).

[50] Per capire meglio il ruolo di Brad Parscale nella vicenda si veda Marantz (2020); Calderini (2019).

[51] Gheoghegan e Corderoy (2018).

moment when everyone is wearing them?"[52]. Bisogna far credere alla gente che gli UGG (stivali nati in Australia divenuti molto popolari tra il genere femminile) non siano brutti. Gli UGG però sono brutti, ma modificando il pensiero del mondo tutti li avranno ai piedi. Lo stesso vale in politica, così come nella *fashion industry*.

Ecco che allora, tramite questa strategia, la campagna vincente di Trump fu incentrata sulla propaganda anti Hillary Clinton, sull'operazione di targeting rivolta agli afroamericani, sulla categorizzazione degli ispanici in microcategorie molto specifiche (si pensi alla questione del muro ai confini con il Messico). Allo stesso modo in cui la campagna *Leave.eu* fu fondata sulle menzogne intorno all'ingresso della Turchia nell'UE o all'impoverimento del sistema sanitario britannico nel caso di permanenza all'interno dell'Unione.

Tutto ciò non sarebbe stato possibile senza *big data*. Magari Hillary Clinton sarebbe stata la prima POTUS (President of the United States) donna della storia, magari il Regno Unito farebbe ancora parte dell'Unione Europea. O magari le vicende sarebbero andate esattamente nello stesso modo in cui sono andate realmente. Chi può dirlo. Di una cosa si può essere sicuri: il *microtargeting* e i *big data* hanno preso parte alle partite elettorali, e in prima linea.

1.4 NON CONTA IL CHI, CONTA IL COME

Dalla concatenazione di eventi sopra descritta si evince facilmente come pochi eventi mediatici abbiano avuto l'eco mondiale che ebbe lo scandalo *Cambridge Analytica*. Forse perché è stato il primo grande scandalo avente ad oggetto beni – immateriali fino ad un certo punto – fino ad allora poco considerati quali i dati personali, che l'ex Garante della privacy, Antonello Soro, definì il "nuovo petrolio dell'economia digitale" durante un'intervista relativa all'attuale debolezza delle imprese nei confronti di attacchi di carattere cyber[53]. Poche sono state le vicende che hanno coinvolto in tal misura attori sia provenienti dal mondo accademico, sia da quello politico, sia da quello imprenditoriale.

---

[52] Ellison (2018).

[53] L'intervista è reperibile sul sito del Garante italiano, documento n. 8136779, "Le imprese sono troppo deboli nelle difese contro gli hacker", del 26 marzo 2018, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8136779.

Sono stati prodotti fiumi di inchiostro, video, reportage, film (si pensi al docu – film di Jehane Noujaim e Karim Amer e prodotto da Netflix "The Great Hack") dove parlano della vicenda e cercano di dare una ricostruzione dei fatti con le prove a disposizione. Quello che però la maggior parte dei media non mettono adeguatamente in rilievo, attirati più dal contesto sociopolitico dove è esploso questo scandalo, sono luce le falle di un'economia dato centrica, con le sue ramificazioni politiche e anche accademiche.

Pur essendo vero che lo scandalo ha coinvolto le più alte sfere governative, è altrettanto vero che la base di tutto è stata una crepa all'interno di una piattaforma social utilizzata quotidianamente da cittadini comuni.

Poca attenzione si presta al fatto che le modalità di raccolta dati attraverso l'app su *Facebook* non rappresentava un *bug* della piattaforma, ma piuttosto una *feature*, un servizio vero e proprio fornito agli inserzionisti (ora rimosso). Che poi lo sfruttamento fosse illecito, come già detto, è indubbio, ma è altrettanto indubbio che la raccolta non era vietata, potenzialmente. Dopotutto, non si è verificato nessun *hack*, ma piuttosto un *data breach*, quindi una violazione vera e propria dell'integrità dei dati personali degli utenti.

Togliendo infatti dalla somma Trump o *Leave.eu*, il risultato non cambia: lo scandalo non è dato dalla vittoria di Trump o dall'uscita del Regno Unito dall'Unione Europea, ma piuttosto di come l'economia dei dati si sia rilevata un colabrodo al primo attacco ben portato.

***

Dopo aver ricostruito fattualmente il caso *Cambridge Analytica*, prima di passare all'analisi della legislazione applicabile e delle sanzioni irrogate ai protagonisti della vicenda, è necessario soffermarsi su alcune definizioni e su alcuni concetti che renderanno più chiari i contorni giuridici della vicenda stessa.

CAPITOLO 2 - DEFINIZIONI E CONCETTI

2.1 IL CONCETTO DI PROFILAZIONE

Il considerando 71 del GDPR stabilisce che l'interessato, ossia il soggetto al quale i dati personali si riferiscono, dovrebbe avere il diritto di non essere sottoposto a una decisione che produca effetti sulla sua sfera giuridica o che possa incidere significativamente sulla sua persona, basata unicamente su un trattamento automatizzato.

Il trattamento automatizzato più diffuso tra le aziende che si occupano di trattamento di dati personali è sicuramente quello della profilazione che, sempre a norma del considerando 71, "consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato, ove ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona". Definizione del tutto simile è fornita anche dall'articolo 22.

Alla luce della pervasività delle tecniche di profilazione, il GDPR afferma quindi che, sebbene non vietata in teoria, in pratica è necessario predisporre adeguate cautele nei confronti dell'interessato, ad esempio attraverso o i) la conclusione o l'esecuzione di un contratto con il titolare del trattamento (cioè la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali), oppure ii) attraverso la raccolta del consenso esplicito da parte dell'interessato.

In ambito commerciale, questa tecnica è largamente utilizzata per fornire servizi individualizzati, come ad esempio la pubblicità comportamentale (si pensi agli episodi in cui pensiamo ad un determinato bene, e poco dopo lo stesso identico bene ci appare in pubblicità mentre utilizziamo un social: non si tratta di magia, ma di un'accurata selezione da parte del social stesso che è in grado di prevedere le nostre preferenze d'acquisto sulla base delle informazioni acquisite durante la nostra navigazione).

Quella della profilazione è una tecnica che fonda le sue radici negli studi di Allport e Odbert[54], che nel 1936 catalogarono tutte le parole che potevano descrivere il comportamento di un individuo, teorizzandone ben 18.000, racchiudendole poi in quattro categorie:

- Gli stati d'animo;
- I giudizi sulla condotta;
- Le caratteristiche fisiche;
- I tratti della personalità.

Il lavoro di Allport e Odbert fu affinato da Cattel[55], che tra il 1943 e il 1945 selezionò 35 variabili della personalità tra i vocaboli individuati da Allport e Odbert nella categoria "tratti della personalità".

Successivamente Fiske[56] procedette ad un'ulteriore riduzione, portando a 22 il numero dei fattori fondamentali. Infine, Tupes e Christal ridussero a cinque il numero delle variabili "relativamente forti e ricorrenti"[57]. Tale ultimo modello fu definito come "Big Five": le variabili riescono a rappresentare la personalità al più alto livello di astrazione, riassumendo un alto numero di specifiche e distinte caratteristiche della personalità di un individuo. Le variabili sono le seguenti (acronimo di OCEAN):

- Openess to experience;
- Conscientiousness;
- Extraversion;
- Agreeableness;
- Neuroticism.

Recentemente, tuttavia, gli studiosi si sono interrogati sulla possibilità di costruire un modello predittivo del profilo psicometrico di una persona, senza ricorrere al test del *Big Five*.

Trovarono terreno fertile proprio nel campo dei *social network*, che l'Enciclopedia Treccani definisce come "un servizio informatico on line che permette la realizzazione di reti sociali virtuali. Si tratta di siti internet o tecnologie che consentono agli utenti

[54] Allport e Odbert (1936).

[55] Cattel (1943 e 1945).

[56] Fiske (1949).

[57] Tupes e Christal (1961 e 1992).

di condividere contenuti testuali, immagini, video e audio e di interagire tra loro […]"[58]. Tali contenuti permettono pertanto all'utente di condividere con il social network la sua personalità "*offline*", che quindi altrimenti rimarrebbe confinata alla cerchia di rete sociale fisica, non anche a quella virtuale, tramite l'integrazione di diverse fonti di informazioni personali. A tal punto che gli utenti stessi riescono a farsi un'idea abbastanza precisa della personalità degli altri solamente sulla base dei loro profili online.

Di ciò ne è ad esempio perfettamente consapevole lo psicologo Michal Kocinski (che tornerà successivamente *infra*), il quale, in un articolo pubblicato nel 2013 insieme a David Stillwell e Thore Graepel sulla rivista Pnas, disse che "human migration to digital environment renders it possible to base such predictions on digital records of human behavior. It has been shown that age, gender, occupation, education level, and even personality can be predicted from people's Web site browsing logs. Similarly, it has been shown that personality can be predicted based on the contents of personal Web sites, music collections, properties of Facebook or Twitter profiles such as the number of friends or the density of friendship networks, or language used by their users. Furthermore, location within a friendship network at Facebook was shown to be predictive of sexual orientation. This study demonstrates the degree to which relatively basic digital records of human behaviour can be used to automatically and accurately estimate a wide range of personal attributes that people would typically assume to be private."[59]

Riassumendo: utilizzando le interazioni relative al tasto "mi piace" su Facebook da parte di 58.000 volontari (un gesto che ormai nel 2022 potremmo definire quasi un movimento meccanico del pollice verso lo schermo di uno *smartphone* in corrispondenza di un contenuto che riteniamo meritevole), lo studio dimostrava come sia possibile ricostruire l'origine etnica di una persona con un grado di accuratezza pari al 95%, e la posizione politica con un grado dell'85%.

Analizzando circa 70 "mi piace", un social network sa più informazioni su di noi rispetto ai nostri amici. Analizzando circa 150 "mi piace", un social network sa più

[58] Si veda social network nell'Enciclopedia Treccani.

[59] Kosinski, Stillwell e Graepel (2013).

informazioni di noi rispetto a nostra mamma. Analizzando circa 300 "mi piace", si supera le informazioni che un individuo stesso conosce di sé.
È proprio su questo terreno che hanno trovato applicazione le tecniche di profilazione utilizzate da *Cambridge Analytica*, grazie al *data mining*[60] e l'analisi di dati, attuava comunicazioni strategiche – *rectius*, profilate – per scopi elettorali.

2.2 IL CONCETTO DI MICROTARGETING

A partire dagli anni '60[61], quindi, si è passati da metodi di profilazione molto basilari, a quella che viene definita la psicografia, cioè un metodo di profilazione basato sul comportamento dei consumatori e che integra non solo tradizionali dati anagrafici e demografici, ma anche e soprattutto elementi più interessanti quali lo stile di vita, variabili di ordine psico – sociale, abitudini, gusti. Ciò al fine di ottenere una classificazione degli utenti il più possibile complessa ed efficace. Il risultato è che è possibile inviare all'utente messaggi e contenuti praticamente personalizzati sulla sua persona, pur mantenendo, in teoria, lo stesso obiettivo: massimizzare il profitto, attraverso un approccio puramente emotivo.
Questa segmentazione dell'audience grazie a sofisticati modelli predittivi computazionali è chiamata *microtargeting*[62].
Le campagne politiche, in particolare negli Stati Uniti, hanno utilizzato queste tecnologie digitali per più di un decennio, sviluppando strumenti e tecniche sempre più sofisticati durante ogni ciclo elettorale e le cosiddette "politiche computazionali" sono diventate procedure operative standard.
Con la pratica di inviare messaggi mirati a elettori selezionati, il *microtargeting* della campagna di Barack Obama era ad esempio riuscito nell'intento di ridurre alla sfera privata il dibattito politico statunitense[63]. Raccogliendo e sfruttando dati, esso consentiva di abbinare a ristretti cluster di votanti micronarrazioni calibrate e specifiche sugli stessi: così era perfettamente possibile che un marito e una moglie

[60] Per maggiori informazioni sul *data mining*, si veda Sandonnini (2020).

[61] Tupes e Christal (1961 – 1992).

[62] Calderini (2019).

[63] Issenberg (2012).

ricevessero due messaggi completamente differenti, senza che nessuno dei due si accorgesse della cosa. In tal modo, inoltre, si evitavano i filtri del dibattito pubblico.
Tale *modus operandi* troverà poi la sua massima espressione nel 2016 con la campagna politica di Donald Trump per la Presidenza degli Stati Uniti e la campagna per la Brexit, durante le quali ebbero un ruolo determinante l'industria pubblicitaria e l'azienda *Cambridge Analytica*, che si vedrà meglio nel capitolo 3.
Infatti, molte delle strategie, degli strumenti e delle tecniche digitali impiegate nelle recenti elezioni politiche sono state inizialmente sviluppate, implementate e perfezionate proprio dal settore commerciale. Come sostenuto da Barbara Calderini, "questo sistema è emerso grazie ad una cultura politica di minima interferenza da parte di governi statali e all'interno di un *laissez-faire* riguardo ad Internet e alle nuove tecnologie. Le pratiche di marketing digitale contemporaneo hanno sollevato a livello globale seri problemi non limitati alla sola *data protection*, ma anche in relazione alla reale tenuta del principio democratico degli Stati e a livello globale."[64].
Il salto in avanti di qualità è dunque evidente: in questo senso, i social si trasformarono immediatamente in un enorme database in grado di fornire profilazioni facilmente accessibili e accurate su caratteristiche prettamente personali da poter usare per i scopi più disparati, tra cui appunto quelli politici e di propaganda. Si vedrà meglio più avanti come il *microtargeting* psicografico utilizzato da *Cambridge Analytica* fu senza dubbio una tipologia di marketing politico innovativo, fondato quasi esclusivamente sulle tracce digitali lasciate dagli elettori – più o meno volontariamente, più o meno consapevolmente.
L'Unione Europea sta invece ora valutando di vietare il *microtargeting* in determinate condizioni, introducendo dei maggiori obblighi di trasparenza per le piattaforme nel campo della pubblicità mirata. Le sanzioni per le violazioni delle regole includono invece multe fino al 4% del reddito annuale di un'azienda. Per la pubblicità online, in particolare, la Commissione dell'UE ha proposto regole che fornirebbero agli utenti delle piattaforme informazioni immediate sulle fonti degli annunci che compaiono sul loro feed, comprese informazioni granulari sul motivo per cui un individuo è targettizzato con un annuncio specifico[65].

[64] Calderini (2019).

[65] Lettig e Stolton (2021).

In questo senso, è molto rilevante l'opinion 02/2022 del 20 gennaio 2022 dello European Data Protection Supervisor (EDPS), secondo cui "given the multitude of risks associated with online targeted advertising, the EDPS urges the co – legislators to consider strict rules, by (1) providing for a full ban of microtargeting for political purposes; and (2) introducing further restrictions of the categories of the data that may be processed for the purposes of political advertising, including targeting and amplification, in particular prohibiting targeted advertising on pervasive tracking."[66]
Come emerge dalla lettura dell'art. 9 del GDPR, secondo il quale: "È vietato trattare dati personali che rivelino 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", salvo poi comunque introdurre delle restringenti deroghe ai commi successivi, le convinzioni politiche di un individuo sono infatti considerate quale dato sensibile, da trattare con una cautela ulteriore rispetto ai dati personali comuni[67].

2.3 IL CONCETTO DI CONSENSO

Si è detto poc'anzi che l'incredibile mole di dati utilizzati per profilare gli utenti dei social network (in particolare, ma non solo) è rilasciata più o meno volontariamente e più o meno consapevolmente proprio dagli utenti stessi.
È quindi necessario ora introdurre il concetto di consenso, che il GDPR, all'articolo 6, individua come una delle basi giuridiche per la liceità del trattamento dei dati personali per una o più finalità[68]. Al successivo articolo 7 ne indica poi le condizioni affinché lo

[66] European Data Protection Supervisor (2022).

[67] Sul punto si veda Saetta (2018).

[68] Ai sensi dell'art. 6 del GDPR, infatti, il trattamento si considera lecito se si verifica almeno una delle seguenti condizioni:
i) espressione del consenso da parte dell'interessato; *ii*) il trattamento è necessario per l'esecuzione di un contratto ovvero di misure precontrattuali; *iii*) è necessario adempiere ad un obbligo legale; *iv*) risulta fondamentale per la salvaguardia di interessi vitali dell'interessato o di altri; *v*) è necessario per soddisfare l'interesse pubblico o per assolvere ad un pubblico potere; *vi*) 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

stesso sia valido, ben riassunte anche nel considerando n. 32: "Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale. Ciò potrebbe comprendere la selezione di un'apposita casella in un sito web, la scelta di impostazioni tecniche per servizi della società dell'informazione o qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto. Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle. Il consenso dovrebbe applicarsi a tutte le attività di trattamento svolte per la stessa o le stesse finalità. Qualora il trattamento abbia più finalità, il consenso dovrebbe essere prestato per tutte queste. Se il consenso dell'interessato è richiesto attraverso mezzi elettronici, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso.".

Il termine consenso nel GDPR ritorna per ben 108 volte, a riprova dell'importanza di tale base giuridica, in quanto – almeno in teoria – responsabilizza l'utente verso i rischi che corre nell'ambito del trattamento dei suoi dati personali.

Il concetto di consenso affonda le sue radici nella definizione dettata dalla direttiva 95/46/CE all'articolo 7, integrata dall'Opinion 15/2011 on the definition of consent (WP187) dell'*Article 29 Data Protection Working Party* del 13 luglio 2011. Ma se nella versione originaria il consenso doveva essere connotato da libertà, specificità e informazione, ora vi si aggiunge anche il concetto di inequivocabilità. In questo modo, si impone che l'assenso si manifesti attraverso un'esplicita dichiarazione ovvero un'azione che non lasci dubbio alcuno circa la volontà dell'utente – interessato di mettere a disposizione i propri dati personali affinché siano utilizzati (cd. regime dell'*opt – in*). E tale azione positiva risulta addirittura rafforzata nel caso sia necessario un consenso connotato da profili di ulteriore specificità, come nel caso di trattamento di categorie particolari di dati (cd. dati sensibili) di cui all'art. 9 del GDPR, nel caso di

dei dati personali, in particolare se l'interessato è un minore. Sulla liceità del trattamento si veda anche Article 29 Data Protection Working Party (2018).

trasferimento di dati verso un paese extra UE, e nel caso già sopra analizzato del trattamento con processi decisionali automatizzati, come la profilazione.

Ma se da un lato l'intento del legislatore europeo è stato quello di spingere in avanti il confine della consapevolezza degli interessati richiedendo uno sforzo aggiuntivo nel momento della manifestazione dell'interesse (al fine di poter esercitare realmente e consapevolmente il diritto di *opt in* e *opt out* rispetto ai trattamenti dei propri dati personali aventi come base giuridica appunto il consenso dell'interessato), dall'altro lato è altrettanto vero che l'utente dev'essere messo nelle condizioni, da parte della piattaforma, di prestare quel consenso nella maniera più libera, consapevole, specifica e informata possibile. È quindi il contemporaneo verificarsi di tali requisiti che rende il trattamento *compliant* con la normativa del GDPR.

Come si vedrà più avanti, tuttavia, tale bontà di intenti resta confinata sulla carta, atteso che i requisiti che ruotano intorno al rilascio del consenso da parte dell'utente si scontrano molto spesso con le finalità per cui il consenso al trattamento dei dati è richiesto. In altre parole, tavolta sembra sopravvivere quel *mismatch* informativo che rischia di portare ad un lento, ma inesorabile declino del concetto di consenso e ad un progressivo svuotamento del suo valore di baluardo a difesa di trattamenti non autorizzati, facendolo assurgere ad uno specchietto per le allodole dietro al quale si nascondono, molto spesso, intenti ben diversi[69].

Infatti, "Transparency is essential, but it is not enough"[70].

[69] Per le modalità di acquisizione del consenso nell'ambito dei cookie, si veda Garante Italiano per la protezione dei dati personali (2014).

[70] Wiewiórowski (2022).

CAPITOLO 3 - IL QUADRO NORMATIVO DI RIFERIMENTO

3.1 IL REGOLAMENTO UE 2016/679 – IN PARTICOLARE SULL'APPLICABILITÁ ALL'ABUSO DI DATI SOCIAL

Si è già detto di come il contemporaneo venire a galla della vicenda *Cambridge Analytica* e l'entrata in vigore del GDPR possano essere considerati quasi un copione di un film da premio oscar.

Nel 2012, infatti, dinanzi ad un quadro europeo molto frastagliato in merito alla tutela dei dati personali, il legislatore europeo intraprese un lungo cammino finalizzato all'individuazione ed alla cristallizzazione di regoli comune europee in questa materia. Le norme alla base della direttiva 95/46/CE non erano più in grado, infatti, di assicurare protezione contro le complesse sfide derivanti dall'innovazione tecnologica, soprattutto derivanti dallo straordinario incremento dell'utilizzo dei social network e dei siti web aventi *data centers* fuori dal territorio dell'Unione[71].

Il GDPR fu quindi approvato dal Parlamento Europeo e dal Consiglio il 27 aprile 2016 e divenne operativo in tutti gli Stati membri a partire dal 25 maggio 2018[72].

Il testo è composto da 99 articoli e 173 considerando e altro non fa se non costituire un quadro normativo che implementi il diritto falla tutela dei dati personali già affermato con la Carta dei diritti fondamentali dell'Unione Europea del 2000 (entrata poi in vigore a fine 2009). .

Ora, per quanto attiene a questo lavoro, interessa capire se le previsioni del GDPR sono o meno applicabili alla vicenda *Cambridge Analytica* e se, nel caso in cui questa normativa fosse già stata vigente all'epoca dei fatti, avrebbe potuto evitare o quantomeno arginare quanto accaduto.

---

[71] È il 25 gennaio 2012 quando la Commissione Europea presenta il pacchetto completo sulla protezione dei dati personali contenente sia la proposta di regolamento che sarebbe poi diventato il GDPR, sia la proposta di direttiva concernente la tutela 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, e la libera circolazione di tali dati, intesa a sostituire la decisione quadro del 2008 sulla protezione dei dati.

[72] Per un approfondimento sul Regolamento in materia di dati personali si veda Biasiotti (2018); Pizzetti (2016).

In un panorama digitale che, come si diceva poc'anzi, travalica i confini nazionali, basando la propria attività sulla circolazione delle informazioni in uno spazio indefinito, è importante definire, come primo aspetto, l'ambito di applicazione delle nuove regole, tramite l'ausilio dell'art. 3 e dei considerando 22, 23 e 24.

Con riferimento in particolare all'ambito di applicazione territoriale, il testo afferma che le norme si applicano non solo ai casi in cui il titolare o il responsabile del trattamento siano localizzati in uno Stato membro, ma anche a tutti quelle attività che coinvolgono dati personali relativi a soggetti che si trovano nell'Unione Europea. In questo senso, i trattamenti devono riguardare anche il monitoraggio degli interessati all'interno dell'Unione, e devono riguardare l'offerta di beni o servizi, anche indipendentemente dall'obbligatorietà di una controprestazione monetaria.

Tale scelta di applicazione territoriale è mutuata dall'orientamento della Corte di Giustizia e dell'*Article 29 Working Group*: infatti, ai sensi della direttiva 95/46/CE, la determinazione dell'ambito di applicazione ruotava essenzialmente intorno al principio di stabilimento, per cui era necessario che il responsabile fosse stabilmente presente all'interno di uno degli Stati membri. Tuttavia, con il progresso tecnologico, della rete Internet e di *player*s come i *social network* che fanno della a-territorialità uno dei loro punti di forza, tale approccio tradizionalistico risultò sempre meno efficace. Sulla scorta dell'opinion 8/2010 del *Working Group*[73] e delle sentenze "Google Spain"[74] e "Weltimmo"[75], il legislatore europeo si orientò verso un'estensione delle norme europee al di là dei confini dell'Unione, dichiarando in maniera specifica al considerando 23 che "onde evitare che una persona fisica venga privata della protezione cui ha diritto in base al presente regolamento, è opportuno che questo disciplini il trattamento dei dati personali degli interessati che si trovano nell'Unione effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione". In questo senso, al considerando 22 si specifica anche che non è determinante la forma giuridica assunta dal titolare o dal responsabile del trattamento, ma è sufficiente che vi sia un'effettiva e reale attività di trattamento

[73] Article 29 Working Party (2010).

[74] Causa C – 131/12, Google Inc. vs. Agencia Española de Protección de Datos, (AEPD) and Mario Costeja González.

[75] Causa C – 230/14, Weltimmo s. r. o vs Nemzeti Adatvédelmi és Információszabadság Hatóság.

nel quadro di un'organizzazione stabile, sia essa una succursale o una filiale dotata di personalità giuridica.

Ecco che quindi non è più solamente il luogo di stabilimento a determinare o meno l'applicazione della norma, ma assurge a criterio fondamentale il bene tutelato, quale fonte di legittimazione della relativa applicabilità: che i dati oggetto di analisi/monitoraggio siano relativi a soggetti che si trovano nel territorio dell'Unione è condizione necessaria e sufficiente affinché il GDPR si ritenga applicabile al trattamento.

Così facendo, è stato possibile tracciare dei confini in un mondo, come quello digitale, che confini non conosce, completamente dedicato ai cittadini europei indipendentemente dal luogo in cui il trattamento venga materialmente effettuato.

Un altro chiaro indicatore dell'applicabilità del GDPR alla vicenda, e alla piattaforma social Facebook in particolare, è la precisazione del considerando 23, laddove afferma che la valutazione deve tenere conto della destinazione d'uso dei beni e dei servizi proposti dall'azienda "indipendentemente dal fatto che vi sia un pagamento correlato". È evidente il richiamo alla tipica ed apparente gratuità dei servizi offerti dai social network.

Tale riferibilità è anche desumibile dal considerando 24, dove, in tema di profilazione, 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."

Ciò premesso, e scendendo più in profondità, bisogna tenere a mente che la vicenda *Cambridge Analytica* non ha avuto origine da un classico *data breach*, quindi non tanto da una violazione dei sistemi di sicurezza di Facebook, ma piuttosto da una divulgazione non autorizzata dei dati degli utenti a favore di terzi da parte di una società partner di Facebook. Tale trasferimento fu reso appunto possibile da una lassività nei controlli preventivi e successivi con riferimento al flusso di dati intercorrente con i partner commerciali.

I dati, quindi, una volta raccolti dallo sviluppatore dell'app, furono venduti, secondo quanto recentementissimamente sostenuto dall'Attorney General del District of Columbia nella causa intentata contro Mark Zuckerberg in data 23/05/2022, per la cifra di 800.000,00 $ ad una società terza[76], *Cambridge Analytica* appunto, il cui *core business* era la profilazione degli utenti a fini politici. Come già evidenziato, la privacy policy (oggi disciplinata ex art. 13 GDPR) di Facebook prevedeva espressamente la possibilità per gli sviluppatori di raccogliere dati degli utenti, ma non ne consentiva la successiva divulgazione, ed in particolare non ne consentiva l'utilizzo per finalità diverse rispetto a quelle dichiarate. Pur tuttavia, di nuovo come sostenuto dall'Attorney General menzionato poco fa, "Facebook did not review the App before it was allowed on the Facebook Platform, nor it verify its claim that the information it collected was for academic purposes". Ma nel momento in cui viene meno la corrispondenza tra i motivi per cui il consenso al trattamento dei dati personali è richiesto e l'effettiva destinazione d'uso, allora, come si vedrà meglio anche più avanti, allora non si può parlare nemmeno tecnicamente di consenso. Tantomeno libero, informato, consapevole. A peggiorare ulteriormente il già complicato quadro fu il fatto che il CEO di Facebook decise di non divulgare immediatamente la notizia e di non avvisare le autorità competenti, nonostante la violazione fosse nota, come visto sopra, sin dal dicembre 2015, ma decise di limitarsi laconicamente a chiedere a *Cambridge Analytica* la distruzione dei dati ricevuti. Con esito, si seppe più tardi, negativo.

In regime di GDPR tale inerzia avrebbe comportato la violazione dell'art. 33, in tema di obblighi in capo al titolare del trattamento, specificatamente il dovere di notifica all'autorità di controllo. L'articolo, infatti, afferma che "In caso di violazione dei dati personali, il titolare del trattamento 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."

[76] Si veda, sul punto, l'atto di citazione formulato dall'Attorney General del District of Columbia Karl A. Racine contro Mark Zuckerberg in data 23/05/2022, consultabile al link https://oag.dc.gov/sites/default/files/2022-05/2022.05%20%283%29.pdf

La segnalazione deve inoltre contenere la natura della violazione, le categorie di dati coinvolti e il presunto numero di soggetti interessati, nonché descrivere le possibili conseguenze dannose: a norma dell'articolo 34, infatti, vanno avvisati anche gli interessati qualora la violazione possa comportare un "rischio elevato per i diritti e le libertà fondamentali delle persone".

La tempestività nell'informazione è quindi ritenuta di fondamentale importanza ai fini della limitazione delle conseguenze pregiudizievoli che potrebbero insorgere in capo agli interessati: ai sensi del considerando 85 "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. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che, conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo."

Facebook avrebbe pertanto dovuto attivarsi immediatamente, informando tutti gli utenti e le autorità di controllo in maniera dettagliata.

Sebbene sia vero che tecnicamente non si sia trattato di un *data breach* nel vero e proprio senso della parola, e quindi che a detta di Facebook non sussisteva alcun obbligo di comunicazione verso gli interessati, è altrettanto vero la normativa sulla tutela dei dati personali è sempre stata imperniata (ed ora resa ancora più orientata verso questo aspetto) da un necessario rapporto di fiducia tra titolare del trattamento e utenti/interessati. Si pensi ad esempio al considerando 7, il quale stabilisce che "è opportuno che le persone fisiche abbiano il controllo dei dati personali che li

riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche". L'analisi, infatti, deve necessariamente partire non tanto dalle misure poste in essere dal social dopo l'entrata in vigore del GDPR, ma piuttosto nella valutazione degli strumenti tecnici ed organizzativi messi a punto preventivamente al fine di evitare il realizzarsi di tali ingerenze esterne alla sfera privata degli utenti, anche in nome del principio di *accountability* che permea la materia.

Inoltre, in una situazione di piena vigenza del GDPR, il social network avrebbe dovuto, prima di dar inizio al trattamento, procedere ad una valutazione d'impatto del trattamento sui diritti fondamentali degli interessati ai sensi dell'art. 35, comma 3, lett. a) (cd. *DPIA – Data Protection Impact Assessment*), con conseguente documentazione di tutte le misure tecnico organizzative messe in atto per garantire la sicurezza dei dati. Ciò in quanto il *social network* effettua regolarmente 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 […]". Ai sensi del successivo articolo 36, inoltre, considerati i papabili esiti della *DPIA*, "Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.".

Infine, considerato anche che l'attività di trattamento includeva il monitoraggio regolare e sistematico degli interessati su larga scala, anche nell'ambito di particolari categorie di dati come definiti dall'art. 9 GDPR, ecco che sarebbe stata necessaria anche la nomina di un *Data Protection Officer* (*DPO*)[77], quale responsabile della

[77] L'art. 37 del Regolamento dispone che nel caso in cui il trattamento sia effettuato da un'autorità pubblica ovvero da un soggetto privato la cui attività principale consiste in un monitoraggio sistematico e regolare di soggetti su larga scala o prevede la raccolta massiva di categorie particolari di dati personali e di dati relativi a condanne penali e reati, il titolare del trattamento debba essere assistito da un professionista che abbia una conoscenza ed un' *expertise* specifica della normativa oggetto di analisi. La nomina del DPO non è obbligatoria, ma fortemente consigliate dal legislatore europeo.

protezione dei dati e garante della corretta applicazione delle norme in materia di tutela dei dati personali.

All'esito di questa lunga carrellata, è desumibile che, nel caso in cui la vicenda si fosse perpetrata in periodo di vigenza del GDPR, la piattaforma Facebook sarebbe stata ritenuta non rispettosa del nuovo sistema di *accountability* del titolare previsto dal Capo IV del GDPR.

Una possibile strada onde evitare che si verifichino ancora situazioni in cui il titolare non si senta *accountable* per una diffusione non autorizzata di dati come quella avvenuta nel caso *Cambridge Analytica* potrebbe essere sicuramente quella di estendere il concetto di *data breach* non solo alle violazioni che riguardano strettamente i sistemi di sicurezza del titolare, ma anche ogni qualvolta in cui lo stesso sia a conoscenza di un trattamento illecito di dati personali che egli stesso ha conferito a terzi, soprattutto quando il numero degli interessati coinvolto sia considerevole, facendo leva sull'aspetto di confidenzialità dei dati.

3.2 LA RISOLUZIONE DEL PARLAMENTO EUROPEO N. 2018/2855

Il Parlamento Europeo reagì alla vicenda emanando la "Risoluzione del Parlamento Europeo del 25 ottobre 2018 sull'utilizzo dei dati degli utenti Facebook da parte di *Cambridge Analytica* e l'impatto sulla protezione dei dati (2018/2855(RSP))"[78].

Richiamandosi alle Carte fondamentali dell'Unione Europea, la risoluzione ripercorre la vicenda, stabilendo fin da subito come la reazione di Facebook alla notizia della fuga di dati verso *Cambridge Analytica* non avesse soddisfatto gli standard attesi, così da non poter consentire lo svolgimento di "un'indagine completa e indipendente e di un audit da parte delle autorità interessate né a livello nazionale né a livello europeo"[79].

La risoluzione continua affermando come, pur non potendosi applicare il GDPR, in quanto la vicenda si è verificata prima dell'entrata in vigore dello stesso, ma sottolineando anche l'opinion del 3 ottobre 2017 del gruppo di lavoro "Articolo 29"[80], il quale si era già espresso nel senso che "la profilazione e il processo decisionale

[78] Consultabile al link https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=CELEX:52018IP0433

[79] Considerando G, Risoluzione Parlamento UE 25 ottobre 2018.

[80] Consultabile al link: https://www.studiorobazza.it/wp-content/uploads/2019/10/linee-guida-profilazione_it.pdf

automatizzato possono comportare rischi significativi per i diritti e le libertà dei singoli, che richiedono adeguate misure di salvaguardia"[81]: queste misure, continua la risoluzione, di carattere tecnico e operativo, dovrebbero essere atte a garantire la trasparenza e la non discriminazione in ogni caso attraverso un processo decisionale automatizzato, ma dovrebbero anche essere tali da vietare il calcolo delle probabilità comportamentali individuali. Ancora, tali misure dovrebbero in particolare "permettere alle persone di comprendere e monitorare le decisioni che le riguardano"[82].

Entrando poi nel merito della vicenda, la risoluzione sottolinea anche che "i cittadini dell'Unione devono poter riconoscere facilmente la pubblicità e la pubblicità e la comunicazione online di carattere politico e a pagamento, nonché il partito, la fondazione o l'organizzazione che le promuove"; "insiste sul fatto che la trasparenza dovrebbe comprendere anche informazioni esaustive riguardo ai criteri di scelta del gruppo di destinatari di specifici messaggi pubblicitari politici e alle dimensioni previste di tale gruppo"[83].

In maniera molto netta, il Parlamento Europeo sottolinea come "reputa opportuno vietare la profilazione a fini politici ed elettorali e la profilazione basata su comportamenti online che possano rivelare preferenze politiche, come l'interazione con i contenuti politici, nella misura in cui, conformemente alla legislazione dell'UE in materia di protezione dei dati, tali profilazioni si riferiscono a opinioni politiche o filosofiche, e ritiene che le piattaforme dei media sociali dovrebbero monitorare e informare attivamente le autorità circa eventuali comportamenti di questo tipo; ritiene opportuno vietare, inoltre, la profilazione basata su altri dati, ad esempio di natura socioeconomica o demografica, a fini politici ed elettorali; invita i partiti politici e gli altri attori coinvolti nelle elezioni ad astenersi dall'utilizzare la profilazione a fini politici ed elettorali; invita i partiti politici a essere trasparenti in merito al loro utilizzo dei dati e delle piattaforme online"[84].

[81] Considerando L, Risoluzione Parlamento UE 25 ottobre 2018.

[82] Considerando AE, Risoluzione Parlamento UE 25 ottobre 2018.

[83] Articolo 5, Risoluzione Parlamento UE 25 ottobre 2018.

[84] Articolo 9, Risoluzione Parlamento UE 25 ottobre 2018.

La risoluzione si conclude con la netta presa di posizione contro Facebook e il suo amministratore delegato Mark Zuckerberg: il colosso di Menlo Park avrebbe consapevolmente stipulato un contratto con una terza parte che aveva dichiaratamente affermato di riservarsi il diritto di cedere i dati collezionati tramite lo sviluppo di un app a terzi. Essendo stato Facebook il titolare del trattamento dei dati personali degli utenti, lo stesso è anche giuridicamente responsabile quando stipula un contratto come quello appena descritto con un fornitore terzo (che diventa così responsabile del trattamento ai sensi dell'art. 28 del GDPR). Se tale fornitore viola previsioni in tema di diritto alla protezione dei dati personali, ne sarà giuridicamente responsabile anche il titolare.

Tale utilizzo improprio di dati personali, recita l'articolo 30 della risoluzione, "incide sui diritti fondamentali di miliardi di persone in tutto il mondo".

3.3 IL RUOLO DELLE DATA PROTECTION AUTHORITIES

3.3.1 IL GARANTE ITALIANO PER LA PROTEZIONE DEI DATI PERSONALI

Oltre che degli apparati governativi, lo scandalo *Cambridge Analytica* costituì terreno d'indagine di svariate Autorità nazionali per la protezione dei dati personali. Volendo restare in ambito domestico, il Garante Italiano per la Protezione dei Dati Personali (d'ora in avanti anche solo il "Garante"), all'esito di una approfondita istruttoria, con provvedimento del 14 giugno 2019 sanzionò Facebook con una multa pari ad 1 milione di euro[85] per gli illeciti compiuti.

L'attività istruttoria iniziò in data 21 marzo 2018 con una prima richiesta di chiarimenti, a cui ne sarebbero seguite diverse altre, rivolte a Facebook Italy e Facebook Ireland Limited in merito all'utilizzo di dati di cittadini italiani da parte di *Cambridge Analytica*, con particolare focus sull'attività di profilazione a fini di carattere politico e/o elettorale.

Dalla ricostruzione del garante, tramite il Facebook Login, la piattaforma comunicava all'app *thisisyourdigitallife* le seguenti categorie di dati personali:

- Dati del profilo pubblico, tra cui nome, cognome e genere;

[85] Garante per la Protezione dei Dati personali (2019).

- Data di nascita;
- La geolocalizzazione;
- Le pagine a cui l'utente aveva messo mi piace;
- La lista degli amici, nel caso le impostazioni del profilo prevedessero la pubblicità di tale lista (può anche essere resa visibile solamente all'utente).

Il conferimento dei dati di cui sopra avvenne secondo due modalità distinte nel tempo: la prima versione del form di consenso non prevedeva una granularità nei consensi, ma bensì richiedeva agli utenti di acconsentire obbligatoriamente alla raccolta di tutti i predetti dati, pena l'impossibilità dell'utilizzo dell'app. La seconda versione invece, proposta a partire dall'aprile 2014 (non sembra una coincidenza), permetteva agli utenti di rinunciare alla trasmissione di talune categorie di dati, dando così la possibilità di scegliere quali comunicare all'app e quali no, al netto dei dati rinvenibili dal profilo pubblico, che risultavano obbligatori per l'utilizzo dell'app.

Con le note del 13 giugno, del 15 giugno e del 9 novembre 2019 Facebook assicurò al Garante che, secondo quanto dichiarato dal Dott. Kogan, non sarebbero stati forniti a *Cambridge Analytica* dati di utenti italiani, ma solo americani.

Dall'attività di indagine svolta emerse infatti che 57 italiani utilizzarono l'app *thisisyourdigitallife* su Facebook. Partendo da questi 57 utenti, tuttavia, l'app ebbe accesso, grazie agli strumenti visti in precedenza, ai dati di oltre 214.000 italiani[86].

Parallelamente, l'istruttoria consentì al Garante di verificare anche il funzionamento di due ulteriori strumenti dell'ambiente Facebook, cioè i prodotti "Candidati" e "Messaggio", nell'ambito delle elezioni del 4 marzo 2018 per il rinnovo dei due rami del Parlamento Italiano. Molto brevemente, Candidati permetteva agli elettori di acquisire informazioni su ogni singolo candidato della propria circoscrizione elettorale; Messaggi invece consentiva di condividere il fatto di aver votato, invitando anche a far conoscere le proprie convinzioni sull'importanza di recarsi alle urne.

Il Garante fu costretto ad osservare come dall'istruttoria non emergesse alcuna prova in merito alla cessione a *Cambridge Analytica* di dati di utenti italiani; tuttavia, sebbene non siano stati comunicati all'azienda di Nix, essi furono di certo comunicati all'app *thisisyourdigitalife*. E tale comunicazione fu realizzata contrariamente a quanto

[86] Zorloni (2019).

prescritto dagli articoli 13[87] e 23[88] del Codice in materia di protezione dei dati personali (d.lgs. 30 giugno 2003 n. 196), in quanto, come già evidenziato, il GDPR non era ancora entrato in vigore all'epoca dei fatti.

[87] Oggi abrogato dal D.lgs. 101/2018, l'articolo 13 stabiliva quanto segue: "1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:
a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti di cui all'articolo 7;
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.
2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.
3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.
4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.
5. La disposizione di cui al comma 4 non si applica quando:
a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;
b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;
c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate. dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile. (18) (20)

Ciò in quanto il trasferimento avvenne da un lato sulla base di un'informativa confusa e incompleta, dall'altro senza rispettare i requisiti di validità del consenso, con modalità ritenute illecite dal Garante, non essendo stato possibile esprimerlo in maniera espressa, libera e specifica in riferimento a un trattamento ben individuato. Lo stesso discorso, continua il Garante, può essere fatto per gli amici degli utenti che hanno utilizzato l'app, i quali non prestarono mai alcun tipo di consenso al trattamento dei loro dati.

Allo stesso modo fu ritenuto illeggittimo anche il trattamento di dati personali realizzato da Facebook nell'ambito dei prodotti "Candidati" e "Messaggi", in quanto avvenuto sulla base di un consenso genericamente espresso dall'utente e sulla base di un'informativa di carattere generale.

Nelle conclusioni, il Garante affermò quindi di ritenere illegittima "la comunicazione, tramite l'app *thisisyourdigitalife*, alla società GSR – Global Science Research e ad altri eventuali destinatari, di dati personali di cittadini italiani", oltre che i trattamenti relativi ai prodotti a carattere elettorale di cui sopra.

Sulla base di quanto sopra, con atto n. 10660/125145 del 28 marzo 2019, il Garante condannava Facebook Italy e Facebook Ireland Limited al pagamento in solido di una sanzione amministrativa pari ad euro 52.000,00, concedendo alle società il pagamento in forma ridotta per le seguenti contestazioni:

5-bis. L'informativa di cui al comma 1 non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum, il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f)."

[88] Oggi abrogato dal D.lgs. 101/2018, l'articolo 23 stabiliva quanto segue: "1. Il trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

2. Il consenso può riguardare l'intero trattamento ovvero una o più operazioni dello stesso.

3. Il consenso è validamente prestato solo se è espresso liberamente e specificamente in riferimento ad un trattamento chiaramente individuato, se è documentato per iscritto, e se sono state rese all'interessato le informazioni di cui all'articolo 13.

4. Il consenso è manifestato in forma scritta quando il trattamento riguarda dati sensibili."

"a) la violazione delle disposizioni di cui all'art. 13 del Codice, sanzionata dal successivo art. 161, con riferimento all'inidoneità dell'informativa resa agli utenti Facebook in relazione alla condivisione dei dati dei medesimi con soggetti terzi in occasione dell'utilizzo di specifici prodotti presenti nel social network;
b) la violazione delle disposizioni di cui all'art. 23 del Codice, sanzionata dal successivo art. 162, comma 2-bis, per aver svolto i trattamenti di dati personali di cui sopra senza aver acquisito dagli interessati un consenso libero, specifico e informato;
c) la violazione prevista delle disposizioni di cui all'art. 157 del Codice, sanzionata dal successivo art. 164, per non aver fornito idoneo riscontro ad una richiesta di informazioni ed esibizione di documenti."
Per la contestazione di cui al capo d), invece, e precisamente: "d) la violazione prevista dall'art. 164-bis, comma 2, del Codice, per aver realizzato le condotte sub a) e b) in relazione a banche dati di particolare rilevanza o dimensioni", non potendo intervenire appunto il pagamento in forma ridotta, il procedimento restò aperto.
Facebook Ireland Limited propose opposizione contro il provvedimento del 28 marzo 2019 avanti il Tribunale di Roma[89], mentre Facebook Italy presentò opposizione avanti il Tribunale di Milano[90], contestando tutto quanto sostenuto dal Garante, oltre al vizio di giurisdizione e legge applicabile, secondo il quale Facebook Ireland Limited non potrebbe essere stato oggetto di esame a norma della legge italiana.
Inoltre Facebook sostenne che gli utenti sono perfettamente coscienti che le app di terze parti, come "*Thisisyourdigitalife*", cercano di raccogliere più dati possibili, ivi incluse quelli degli amici degli utenti. E ciò in quanto "nell'ambito del servizio la posizione predefinita è che le informazioni saranno condivise a meno che gli utenti esercitino le opzioni disponibili per modificare tale impostazione". E siccome Facebook è un social network "è nella sua natura che gli utenti si registrino allo scopo di reperire e condividere informazioni con i loro amici e familiari".

[89] Tribunale di Roma, R.G. 21580/2019, Dott.ssa Sangiovanni.

[90] Tribunale di Milano, R.G. 13161/2019, I Sez. Civile, Dott. Di Pilotti.

Il Garante prese a sua volta posizione con l'ordinanza di ingiunzione del 14 giugno 2019[91]. Nella stessa, screditando tutto l'impianto difensivo di Facebook, sia in termini procedurali che nel merito, il Garante prende posizione anche sul capo d) di cui sopra. Uno dei passaggi più interessanti del provvedimento recita quanto segue:

"con riferimento al merito della questione, se da un lato appare sorprendente che Facebook Ireland si qualifichi, contraddicendo le proprie stesse premesse, quale mero intermediario, una sorta di "regolatore del traffico" in uno spazio nel quale interagiscono con differenziati e non sempre adeguati livelli di consapevolezza utenti del social network e autonomi titolari del trattamento, dall'altro risulta del tutto inconferente, in relazione alla normativa sulla protezione dei dati personali, l'assunto che le criticità individuate nell'istruttoria possano essere "neutralizzate" dalla semplice considerazione che "Facebook è un social network la cui missione è dare alle persone il potere di costruire una comunità e di avvicinare il mondo" e che "è carattere intrinseco di un social network - è nella sua natura - che gli utenti si registrino allo scopo di reperire e condividere informazioni con i loro amici e familiari esistenti e con i loro futuri contatti";

- da tale scenario, delineato dalle impostazioni di default degli utenti Facebook con riferimento alla condivisibilità delle informazioni rilevabili dal proprio profilo, è emersa la circostanza, sproporzionata e abnorme, in base alla quale l'utilizzo, da parte di 57 utenti italiani, dell'applicazione *thisisyourdigitallife* mediante la funzione Facebook login ha determinato la condivisione dei dati personali di ben 214.077 ulteriori utenti;
- il dato, di per sé, è idoneo ad evidenziare che, oltre alle criticità rilevate nel Provvedimento, aventi ad oggetto il rilascio dell'informativa e l'acquisizione del consenso da parte di Facebook, gli stessi elementi presentati da Facebook Ireland in sede di memoria difensiva risultano del tutto insufficienti a delineare una prassi operativa, nella gestione delle applicazioni di terzi all'interno del social network, rispettosa delle norme del Codice;".

Chiude le sue osservazioni sostenendo, con riguardo alla contestazione sub d) di cui sopra, che "per la consistenza della complessiva banca di dati formata a seguito della

[91] Consultabile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9121486

comunicazione delle informazioni a *thisisyourdigitallife* la stessa deve qualificarsi "di particolare rilevanza o dimensioni", deve ritenersi pienamente configurata, nei confronti delle medesime società, la violazione di cui all'art. 164-bis, comma 2, del Codice;"[92].

Alla luce di quanto sopra, e tenuto conto dei dati relativi al fatturato complessivo delle società, al numero di utenti iscritti alla piattaforma, ai sensi del comma 4 dell'art. 164 – bis del Codice 196/2003 ingiunse pertanto alle società di pagare in solido la somma di euro 1.000.000,00 a titolo di sanzione amministrativa pecuniaria.

Il 28 giugno 2019, in audizione presso la Commissione Bilancio del Senato, il Presidente del Garante Dott. Antonello Soro commenterà così l'ordinanza, con una vena polemica nei confronti della politica: "Ha ragione il senatore Pesco, non saranno certo le sanzioni da un milione di euro a scongiurare rischi futuri nella dimensione digitale. E infatti in futuro esse saranno irrogate sulla base del nuovo Regolamento europeo in materia di protezione dati (Gdpr), che prevede sanzioni fino al 4% del fatturato globale dell'impresa. Il senatore dovrebbe sapere che su violazioni verificatesi precedentemente al 25 maggio 2018 si applicano le leggi preesistenti e non il Gdpr. E tuttavia non saranno solo le sanzioni pesanti a cambiare il regime della rete: occorrerà una più generale consapevolezza dei diritti delle persone da parte dei big tech, dei governi e degli utenti. Nell'attesa, sarebbe auspicabile che i senatori leggessero almeno un comunicato stampa per intero."[93]

---

[92] Oggi abrogato dal D.lgs. 101/2018, l'articolo 164 - bis stabiliva quanto segue: 1. Se taluna delle violazioni di cui agli articoli 161, 162, 162 ter, 163 e 164 è di minore gravità, avuto altresì riguardo alla natura anche economica o sociale dell'attività svolta, i limiti minimi e massimi stabiliti dai medesimi articoli sono applicati in misura pari a due quinti.

2. In caso di più violazioni di un'unica o di più disposizioni di cui al presente Capo, a eccezione di quelle previste dagli articoli 162, comma 2 e 164, commesse anche in tempi diversi in relazione a banche di dati di particolare rilevanza o dimensioni, si applica la sanzione amministrativa del pagamento di una somma da cinquantamila euro a trecentomila euro. Non è ammesso il pagamento in misura ridotta.

3. In altri casi di maggiore gravità e, in particolare, di maggiore rilevanza del pregiudizio per uno o più interessati, ovvero quando la violazione coinvolge numerosi interessati, i limiti minimo e massimo delle sanzioni di cui al presente Capo sono applicati in misura pari al doppio.

4. Le sanzioni di cui al presente Capo possono essere aumentate fino al quadruplo quando possono risultare inefficaci in ragione delle condizioni economiche del contravventore.

[93] Zorloni (2019); Garante per la Protezione dei dati personali (2019).

3.3.2 L'INFORMATION COMMISIONER'S OFFICE

Primo in ordine di tempo, il 25 ottobre 2018 l'ICO (Information Commissioner's Office), la Data Protection Authority del Regno Unito, impose una sanzione pecuniaria per 500.000,00 sterline (pari a circa 580.000,00 euro) a Facebook, sulla base del Data Protection Act del 1998, la legislazione vigente all'epoca dei fatti prima dell'entrata in vigore del GDPR (e dell'UK GDPR a seguito della Brexit, *ndr*). Come ebbe modo di dire l'Autorità, la somma era la massima prevista dalla legislazione applicabile, ma sarebbe stata ben più alta se fosse stato in vigore il GDPR, a riprova della gravità della condotta di Facebook. Secondo l'ICO, furono almeno 1 milione gli abitanti del Regno Unito i cui dati furono utilizzati impropriamente nell'ambito dello scandalo *Cambridge Analytica*[94].

Così come ebbe a rilevare anche il Garante italiano, la Data Protection Authority del Regno Unito decise di sanzionare Facebook perché riteneva che non avesse protetto i dati degli utenti e non avesse impedito che questi venissero utilizzati in modo scorretto, anche dopo essere venuto a conoscenza delle irregolarità nel dicembre 2015. Testualmente, l'ICO affermò che "Our investigation found that between 2007 and 2014, Facebook processed the personal information of users unfairly by allowing application developers access to their information, without sufficiently clear and informed consent, and allowing access even if users had not downloaded the app, but were simply 'friends' of people who had. Facebook also failed to keep the personal information secure because it failed to make suitable checks on apps and developers using its platform."

Con riferimento invece all'utilizzo dei dati per fini di profilazione in relazione a campagne elettorali (si ricorda che i dati furono utilizzati dal partito Leave.eu nell'ambito del referendum relativo alla cd. Brexit), l'ICO affermò che "Facebook has not been sufficiently transparent to enable users to understand how and why they might be targeted by a political party or campaign. The Facebook ads preference setting allows users to block individual ads, or block ads from a particular advertiser, so they

[94] Sul punto si veda Information Commissioner Office consultabile al link https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

are able to ask not to receive adverts from a particular political party, but it does not allow them to block political advertising based on issues – which is an increasing feature of political advertising, as demonstrated from recent election campaigns. Individuals can opt out of particular interests, and that is likely to reduce the number of ads they receive on political issues, but it will not completely block them. These concerns about transparency lie at the core of our investigation. Whilst these concerns about Facebook's advertising model exist in relation in general terms and its use in the commercial sphere, the concerns are heightened when these tools are used for political campaigning."[95]

Inizialmente Facebook si rifiutò di pagare la somma, proponendo opposizione, salvo poi, circa un anno dopo, nell'ottobre 2019, ritirarlo e decidere di pagare interamente la somma contestatagli, pur non riconoscendo né ammettendo alcuna responsabilità implicita da tale scelta. James Dipple-Johnstone, vice commissario dell'Ico, commentò così la decisione di Facebook: "La protezione delle informazioni personali e della privacy è di fondamentale importanza, non solo per i diritti degli individui, ma anche per la democrazia. Siamo felici di apprendere che Facebook abbia fatto e continuerà a fare passi significativi per aderire ai principi fondamentali della protezione dei dati"[96].

3.3.3 LA FEDERAL TRADE COMMISSION

Anche la Federal Trade Commission ("FTC"), istituita nel 1914 a seguito della Federal Trade Commission Act, il cui compito principale è la promozione della tutela dei consumatori, iniziò la sua attività istruttoria sullo scandalo nel 2018, a seguito della fuga di notizie, arrivando, nel luglio 2019, a sanzionare – a seguito di patteggiamento - Facebook con una multa di 5 miliardi di dollari, la più importante sanzione mai comminata una compagnia per violazione della privacy degli utenti[97].

Rispetto alle sanzioni comminate dalle altre Data Protection Authorities prese in considerazione nei paragrafi precedenti, la FTC non si limitò tuttavia ad una sanzione

[95] Sul punto si veda Information Commissioner Office consultabile al link https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

[96] Garofalo (2019).

[97] Federal Trade Comission (2019).

pecuniaria, ma impose anche tutta una serie di nuove restrizioni sulla gestione della privacy (non solo di Facebook, ma anche di WhatsApp e Instagram), e di modifiche alla struttura aziendale della società.

Nella nota con cui la FTC rese pubblica la notizia, ci tenne a precisare che la sanzione "is the largest ever imposed on any company for violating consumers' privacy and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide. It is one of the largest penalties ever assessed by the U.S. government for any violation.", ancora una volta a riprova della gravità della condotta della società di Menlo Park.

Ma appunto come già evidenziato, il patteggiamento non si limitò alla sanzione pecuniaria, ma impose a Facebook di ristrutturare il suo approccio alla privacy in senso *topdown* e stabilì nuovi meccanismi per garantire l'*accountability* in capo ai dirigenti di Facebook rispetto alle decisioni in tema di protezione dei dati personali, nonché la previsione di una supervisione significativa nelle scelte aziendali sul tema.

Sostanzialmente le violazioni contestate a Facebook sono le stesse già viste in precedenza, aggravate tuttavia dal fatto che la FTC già nel 2012 aveva ordinato a Facebook di prestare più attenzione al modo in cui trattava i dati degli utenti[98]. In particolare, tale ordine "prohibited Facebook from making misrepresentations about the privacy or security of consumers' personal information, and the extent to which it shares personal information, such as names and dates of birth, with third parties. It also required Facebook to maintain a reasonable privacy program that safeguards the privacy and confidentiality of user information. The FTC alleges that Facebook violated the 2012 order by deceiving its users when the company shared the data of users' Facebook friends with third-party app developers, even when those friends had set more restrictive privacy settings."

In sintesi, i punti salienti del patteggiamento furono:

- La creazione di un comitato indipendente del consiglio di amministrazione per supervisionare le decisioni sulla privacy;
- La rimozione del CEO Zuckerberg da tutti i compiti relativi alla protezione dei dati personali;

[98] Raice e Angwin (2012)

- La nomina di *compliance officers* responsabili dei programmi privacy di Facebook;
- Zuckerberg e i *compliance officers* furono obbligati ad inviare, ogni 3 mesi, dichiarazioni certificative che la società è compliant con il programma privacy stabilito nel patteggiamento, e una volta all'anno una dichiarazione di essere globalmente compliant con la normativa di riferimento;
- La creazione di una commissione indipendente con la capacità di valutare l'efficacia del programma privacy di Facebook e individuare eventuali gap;
- Effettuare un assessment di conformità rispetto ad ogni prodotto e ad ogni novità introdotta non solo su Facebook, ma anche su Whatsapp ed Instagram, dando conto di ogni decisione in tema privacy;
- Documentare ogni incidente privacy che coinvolga più di 500 utenti, unitamente ai rimedi che intende mettere in campo al fine di limitarne gli effetti negativi sugli utenti;
- Un alto grado di supervisione sulle app sviluppate da terze parti, ivi inclusa riservarsi la possibilità di eliminare tali app se non compliant alla normativa in tema di privacy.

Joseph Simons, chairman dell'FTC, nella conferenza di stampa in cui annunciava pubblicamente la decisione del patteggiamento si esprimerà così: "This settlement is the result of an exhaustive investigation which concluded that Facebook betrayed the trust of its users and deceive them about their ability to control their personal information"[99].

Il valore aggiunto della decisione dell'FTC fu quindi quello di individuare una nuova e stringente architettura privacy per Facebook, imponendo alla stessa dei cambiamenti a livello di governance societaria secondo due direttrici principali: da un lato, rendere giuridicamente responsabili i vertici societari anche delle scelte in tema di tutela dei dati personali; dall'altro, la necessità di rendere più trasparenti possibili tali scelte, quasi a costo di poter sembrare una interferenza malcelata nella libertà imprenditoriale, tanto cara nel mondo anglosassone: pur tuttavia, è proprio questa sacrificio all'altare

[99] Sul punto si veda lo speech del Presidente della Federal Trade Commission Joseph Simons: Facebook betrayed the trust of its users , in https://www.youtube.com/watch?v=LuXEtOpqzYc

della tutela dei dati che rende la misura della portata dello scandalo e delle conseguenze negative che ha causato nell'opinione pubblica.

3.3.4 L'ATTORNEY GENERAL OF MASSACHUSETTS

Sebbene più complicata da un punto di vista procedurale che non fattuale, anche l'investigazione condotta dall'Attorney General dello Stato del Massachusetts Maura Healey riveste importanza e merita di essere citata, sebbene la vicenda non sia ancora conclusa.

Nel marzo 2018 il procuratore generale aprì un'indagine civile sul potenziale uso improprio dei dati personali dei consumatori da parte degli sviluppatori di app utilizzate nell'ambito della piattaforma Facebook. All'esito dell'istruttoria, nel novembre 2018 il procuratore generale emanò una Civil Investigate Demand ("CID") ai sensi della sezione 6 della General Laws dello stato del Massachusetts, Parte I, Title XV, Chapter 93A[100] chiedendo alla società, tra le altre cose, l'identità e le informazioni fattuali su app e sviluppatori che potrebbero aver utilizzato in modo improprio i dati dei consumatori, e le comunicazioni interne di Facebook riguardanti tali app e sviluppatori. In risposta, Facebook affermò di non poter condividere tali informazioni con l'ufficio del procuratore, in quanto coperte da segreto professionale. Secondo Facebook, infatti, le stesse informazioni erano emerse nell'ambito di un'indagine interna (cd. App Developer Investigation – ADI) commissionata ad alcuni avvocati esterni all'organizzazione, e pertanto coperte da segreto.

Nell'appello presentato dall'Attorney General avanti alla Corte Suprema dello Stato del Massachusetts in data 30/09/2020[101], si legge come l'obiettivo del procuratore fosse il seguente: "The Attorney General sought to learn whether Facebook enforced its policies restricting third-party app developers from selling or disclosing Facebook user data, and to learn whether other app developers misused Facebook user data in a manner that might violate the Consumer Protection Law".

[100] Per il testo integrale dell'articolo si veda
https://malegislature.gov/laws/generallaws/parti/titlexv/chapter93a/section6

[101] Per il testo integrale si veda
https://archive.epic.org/Appellee%20Commonwealth%20Redacted%20Brief.pdf

Inizialmente il Procuratore depositò il ricorso presso la Corte Suprema del Suffolk, il 5 agosto 2019[102], alla quale Facebook si oppose attraverso le contestazioni di carattere procedurale viste poc'anzi. Tuttavia, in data 16 gennaio 2020, la Corte Suprema ordinò a Facebook l'esibizione della documentazione. La società fece allora appello alla Corte Suprema dello Stato, in data 4 febbraio 2020.

Sulla falsa riga di quanto evidenziato sopra per l'FTC, nella sua memoria difensiva avanti alla Corte Suprema dello Stato anche il procuratore del Massachusetts evidenziò come, sin dal 2012, Facebook "made promises and representations to users regarding what Facebook permitted and prohibited app developers from doing with user data. For example, in late 2012 Facebook told users that "[y]our privacy is very important to us," and assured users that, if one of their Friends installed an app, and that app took the user's data, Facebook only permitted the developer to use it "in connection with the person [i.e., Friend] that gave the permission, and no one else." Continuava dicendo che "Facebook expressly prohibited developers from selling user data to third parties, allowing them to "only request the data you need to operate your application.", salvo poi tradire la fiducia degli utenti: "Facebook failed to detect or prevent a large-scale misuse of Facebook user data by Professor Alexander Kogan, the developer of an app called "*thisisyourdigitallife*". In merito poi alla cession dei dati, si dice che "Having obtained this trove of personal data, Kogan then sold some or all of it, in direct violation of Facebook's policies prohibiting the sale or transfer of Facebook user data, to a data analytics and advertising firm, *Cambridge Analytica* and other affiliated entities. According to public reports, *Cambridge Analytica* used this data without consumers' knowledge or consent to target Facebook users with political advertising during the 2016 Presidential election."

La memoria continua poi elencando le misure di contenimento messe in atto da Facebook successivamente alla pubblicazione dello scandalo, le audizioni presso il Congresso degli Stati Uniti di Mark Zuckerberg, nonché gli aggiornamenti regolari sull'investigazione interna condotta dalla società sulle app dello store in merito alla loro conformità con le policy del social.

[102] Per il testo integrale si veda https://epic.org/wp-content/uploads/amicus/massachusetts/facebook/AG-v-Facebook-SJC-Opinion.pdf

L'investigazione portata avanti sin dal marzo 2018 dal procuratore generale però non si limitava all'app *thisisyourdigitalife*, ma andava oltre, e qui si può riconoscere il valore aggiunto dell'azione legale: "Among other things, the investigation sought to determine whether any other apps (in addition to Kogan's App) misused Facebook user data, the extent of misuse, and to assess whether Facebook acted consistently with its commitments to users in its policies". Una sorta di azione preentiva onde evitare ulteriori casi *Cambridge Analytica*.

E fu proprio questo il motivo di doglianza da parte di Facebook: secondo la società infatti tali informazioni (quelle cioè risultanti dall'investigazione interna alla società) non potevano essere rese note al procuratore in quanto anticipatorie rispetto ad una possibile *litigation*. La Corte del Suffolk tuttavia "concluded that the information from the ADI called for in the Contested Requests was not "prepared in anticipation of litigation" because it "would have been created 'irrespective of the prospect of litigation.'" e che "that the ADI is just another iteration of" Facebook's "normal business operations" to review Platform apps for policy violations".

Pur rivestendo la vicenda giudiziaria un carattere più procedurale che fattuale, si evince comunque come anche in questo caso l'occhio della giustizia sia stato ben focalizzato nel cercare di ottenere più informazioni possibili in merito allo scandalo, al fine di poter in futuro evitare altre situazioni che possano avere impatti negativi sugli utenti delle piattaforme social. Si ritiene che, all'esito della vicenda giudiziale, se verrà concesso al procuratore di avere accesso alla documentazione attualmente negata, potrebbe aprirsi un nuovo filone di indagini e, in ultima istanza, ad un' ulteriore sanzione di importante portata nei confronti di Facebook.

***

All'esito di questa carrellata, che avrebbe potuto accogliere anche esempi di altre Data Protection Authorities che si attivarono all'alba dello scandalo[103], si evince facilmente come il ruolo delle Autorità Garanti per la protezione dei dati personali sia stato

[103] Si veda, ex multis, l'investigazione portata avanti dall'Office of the Privacy Commissioner of Canada (https://www.priv.gc.ca/en/opc-news/speeches/2019/s_d_20190425/) e quella portata avanti dall'Irish Data Protection Commission, "Ireland's Data Protection Commissioner "following up" with Facebook over Cambridge Analytica", in The Journal, https://www.thejournal.ie/facebook-investigations-data-3913631-Mar2018/

fondamentale sin dalle prime battute e dalle prime fughe di notizie in merito allo scandalo. Senza il loro contributo, probabilmente anche la risposta di Facebook, in termini di investigazioni interne, nonché di rimedi da mettere in atto al fine di prevenire il verificarsi di nuove situazioni simili, sarebbe stata più tenue, financo nulla, se l'esperienza della vicenda insegna qualcosa.

Sebbene a distanza di anni, in data 23/05/2022 l'Attorney General del District of Columbia Karl A. Racine ha depositato il suo atto di citazione contro Mark Zuckerberg in qualità di persona fisica per il suo ruolo nell'ambito della vicenda *Cambridge Analytica*, a riprova che i contorni giudiziari del caso sono ancora ben lontani da una conclusione.

"Sorry is not enough"[104] è la dichiarazioni di intenti, una promessa fatta ai cittadini di tutto il mondo l'11 aprile 2018 dal Working Party Article 29, il gruppo che, prima dell'entrata in vigore del GDPR, riuniva tutte le Autorità Garanti Europee, ora riunite nell'European Data Protection Board (EDPB).

Andrea Jelinek, Presidente del Working Party, annunciando la creazione di una commissione specializzata sui social media, disse: "We are at the start of a new era of data protection. The protection of individuals against unlawful use of their personal data on social media platforms will be one of our key priorities. A multi-billion dollar social media platform saying it is sorry simply is not enough. While *Cambridge Analytica* and Facebook are on top of everyone's mind we aim to cast our net wider and think longterm. This is why we are creating a Social Media Working Group. What we are seeing today is most likely only one instance of the much wider spread practice of harvesting personal data from social media for economic or political reasons. WP29 is fully aware, however, that the issue is broader and concerns other actors, such as app developers and data brokers. The work of this Social Media Working Group will continue after the establishment of the European Data Protection Board. The EDPB will have a wide range of competences in order to ensure the consistency of the application of the GDPR".

[104] Slogan scelto dal Social Meda Working Group dell'Article 29 Working Party durante la conferenza stampa di presentazione dell'11 aprile 2018, il cui testo è rinvenibile al seguente link https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf

Concludendo, le Autorità Garanti hanno dimostrato di essere delle watchdogs efficienti e attente nell'ambito della difesa dei dati personali dei cittadini, a riprova di quanto essi siano preziosi e da tutelare nella misura in cui una società si professi libera e democratica.

CAPITOLO 4 – SVILUPPI FUTURI

4.1 INTELLIGENZA ARTIFICIALE E GDPR

Da quanto descritto nei capitoli precedenti, sembra quasi affacciarsi uno scontro epocale tra la tutela di un diritto fondamentale, come quello alla tutela dei dati personali degli individui, e le esigenze dei colossi dei sistemi informatici (siano essi Facebook, Google, Twitter…) che fanno di quei dati personali la benzina delle loro potentissime macchine informatiche, le quali fagocitano dati alla velocità della luce per rielaborarli e tradurli sotto forma di guadagno economico.

E nulla sarebbe possibile senza i continui progressi della tecnologia nel campo dell'intelligenza artificiale e del machine learning. L'intelligenza artificiale (AI) è l'abilità di una macchina di mostrare capacità umane quali il ragionamento, l'apprendimento, la pianificazione e la creatività. L'intelligenza artificiale permette ai sistemi di capire il proprio ambiente, mettersi in relazione con quello che percepisce e risolvere problemi, e agire verso un obiettivo specifico. Il computer riceve i dati (già preparati o raccolti tramite sensori, come una videocamera), li processa e risponde. I sistemi di AI sono capaci di adattare il proprio comportamento analizzando gli effetti delle azioni precedenti e lavorando in autonomia[105].

Ma questo tipo di intelligenza, che ha ricadute pratiche nella nostra vita quotidiana, come si concilia con le esigenze del diritto alla tutela dei dati personali degli individui? Il diritto è effettivamente in grado di stare al passo con la velocità con cui questo tipo di tecnologia evolve, che rappresenta talvolta una "risorsa" e talvolta un "problema"?[106]E l'AI è in grado di venire incontro a quelle categorie per certi versi immutabili (si pensi ai dettami costituzionali, per esempio) proprie del diritto?

Tra le molte dichiarazioni che cercano di indicare una via per un amichevole rapporto tra diritto e AI si possono citare la Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica[107] e il documento "Getting the future right – Artificial intelligence and

[105] (Parlamento Europeo 2020).

[106] (Nicotra 2018).

[107] Per il testo completo, cfr. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_IT.html

fundamental rights", pubblicato il 14 dicembre 2020 dalla European Union Agency for fundamental rights, a riprova di come intelligenza artificiale e diritti fondamentali della persona siano ormai indissolubilmente legati[108]. Quest'ultimo documento afferma come "Data protection is critical in the development and use of AI. Article 8 (1) of the Charter and Article 16 (1) of the TFEU provide that everyone has the right to the protection of their personal data. […] The interviewees indicated that most of the AI systems they employ use personal data, meaning data protection is affected in many different ways. However, a few applications – according to the interviewees – do not use personal data, or only use anonymised data, and hence data protection law would not apply. If personal data are used, all data protection related principles and provisions apply." Il document dedica anche un paragrafo specifico proprio al *targeted advertising*, sostenendo che "When considering fundamental rights safeguards in relation to targeted advertising and the underlying mechanisms regarding profiling in particular, the EU legal framework on privacy and data protection provides the most relevant fundamental rights provisions. The protection of privacy and personal data holds a status that takes precedence over economic benefits. Hence, rules on processing of (special categories of) personal data are relevant for companies operating in the area of or applying targeted advertising in that they place companies under certain obligations."

Addirittura il documento sostiene come, a fronte di una lacuna legislativa in tema di regolazione dell'AI, la normativa a tutela dei dati personali sia ritenuta l'unica in grado di recare, attualmente, le tutele minime necessarie.

Il documento, così come l'altro sopra richiamato, cercano di stressare l'importanza di un'AI che si possa definire non dato – centrica, ma bensì umano – centrica, in quanto connotata da finalità etiche e dalla conformità ai valori fondamentali della società civile, ivi inclusi, per quanto qui attiene, il rispetto della dignità umana e dei diritti fondamentali dell'invidividuo, alla libertà di autodeterminazione. Tali valori si traducono anche nella possibilità, per un individuo, di essere libero di scegliere quando conferire o meno i propri dati in ritorno di un servizio fornito a tutti gli effetti da una macchina.

[108] Per il testo completo, cfr. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf

Tali desiderata sono confluiti nella proposta di Regolamento quadro presentata dalla Commissione Europea il 21 aprile 2021 intitolato "the Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts"[109].

In termini giuridici, si ritiene che lo sviluppo dell'AI abbia bisogno di essere accompagnato e guidato da un pensiero di tipo costituzionale, per definizione orientato alla tutela dei diritti fondamentali dei cittadini, senza pensare che il concetto principe del trattamento dei dati personali, il consenso, possa essere l'unico baluardo a difesa di trattamenti illegittimi. O che un consenso più o meno liberamente manifestato possa risolvere qualsiasi dubbio etico sul tema. Si vedrà nei prossimi paragrafi come si stia probabilmente assistendo – inermi, per lo più – alla crisi del modello del consenso consapevole.

Il caso *Cambridge Analytica* ci dice che le garanzie costituzionali che si estrinsecano anche nella tutela dei dati personali possono essere minate anche senza che noi ce ne accorgiamo: si pensi alla libertà di autodeterminazione, alla libertà politiche, alla libertà di pensiero, al principo di eguaglianza.

4.2 CONSENSO CONSAPEVOLE

Come descritto nei capitoli precedenti, una delle falle più grandi relative alla vicenda *Cambridge Analytica* fu rappresentato dalla condivisione da parte della piattaforma di informazioni personali raccolte direttamente dai profili pubblici degli utenti dell'app, ma anche degli amici di questi. E di certo, come illustrato, né le condizioni d'uso della piattaforma né tanto meno l'informativa privacy rilasciata propendevano a favore di una scelta consapevole da parte dell'utente. La sezione 2 della "Dichiarazione dei diritti e delle responsabilità" della piattaforma prevedeva infatti che, con riferimento ai contenuti pubblicati dall'utente, lo stesso riconosceva a Facebook una "licenza non esclusiva, trasferibile, che [poteva] essere concessa come sottolicenza, libera da royalty e valida in tutto il mondo, che [consentiva] l'utilizzo dei contenuti pubblicati su Facebook o in connessione con Facebook".

[109] Per il testo completo, cfr. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

La sezione 9 invece rincavarava la dose, specificando che l'utente accettava anche di concedere "l'autorizzazione a utilizzare il […] 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 nessuna compensazione. Se l'utente ha selezionato un pubblico specifico per i propri contenuti o informazioni, rispetteremo la sua scelta al momento dell'utilizzo." Secondo la piattaforma la trasmissione di tali dati sarebbe stata possibile solo previo rilascio del consenso esplicito dell'utente, salvo non indicare alcunchè in merito alle modalità di rilascio di tale consenso.

Ma appunto come sopra descritto, la condivisione non si limitava alla piattaforma Facebook, ma si spingeva ad applicazioni e siti web sviluppati da terze parti, proprio come il caso di thisisyourdigitalife e *Cambridge Analytica*: un panorama di condivisioni che non può che sfuggire totalmente al controllo dell'utente (e anche della piattaforma, come si è visto). Anche in questo senso le condizioni d'uso di Facebook risultavano estremamente carenti e fuorvianti, permettendo di fatto a soggetti terzi di arricchirsi di un numero enorme di dati personali di utenti sparsi in tutto il mondo, che cedevano i propri dati a nuovi titolari. Tale falla ha rappresentato e rappresenta tuttora un momento inaccettabile per una società democratica, anche nel bel mezzo di una rivoluzione tecnologica – digitale.

Sebbene alcuni degli impatti negativi verificatisi avrebbero infatti avuto sicuramente vita più dura in costanza di vigenza del GDPR, è altresì vero che, basandosi lo stesso sul concetto di consenso consapevole, probabilmente la catena di condivisione delle informazioni personali, proprio perché basata, comunque, su una sorta di consenso rilasciato dall'utente, sarebbe stata comunque molto consolidata, mettendo in dubbio la piena efficacia del Regolamento. L'utente, una volta rilasciato il consenso, avrebbe perso comunque il controllo sui suoi dati personali, in una spirale turbolenta ed inditerminata di continue utilizzazioni per fini prettamente economici.

Sulla crisi del modello del consenso consapevole che non può più assurgere a cavaliere della legittimità dei trattamenti di dati personali, è da sottolineare il lavoro di ricerca scientifica del Professor Fred Cate dell'Università dell'Indiana[110].

Nello speech tenuto nell'ambito della conferenza TEDx il 16 gennaio 2020[111], egli dirà che "We are sorrounded by data that seems to be falling out of control: data being lost by corporations, data being stolen from government agencies, data that has been collected about us, billions of bytes a day that seems hopelessly out of control and […] it seems to be getting worse." Analizzando la sfida tra dati personali e privacy, il Professor Cate sottolinea come la stragrande maggioranza dei dati presenti online sono dati che noi stessi volontariamente rilasciamo (messaggi, foto, video, audio…), con tremendi impatti sulla nostra privacy. Talvolta i dati sono perfino creati, non esistendo "naturalmente": sono un buon pagatore? Qual è il mio merito creditizio? E via dicendo.

Tra la moltitudine di cause individuate da Cate, egli porta l'attenzione proprio sul ruolo controverso del consenso. Partendo dalla definizione di privacy resa dalla Corte Suprema degli Stati Uniti nel 1989 nel caso Department of Justice versus Reporters Committee for Freedom of the Press ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person")[112], Cate sostiene come sia *impractical* e *undesirable* focalizzarsi sul consenso come strumento di tutela dei dati. Ciò per le seguenti ragioni:

- La complessità delle informative privacy e cookie: con una vena di sarcasmo, sottolinea come l'informativa di Paypal, gigante delle transazioni online, sia più lunga dell'Amleto di Shakespear; come la privacy policy di iTunes (servizio di matrice Apple) sia più lunga del MacBeth; e che, secondo uno studio del 2008[113], per leggere le informative dei 45 siti più importanti del web ci vorrebbero 30 giorni lavorativi full time;
- In secondo luogo, tali informative sarebbero per lo più inaccessibili, soprattutto da dispositivi mobili, o in situazioni di gruppo (ad esempio nel caso di

[110] Per ulteriori informazioni, si veda Cate e Mayer-Schönberger (2013).

[111] Per la visione del video si rimanda al link: https://www.youtube.com/watch?v=2iPDpV8ojHA (ultima consultazione 21 aprile 2022).

[112] Cate e Cate (2012).

[113] McDonald e Cranor (2008-2009).

registrazioni di video proprio durante speech, o nell'ambito di foto scattate lungo la strada);

- In terzo luogo, afferma che il consenso si sarebbe dimostrato incredibilmente inefficace principalmente perché gli utenti lo ignorano, citando una dichiarazione del 2009 di John Leibowitz, ex Presidente della FTC, durante una sessione delle Roundtable on Exploring Privacy, secondo il quale "We all agree that consumers don't read privacy policies" e una dichiarazione di Timothy J. Muris, anch'egli ex Presidente dalla FTC, il quale, durante una conferenza stampa, il 4 ottobre 2001 disse che "Acres of trees died to produce a blizzard of barely comprehensible privacy notices". In questo modo il consenso avrebbe una funzione puramente illusoria: in questo senso richiama ad esempio il consenso rilasciato al momento dell'aggiornamento del software del cellulare. Non procedere con l'aggiornamento significa incappare in una serie di impatti negativi (durata batteria peggiore, app che non si possono più installare, malfunzionamenti vari) che rendono di fatto impossibile non rilasciare il consenso, a fronte delle innumerevoli pagine di condizioni generali d'uso che nessuno di noi si sognerebbe mai di leggere, se non per mera curiosità tecnologica, forse.
- Quello che generalmente viene definito un diritto a favore dell'individuo, quasi un diritto umano dice, molto spesso in verità si tramuta invece in un onere in capo all'utente: il rilascio del consenso ha infatti la funzione preminente di spostare la responsabilità giuridica da chi propone il trattamento dei dati (o per meglio dire dal titolare del trattamento dei dati, cioè colui che determina i mezzi e le finalità del trattamento) all'interessato, cioè colui ai quali i dati personali si riferiscono. Una sorta di manleva si potrebbe dire. Ecco che quello che sembra un diritto, a detta del Professor Cate si trasforma in un onere, una assunzione totale di responsabilità da parte dell'utente rispetto all'utilizzo dei suoi dati al quale ha acconsentito;
- Ci sono dei trattamenti per cui il consenso perde la sua funzione di protezione: si pensi alle finalità di ricerca, oppure alle finalità di antifrode, o di anticrimine, per le quali la società vuole essere costantemente informata, senza necessità di chiedere il consenso agli interessati;

- L'ultimo motivo, secondo Cate, è che l'utente esprime un consenso, che dovrebbe tutelare la privacy dello stesso, a far sì che quella stessa privacy, che quella stessa protezione venga meno.

Cate non si limita tuttavia ad evidenziare le criticità legate al consenso, ma indica una serie di misure che sarebbe necessario attuare per riportare l'individuo in controllo dei suoi dati: restituire credibilità ed efficienza al consenso *right here* e *right now*, e rendere i titolari del trattamento completamente responsabili (utilizza la parola *steward*) delle conseguenze negative che potrebbero derivare dall'utilizzo dei dati, così che possano agire nel miglior interesse dei clienti – utenti, proprio come un avvocato, un dottore, un banchiere, ripristinando quel rapporto di fiducia che deve stare necessariamente alla base di tutto.

4.3 CULTURA, DEMOCRAZIA, LIBERTÀ

È evidente che quella dell'efficace tutela dei dati personali è una strada ancora molto lunga, più in salita che in discesa, costellata di ostacoli sempre nuovi da studiare e monitorare, senza cadere nel paradosso di rifuggere l'evoluzione tecnologica e digitale, ma piuttosto cercando di trovare un minimo comune denominatore che possa portare benefici agli utenti, agli individui. In questo modo il legislatore non sarà mai staccato dalla realtà e sarà in grado di prevenire e scongiurare i rischi. Com'è stato giustamente evidenziato da F. Pizzetti, "è necessario accettare la sfida e difendere le ragioni delle regole, che poi sono anche quelle della libertà e della democrazia"[114].

Al giorno d'oggi la democrazia per come la conosciamo è minacciata da una moltitudine di fattori. Ma quello che è successo nel caso *Cambridge Analytica*, nell'ambito delle campagne elettorali sopra menzionate, scuote la democrazia proprio nelle sue fondamenta: nel momento in cui i cittadini hanno il diritto (e il dovere) di scegliere i loro rappresentanti liberamente. Perché in democrazia il potere è sì esercitato dal popolo, ma attraverso i suoi rappresentanti, che elegge con elezioni che devono essere totalmente libere.

[114] Pizzetti (2006).

Ma se invece quel popolo viene influenzato, attraverso l'improprio utilizzo dei dati delle singole persone che compongono quel popolo, allora ecco che il concetto di democrazia si svuota di tutto il suo significato.

In una sorta di *j'accuse*, Christopher Wiley, ex dipendente di *Cambridge Analytica*, nel suo libro autobiografico "Il mercato del consenso - Come ho creato e poi distrutto *Cambridge Analytica*" a pagina 85 e ss. dirà quanto segue: "Se, usando informazioni personali, possiamo misurare o desumere determinati tratti negli individui, e poi impiegare quegli stessi tratti per descrivere una cultura, allora possiamo tracciare una metrica approssimativa di quest'ultima, una sua curva di distribuzione. In una simile cornice, noi proponevamo l'utilizzo dei dati ricavati da social media, clickstream o rivenditori specializzati per identificare, per esempio, gli italiani più estroversi, analizzando i loro schemi comportamentali di consumatori e utenti. […] In altre parole, il cambiamento culturale può essere definito come una spintarella verso l'alto o verso il basso su una curva di distribuzione. I dati ci consentivano di disaggregare una cultura in individui, che diventavano unità discrete e rimodulabili di una data società".

Sembra quasi sentire parlare un professore di fisica di un problema di fisica quantistica, o uno statistico.

"Ora, per capire in che modo questa analisi possa trasformarsi in una campagna vera e propria, pensate alla sanità pubblica. […] Ecco, lo stesso tipo di strategia si può adottare per modificare una cultura. Per aumentare la resistenza di una popolazione alle derive estremistiche, per esempio, vanno innanzittuto identificate le persone più suscettibili a quel tipo "messaggi armati": si determinano i tratti che le rendono vulnerabili a una narrazione contagiosa e le si sottopone a un trattamento di contronarrazione, nel tentativo di cambiarne il comportamento."

Quello che qui è messo in discussione è l'aspirazione, il diritto fondamentale di ogni individuo all'autodeterminazione non tanto dei popoli, principio caro al diritto internazionale, ma di sé stesso in prima persona, come essere in grado di formarsi una coscienza autonoma e di portare avanti le idee in cui crede. Diritto che il legislatore europeo sembra più volte aver compreso e proposto di difendere, e questo rappresenta una grande fonte di ricchezza per i cittadini europei. Ma questa autodeterminazione

dev'essere libera da qualsiasi tipo di influenza. Parlando della tecnica del *priming*[115], Wiley dirà: "Ed è così, in sintesi, che si trasformano i dati in armi: si scopre quali informazioni mettere in primo piano per influenzare lo stato d'animo di una persona, ciò in cui crede e il modo in cui si comporta."

La privacy non è un riflesso condizionato, come il bere acqua o la respirazione. Il motivo per cui essa riveste una tale importanza è che il comportamento degli individui cambia drasticamente quando sanno di essere osservati, monitorati. Le opzioni comportamentali si riducono in maniera evidente, e diversi studi psicologici[116] dimostrano che quando un individuo è osservato, tende ad essere più conformista e remissivo. Ed ecco che quindi in questo contesto, l'individuo prenderà delle decisioni che non saranno frutto della sua coscienza, ma la risposta alle aspettative degli altri e in generale della società.

Questa filosofia di pensiero fu studiata approfonditamente dal filoso Jeremy Bentham nel diciottesimo secolo, il quale prospettò, nel 1791, la creazione di una struttura architettonica chiamata panottico, previsto inizialmente per le carceri, la cui prima caratteristica consisteva nella costruzione di una torre al centro della prigione, in cui il governatore della prigione potesse controllare in ogni momento tutti i carcerati contemporaneamente, mentre al contrario questi non erano in grado di vedere nel panottico. Quindi non potevano sapere se in quel dato momento fossero stati controllati o meno. In questo modo, i prigioneri pensavano di essere monitorati in ogni momento, inducendo quindi ordine e disciplina al massimo livello. Il filosofo francese Michel Foucault[117], su questa scorta, intuì che tale modello di controllo poteva essere utilizzato anche dalle istituzioni che volevano controllare il comportamento umano: in questo modo le moderne società occidentali non avevano più bisogno del re tiranno, ma piuttosto di un sistema di controllo delle masse in grado di creare degli stili

---

[115] Il *Priming* è una forma di riconoscimento mnemonico non cosciente che consente a uno stimolo, al quale si è stati esposti una prima volta, di essere identificato durante le successive esposizioni senza averne consapevolezza. Questa capacità evolutiva dell'essere umano provoca notevoli effetti sull'interpretazione e sulla valutazione dell'informazione.

Per saperne di più, Fiore (2016).

[116] *Ex multis*, si veda Allport (1919); Goffman et al. (2006).

[117] Michel Foucault (15 ottobre 1926–25 giugno 1984) fu un filosofo francese noto per l'analisi dei rapporti di potere. Per i suoi studi sul panottico, si veda Surveiller et punir: Naissance de la prison, 1975.

comportamentali, annullando la libertà di agire dell'individuo[118]. Ecco perché quando si permette l'esistenza di una società in cui l'individuo è soggetto a costante monitoraggio (e non solo da parte delle autorità governative, anzi), automaticamente si indebolisce gravemente l'essenza della libertà umana[119].

Il problema quindi, lo si capisce, non si limita a Facebook o a *Cambridge Analytica*, ma permea tutto il sistema in cui l'individuo estrinseca la sua personalità, permea la società[120].

Brittany Kaiser, altra ex dipendente pentita di *Cambridge Analytica*, nel suo libro "La dittatura dei dati", dirà: "Il problema non era soltanto Cambridge; il problema erano i big data. Era Facebook, che aveva permesso alle aziende come Cambridge di acquisire i dati di miliardi di persone, e il meccanismo che consentiva a queste aziende di rivendere i dati raccolti al miglior offerente. Tutto questo andava avanti fin da quando le nostre vite erano diventate digitali, senza che ce ne accorgessimo, e senza la supervisione del governo. E quelle poche leggi che proteggevano i nostri dati non avevano alcun potere."

Un cittadino europeo, i cui dati personali sono tutelati da una normativa pervasiva come quella del GDPR, forse leggerebbe queste parole con meno trasporto, rispetto ad un cittadino americano i cui dati personali possono essere strumentalizzati con maggiore libertà[121].

Continua con una dichiarazione di intenti: "I big data, Trump e Facebook hanno violato la nostra democrazia. Ma ora ci viene offerta un'opportunità: possiamo raccogliere i pezzi e riunirli nel segno di una comunità globale etica, giusta e stabile, che possa impegnarsi per un cambiamento positivo, oppure lasciare quei pezzi a terra, aspettando che sia troppo tardi per poterli riunire. […] Infine, c'è ancora un flusso gigantesco di dati non regolati da norme e non tracciabili. Una volta là fuori, non possono più tornare indietro. Dobbiamo esigere dei cambiamenti, dobbiamento esigere che ci vengano riconosciuti i diritti sui nostri dati, prima che il sistema crolli del tutto. Come mi ha detto una volta Paul Hilder: "Sono un'ottimista, credo che le cose rotte si possano

[118] Demichelis (2019).

[119] Greenwald (2014).

[120] Demichelis (2019).

[121] Si pensi, ad esempio, alla normativa FISA 702.

aggiustare". Vorrei che fosse questo l'atteggiamento dei nostri futuri politici. Vorrei che ci dessero di nuovo qualcosa in cui sperare, qualcosa che ci restituisca potere. Vanno cambiate le leggi, e bisogna investire in soluzioni tecnologiche che possano permetterci di applicare queste nuove norme".
Parole da sottoscrivere, per un futuro più umano – centrico, in un mondo di dati.

4.4 BUONI PROPOSITI

Il tema della tutela dei dati personali, sebbene affondi le sue radici nell'essenza dell'individualità umana, è una tema abbastanza recente, di cui solo le ultime generazioni si sono interessate. Dovremmo guardare a chi sfrutta illeggittimamente i nostri dati alla stessa maniera – quasi inquisitoria – con cui guardiamo chi sfrutta illeggittimamente la terra, gli animali, l'acqua.
La vera domanda che ci si pone è: come può il singolo individuo riprendere il controllo della sua vita digitale, dei suoi dati personali, come può ad esempio il singolo cittadino europeo trarre il massimo beneficio dalla nuova regolamentazione in tema di dati personali e di intelligenza artificiale?
Ad esempio, ed in primo luogo, attraverso la (*i*) consapevolezza digitale: una sorta di alfabetizzazione che permetta al cittadino di comprendere meglio l'ambiente digitale, imparando a diffidare delle fake news e di notizie convenienti, valutando le fonti, cercando la trasparenza e non solo il risparmio economico nell'ambito degli acquisti online, come vengono acquisiti i dati, dove vengono trasferiti, come vengono utilizzati e per che finalità[122]. Perché "If this is the age of information, then privacy is the issue of our times"[123]. È necessario ridurre al minimo l'asimetria informativa tra chi i dati li comunica e chi i dati li detiene e li sfrutta[124].
(*ii*) Seguendo da vicino tutte le iniziative legislative che riguardano i dati personali: sono in via di definizione il Regolamento sull'Intelligenza Artificiale di cui si è parlato sopra, nonché il Regolamento E – Privacy, che affiancherà il GDPR e servirà a regolamentare tutte le comunicazioni online, ma che non sarà probabilmente approvato

[122] In tema di alfabetizzazione digitale, si rimanda al sito web https://www.ownyourdata.eu/en/ (ultima consultazione 21 aprile 2022).

[123] Acquisti, Brandimarte e Loewenstein (2015).

[124] Acquisti, Brandimarte e Loewenstein (2015).

prima del 2023. L'iniziativa legislativa sarà fondamentale per bilanciare gli interessi dei cittadini contro lo strapotere delle aziende commerciali che fanno dei dati la loro linfa vitale.

(*iii*) Sostenendo ed informarsi in merito all'attività delle Data Protection Authorities – ed in particolare del Garante Italiano per la protezione dei dati personali – che hanno dimostrato di essere delle autorità realmente interessate alla tutela dei cittadini e della loro ricchezza digitale. In questo senso, sarà compito di queste autorità specializzate perseguire quei soggetti che operano in maniera illecita nel mercato digitale con riferimento ai dati personali degli utenti, facendo sì che le sanzioni siano non solo efficaci, ma anche deterrenti rispetto ai comportamenti futuri.

(*iv*) Tutelando di più – *rectius*, meglio – la nostra vita privata. Non c'è dubbio che l'uomo sia un essere sociale che sente la necessità di condividere con gli altri alcune informazioni per sentirsi interconnesso. Si pensi ad esempio alla teoria della penetrazione sociale[125], secondo cui le relazioni iniziano e si approfondiscono prima di tutto attraverso la rivelazione di sé. Ma questo non può avvenire se non con un livello di privacy molto basso, per non dire nullo. E quindi ecco che i social media forniscono un terreno di pubblicità incredibilmente efficacia per l'estrinsecazione della persona, ma senza dimenticare che il prezzo da pagare può essere molto alto, e che una volta messi in vetrina gli aspetti più o meno intimi della personalità, sarà molto difficile poterli controllare, se un giorno si decidesse di spegnere le luci di quella vetrina.

[125] Altman e Taylor (1973).

CONCLUSIONI

Martedì 12 aprile 2022 Tim Cook, CEO di Apple, al Global Privacy Summit 2022 di IAPP, dirà queste parole: "Privacy is the most essential battle of our time"[126].

A distanza di pochi giorni, invece, rimbalza sule fonti di informazioni che Facebook sarebbe nel bel mezzo di uno "tsunami" della privacy, che non gli permette di avere il controllo sui dati che transitano sulla piattaforma[127]. In un documento fatto circolare in rete e redatto da uno degli ingegneri del dipartimento Ad e Business Product di Facebook, si legge infatti che "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, this is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation".

Ma allora che lezione abbiamo imparato dal caso *Cambridge Analytica*, se ne abbiamo imparata una?

I cittadini, innanzitutto, devono riconoscere che i loro dati hanno un valore. Economico, morale, identitario. I cittadini, specialmente quelli europei, dovrebbero sfruttare di più e meglio i diritti che sono loro garantiti dalla legislazione europea e nazionale, perché i veri proprietari dei dati sono i cittadini, non le aziende che li utilizzano. E allora bisognerebbe comportarsi come tali: come *domini*.

È necessaria una rivoluzione etico – digitale anche in seno alle aziende che sfruttano i dati personali dei loro clienti, garantendo maggior trasparenza, a partire dagli amministratori di queste aziende, proprio come se i dati illeggittimamente sfruttati fossero proprio i loro, o quelli di un loro familiare.

E tale rivoluzione deve essere accompagnata e guidata dal legislatore, che, almeno limitatamente all'Europa, molto ha fatto, ma molto ha ancora da fare, proprio perché nel mondo della tecnologia è solo un *hic et nunc*, a discapito del *pro futuro*, vista la velocità con cui evolve, si modifica, cambia.

[126] Bracy (2022).

[127] Franceschi – Bicchierai (2022).

Presto non avremo più solo i smart – phones: avremo le smart cities, le smart – car, le smart – homes, le smart – companies. Fino a poco tempo fa l'uomo era l'unico essere smart sulla Terra, ora sembra non poterlo più essere senza le smart – cose di cui sopra. Si sono già elencate sopra tutte le misure legislative e normative e regolamentarie che si potrebbero prendere per evitare altri casi *Cambridge Analytica*, e sarebbe ridondante ripeterle. Quello che non si è ancora detto, a chiusura, è che è necessario ripensare al diritto alla tutela dei dati personali come al diritto alla tutela della nostra identità. Il cuore della privacy è proprio il diritto all'identità, se ci si pensa bene. "The trend goes from programming computers to programming people"[128] è tutto quello che non vorremmo mai sentire, ma che rischia di essere una triste verità.

Ed ecco che allora più che proteggere il concetto di privacy, il legislatore dovrebbe proteggere il diritto alla privacy, che in ultima analisi è il diritto all'identità personale, che non deve essere violato e manipolato per interessi di parte. È illuminante sul punto un passaggio del saggio Privacy and Identity di Mireille Hildebrandt del 2006[129], la quale dice: "This type of identity presumes that humans are not *born* as individual persons, but *develop into* persons as they relate to their environment and interact with others. Developing into a person means that one is constituted as a subject, a *self*. The self lives at the nexus of two aspects of identity, that are never given: identity of the *self* (ipse) has to be claimed *versus others*, and the self has to be claimed as being *the same* (idem) *over the course of time*. […] From this perspective, privacy can now be understood as the process of boundary negotiations that allows a person *to hold together while changing*; it presumes some measure of autonomy, some real contact like intimacy and some space to rebuild the self in accordance with one's past while anticipating one's future".

Per continuare nella strenua difesa del diritto fondamentale alla tutela dei propri dati personali, per non dover più assistere inermi a casi come quello Facebook – *Cambridge Analytica*, è quindi necessario che la privacy sia vista come un valore, qualcosa da proteggere, utilizzando tutti gli strumenti che sono messi a disposizione (legislativi, tecnologici, digitali, elettorali), in ultima battuta come un qualcosa che merita protezione se violata.

[128] Helbing et al. (2017).

[129] Hildebrandt (2006).

“At least in Europe, we consider the right to privacy a fundamental right, and it is a very serious matter”[130].

[130] Josè Manuel Barroso, ex Presidente della Commissione Europea durante uno speech nel 2004.

Lloyd, perché mi sembra che tutti siano più talentuosi, intelligenti e capaci di me?"

"Perché credo che alcuni effettivamente abbiano più talento, intelligenza e capacità di lei, sir"

"E io cosa ho allora, Lloyd?"

"L'umiltà di conoscersi e l'ambizione per potersi migliorare, sir"

"Basteranno per arrivare da qualche parte, Lloyd?"

"Di sicuro per non rimanere dove si è, sir"

"E questo è l'importante, giusto?"

"Decisamente lo è, sir"

BIBLIOGRAFIA

Acquisti, Alessandro, Brandimarte, Laura e Loewenstein, George. 2015. Privacy and human behavior in the age of information. *Science* 347: 509-514.

Aguzzi, Stefania, Bradshaw, David, Canning, Martin, Cansfield, Mike, Carter, Philip, Cattaneo, Gabriella, Gusmeroli, Sergio, Micheletti, Giorgio, Rotondi, Domenico e Stevens. Richard. 31/03/2016. Communications Networks, Content & Technology, Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination, Final Report. European Commission, Directorate-General of Communications Networks. Utimo accesso 07/05/2022. http://publications.europa.eu/resource/cellar/35f3eccd-f7ce-11e5-b1f9-01aa75ed71a1.0001.01/DOC_1

Allport, Gordon W. e Floyd, Henry. 1919. Behavior and experiment in social psychology. *The Journal of Abnormal Psychology* 14: 297–306.

Allport, Gordon W. e Odbert, Henry S. 1936. Trait-names: A psycho-lexical study. Psychological Monographs. *Harvard Psychological Laboratory* 47: 171.

Altman, Irwin e Taylor, Dalmas.1973. Social Penetration: The Development of interpersonal relationships. New York: Holt, Rineheart & Winston.

Biasiotti, Adalberto. 2018. *Il nuovo Regolamento europeo sulla protezione dei dati*. Roma: EPC Editore.

Cattel, Raymond B. 1943. The description of personality: Basic traits resolved into clusters. *Journal of Abnormal and Social Psychology* 38: 476-506.

Cattel, Raymond B. 1945. The description of personality: Principles and findings in a factor analysis. *American Journal of Psychology* 58: 69-90.

Cattel, Raymond B. 1945. The principle trait clusters for describing personality. *Psychological Bulletin* 42: 129-161.

Costa, Paul T. jr. e McCrae, Robert R. 1988. Personality in adulthood: A six-year longitudinal study of self-report and spouse ratings on the NEO Personality Inventory. *Journal of Personality and Social Psychology* 54: 853-863.

Costa, JR. Paul T. e McCrae, Robert R.. 1996. Toward a new generation of personality theories: Theoretical contexts for the five-factor model. *The five-factor model of personality: Theoretical perspectives*. New York: The Guilford Press.

Fiske, Donald W. 1949. Consistency of the factorial structures of personality ratings from different sources. *Journal of abnormal and social psychology* 44: 329-344.

Foucault, Michel. 1975. *Surveiller et punir: Naissance de la prison*. Parigi: Edition Gallimard.

Kaiser, Brittany. 2019. *La dittatura dei dati*. Milano: Harper Collins.

Mayer–Schonberger, Viktor e Cukier, Kenneth N.. 2013. Big Data, Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà. Milano: Garzanti.

Olivieri, Gustavo e Falce, Valeria. 2016. *Smart cities e diritto dell'innovazione.* Milano: Giuffrè Editore.

Papa, Anna. 2009. *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*. Torino: Giappichelli Editore.

Pizzetti, Francesco. 2016. *Privacy e il diritto europeo alla protezione dei dati personali. Il Regolamento europeo 2016/679. Vol. 2*. Torino: Giappichelli Editore.

Tupes, Ernest e Christal, Raymond, 1961 – 1992. Recurrent personality factors based on trait ratings. *USAF ASD Technical Report No. 61-97* 60 (2): 225 – 251.

Warren, Samuel D. e Brandeis, Louis D. 1890. The right to privacy. *Harvard Law Review* 4 (5): 193-220.

Wiley, Christopher. 2020. *Il mercato del consenso. Come ho creato e poi distrutto Cambridge Analytica*. Milano: Longanesi

SITOGRAFIA

AGI. 26/03/2018. Perché non salta fuori il nome del partito italiano per cui lavorò *Cambridge Analytica*?. *AGI*. Ultimo accesso 25 marzo 2022, https://www.agi.it/politica/partito_italiano_cambridge_analytica_intervista_wylie-3684939/news/2018- 03-26/

Anderson, Emma. 22/05/2018. Mark Zuckerberg hearing: As it happened. *Politico*. Ultimo accesso, https://www.politico.eu/article/mark-zuckerberg-european-parliament-hearing-live-blog

Article 29 Working Party. Ultimo aggiornamento 23/11/2016. *Opinion 8/2010 on applicable law (WP179*). Ultimo accesso 5 aprile 2022, https://ec.europa.eu/newsroom/article29/items/640614

Article 29 Working Party. Ultimo aggiornamento 11/04/2018 a. *"Sorry is not enough": WP29 establishes a Social Media Working Group*. Ultimo accesso 25 maggio 2022, https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf

Article 29 Working Party. Ultimo aggiornamento 22/08/2018 b. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. Ultimo accesso 5 aprile 2022, https://ec.europa.eu/newsroom/article29/items/612053

Article 29 Working Party. Ultimo aggiornamento 22/08/2018 c. *Guidelines on transparency under Regulation 2016/679*. Ultimo accesso 10 aprile 2022, https://ec.europa.eu/newsroom/article29/items/622227/en

BBC News. 22/03/2018 a. *Cambridge Analytica*: The data firm's global influence. *BBC News*. Ultimo accesso 2 aprile 2022, https://www.bbc.com/news/world-43476762

BBC. 18/05/2018 b. *Cambridge Analytica* starts bankruptcy proceedings in US. *BBC News*. Ultimo accesso 2 aprile 2022, https://www.bbc.com/news/technology-44167000

Berlocco, Riccardo. 27/06/2019. I social network e il sovraccarico di informazioni. *Culture Digitali*. Ultimo accesso 15 marzo 2022, https://www.culturedigitali.org/i-social-network-e-il-sovraccarico-di-informazioni

Bloomberg Government. 10/04/2018 a. Transcript of Mark Zuckerberg's Senate hearing. *Washington Post*. Ultimo accesso 1 aprile 2022, https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing

Bloomberg Government. 11/04/2018 b. Transcript of Zuckerberg's appearance before House committee. *Washington Post*. Ultimo accesso 1 aprile 2022, https://www.washingtonpost.com/news/the-switch/wp/2018/04/11/transcript-of-zuckerbergs-appearance-before-house-committee

Bracy, Jedidiah. 12/04/2022. Apple's Tim Cook: Protecting privacy 'most essential battle of our time'. *IAPP*. Ultimo accesso 21 aprile 2022, https://iapp.org/news/a/apples-tim-cook-protecting-privacy-most-essential-battle-of-our-time/

Cadwalladr, Carole e Graham-Harrison, Emma. 17/03/2018. Revealed: 50 million Facebook profiles harvested for *Cambridge Analytica* in major data breach. *The Guardian*. Ultimo accesso 25 marzo 2022, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Calderini, Barbara. 13/11/2019. Microtargeting per la pubblicità politica: come funziona, per Usa 2020. *Agenda Digitale*. Ultimo accesso 12 marzo 2022,

https://www.agendadigitale.eu/sicurezza/privacy/microtargeting-per-la-pubblicita-politica-rischi-e-contromisure-in-vista-di-usa-2020/

Chang, Alvin. 23/03/2018. The Facebook and *Cambridge Analytica* scandal, explained with a simple diagram. *Vox*. Ultimo accesso 3 aprile 2022, https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

D'Alessandro, Jaime. 02/05/2018. Chiude *Cambridge Analytica*, la società dello scandalo dei dati di Facebook. *La Repubblica*. Ultimo accesso 10 aprile 2022. https://www.repubblica.it/tecnologia/social-network/2018/05/02/news/chiude_cambridge_analytica_la_societa_coinvolta_nello_scandalo_dei_dati_di_facebook-195348563/, ultima consultazione 10 aprile 2022

Ellison, Jo. 20/03/2018. The Ugg-ly truth: Trump and the making of a trend. *The Financial Times*. Ultimo accesso 2 aprile 2022, https://www.ft.com/content/fb11c1a8-2c3b-11e8-9b4b-bc4b9f08f381

Enciclopedia Treccani. *Social Network*. Ultimo accesso 30 marzo 2022, https://www.treccani.it/enciclopedia/social-network/

European Data Protection Supervisor. 20/01/2022. Opinion on the Proposal for Regulation on the transparency and targeting of political advertising. Ultima consultazione 7 maggio 2022, https://edps.europa.eu/data-protection/our-work/publications/opinions/edps-opinion-proposal-regulation-transparency-and_en

Facebook. *Normativa sui Dati*. Ultimo accesso 2 aprile 2022, https://www.facebook.com/privacy/explanation/

Fiore, Francesca. 25/02/2016. Priming: un fenomeno mnemonico inconsapevole – Introduzione alla Psicologia. *State of Mind – Il giornale delle scienze psicologiche*.

Ultimo accesso 20 aprile 2022, https://www.stateofmind.it/2016/02/priming-effetto-psicologia/

Garante per la Protezione dei dati personali. 26/03/2018. Le imprese sono troppo deboli nelle difese contro gli hacker. Documento n. 8136779. Privacy, l`allarme di Soro: "Le imprese sono troppo deboli nelle difese... - Garante Privacy

Garante per la Protezione dei dati personali. Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - provvedimento n. 229, dell'8 maggio 2014 (pubblicato sulla Gazzetta Ufficiale n. 126 del 3 giugno 2014), http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3118884

Garofalo, Luigi. 30/10/2019. *Cambridge Analytica*, Facebook decide di pagare la multa in Uk. Ammissione di colpa?. *Key4biz*. Ultimo accesso 14 aprile 2022, https://www.key4biz.it/cambridge-analytica-facebook-decide-di-pagare-la-multa-in-uk-ammissione-di-colpa/277367/

Gheoghegan, Peter e Corderoy, Jenna. 19/12/2018. Revealed: Arron Banks Brexit campaign's 'secret' meetings with *Cambridge Analytica*. *Open Democracy*. Ultimo accesso 2 aprile 2022, https://www.opendemocracy.net/en/dark-money-investigations/revealed-arron-banks-brexit-campaign-had-more-meetings-w/

Glenn Greenwald. 10/10/2014. Why privacy matters. *TedX*. Ultimo accesso 20 aprile 2022, https://www.youtube.com/watch?v=pcSlowAhvUk&t=481s

Granville, Kevin. 19/03/2018. Facebook and *Cambridge Analytica*: What you need to know as fallout widens. *The New York Times*. Ultimo accesso 10 aprile 2022, https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html/

Hamilton, Isobel Asher. 23/08/2019. Facebook just published emails showing how much employees knew about the giant *Cambridge Analytica* data scandal 2 years before the story exploded. Ultimo accesso 23 maggio 2022, https://www.businessinsider.com/facebook-emails-show-workers-knew-cambridge-analytica-2015-2019-8?r=US&IR=T

Hartmans, Avery. 22/03/018. It's impossible to know exactly what data *Cambridge Analytica* scraped from

Facebook — but here's the kind of information apps could access in 2014. *Business Insider*. Ultimo accesso 10 aprile 2022, https://www.businessinsider.com/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3?r=US&IR=T

Helbing, Dirk, Frey, Bruno S., Gigerenzer, Gerd, Hafen, Ernst, Hagner, Michael, Hofstetter, Yvonne, Van den Hoven, Joroen, Zicari, Roberto V. e Zwitter, Andrej. 25/02/2017. Will Democracy Survive Big Data and Artificial Intelligence?. *Scientific American*. Ultimo accesso 21 aprile 2022, https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/

Hildebrandt, Mireille. 2006. Privacy and Identity. *Oxford – Antwerp Privacy and the Criminal Law*. Ultimo accesso 21 aprile 2022, http://works.bepress.com/ildebra_hildebrandt/6/

Irish Data Protection Commission. 31/03/2018. Ireland's Data Protection Commissioner "following up" with Facebook over *Cambridge Analytica*. *The Journal*. Ultimo accesso 15 aprile 2022, https://www.thejournal.ie/facebook-investigations-data-3913631-Mar2018/

Issenberg, Sasha. 19/12/2012. How Obama's Team Used Big Data to Rally Voters. *MIT Technology Review*. Ultimo accesso 1 aprile 2022,

https://www.technologyreview.com/2012/12/19/114510/how-obamas-team-used-big-data-to-rally-voters/

Johnson, Bobbie. 11/01/2010. Privacy no longer a social norm, says Facebook founder. *The Guardian*. Ultimo accesso 19 marzo 2022, https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Kosinski, Michal, Stillwell, David e Graepel, Thore. 11/03/2013. Private traits and attributes are predictable from digital records of human behavior. *PNAS Journal*. Ultimo accesso 12 marzo 2022, https://www.pnas.org/doi/10.1073/pnas.1218772110

Lettig, Daniele e Stolton, Samuel. 04/03/2021. La Commissione europea potrebbe vietare il microtargeting per la pubblicità politica online. *Euractiv*. Ultimo accesso 25 marzo 2022, https://euractiv.it/section/digitale/news/la-commissione-europea-potrebbe-vietare-il-microtargeting-per-la-pubblicita-politica-online/

Madsbjerg, Saadia. 14/11/2017. It's Time to Tax Companies for Using Our Personal Data. *The New York Times*. Ultimo accesso 10 marzo 2022, https://www.nytimes.com/2017/11/14/business/dealbook/taxing-companies-for-using-our-personal-data.html

Marantz, Andrew. 09/03/2020. The Man Behind Trump's Facebook Juggernaut. *The New Yorker*. Ultimo accesso 5 aprile 2022, https://www.newyorker.com/magazine/2020/03/09/the-man-behind-trumps-facebook-juggernaut

Mawston, Neil. 24/06/2021. Strategy Analytics: Half the World Owns a Smartphone. *Strategy Analytics*. Ultimo accesso 24 marzo 2022, https://www.strategyanalytics.com/access-services/devices/mobile-phones/smartphone/smartphones/reports/report-detail/half-the-world-now-owns-a-smartphone

NaturPhilosophie. 03/02/2017. Psychometrics and “big data” – Who do they think you are?”. *NaturPhilosophie*. Ultimo accesso 25 marzo 2022, https://www.naturphilosophie.co.uk/psychometrics-big-data-think/

Office of the Attorney General for the District of Columbia. 23/05/2022. AG Racine Sues Mark Zuckerberg for Failing to Protect Millions of Users' Data, Misleading Privacy Practices. Ultimo accesso 25 maggio 2022, https://oag.dc.gov/release/ag-racine-sues-mark-zuckerberg-failing-protect

Presa Diretta. Reportage del 10/02/2020, https://www.youtube.com/watch?v=cckZ6Eom2Bu

Reuters. 21/03/2018. What are the links between *Cambridge Analytica* and a Brexit campaign group?. *Reuters*. Ultimo accesso 25 marzo 2022, https://www.reuters.com/article/us-facebook-cambridge-analytica-leave-eu/what-are-the-linksbetween-cambridge-analytica-and-a-brexit-campaign-group-idUSKBN1GX2IO

Rociola, Arcangelo. 20/03/2018. Cosa ha rivelato il numero uno di *Cambridge Analytica* nell’inchiesta di Channel 4. *AGI*. Ultimo accesso 3 aprile 2022, https://www.agi.it/estero/cambridge_analytica_inchiesta_facebook-3645205/news/2018-03-20/

Rosenberg, Matthew, Confessore, Nicholas e Cadwalladr, Carole. 17/03/2018. How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*. Ultimo accesso 25 marzo 2022, https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

Ryskamp, Dani Alexis. 23/06/2020. Facebook Faces Shareholder Lawsuit Over *Cambridge Analytica* Data Security Concerns. *Expert Institute*. Ultimo accesso,

https://www.expertinstitute.com/resources/insights/facebook-faces-shareholder-lawsuit-over-cambridge-analytica-data-security-concerns/

Saetta, Bruno. 22/04/2018. Micro-targeting, profilazioni, algoritmi: il vero problema etico è l'uso da parte della politica dei dati dei cittadini. *Valigia Blu*. Ultimo accesso 25 marzo 2022, https://www.valigiablu.it/algoritmi-politica-dati-cittadini/

Salinas, Sara. 21/03/2018. Zuckerberg on *Cambridge Analytica*: 'We have a responsibility to protect your data, and if we can't then we don't deserve to serve you. *CNBC*. Ultimo accesso, https://www.cnbc.com/2018/03/21/zuckerberg-statement-on-cambridge-analytica.html

Sandonnini, Pierluigi. 31/01/2020. Data mining: cos'è, perché conviene utilizzarlo e quali sono le attività tipiche. *Big Data 4 innovation*. Ultimo accesso 2 aprile 2022, https://www.bigdata4innovation.it/data-science/data-mining/data-mining-cose-perche-conviene-utilizzarlo-e-quali-sono-le-attivita-tipiche/

Symeonidis, Iraklis, Tsormpatzoudi, Pagona e Preneel, Bart. Ultimo aggiornamento 23/03/2018. Collateral damage of Facebook Apps: an enhanced privacy scoring model. *Università di Leuven*. Ultimo accesso 10 aprile 2022, https://www.esat.kuleuven.be/cosic/publications/article-2535.pdf

Tufekci, Zeynep. 19/03/2018. Facebook's Surveillance Machine. *The New York Times*. Ultimo accesso 10 aprile 2022, https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html

Twitter. *Tweet di Edward Snowden*. Ultimo accesso 25 marzo 2022, https://twitter.com/snowden/status/975106627513729024

Valsania, Marco. 02/05/2018. *Cambridge Analytica* travolta dal Datagate: bancarotta e chiusura immediata. *Ilsole24ore*. Ultimo accesso 2 aprile 2022,

https://www.ilsole24ore.com/art/cambridge-analytica-travolta-datagate-bancarotta-e-chiusura-immediata-AEAKYxhE?refresh_ce=1

Vengattil, Munsif. 03/05/2018. *Cambridge Analytica* begins insolvency proceedings in the UK. *Financial Review*. Ultimo accesso 2 aprile 2022, https://www.afr.com/technology/cambridge-analytica-begins-insolvency-proceedings-in-the-uk-20180503-h0zkgg

Wagner, Kurt. 17/03/2018. Here's how Facebook allowed *Cambridge Analytica* to get data for 50 million users". *Vox Recode*. Ultimo accesso 25 marzo 2022, https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data

Weiss, Brennan. 17/03/2018. Trump-linked firm *Cambridge Analytica* collected personal information from 50 million Facebook users without permission. *Business Insider*. Ultimo accesso 10 aprile 2022, https://www.businessinsider.com/cambridge-analytica-trump-firm-facebook-data-50-million-users-2018-3?r=US&IR=T

Wiewiórowski, Wojciech. 14/03/2022. It is time to target online advertising. *European Data Protection Supervisor*. Ultimo accesso 25 marzo 2022, https://edps.europa.eu/press-publications/press-news/blog/it-time-target-online-advertising_en

Zorloni, Luca. 28/06/2019. Facebook paga anche in Italia per lo scandalo *Cambridge Analytica*: 1 milione di multa. *Wired*. Ultimo accesso 14 aprile 2022, https://www.wired.it/internet/social-network/2019/06/28/scandalo-cambridge-analytica-facebook/

PROCEDIMENTI GIUDIZIARI

Causa C – 131/12, Google Inc./ Agencia Española de Protección de Datos, (AEPD) and Mario Costeja González, in https://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=IT

Causa C – 230/14, Weltimmo s. r. o/ Nemzeti Adatvédelmi és Információszabadság Hatóság, in https://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=IT