ARCHIVIO ANTROPOLOGICO MEDITERRANEO

Archivio antropologico mediterraneo

Anno XXIV, n. 23 (1) | 2021
Dossier monografico e Miscellanea

GDPR tra protezione dei dati personali e privacy. Intervista a Giulia Barrera

Elena Bougleux, Francesca Declich e Giulia Barrera

OpenEdition Journals

Edizione digitale
URL: https://journals.openedition.org/aam/4089
DOI: 10.4000/aam.4089
ISSN: 2038-3215

Editore
Dipartimento Culture e Società - Università di Palermo

Notizia bibliografica digitale
Elena Bougleux, Francesca Declich e Giulia Barrera, «GDPR tra protezione dei dati personali e privacy. Intervista a Giulia Barrera», *Archivio antropologico mediterraneo* [Online], Anno XXIV, n. 23 (1) | 2021, online dal 30 juin 2021, consultato il 02 juillet 2021. URL: http://journals.openedition.org/aam/4089 ; DOI: https://doi.org/10.4000/aam.4089

GDPR tra protezione dei dati personali e privacy. Intervista a Giulia Barrera

Elena Bougleux, Francesca Declich e Giulia Barrera

1 *EB/FD Perché secondo te l'Unione Europea ha voluto emanare un regolamento relativo alla protezione dei dati personali (il così detto GDPR[1]), dal momento che già esisteva una direttiva europea sulla protezione dei dati, recepita da tutti i paesi dell'Unione?*

2 GB Prima di rispondere alla vostra domanda, vorrei fare un passo indietro e ricordare perché era stata adottata la direttiva che menzionate. L'esigenza di proteggere i dati personali con una normativa specifica si è andata affermando internazionalmente con lo sviluppo dell'informatica. Rispetto al vecchio mondo della carta, la creazione di banche dati ha determinato pericoli inediti per le libertà individuali e i diritti dei cittadini. Inizialmente confinato tra i giuristi, il dibattito in materia si andò estendendo progressivamente al grande pubblico nel corso degli anni Settanta del Novecento. "In Germania, la proposta di censimento nazionale nel 1983 fu accolta, in un clima politico di grande tensione, da una generale opposizione."[2] Data l'esperienza storica della Germania, un censimento informatizzato faceva temere all'opinione pubblica tedesca la possibilità di sviluppo di nuove forme di controllo autoritario sui cittadini; non a caso, proprio in Germania sono state introdotte le prime normative sulla protezione dei dati personali. Fu sempre l'attenzione ai pericoli per i diritti individuali che lo sviluppo dell'informatica avrebbe potuto comportare, ad indurre l'Unione Europea ad adottare, nel 1995, una direttiva sulla protezione dei dati personali[3], che fissò già i principi fondamentali che troveremo poi nel GDPR.
Rispetto al 1995, le esigenze di tutela dei dati personali sono aumentate esponenzialmente: basti pensare che nel 1995 Internet stava ancora muovendo i primi passi, Google e Facebook ancora non esistevano, non esistevano i social network ed Amazon aveva appena iniziato ad operare, ma solo come venditore di libri. Lo sviluppo tumultuoso di internet a partire dalla fine del XX-inizio del XXI secolo, ha fatto maturare fra i legislatori della UE la convinzione che era necessario rafforzare

fortemente la normativa a protezione dei dati personali. Nel GDPR, i principi fondamentali sono gli stessi già fissati dalla direttiva del 1995, ma la norma è diventata assai più cogente, si sono precisati gli obblighi per chi tratta i dati ed i diritti delle persone a cui i dati si riferiscono e sono state fortemente aumentate le sanzioni, che precedentemente erano talmente modeste da non avere alcun potere deterrente nei confronti dei giganti del web. Emblematico al riguardo il caso della sanzione a Google per la raccolta fraudolenta di dati per mezzo di "Street View".

Sin dal suo esordio, le automobili di Street View che – mediante telecamere a 360° collocate sul tetto – catturavano tutte le immagini nel loro raggio di azione, avevano suscitato una significativa preoccupazione, per la loro possibilità di catturare e diffondere immagini delle persone, ma questo era nulla rispetto a quanto successivamente emerse. "Nel 2010, la commissione federale tedesca per la protezione dei dati annunciò che le operazioni di Google Street View celavano un furto di dati. Le auto di Street View raccoglievano segretamente dati personali dalle reti wi-fi private."[4] Lo scandalo fu enorme, ma la sanzione modestissima, per un gigante come Google: l'autorità garante di Amburgo, che per prima si era accorta "della raccolta illecita di dati operata da Street View, fece pagare a Google una multa di 145.000 euro, poco meno dei 150.000 richiesti inizialmente. Si trattava della multa più cara mai comminata in Europa" per violazioni della normativa a protezione dei dati personali[5], ma non certo tale da impensierire Google. Oggi le sanzioni per la violazione del GDPR possono arrivare fino a 20 milioni di euro, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente (art. 83).

3 *EB/FD Che differenza c'è fra difesa della privacy e protezione dei dati personali?*

4 GB L'idea che dovesse esistere un "diritto alla privacy" venne formulata per la prima volta da due giuristi statunitensi, Samuel Warren e Louis Brandeis, in un articolo pubblicato nel 1890 e diventato poi celeberrimo[6], che parlava di un "diritto ad essere lasciati soli", reagendo ad una campagna di stampa particolarmente intrusiva nella vita personale della moglie di Warren. La privacy era concepita come una sfera privata da proteggere nei confronti di intrusioni esterne. L'idea che esista il diritto ad uno spazio personale a cui gli altri non debbono avere accesso aveva già trovato traduzione normativa in molti ordinamenti, nel riconoscimento della inviolabilità del domicilio e della segretezza della corrispondenza; la proposta di Warren e Brandeis, successivamente recepita dalla Corte suprema statunitense, estendeva questa nozione di sfera privata.

Oggi, siamo noi stessi a disseminare al di fuori della nostra sfera privata informazioni su di noi: lo facciamo ogni volta che navighiamo in internet e in mille altre occasioni della nostra vita quotidiana. Non potremmo lavorare da casa, comprare un biglietto aereo on line, firmare un appello lanciato da un'organizzazione umanitaria, fare ricerche sulla rete, o dialogare con i nostri "amici" su Facebook senza disseminare dati personali. Il punto quindi non è più tanto quello di proteggere la sfera privata da intrusioni esterne, ma di permettere alle persone di avere il controllo sull'uso che viene effettuato dei dati personali che loro stessi disseminano.

L'esigenza di proteggere i dati personali è diventata particolarmente acuta da quando hanno iniziato ad essere oggetto di commercializzazione, all'inizio del XXI secolo, diventando ben presto una delle merci più redditizie del pianeta. Il fenomeno è stato studiato dalla sociologa statunitense Shoshana Zuboff, che ha messo a fuoco come siamo entrati nell'era che lei ha definito del "capitalismo della sorveglianza". Il capitalismo, ha spiegato Zuboff, si è sempre caratterizzato per la capacità di

trasformare in merci le risorse naturali (pensate alla terra, al lavoro umano o all'acqua); nell'ultimo ventennio ha scoperto come trasformare in merce i dati relativi all'esperienza umana. L'esperienza umana viene prima trasformata in dati, secondo un processo che Zuboff ha definito "datificazione"; i dati diventano quindi strumento di profilazione e commercializzati. Google che è stato il capofila di questa trasformazione: nel 2001, quando ha iniziato a utilizzare i dati relativi alle ricerche effettuate dagli internauti a fini di profilazione, i suoi profitti sono aumentati, nel giro di un anno, del 400 per cento, e hanno poi continuato a galoppare incessantemente. È grazie alla commercializzazione dei dati personali che i giganti della rete, come Google e Facebook, hanno potuto accumulare nel giro di un ventennio patrimoni astronomici[7].

5 *EB/FD C'è chi asserisce che la profilazione serve sostanzialmente per la pubblicità, per far arrivare ad ognuno una pubblicità più adatta al proprio livello, stratificazione sociale, e interessi. Spesso la risposta data a chi considera questo come problematico è: "In definitiva, se raccolgono i miei dati non è un problema dal momento che io non ho nulla da nascondere".*

6 GB Questa è una obiezione che spesso le persone pongono perché pensano che l'unica conseguenza della profilazione sia di ricevere pubblicità mirata, mentre in realtà la profilazione si presta a moltissimi altri utilizzi, già oggi e non in un lontano futuro distopico, né soltanto in paesi autoritari come la Cina. Faccio alcuni esempi: tra gli acquirenti di profili ci sono le compagnie di assicurazione, alle quali conoscere in dettaglio le abitudini dei potenziali clienti (consumano alcolici? fumano? fanno consumo di droga? amano correre con la macchina? hanno malattie ereditarie in famiglia? ecc.), permette di proporre polizze assicurative tagliate esattamente sul profilo di rischio individuale; in tal modo, le compagnie di assicurazione minimizzano i propri rischi e massimizzano i profitti.

Per i datori di lavoro, è ormai pratica comune, prima di assumere qualcuno, cercare su internet informazioni sui possibili nuovi dipendenti. Negli Stati Uniti, dove la protezione dei dati personali è molto più bassa che nella UE, perché non esiste una legge federale di protezione dei dati personali paragonabili al GDPR, questo tipo di indagine viene fatta rivolgendosi a società specializzate in *background checking* (come Thruthfinder.com, BeenVerified.com, Peoplelooker.com, Instantcheckmate.com, ecc.) che controllano la fedina penale dei candidati (pratica proibita da noi, salvo casi particolari), e attingono a molte altre fonti pubbliche e private, per creare profili dettagliati e molto intrusivi. Si può facilmente immaginare quanto simili pratiche possano presentare rischi di discriminazione.

Un altro campo in cui si fa largo uso della profilazione è quello della propaganda politica. Poter indirizzare messaggi propagandistici mirati rispetto al profilo dei destinatari è molto più efficace rispetto alla propaganda indifferenziata. Le organizzazioni politiche che acquisiscono dati di profilazione degli elettori si assicurano un vantaggio incalcolabile rispetto agli oppositori politici.

Il caso di Cambridge Analitica (la società di consulenza britannica che ottenne da Facebook i dati relativi a milioni di utenti) è noto[8]. Meno noto è che nel 2012 alcuni ricercatori di Facebook hanno pubblicato i risultati di un esperimento di condizionamento politico effettuato con successo da Facebook stesso. L'esperimento ha permesso a Facebook di dimostrare di aver influenzato con messaggi non espliciti l'attitudine al voto: i messaggi non erano a favore di un determinato candidato, ma intendevano convincere ad andare a votare. Coloro che sono stati esposti – si badi bene, inconsapevolmente – a tali messaggi, hanno mostrato una partecipazione al voto maggiore del campione di controllo. La partecipazione al voto è cresciuta del 2 per

cento[9], che può sembrare una percentuale molto piccola, ma se si pensa a come le elezioni presidenziali statunitensi siano state in più occasioni decise da poche migliaia di voti, si comprende come spostare anche solo il 2 per cento dei voti possa contare moltissimo.

7 *EB/FD Qui però più che di protezione dei dati a questo punto stai parlando di diritto al lavoro, diritto alla salute, di garanzia di trasparenza nel processo politico: è così?*

8 GB Sì, infatti la protezione dei dati personali è considerata un prerequisito per l'esercizio di molti altri diritti. Per questo l'Unione Europea, nel redigere la sua Carta dei diritti fondamentali, ha posto la protezione dei dati personali tra i diritti fondamentali di libertà. La carta, si noti, include sia un articolo sulla protezione della privacy[10]sia un articolo specifico sulla protezione dei personali[11].
La Carta della UE è stata approvata nel 2000; la nostra Costituzione, precedente di oltre cinquant'anni, ovviamente non parlava di protezione dei dati personali, ma i giuristi ritengono che l'Articolo 2, che "riconosce e garantisce i diritti inviolabili dell'uomo" debba essere considerato la base costituzionale per la protezione dei dati personali, in quanto tutela il libero sviluppo della persona umana. Contemporaneamente, sia la Carta dei diritti fondamentali della UE che la Costituzione proteggono la ricerca scientifica e la libertà di espressione. Secondo entrambe le carte, la protezione dei dati personali deve essere infatti bilanciata con altri interessi costituzionalmente tutelati.

9 *EB/FD Pur non volendo entrare troppo in dettagli tecnici potresti dire qualcosa di più sullo spirito complessivo del GDPR e i principi fondamentali che ne sono alla base?*

10 GB Come ho già ricordato, i principi fondamentali del GDPR sono gli stessi della Direttiva europea del 1995. Il GDPR, però, ha introdotto una logica di forte responsabilizzazione del titolare del trattamento (il titolare è la persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali). In sostanza, il GDPR non prescrive adempimenti assolti i quali si è "a posto", ma assegna al titolare la responsabilità di trattare i dati in modo tale da garantire che dal trattamento non possano derivare rischi per i diritti e le libertà degli interessati. Le misure specifiche da adottare saranno diverse a seconda dei casi; starà al titolare valutare, caso per caso, quali siano le misure appropriate.
Ad esempio, il GDPR prevede che il titolare debba garantire la sicurezza dei dati, il che vuol dire sia prevenire accessi non autorizzati e fughe di dati, sia prevenire la perdita accidentale dei dati. Se un ospedale perde le cartelle cliniche dei pazienti, provoca un danno gravissimo; se l'INPS perde i dati degli assicurati, provoca anch'esso un danno gravissimo; se una carta di credito non protegge a sufficienza i dati dei clienti, li espone ad alti rischi, e così via. Il GDPR non dice in che modo deve essere raggiunto l'obiettivo di garantire la sicurezza dei dati; afferma che tale obiettivo deve essere perseguito con mezzi che dovranno essere commisurati al danno che potrebbe derivare alle persone. Quindi, tanto per fare un esempio, un circolo degli scacchi e un ospedale dovranno mettere in atto misure di sicurezza molto diverse, perché molto diverse sono le conseguenze per gli interessati, in caso di perdita dei dati, o accesso non autorizzato ad essi.
Il GDPR è lontano dalla logica dei controlli formali, a cui siamo abituati in Italia, e che spesso ci induce a concentrare l'attenzione sui formalismi, perdendo di vista il nocciolo della questione. Il nocciolo del GDPR, che dobbiamo avere sempre presente, è costituito dai principi fondamentali enunciati nell'art. 5, apparentemente molto semplici, ma densi di conseguenze. Non possiamo in questa sede esaminarli tutti, ma vorrei almeno

ricordarne due di particolare rilevanza per la ricerca antropologica. Il primo è che i dati personali devono essere trattati in modo lecito, corretto e trasparente. Dal principio della trasparenza deriva l'obbligo di informare la persona intervistata sulla ricerca che si sta effettuando, con un linguaggio semplice e comprensibile. Non c'è bisogno di farcire le informative con mille riferimenti giuridici; è invece necessario che l'interessato, anche se ha un livello d'istruzione basso, possa capire perché vengono raccolti i suoi dati, con quale finalità, come verranno conservati, come verranno di utilizzati, da chi, eccetera.

Un altro principio fondamentale stabilito dall'art. 5 del GDPR, e che non ammette eccezioni, è il principio della minimizzazione dei dati. In estrema sintesi, si deve cercare di trattare meno dati personali possibile. Ciò non vuol dire fare meno ricerca: significa, ad esempio, che quando pubblichiamo dobbiamo rendere identificabili le persone a cui si riferiscono i dati soltanto se veramente è necessario (a meno che l'interessato non abbia esplicitamente dato il proprio consenso alla pubblicazione del suo nome). Molto spesso si può scrivere senza fare riferimento a specifiche persone o comunque trattare i dati in forma tale da non permettere l'identificazione delle persone cui si riferiscono i dati, senza arrecare alcun danno alla qualità scientifica della ricerca.

Gli antropologi debbono inoltre considerare che il GDPR pone forti restrizioni alla possibilità di trattare quelle che chiama "categorie particolari di dati" e che nella precedente normativa venivano definiti "dati sensibili": si tratta dei dati concernenti 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 (art. 9).

In sintesi: il GDPR proibisce il trattamento di questi dati, salvo che in determinate eccezioni, una delle quali è se i dati vengono trattati a fini di ricerca. La deroga a favore della ricerca è però soggetta a una serie di condizioni: la prima riguarda l'osservanza del principio della minimizzazione dei dati personali. Inoltre è sempre necessario, in via prioritaria, garantire la tutela dei diritti e delle libertà degli interessati. Tutelare i diritti e le libertà delle persone a cui si riferiscono i dati che trattiamo deve essere sempre la nostra stella polare.

NOTE

1. 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).

2. Douwe Korff e Marie Georges, con il contributo del Garante italiano per la protezione dei dati personali & dei Partner del progetto T4Data, Manuale RPD. Linee guida destinate ai Responsabili della protezione dei dati nei settori pubblici e parapubblici per il rispetto del Regolamento

generale sulla protezione dei dati dell'Unione Europea (versione approvata dalla Commissione, luglio 2019), p. 13.

3. Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

4. S. Zuboff, *Il capitalismo della sorveglianza: il futuro dell'umanità nell'era dei nuovi poteri*, Roma, Luiss University Press, 2019: 154.

5. *Ibid.*: 160.

6. S. Warren, L. Brandeis, "The Right to Privacy", *Harvard Law Review*, IV (5), (15 dicembre 1890): 193-220.

7. Zuboff, *Il capitalismo della sorveglianza* cit., p. 97 e passim.

8. Si veda, sul sito del Garante per la protezione dei dati personali: Caso Cambridge Analytica - www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/8376626

9. Zuboff, *Il capitalismo della sorveglianza* cit.: 315-17.

10. Carta dei diritti fondamentali dell'Unione europea, art. 7: "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni."

11. Art. 8: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

AUTORI

ELENA BOUGLEUX

Università degli studi di Bergamo, Dipartimento di Lingue, Letterature e Culture Straniere
elena.bougleux@unibg.it

FRANCESCA DECLICH

Università degli Studi di Urbino Carlo Bo, Dipartimento di Scienze della Comunicazione, Studi Umanistici e Internazionali francesca.declich@uniurb.it

GIULIA BARRERA

Ministero per i beni e le attività culturali, Direzione generale archivi
giulia.barrera@beniculturali.it