GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

I Capitolo

Nuove fonti del diritto alla protezione dei dati personali

II Capitolo

Le principali novità introdotte dal Regolamento 679/2016 sulla Data Protection

Origini e sviluppo di un nuovo diritto: il diritto all'oblio

Il caso Costeja - *Corte di Giustizia UE 13 maggio 2014, causa C-131/12* -

Critiche alla sentenza Google – Spain

Riflessioni sulla portata della sentenza Google Spain Giurisprudenza nazionale

Come fare per ottenere la cancellazione dei propri dati dai risultati di Google?

Il diritto alla portabilità dei dati

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

Una nuova figura di garanzia di tutela dei dati: il Responsabile Dati personali

Capitolo III

La Datacrazia

Tecnologia e democrazia

Le responsabilità di Facebook nel "caso Cambridge Analytica", le tutele offerte dal nuovo Regolamento ed i rischi per la democrazia

L'inconsapevolezza degli utenti come fonte di ricchezza dei Big del web e strumento di sorveglianza di massa dei governi

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

I Capitolo

Nuove fonti del diritto alla protezione dei dati personali

Il 14 aprile 2016 il Parlamento dell'Unione europea approvava in via definitiva il nuovo pacchetto protezione dati con l'obiettivo di consentirne l' applicazione entro i successivi due anni.

In particolare, l'assemblea plenaria del Parlamento Europeo adottava in seconda lettura il Regolamento europeo 2016/679 in materia di *protezione dei dati personali* e la Direttiva 2016/680 *sulla protezione dei dati nelle attività di polizia e giustizia*, concludendo un *iter* legislativo durato oltre 4 anni e determinando l'introduzione in tutti i paesi membri di un sistema di regole in materia di protezione dati unico ed armonizzato.

Il nuovo "pacchetto protezione dati" punta a garantire maggiori opportunità e tutele per cittadini ed imprese, adeguando una normativa europea anacronistica ed incapace di soddisfare bisogni sorti dallo sviluppo delle nuove tecnologie e dai nuovi modelli di crescita economica.

La precedente normativa, infatti, risale al 1996, un'epoca in cui Internet, le app., i dispositivi portatili, i *cloud* ed i social network non avevano ancora dispiegato tutta la loro potenza.

Tra i principali obiettivi, il nuovo Regolamento si propone di introdurre una legislazione in materia di protezione dati uniforme e valida in tutta Europa, affrontando temi innovativi, come il diritto all'oblio e la portabilità dei dati, e stabilendo criteri volti a responsabilizzare imprese ed enti rispetto alla protezione dei dati personali, nonché ad introdurre semplificazioni per chi è tenuto al rispetto delle regole. Infatti, nonostante la protezione dei dati personali godesse della copertura della Direttiva 95/46 Ce, il suo recepimento negli ordinamenti dei singoli Stati membri aveva portato ad una frammentazione in 28 discipline nazionali, pregiudicando il principale obiettivo comunitario della creazione di un mercato unico a scapito degli scambi economici interni, della competitività e dell'adeguata difesa dei diritti. Le imprese che operano in più Paesi membri non hanno potuto applicare un regime unitario e si sono dovute interfacciare con autorità di supervisione munite di poteri diversi e con approcci interpretativi poco coordinati[1].

[1] Cybersicurezza, "La nuova privacy" Il sole 24ore . Pubblicazione settimanale n.5/2018.

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

La Direttiva, secondo elemento fondamentale del pacchetto, stabilisce, per la prima volta, norme comuni per il trattamento dei dati a fini giudiziari e di polizia all'interno di tutti gli Stati membri. Obiettivo della Direttiva è quello di innalzare le garanzie per la privacy dei cittadini quando i loro dati sono "trattati" per motivi giudiziari e di polizia, nonché agevolare lo scambio e l'uso delle informazioni utili per contrastare fenomeni come criminalità e terrorismo.

In concreto, la Direttiva, in vigore già dal 5 maggio, ha obbligato gli Stati membri a recepire le sue disposizioni nel diritto nazionale entro 2 anni, mentre il Regolamento è entrato in vigore 20 giorni dopo la pubblicazione in GUUE, per poi diventare definitivamente applicabile in via diretta in tutti i Paesi dell'UE a partire dal 25 maggio 2018, quando dovrà essere garantito il perfetto allineamento fra la normativa nazionale e le disposizioni europee.

Si tratta, infatti, di un Regolamento ad efficacia differita; ciò risponde alla necessità di soddisfare esigenze di carattere pratico, dando il tempo ai destinatari delle nuove norme di adeguarsi gradualmente alla nuova disciplina.

Si specifica altresì che la raccolta dei dati avvenuta prima dell'introduzione della normativa *de quo* sarà considerata regolare se

avvenuta secondo modalità conformi al Regolamento 2016/679. Non sarà quindi necessario che l'interessato presti nuovamente il consenso se lo stesso è stato, *ab origine*, espresso mediante "*qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile"*(art.4, par. GDPR).

Il Regolamento, particolarmente coeso ai fini dell'uniformità, è altresì flessibile. Il legislatore europeo ha infatti optato per un approccio per principi e criteri guida, sia per evitare una rapida obsolescenza e disapplicazione di una disciplina di dettaglio , sia per rendere più agevole il superamento dei problemi derivanti dal frequente e complesso intreccio delle norme europee con quelle nazionali.

Infatti in primo luogo, si segnala che, in ambito di *data protection*, è ancora vigente nel nostro Paese il Codice della Privacy (D.Lgs 196/2003) che raccoglie la maggior parte delle disposizioni inerenti alla privacy ed al trattamento dei dati vigenti nei primi anni del 2000.

In secondo luogo, che gli atti legislativi europei, tra cui i Regolamenti, sono collocati nel sistema delle fonti di diritto domestico, immediatamente al di sotto della carta costituzionale, prevalendo sia sul diritto interno già vigente che su quello successivo e, pertanto, il Regolamento prevale sulla legge nazionale interna.

Tuttavia, la sola esistenza ed applicazione del GDPR non comporta, provenendo questo da un ordinamento diverso da quello nazionale, l'abrogazione automatica della legge statale regolante la medesima materia, ma solo la disapplicazione di quelle norme codicistiche in contrasto con la nuova disciplina[2].

A conferma di quanto detto, il considerando 10 del GDPR, secondo cui *"per quanto riguarda il trattamento dei dati personali per l'adempimento di un obbligo legale, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, gli Stati membri dovrebbero rimanere liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del presente regolamento*".

Il D.lgs. 196/2003 non subisce dunque alcuna abrogazione diretta, al contrario, mantiene la sua forza normativa attraverso una"rilettura in chiave GDPR", in base alla quale: dove non vi è compatibilità tra quanto

[2] Alla data odierna (27/3/2018) in attuazione dell'art. 13 della legge di delegazione europea 2016-2017 (legge 25 ottobre 2017, n. 163), è stato approvato in via preliminare lo schema di decreto legislativo di adeguamento del quadro normativo nazionale alle disposizioni del GDPR, che prevede, tra le tante, l'espressa abrogazione delle disposizioni del codice in materia di trattamento dei dati personal incompatibili con le disposizioni contenute nel regolamento (UE) 2016/679. Tuttavia, lo schema di decreto delegato deve ancora essere inviato alle Commissioni parlamentari (non ancora costituite) ed, in seguito, al Garante per acquisirne il parere, pertanto *l'iter* non può dirsi ufficialmente concluso.

disposto dal Codice della Privacy e quanto previsto dal Regolamento 679/2016, la legge statale viene disapplicata in favore del GDPR; invece, laddove vi sia compatibilità tra le due norme, il d.lgs. 196/2003 rimane applicabile continuando a dettare legge, addirittura in modo più dettagliato rispetto al GDPR.

Pertanto, il legislatore europeo rimette agli Stati Membri il potere normativo di derogare ed integrare la disciplina sovranazionale nonché di emanare le cd norme interstiziali, vale a dire norme con cui i legislatori nazionali mantengono ovvero introducono *ex novo* requisiti ulteriori o più specifici in considerazione del proprio contesto economico, sociale e culturale.

Tra i casi in cui sono concessi poteri derogatori ovvero integrativi agli Stati Membri, si riportano i seguenti:

- in ordine all'esercizio dei poteri sanzionatori: "*Gli Stati membri determinano le sanzioni per le violazioni del presente regolamento, in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 79, e prendono tutti i provvedimenti necessari per la loro applicazione. Tali sanzioni sono effettive, proporzionate e dissuasive" (art. 79 ter).*

- in ordine alla liceità del trattamento *(Lawfulness of processing)*, il paragrafo 2 dell'art. 6 GDPR dispone che "*gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX.*"

- in ordine al *"Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione" ('Automated individual decision-making*, including profiling'), l'art. 22 paragrafo 2 let.b (relativo al diritto dell'interessato di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato) dispone che il paragrafo 1 "*non si applica nel caso in cui la decisione sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento*".

- in ordine al "*Trattamento e la libertà d'espressione e di informazione*" ove gli Stati membri "*possono prevedere esenzioni o deroghe rispetto ai capi II (principi), III (diritti dell'interessato), IV (titolare del trattamento e responsabile del trattamento), V (trasferimento di dati personali verso*

paesi terzi o organizzazioni internazionali), VI (autorità di controllo indipendenti), VII (cooperazione e coerenza) e IX (specifiche situazioni di trattamento dei dati) qualora siano necessarie per conciliare il diritto alla protezione dei dati personali e la libertà d'espressione e di informazione".

Più in generale, deroghe e specificazioni da parte degli Stati membri sono ammesse dal Capo IX (artt. 85 – 91) contenente "*Disposizioni relative a specifiche situazioni di trattamento dati*" ("*Provisions relating to specific processing situations*").

A sostegno dell'introduzione del nuovo pacchetto privacy, il discorso del Presidente dell'Autorità Garante per la protezione dei dati personali, Antonello Soro, secondo cui *"l'approvazione del Regolamento e della Direttiva rappresentano per l'Unione un traguardo importante, atteso da tempo*." Ed ancora, il giorno dell'adozione dei provvedimenti, lo stesso sosteneva: *"Oggi è una giornata importante per i cittadini europei e per la tutela dei loro diritti. Con la pubblicazione in Gazzetta Ufficiale dell'Unione Europea dei testi del Regolamento in tema di protezione dei dati e della Direttiva nelle attività di polizia e giustizia, si conclude uno dei più complessi, travagliati e rilevanti percorsi di riforma dell'Unione europea. Il Regolamento porta grandi novità sul piano della tutela dei diritti e degli*

strumenti previsti per responsabilizzare maggiormente le imprese stabilendo, al contempo, significative semplificazioni.

Le nuove regole raccolgono certamente la sfida più importante: adeguare le norme di protezione dei dati ai cambiamenti determinati dall'incessante evoluzione delle tecnologie. Ma, soprattutto - aggiunge Soro - *nel momento in cui si fanno sempre più forti le spinte anacronistiche a creare "barriere" alla libera circolazione di beni e persone, il Regolamento raggiunge l'ambizioso obiettivo di assicurare una disciplina uniforme ed armonizzata tra tutti gli Stati membri, eliminando definitivamente le numerose asimmetrie che si erano create nel tempo.*

L'Europa, per quanto debba ancora ampiamente esprimere le sue potenzialità nello sviluppo di un vero mercato digitale, ha oggi la straordinaria opportunità di dimostrare la propria capacità di evolvere e di esportare, su scala mondiale, il proprio modello di protezione dei dati capace di coniugare al punto più alto i diritti delle persone con le esigenze delle imprese e del mercato".

Nonostante la conclamata importanza della nuova disciplina, le sanzioni che la stessa prevede e l'approssimarsi del 25 maggio 2018, *deadline* per le aziende che devono conformarsi alle nuove regole, *"in Italia, oltre la metà delle aziende – ma anche tante Pubbliche amministrazioni – non è*

ancora pronta ad allinearsi ai provvedimenti Ue in materia di data protection".[3]

Quanto sostenuto sul sito dell'Agenda Digitale (Agid) a meno di 4 mesi dalla diretta applicazione del Regolamento europeo in materia di dati personali, è preoccupante: la percezione è che le aziende di grandi dimensioni operanti nei settori del mercato consumieristico abbiano affrontato e stiano effettivamente affrontando progetti di adeguamento, ma anche che, diversamente, le Pubbliche amministrazioni e gli enti pubblici siano drasticamente arretrati nell'affrontare il problema.

Sarebbe inoltre auspicabile, come segnalato dalla "Guida per la protezione dei dati personali ed aziendali" del Sole 24 ore, che le aziende si adeguino a quanto previsto dal nuovo Regolamento non solo per evitare le ingenti sanzioni, ma anche e soprattutto per sentirsi parte attiva in una battaglia di civiltà a favore dei cittadini e contro il capillare controllo che le tecnologie digitali rendono possibile sulle loro vie[4].

[3] https://www.agendadigitale.eu/cittadinanza-digitale/gdpr-tutto-cio-che-ce-da-sapere-per-essere-preparati/

[4] Cybersicurezza, "La nuova privacy" Il sole 24ore . Pubblicazione settimanale n.5/2018.

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

II Capitolo

Le principali novità introdotte dal Regolamento 679/2016 sulla Data Protection :

Il nuovo Regolamento comprende disposizioni di portata trasversale.

In estrema sintesi, tra le principali novità introdotte dal GDPR (*General Data Protection Regulation*) saranno oggetto di trattazione del presente lavoro:

- l'introduzione di nuovi diritti: il diritto all'oblio ed il diritto alla portabilità dei dati;
- l'analisi di una nuova figura: il Responsabile della protezione dei dati (DPO)

Origini e sviluppo di un nuovo diritto: il diritto all'oblio

La dimensione assunta da Internet negli ultimi anni e l'immenso spazio di libertà, di scambio e di conoscenza che lo stesso ha creato ha reso indispensabile l'elaborazione di uno strumento idoneo a tutelare nuove posizioni giuridiche.

A tal fine nel 2015, in Italia, veniva istituita in sede parlamentare una Commissione di studio sui diritti e i doveri relativi ad Internet con il compito di elaborare la Dichiarazione dei Diritti in Internet, approvata e pubblicata il 28 luglio 2015.

L'importanza del web al giorno d'oggi è ribadita nel breve preambolo del testo ove si afferma che *"Internet ha contribuito in maniera decisiva a ridefinire lo spazio pubblico e privato, a strutturare i rapporti tra le persone e tra queste e le Istituzioni. Ha cancellato confini e ha costruito modalità nuove di produzione e utilizzazione della conoscenza. Ha ampliato le possibilità di intervento diretto delle persone nella sfera pubblica. Ha modificato l'organizzazione del lavoro. Ha consentito lo sviluppo di una società più aperta e libera. Internet deve essere considerato come una risorsa globale che risponde al criterio della universalità"*[5].

Nel merito, l'"*Internet Bill of rights*" italiano tocca temi delicati, tra cui il diritto all'oblio disciplinato dall'art. 11 che recita: "**1.** *Ogni persona ha diritto di ottenere la cancellazione dagli indici dei motori di ricerca dei riferimenti ad informazioni che, per il loro contenuto o per il tempo*

5 http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/dichiarazione_dei_diritti_internet_pubblicata.pdf

*trascorso dal momento della loro raccolta, non abbiano più rilevanza pubblica. **2.** Il diritto all'oblio non può limitare la libertà di ricerca e il diritto dell'opinione pubblica a essere informata, che costituiscono condizioni necessarie per il funzionamento di una società democratica. Tale diritto può essere esercitato dalle persone note o alle quali sono affidate funzioni pubbliche solo se i dati che le riguardano non hanno alcun rilievo in relazione all'attività svolta o alle funzioni pubbliche esercitate. **3.** Se la richiesta di cancellazione dagli indici dei motori di ricerca dei dati è stata accolta, chiunque può impugnare la decisione davanti all'autorità giudiziaria per garantire l'interesse pubblico all'informazione.*

Secondo parte della dottrina, si tratterebbe di un mero diritto di deindicizzazione che non considera la possibile rimozione della notizia dalla fonte primaria e di portata limitata rispetto alla sentenza della Cassazione n. 5525 del 2012 sugli archivi storici dei quotidiani.

Infatti, con la sentenza n. 5525/2012 la Suprema Corte, pronunciandosi in merito ad un caso che vedeva coinvolto un politico che lamentava come tramite una ricerca in Internet emergesse sul sito del "Corriere della Sera" la notizia del suo arresto senza alcun riferimento al successivo epilogo favorevole della vicenda giudiziaria, affermava che

l'interessato ha diritto a che "*l'informazione oggetto di trattamento risponda ai criteri di proporzionalità, necessità, pertinenza allo scopo, esattezza e coerenza con la sua attuale ed effettiva identità personale o morale (c.d. principi di proporzionalità, pertinenza e non eccedenza)*", nonché che l'interessato ha il diritto di sapere "*chi è in possesso dei suoi dati personali e come li adopera, nonché di opporsi al trattamento dei medesimi, ancorché pertinenti allo scopo della raccolta, ovvero di ingerirsi al riguardo, chiedendone la cancellazione, la trasformazione, il blocco, ovvero la rettificazione, l'aggiornamento, l'integrazione.*" [6]

Pertanto, secondo gli ermellini, al fine di tutelare l'identità sociale del soggetto cui si riferisce la notizia di cronaca bisogna garantire al medesimo la cancellazione ovvero l'aggiornamento della notizia attraverso l'automatico collegamento, mediante il sito internet, alle informazioni pubblicate successivamente relative all'evoluzione della vicenda. Si tratta, infatti, di notizie ed informazioni idonee a completare o, addirittura, mutare il quadro sorto a seguito della notizia originaria.

Nel caso di specie, quindi, se l'interesse pubblico alla persistente conoscenza di un fatto avvenuto in epoca di molto anteriore trova giustificazione nell'attività politica svolta dal soggetto titolare dei dati,

[6] Cassazione Civile, sez. III, sentenza 05/04/2012 n° 5525

non si può prescindere dal suo aggiornamento, diversamente la notizia sarebbe da considerarsi non vera e, pertanto, da eliminare.

Inoltre, la Corte aggiungeva che, come è noto, essendo le notizie presenti in rete organizzate in maniera casuale e diffusa, il motore di ricerca, deve essere considerato "*un mero intermediario telematico che offre un sistema automatico di reperimento di dati e informazioni attraverso parole chiave;* in pratica, "*un mero fornitore del servizio di fruizione della rete, che si limita a rendere accessibile sul sito web i dati dei c.d. siti sorgente, assolvendo ad un'attività di mero trasporto delle informazioni".* Ed ancora, la Corte sottolineava "*come Google è notoriamente un motore di ricerca che si limita ad offrire ospitalità sui propri server a siti internet gestiti dai relativi titolari in piena autonomia, i quali negli stessi immettono e memorizzano le informazioni oggetto di trattamento (cfr. Trib.Milano, 24/3/2011)".*

Dunque, alla luce di quanto sostenuto dalla Corte, il compito di aggiornare gli archivi spetta al titolare del sito (nel caso di specie Rcs Quotidiani s.p.a.) e non al motore di ricerca su cui grava solo "*il potere-dovere di impedirne la indicizzazione ed il posizionamento delle notizie una volta venuto a conoscenza del contenuto illecito delle medesime contenute nei siti sorgente*".

In sintesi, il merito da riconoscere alla pronuncia *de quo* è aver affermato, con netto anticipo rispetto all'evoluzione della normativa ma (già) in linea con le proposte di riforma europee, che il trascorrere del tempo è elemento costitutivo del diritto all'oblio. In sostanza, la Suprema Corte ha affermato la possibilità di chiedere la rimozione di dati non più necessari in relazione alle finalità di trattamento, salvo che il mantenimento degli stessi non sia giustificato da ragioni storiche, statistiche e scientifiche, quindi diverse da quelle di cronaca originarie.

Nel tempo la giurisprudenza ha continuato a svolgere un ruolo fondamentale per l'affermazione del diritto all'oblio. In particolare, con la sentenza monito C-131/12 -Mario Costeja Gonzales e AEPD contro Google Spain e Google Inc - la Corte di Giustizia dell'Ue ha definito la portata del *right to be forgotten*.

Relativamente al trattamento dei dati da parte dei motori di ricerca, il Presidente Rodotà, primo Garante della privacy italiano, aveva inizialmente escluso che i motori di ricerca potessero essere considerati responsabili del trattamento dei dati personali relativi alle pagine Internet indicizzate e rese reperibili tramite il motore stesso (Garante privacy, 3 Marzo 2005, n. 1149178 in www.garanteprivacy.it , nel caso specifico i resistenti erano Google, Microsoft e Yahoo) e solo nel 2006

mutava il proprio orientamento. In proposito, tra i tanti, si riporta il Provvedimento del 18.01.2006, n. 1242501 relativo ad una signora che chiedeva la cancellazione del proprio nome da una pagina che riportava la notizia, risalente nel tempo, del proprio arresto, senza alcun riferimento, tra l'altro, all'assoluzione con formula piena.

La signora segnalava al Garante che, dopo l'avvenuta cancellazione della notizia da parte del sito internet, la stessa ricompariva attraverso i motori di ricerca che, una volta inserito il suo nome, la indicizzavano e rendevano visibile.

Dal punto di vista tecnico, la fonte del problema risiedeva nella non avvenuta cancellazione da parte del motore di ricerca coinvolto (Google) della c.d. "*copia cache*", che continuava ad essere indicizzata, quindi ad apparire tra i risultati della ricerca.

In seguito al ricorso contro Google, che si era difeso sulla base della precedente decisione del marzo 2005, il Garante stabiliva che "*presso il motore di ricerca in questione risulta effettuato un autonomo trattamento di dati personali della ricorrente, in particolare attraverso la creazione e la conservazione di cosiddette copie cache di pagine web pubblicate su siti "sorgente".*

Tuttavia, nel caso de *quo* il Garante non aveva ritenuto di poter intervenire nei confronti di Google in quanto "*nella fattispecie non risultava provato che il trattamento contestato, svolto attraverso il sito "www.google.it", fosse stato effettuato da un soggetto stabilito sul territorio dello Stato, ovvero da un soggetto che, per tale trattamento, si avvaleva di strumenti situati nel medesimo territorio (art.5,comma2,del Codice)".*

Il Garante aveva sostanzialmente glissato la questione, e, pur riconoscendo la autonoma titolarità del trattamento dei dati in capo al motore di ricerca nella attività di indicizzazione delle pagine, non aveva ritenuto possibile applicare la normativa nazionale al gestore del motore di ricerca.

Il GDPR ha poi fatto propria la tesi citata, riconoscendo l'applicabilità delle disposizioni europee in presenza di una stretta connessione tra le attività di uno stabilimento dell'UE e quelle di uno situato fuori dai confini europei.In particolare, la sussistenza della connessione è indiscussa quando l'attività svolta dal primo è volta a rendere economicamente redditizi i servizi svolti dal secondo.

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

Il caso Costeja - *Corte di Giustizia UE 13 maggio 2014, causa C-131/12 -*

Il protagonista del caso in oggetto è un cittadino spagnolo interessato, nel 1998, da una procedura di riscossione coattiva di crediti previdenziali ed il cui nome era stato pubblicato dal quotidiano spagnolo «La Vanguardia» tra gli avvisi relativi ad un'asta immobiliare.

Il Costeja lamentava la circostanza per cui, a distanza di 16 anni, digitando il suo nome sul motore di ricerca "Google Search", si veniva rimandati alle pagine web del quotidiano in cui comparivano gli annunci che lo riguardavano.

Per evitare che le notizie continuassero a comparire nei risultati di ricerca e nei collegamenti a *La Vanguardia*, l'interessato si rivolgeva alla Agencia Española de Protección de Datos (AEPD) e, in particolare, chiedeva a Google Spain e a Google Inc. (società madre del gruppo Google con sede sociale negli Stati Uniti) la rimozione dei suoi dati personali, ed al periodico di cancellare e di deindicizzare le pagine web che lo menzionavano.

Esaminato il ricorso, AEPD rigettava le richieste rivolte al giornale motivando che la pubblicazione degli annunci incriminati, peraltro avvenuta su ordine della magistratura, era da ritenersi legittima, ma

accoglieva le istanze contro Google, ordinando la immediata sospensione della indicizzazione nonchè la rimozione dei dati del sig. Costeja Gonzales.

Contro tale decisione Google Spain e Google Inc. presentavano ricorso alla Audiencia Nacional, che, formulando i quesiti pregiudiziali di seguito riportati relativi all' applicabilità della Direttiva europea che regolamenta il diritto all'oblio, sospendeva il processo e rimetteva gli atti (ex. art. 267 TFUE)alla Corte.

Con riferimento al contesto normativo, la CGUE indicava applicabile la direttiva 95/46, i relativi considerando e la legge organica di recepimento n. 15/1999 in materia di tutela dei dati personali.

Entrando nel merito, la prima questione pregiudiziale riguardava la applicabilità a Google Inc. della Direttiva 95/46.

La Corte spagnola chiedeva cioè di stabilire se, in ordine a Google Spain ed alla attività da questo esercitata, esistesse o meno uno "stabilimento" ai sensi dell'articolo 4.1. della Direttiva.

In seguito, con la seconda questione pregiudiziale chiedeva se *"nel localizzare le informazioni pubblicate o messe in rete da terzi, nell'indicizzarle in maniera automatica, nel memorizzarle temporaneamente e infine nel metterle a disposizione degli utenti di*

Internet" la succursale svolgesse un "*trattamento*" ai sensi del Direttiva e se la stessa fosse da considerarsi "titolare" del trattamento *de quo.*

In caso di risposta positiva, in subordine, si chiedeva se fosse ammissibile per l'interessato rivolgersi direttamente (quindi senza preventivo ricorso al sito originario) al motore di ricerca per chiedere la cancellazione dei dati, ovvero se il motore di ricerca fosse da considerarsi esonerato dall'obbligo di cancellazione qualora la notizia fosse stata pubblicata lecitamente (come nel caso in questione); e, in generale, se l'interessato avesse il diritto di rivolgersi ad un motore di ricerca per impedire "*l'indicizzazione delle informazioni riguardanti la sua persona pubblicate su pagine web di terzi, facendo valere la propria volontà a che tali informazioni non fossero conosciute dagli utenti di Internet, ove egli reputasse che la loro divulgazione potesse arrecargli pregiudizio o desiderasse che tali informazioni fossero dimenticate, anche quando si trattasse di informazioni pubblicate da terzi lecitamente".*

Appare i*ctu oculi* evidente che il problema principale non fosse la legittimità della pubblicazione, quanto la sua continua conoscibilità tramite Internet giacchè *le" modalità di funzionamento della rete consentono, in particolar modo attraverso l'utilizzo di motori di ricerca, di*

rinvenire un consistente numero di informazioni, riferite a soggetti individuati, più o meno aggiornate e di natura differente."[7]

Venendo alla decisione della Corte di Giustizia, in merito alla prima questione pregiudiziale, la Corte rispondeva affermativamente argomentando le sue ragioni sulla base dell'attività svolta da Google Spain, indirizzata ai cittadini spagnoli e destinata alla promozione e alla vendita degli spazi pubblicitari proposti dal motore di ricerca (Google Inc.). In particolare, la Corte sottolineava che si è in presenza di uno "stabilimento" quando, mediante un'organizzazione stabile, viene esercitata una attività; nel caso concreto consistente nella raccolta pubblicitaria a favore del motore di ricerca.

Rispetto all' eccezione sollevata da Google, secondo cui il trattamento di dati personali sarebbe stato svolto non da Google Inc ma da Google Spagna, la Corte ricordava che l'articolo 4.1.(a) della Direttiva, ai fini della configurazione di uno "stabilimento", non richiedeva che il trattamento fosse svolto dallo stabilimento interessato, ma che fosse

[7] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb display/docweb/1116068 - Reti telematiche e Internet - Motori di ricerca e provvedimenti di Autorità indipendenti: le misure necessarie a garantire il c.d. "diritto all'oblio"-

sufficiente che lo stesso venisse realizzato "nel contesto delle attività" di tale stabilimento.

Fatte queste premesse, i giudici di Lussemburgo affermavano che "*le attività del gestore del motore di ricerca e quelle del suo stabilimento, situato nello Stato membro interessato, erano inscindibilmente connesse dal momento che le attività relative agli spazi pubblicitari costituivano il mezzo per rendere il motore di ricerca in questione economicamente redditizio e che tale motore è, al tempo stesso, lo strumento che consente lo svolgimento di dette attività*".

Dunque, il motore di ricerca e le attività di promozione pubblicitaria venivano considerati aspetti inscindibili, in quanto il primo dipende proprio dalla pubblicità che lo rende economicamente redditizio.

Per quanto concerne la nozione di "*titolare del trattamento*", la sentenza sottolineava che, nel raccogliere i dati personali contenuti nelle pagine oggetto della indicizzazione, il motore di ricerca svolge una attività di trattamento di dati personali autonoma rispetto ai siti originari, in particolare, mentre questi ultimi hanno unicamente lo scopo di rendere disponibili alcuni contenuti, il motore di ricerca si caratterizza per la capacità di raccogliere, attraverso criteri autonomamente scelti, tutte le

informazioni disponibili riguardo un certo argomento o un certo soggetto.

Pertanto, coerentemente con quanto esposto, la Corte rispondeva positivamente alla successiva questione pregiudiziale relativa alla possibilità di destinare direttamente al motore di ricerca, ed indipendentemente dal fatto che la pagina web originale fosse stata cancellata o meno, la domanda di cancellazione dei dati.

Infatti, secondo i giudici europei, la qualifica di Google come autonomo titolare del trattamento presuppone, come naturale conseguenza, l'idoneità dello stesso ad essere sottoposto, in via altrettanto autonoma, all'esercizio dei diritti da parte degli interessati.

Chiaramente, la Corte considerava altresì l' effetto di tale decisione sul principio della libera circolazione delle informazioni, sostenendo che "*nel cercare l'equilibrio tra i contrapposti interessi, occorre verificare se l'interessato abbia diritto a che l'informazione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome. In proposito occorre sottolineare che la constatazione di un diritto siffatto non presuppone che l'inclusione dell'informazione in questione nell'elenco dei risultati arrechi un pregiudizio all'interessato.*"

Alla luce dei provvedimenti del Garante sopra menzionati (v. pag. 14) l'aspetto rivoluzionario di questa pronuncia non risiede tanto nell'aver qualificato il motore di ricerca come un autonomo titolare del trattamento dei dati avente scopi e finalità indipendenti rispetto ai siti originari, ma nell'aver dichiarato applicabile a Google la Direttiva Europea.

Si tratta di una sentenza storica per i cittadini europei, grazie alla quale gli stessi sono diventati titolari del diritto di richiedere al motore di ricerca di rimuovere ogni collegamento tra il proprio nome e una determinata pagina web, anche se quest'ultima è stata legittimamente pubblicata.

Critiche alla sentenza Google – Spain

"*Immaginate una biblioteca enorme, diffusa su decine di edifici, con milioni di scaffali, centinaia di milioni di volumi, trilioni di pagine. Una gran parte dello scibile umano è lì, sotto i vostri occhi, oltre la barriera dell'ingresso. A voi serve un titolo. Cercate una monografia sulla politica indiana degli ultimi 10 anni, perchè ci sono appena state le elezioni e volete capirci di più. Il volume è lì, da qualche parte fra milioni di altri. Però, da ieri, non*

potete più chiedere al bibliotecario di aiutarvi a trovarlo, perchè la Corte di Giustizia Europea gli ha ingiunto di non dare più accesso a quell'opera, su richiesta di un tizio citato nel libro, una figura secondaria, a cui non piace che quelle informazioni siano disponibili."[8]

La metafora della biblioteca è utilizzata da Lucio Scudiero, avvocato esperto in privacy, per descrivere criticamente gli effetti della sentenza Google – Spain.

Tra i principali rilievi evidenziati dalla dottrina contraria alla giurisprudenza europea emerge l' ingiustificata compressione della libertà economica del motore di ricerca, peraltro in contrasto con il precedente indirizzo giurisprudenziale inaugurato dagli stessi giudici europei con la sentenza ASNE (ove erano parti la Asociación Nacional de Establecimientos Financieros de Crédito, Federación de Comercio Electrónico y Marketing Directo (FECEMD) contro la Administración del Estado), a cui danno luogo le conclusioni della Corte.

Il lavoro citato (v. nota 5) evidenzia altresì l'inopportunità della scelta della Corte di rendere operativo un diritto, ai tempi non ancora normativizzato, "*dai contorni poco chiari e dalla realizzazione tecnica*

[8] http://www.stradeonline.it/9-innovazione-e-mercato/618-la-corte-di-giustizia-contro-google-fiat-privacy-pereat-internet di Lucio Scudiero

incerta senza riguardo di altri diritti", in primis quello all'informazione, costretto a soccombere.

E' stato altresì stato sostenuto che con la pronuncia *de qua* la Corte ha sancitola (quasi) assoluta prevalenza del diritto al rispetto della propria vita privata e alla protezione dei dati personali, ex artt. 7 e 8 Cedu, rispetto alla libertà di espressione e di informazione, garantita dall'art. 11 della medesima Carta[9].

A sostegno di quanto affermato, si riportano le considerazioni, rimaste inascoltate da parte della Corte, dell'Avvocato Generale che, in sede processuale, affermava «*Un fornitore di servizi di motore di ricerca su Internet esercita legalmente tanto la sua libertà di impresa quanto la sua libertà di espressione quando rende disponibili su Internet strumenti di localizzazione delle informazioni sulla base di un motore di ricerca. La costellazione particolarmente complessa e difficile di diritti fondamentali che questo caso presenta osta alla possibilità di rafforzare la posizione giuridica della persona interessata ai sensi della direttiva riconoscendole*

9 v. D. Miniussi, *Il "diritto all'oblio": i paradossi del caso Google,* cit., 217; G. Scorza, *Corte di Giustizia e diritto all'oblio*, cit., 1481. Per un'analisi critica su questo aspetto si rimanda a O. Pollicino, *Un digital right to privacy preso (troppo) sul serio,* cit., 569 ss.; S. Sica - V. D'Antonio*, La procedura di deindicizzazione*, cit., 714, che mettono in evidenza come la pronuncia in esame risulti "gravemente deficitaria, nella misura in cui offre una visione profondamente restrittiva dell'art. 11 della Carta dei diritti fondamentali".

un diritto all'oblio. Ciò vorrebbe dire sacrificare diritti primari come la libertà di espressione e di informazione».

Dunque, la responsabilità dei *search engines* sarebbe da escludersi a causa della loro incapacità di esercitare un controllo editoriale analogo a quello dei *contenent providers* (vale a dire gli editori titolari ei siti "sorgente").

Tra le argomentazioni a sostegno di questa tesi, una sentenza della stessa Corte (Google vs Vuitton[10]) nonché il considerando 42 della Direttiva 2000/31/CE, secondo cui «*le deroghe alla responsabilità stabilita nella presente direttiva riguardano esclusivamente il caso in cui l'attività di prestatore di servizi della società dell'informazione si limiti al processo tecnico di attivare e fornire accesso ad una rete di comunicazione sulla quale sono trasmesse o temporaneamente memorizzate le informazioni messe a disposizione da terzi al solo scopo di rendere più efficiente la trasmissione. Siffatta attività è di ordine meramente tecnico, automatico e passivo, il che implica che il prestatore di servizi della società dell'informazione non conosce né controlla le informazioni trasmesse o memorizzate».*

[10] Google France SARL e Google Inc. contro Louis Vuitton Malletier SA (C-236/08)

Secondo, Camilla Bistolfi, membro del cda dell'Istiuto Italiano privacy, all'interno di queste attività ricadrebbe proprio quella svolta dal motore di ricerca "*giacché esso fornisce l'accesso ai contenuti della rete mediante l'indicizzazione dei risultati di ricerca per renderne più facile il reperimento, nonché per garantire all'utente il diritto di accesso alle informazioni che circolano sul web*. "[11], pertanto l'attività del motore di ricerca consisterebbe unicamente nella veicolazione delle informazioni finalizzata a garantirne la reperibilità e l'accessibilità.

Inoltre, l'esperta aggiunge che "*alterare i risultati di ricerca, mantenendo comunque i contenuti sul sito web dell'editore, va contro le nozioni di pluralismo e di libertà di informazione, ponendo la decisione della Corte di Giustizia europea in un potenziale contrasto con quanto previsto dallo stesso articolo 10 della CEDU. "*

*L*a decisione di affidare la responsabilità di tutela dei dati personali ai motori di ricerca e non solo ai siti web che pubblicano i contenuti ha ricevuto altrettante critiche dall'esperto del settore Luca Bolognini, presidente dell'Istituto Italiano privacy, che ha commentato così il provvedimento: "*Sul diritto all'oblio, ci sembra che il nostro Garante*

[11]http://www.stradeonline.it/monografica/1014-diritto-all-oblio-sui-m...i-di-ricerca-le-conseguenze-indesiderate-di-una-sentenza-pericolosa
C.Bistolfi , 20.3.21015

Privacy italiano abbia fatto molto meglio della Corte di Giustizia. Da anni, porta avanti un'interpretazione ragionevole che pone gli oneri di cancellazione o modifica dei dati pubblicati sul web a carico dei content provider, come gli editori di giornali, perché sono loro – per scopi professionali del tutto legittimi – a diffondere i dati in internet. Fatto sta che nell'interpretazione della Corte, un motore di ricerca – che è un mero sistema di indicizzazione/consultazione di contenuti – diventa Titolare del trattamento dei dati delle persone di cui i siti pubblicano i dati e come tale deve rispondere alle richieste di cancellazione degli interessati. Questo ci sembra parossistico"[12].

Della stessa opinione anche l'avvocato Guido Scorza, esperto di diritto digitale: "*Privacy e libertà di informazione sono due diritti fondamentali dell'uomo da maneggiare con estrema attenzione ed è preoccupante che la loro tutela – anche se solo in prima battuta – resti affidata ai gestori dei motori di ricerca fuori da ogni preventivo controllo da parte di un Giudice o di un'Autorità."* [13]

[12] https://www.corrierecomunicazioni.it/digital-economy/diritto-all-oblio-bolognini-sentenza-ue-non-al-passo-con-l-evoluzione-tecnologica/

[13] http://scorza.blogautore.espresso.repubblica.it/2014/05/13/si-chiama-"privacy"-il-tornado-che-si-abbatte-motori-di-ricerca/

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio
Copyright © 2017 – Giuricivile – ISSN: 2532-201X
Redazione: redazione@giuricivile.it

Riflessioni sulla portata della sentenza Google Spain

"Se fin dalle origini dell'umanità, dimenticare è stata la norma e ricordare l'eccezione, oggi, con l'avvento della tecnologia digitale e dei network globali, questo equilibrio si è ribaltato, tanto che dimenticare è diventato l'eccezione e ricordare la norma"[14],

E' questa inversione di tendenza, propria del nostro secolo, che rivela come le nuove tecnologie, in primis Internet, abbiano fatto sorgere la necessità di delineare un preciso quadro di obblighi e responsabilità in capo ai soggetti che offrono i propri servizi sul web, al fine di soddisfare le nuove esigenze di tutela dei diritti fondamentali della persona.

Come rilevato da parte della dottrina, la Corte europea più che affermare il diritto ad essere dimenticati, con la sentenza di cui si discute si è espressa su un frammento di questo diritto ed, in particolare, sul diritto alla dissociazione del proprio nome da un dato risultato di ricerca[15]" ovvero sul cd. "*right not to be found easily*" (letteralmente, diritto a non essere trovato facilmente), diretto ad ottenere non la cancellazione del dato, ma solo la sua deindicizzazione da parte dei motori di ricerca .

[14] V. Mayer- Schönberger, Delete: il diritto all'oblio nell'era digitale,

[15]. Sica - V. D'Antonio, La procedura di de-indicizzazio- ne, in Dir. inf., 2014, 704 ss.

Un'attribuzione non marginale dati gli effetti dirompenti che la deindicizzazione è idonea a produrre, infatti *"sebbene l'informazione continui ad essere reperibile nella sua collocazione originaria, sul piano concreto, risulterà pressoché irraggiungibile dalla maggior parte degli utenti."* [16]

Nel delineare le caratteristiche ed i presupposti del diritto di deindicizzazione la Corte ha chiarito che *"il suo esercizio è ammesso anche in assenza di un pregiudizio in capo all'interessato e che ciò che occorre verificare, invece, è che le informazioni risultanti in esito ad una ricerca su Internet appaiano incompatibili con l'art. 6, par. 1, lett. c), d) ed e) della direttiva, in quanto "inadeguate, non pertinenti o non più pertinenti, ovvero eccessive in rapporto alle finalità del trattamento", ovvero siano conservate in modo tale da consentire l'identificazione delle persone interessate per un periodo di tempo superiore a quello necessario"* [17].

Al fine di indicare in modo compiuto i casi in presenza dei quali, nel giudizio di bilanciamento, il diritto alla deindicizzazione è destinato a

[16] Diritto all'oblio e motori di ricerca: la prima pronuncia dei Tribunali italiani dopo il caso Google Spain, commento di Francesca Russo, Riv. Internet e tutela della privacy 3/2016.

[17] Cfr. punto 94 della sentenza.

soccombere rispetto al diritto all'informazione ed al diritto di acquisire in modo celere le informazioni tramite i motori di ricerca, il 25 novembre 2014, l'Article 29 Data Protection Working Party ha pubblicato un documento contenente l'indicazione di criteri chiari e univoci che il gestore del motore di ricerca deve utilizzare per valutare se è necessario procedere o meno alla cancellazione dei link dai risultati indicizzati.

A seguito dell'introduzione del Regolamento 2016/679 il Working Party Art. 29 è stato sostituito dal Comitato dei Garanti del quale rimarca al composizione e l'autonomia, ma che gode di maggiori poteri ed a cui sono assegnati più compiti.

Le Linee Guida forniscono una serie di chiarimenti relativi alla pronuncia ed alle modalità con cui le autorità nazionali sulla protezione dei dati personali devono intervenire.

In proposito, si evidenzia un aspetto critico: l'affidamento, almeno all'inizio, ad un'autorità privata del bilanciamento degli interessi in gioco. Infatti, solo qualora il gestore del motore di ricerca non dia seguito alla domanda di cancellazione, è ammesso che l'interessato si rivolga al Garante della privacy, ovvero all'autorità giudiziaria, "*affinché queste*

effettuino le verifiche necessarie e ordinino al suddetto responsabile l'adozione di misure precise conseguenti"[18] .

A questo proposito, l'avvocato Guido Scorza, esperto di diritto digitale, nell' articolo dal titolo emblematico "*Non lasciamo Google (da solo) a scrivere la storia"* afferma che *"questa previsione ha in sé il germe della sconfitta dello Stato di diritto che, in un settore drammaticamente rilevante per l'equilibrio democratico e lo sviluppo economico di ogni Paese, abdica l'amministrazione della giustizia a favore di un soggetto privato, lasciato solo ad agire da arbitro di ciò che i cittadini hanno diritto a leggere e ciò che è bene non leggano e non sappiano"* ed aggiunge *"la questione potrebbe essere estesa anche ai social media; non solo Google, ma tutti i social network. Nel caso, potremmo rischiare di vedere delegata alla discrezionalità di Facebook, Twitter e quanti altri la decisione su quali contenuti siano da considerare 'riservati' e quali no. "*

Secondo parte della dottrina, "*vista l'importanza degli interessi in gioco e la possibilità che Google si tramuti, de facto, in un arbitro della fruibilità dell'informazione on-line*, *sarebbe stata preferibile la prefigurazione di un meccanismo di partecipazione immediata dell'Autorità amministrativa,*

[18] Punto 77 della sentenza

che ben avrebbe potuto svolgere un compito di mediazione tra i differenti interessi in conflitto" [19].

Tornando alla procedura *de qua,* a seguito del mancato accoglimento da parte del motore di ricerca delle richieste di deindicizzazione le autorità nazionali dovranno seguire i criteri stabiliti dal WP29[20]. In particolare, dovranno tener conto:

- della natura del richiedente (ad esempio si dovrà valutare se riveste un ruolo di rilievo pubblico; circostanza attribuibile ai politici, agli iscritti in albi professionali nonché agli alti funzionari pubblici ed agli uomini d'affari);

- dell' età del richiedente al momento della pubblicazione dell'informazione. L'orientamento dominante ritiene che la minore età debba favorire l'accoglimento di una richiesta di deindicizzazione;

- dell'attinenza dell'informazione all'ambito professionale o personale dell'interessato;

- della possibilità che la disponibilità di un determinato risultato di ricerca arrechi pregiudizio all'interessato o metta a rischio la sicurezza

[19] Mantelero, Il futuro Regolamento EU sui dati personali e la valenza "politica" del caso Google: ricordare e dimenticare nella *digital economy*, in Dir. inf., 2014, 687.

[20] http://ec.europa.eu/newsroom/article29/news-overview.cfm

dello stesso.

Le pronunce del Garante e la giurisprudenza italiana dopo Google - Spain

A seguito della sentenza della Corte di Giustizia, il Garante privacy ha adottato i primi provvedimenti in merito alle segnalazioni presentate da cittadini dopo il mancato accoglimento da parte di Google delle loro richieste di deindicizzazione delle pagine web che riportavano i loro dati personali

Le richieste pervenute al Garante si riferiscono ad articoli relativi a vicende processuali ancora recenti e, in alcuni casi, non concluse.

In sette[21] casi su nove il Garante non ha accolto la richiesta degli interessati, ritenendo prevalente l'interesse pubblico ad accedere alle informazioni. In particolare, ha rilevato come le vicende processuali descritte nelle pagine web contestate fossero troppo recenti, e come, in alcuni casi, i relativi procedimenti non si fossero ancora conclusi[22].

[21] doc. web nn. 3623819, 3623851, 3623897, 3623919, 3623954, 3624003 e 3624021]

[22] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3623678#1

In due casi[23], invece, il Garante ha accolto la richiesta dei segnalanti, rilevando, in un caso, che i documenti pubblicati sul sito fornivano più informazioni rispetto a quelle necessarie a soddisfare il diritto di cronaca ed, inoltre, la circostanza per cui alcune di esse si riferivano a persone del tutto estranee alla vicenda giudiziaria narrata, e nell'altro caso, che la notizia pubblicata era inserita in un contesto idoneo a ledere la sfera privata della persona.

Pertanto, il Garante ha prescritto a Google Inc. di deindicizzare le URL segnalate.

Di recente ,[24], il Garante della privacy è tornato ad occuparsi del tema e, con Provvedimento n. 30 del 26 febbraio, ha accolto il ricorso proposto da un residente italiano diretto ad ottenere la rimozione dal motore di ricerca Y.! del link alla pagina di un sito statunitense nella quale erano riportate notizie relative ad una vicenda giudiziaria in cui era stato coinvolto, senza peraltro alcun riferimento alla successiva derubricazione del reato in una fattispecie di minore gravità.

[23] doc. web nn. 3623877 e 3623978]

[24] Diritto all'oblio in rete, motori di ricerca e ambito della giurisdizione dell'autorità di protezione dei dati personali: una pronuncia del Garante della Privacy- 8.03.2017 - .

In conformità con la posizione dominante in giurisprudenza, il Garante accoglieva la richiesta di rimozione dei contenuti lesivi da parte della ricorrente, ma non solo. Rigettando l'eccezione del *provider*, secondo cui il titolare del trattamento dei dati personali in oggetto era solo la società irlandese (Y.!E. Limited con sede in Irlanda) in quanto gestore- capo del motore di ricerca ed unico titolare del potere decisionale in ordine alle modalità di trattamento, il Garante affermava, per la prima volta, la propria giurisdizione asserendo che l'attività svolta dalla prima era funzionale a rendere economicamente redditizio il servizio reso da Y.! E. Limited.

"*Il provvedimento conferma la linea di tendenza giurisprudenziale volta a rendere quanto più accessibile ed effettiva possibile la tutela dell'individuo di fronte a casi di trattamento illegittimo dei dati personali da parte di titolari del trattamento stranieri e/o con pluralità di stabilimenti in Europa.*"[25]

Con provvedimento n. 7465315 del 21.12.2017 il Garante ha fatto un ulteriore passo in avanti, ordinando a Google di deindicizzare sia gli url

---

25 http://www.diritto24.ilsole24ore.com/art/avvocatoAffari/mercatiImpresa/2017-03-08/diritto-oblio-rete-motori-ricerca-e-ambito-giurisdizione-autorita-protezione-dati-personali-pronuncia-garante-privacy-164620.php nota di Luigi Manna, Martini Manna Avvocati – Milano

europei che extraeuropei fra i risultati di ricerca ottenuti digitando nome e cognome di un cittadino italiano.

In particolare, l'Autorità ha sostenuto che "*tali Url rimandano ad articoli anonimi gravemente offensivi della dignità e della reputazione pubblicati su forum o siti amatoriali contenenti informazioni afferenti al presunto stato di salute dell'interessato e a supposti reati gravi connessi alla sua attività di professore universitario in realtà mai commessi e per i quali non* è *stato mai indagato;* ed, ancora *che, tali notizie, proprio perché false, non recano alcuna prova dei fatti*"[26] per cui la "perdurante reperibilità" sul web di tali contenuti (incorretti e inesatti) da luogo ad una lesione "sproporzionatamente negativa" della sfera privata del ricorrente. Il Garante, inoltre, ha chiarito che *"la deindicizzazione deve essere giudicata con maggiore favore in presenza di risultati contenenti dati che sembrano avere natura oggettiva ma che sono, in realtà, inesatti, in termini reali"*, soprattutto *"se ciò genera un'impressione inadeguata o fuorviante rispetto alla persona interessata."*

[26] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7465315

Con riferimento ai presupposti in presenza dei quali non trova accoglimento da parte del Garante la richiesta di deindicizzazione, si segnala il provvedimento del 6 ottobre 2016 n. 5690378, emesso a seguito della richiesta di rimozione di alcuni url da Google, proveniente da un ex consigliere comunale coinvolto in un'indagine per corruzione e truffa.

Nel rigettare la richiesta, l'Autorità, alla luce delle Linee guida dei Garanti europei, ha rilevato che, *"nonostante il decorso del tempo dall'accadimento dei fatti, sussiste il preponderante interesse pubblico al reperimento di notizie relative a reati particolarmente gravi, quali quelli commessi dal ricorrente a danno della sanità regionale, atteso anche l'attuale interesse dei mezzi di comunicazione di massa e dell'opinione pubblica verso tutti i reati contro la pubblica amministrazione che rende le notizie in questione ancora attuale*" ed aggiunge che, *"come riportato anche nelle Linee Guida, il c.d. diritto all'oblio non sussiste rispetto a "reati più gravi" quali sono i crimini di cui si è reso protagonista il ricorrente; e ciò, nonostante la pena a carico del ricorrente sia stata interamente condonata per effetto dell'indulto"*[27].

[27] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/5690378

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

Giurisprudenza nazionale

Con la sentenza del 3 dicembre 2015 n. 23771 il Tribunale di Roma, in conformità con gli orientamenti giurisprudenziali europei rigettava le richieste del ricorrente volte ad ottenere la deindicizzazione di quattordici links risultanti da una ricerca a proprio nome effettuata tramite Google ed in cui si faceva riferimento ad una vicenda giudiziaria che lo vedeva coinvolto, unitamente ad altri personaggi romani (tra cui, esponenti del clero ed appartenenti alla cd. banda della Magliana) in presunte truffe e guadagni illeciti.

La decisione in esame presenta profili di interesse in quanto costituisce la prima attuazione, da parte della giurisprudenza di merito, dei principi elaborati dalla Corte di Giustizia UE nella celebre sentenza Google Spain. Richiamando la pronuncia europea, il tribunale capitolino sosteneva che gli utenti non potessero ottenere dal gestore del motore di ricerca la cancellazione dai risultati di una notizia che li riguardasse qualora questa fosse recente e di rilevante interesse pubblico, in quanto il diritto all'oblio, deve comunque essere bilanciato con il diritto di cronaca e con l'interesse pubblico a rinvenire notizie sul web attraverso *links* forniti dal motore di ricerca. Infatti, in linea di principio, se è vero che i diritti fondamentali di cui sopra prevalgono sull'interesse economico del

gestore del *engine search*, nonchè sull'interesse del pubblico a reperire un' informazione, è altresì vero che, in presenza di particolari presupposti, come nella fattispecie in oggetto, tra cui, il ruolo ricoperto da tale persona nella vita pubblica nonchèla natura piuttosto recente delle notizie indicizzate (i fatti narrati erano relativi a vicende avvenute poco più di due anni prima), è da escludersi la sussistenza di un diritto alla deindicizzazione delle informazioni e deve quindi ammettersi l'ingerenza nei diritti fondamentali dell'interessato.

La seconda questione affrontata dal Tribunale di Roma è relativa alle doglianze del ricorrente in merito alla falsità delle notizie riportate dai siti web che compaiono tra i risultati del motore di ricerca.

In particolare, il tribunale ha chiarito che *"il ricorrente non può dolersi della falsità delle notizie riportate dai siti visualizzabili per effetto della ricerca a suo nome, non essendo configurabile alcuna responsabilità al riguardo da parte del gestore del motore di ricerca (nella specie Google), il quale opera unicamente quale "caching provider" ex art. 15 d.lgs. n. 70/2003: in tale prospettiva pertanto il medesimo avrebbe dovuto agire a tutela della propria reputazione e riservatezza direttamente nei confronti dei gestori dei siti terzi sui quali è avvenuta la pubblicazione del singolo articolo di cronaca, qualora la predetta notizia non sia stata riportata*

fedelmente, ovvero non sia stata rettificata, integrata od aggiornata coi successivi risvolti dell'indagine, magari favorevoli all'odierno istante (il quale peraltro deduce di non aver riportato condanne e pro- duce certificato negativo del casellario giudiziale). (…) In conclusione, nell'ottica del sopra menzionato bilanciamento, l'interesse pubblico a rinvenire sul web, attraverso il motore di ricerca gestito dalla resistente, notizie circa il ricorrente deve prevalere sul diritto all'oblio dal medesimo vantato."

Come fare per ottenere la cancellazione dei propri dati dai risultati di Google?

Sicuramente il metodo più semplice e risolutivo per esercitare il diritto all'oblio di cui si è titolari è inviare una diffida al titolare dei contenuti, ossia il giornale web ovvero il motore di ricerca, chiedendo la rimozione della pagina, l' eliminazione del tag che consente l'indicizzazione o la rimozione del proprio nome (e dei relativi tag).

"Big G."[28] offre un'apposita sezione, all'interno dell'area di supporto legale, per spiegare agli utenti come presentare la "Richiesta di

[28]https://quifinanza.it/lavoro/google-online-form-per-cancellarsi-adesso-faccia-anche-facebook/3155/

rimozione di risultati di ricerca ai sensi della legislazione europea per la protezione dei dati personali" qualora ritengano che i links indicizzati dal motore di ricerca contengano informazioni *"inadeguate, irrilevanti o non più rilevanti, o eccessive in relazione agli scopi per cui sono stati pubblicati.*

Attraverso la compilazione di un modulo web, cui segue la risposta automatica che conferma la ricezione della richiesta, il motore di ricerca valuta, caso per caso, i presupposti per l'accoglimento dell'istanza, bilanciando i diritti sulla privacy della persona con il diritto della generalità dei consociati di conoscere e distribuire le informazioni". In particolare, "*se vi è un interesse pubblico a che le informazioni rimangano nei risultati delle ricerche, ad esempio se riguardano frodi finanziarie, negligenza professionale, condanne penali o una condotta pubblica in relazione a un pubblico ufficio (eletto o non eletto)"*[29].

Al momento della presentazione dell' istanza, l'utente dovrà identificarsi mediante copia digitale del proprio documento; indicare il Paese le cui leggi regolano la richiesta; identificare i risultati di ricerca che si desidera vengano rimossi e spiegare i motivi della richiesta di rimozione.

---

[29] https://www.google.com/intl/it_it/policies/faq/

Infine, al modulo dovrà essere apposta la firma elettronica dell'istante.

Secondo quanto riportato dall'articolo ItaliaOggi del 16 Gennaio 2017 di Maria Chiara Furlo[30], giornalista presso Ansa, sono quasi 41 mila le istanze di oblio indirizzate a Google negli ultimi due anni e mezzo ed oltre 133 mila il numero di pagine web (corrispondenti ad altrettanti url) che gli utenti in rapporto con l'Italia hanno chiesto a Google di rimuovere. Tuttavia, solo il 33% degli url è stato rimosso dal motore di ricerca.

Il motivo di risultati così modesti, oltre a risiedere in ragioni di carattere pratico, in particolare nella previsione legislativa che affida, almeno in prima battuta, l'amministrazione della giustizia allo stesso gestore del motore di ricerca (cfr pag.26), è riconducibile a ragioni di carattere sostanziale, infatti, secondo gli esperti, la maggior parte delle richieste non possono essere accettate perchè non trovano fondamento nella disciplina *de qua.*

In proposito, si riporta il dettato normativo del Preambolo del Gdpr nelle parti in cui si occupa del diritto all'oblio, nonché l'art.17 dello stesso che, in modo chiaro e compiuto, elenca, al I comma, i casi in cui l'interessato

[30]https://www.leggioggi.it/2016/03/09/diritto-alloblio-quando-i-nostri-dati-devono-essere-cancellati-da-internet-e-da-google/

ha diritto di ottenere la cancellazione dei propri dati personali ed al III comma le circostanze in presenza delle quali il diritto ad essere dimenticati soccombe rispetto ad altri diritti o interessi ritenuti prevalenti, trattandosi infatti di un diritto non assoluto.

Al comma II, invece, viene disciplinato l'obbligo di cancellazione a carico del titolare del trattamento che abbia reso pubblici dati personali.

Nel Preambolo del Gdpr il diritto all'oblio risulta oggetto di tre considerando:

(65) Una persona fisica dovrebbe avere il diritto di rettificare i dati personali che la riguardano e il "diritto all'oblio", se la conservazione di tali dati non è conforme al presente regolamento o al diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento. In particolare, l'interessato dovrebbe avere il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al presente regolamento. Tale diritto è in particolare rilevante se l'interessato ha

dato il proprio consenso quando era minore, e quindi non pienamente consapevole dei rischi derivanti dal trattamento, e vuole successivamente eliminare questo tipo di dati personali, in particolare da Internet. L'interessato dovrebbe poter esercitare tale diritto indipendentemente dal fatto che non è più un minore. Tuttavia, dovrebbe essere lecita l'ulteriore conservazione dei dati qualora sia necessaria per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, per finalità di archiviazione nel pubblico interesse, per finalità di ricerca scientifica e storica o finalità statistiche o per accertare, esercitare o difendere un diritto in sede giudiziaria.

(66) Per rafforzare il "diritto all'oblio" nell'ambiente on line, è opportuno che il diritto di cancellazione sia esteso in modo da obbligare il responsabile del trattamento che ha pubblicato dati personali a informare i responsabili del trattamento che stanno trattando tali dati affinché cancellino qualsiasi link verso tali dati personali o copia o riproduzione di detti dati. Per garantire l'informazione sopramenzionata, è opportuno che il responsabile del trattamento prenda misure

ragionevoli, tenuto conto della tecnologia disponibile e dei mezzi a sua disposizione, anche di natura tecnica, per informare i responsabili del trattamento che stanno trattando i dati della richiesta dell'interessato.

(125) Gli Stati membri dovrebbero essere autorizzati a fornire, a particolari condizioni e in presenza di adeguate garanzie per gli interessati, specifiche e deroghe relative ai requisiti in materia di informazione, alla rettifica, alla cancellazione, al diritto all'oblio, alla limitazione del trattamento e al diritto alla portabilità dei dati, nonché al diritto di opporsi in caso di trattamento di dati personali per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche.

Articolo 17

Diritto alla cancellazione ("diritto all'oblio")

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

a) i dati non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b) l'interessato ritira il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro motivo legittimo per trattare i dati;

c) l'interessato si oppone al trattamento dei dati personali ai sensi dell'articolo 19, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento dei dati personali ai sensi dell'articolo 19, paragrafo 2;

d) sono stati trattati illecitamente;

e) i dati devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento;

f) i dati sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1. bis.

Il responsabile del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione prende le misure

ragionevoli, anche tecniche, per informare i responsabili del trattamento che stanno trattando i dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento dei dati personali sia necessario:

a) per l'esercizio del diritto alla libertà di espressione e di informazione;

b) per l'adempimento di un obbligo legale che richieda il trattamento dei dati personali previsto dal diritto dell'Unione o degli Stati membri cui è soggetto il responsabile del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il responsabile del trattamento;

c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e h ter), e dell'articolo 9, paragrafo 4;

d) per finalità di archiviazione nel pubblico interesse o per finalità di ricerca scientifica e storica o per finalità statistiche conformemente all'articolo 83, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il

conseguimento delle finalità di archiviazione nel pubblico interesse o delle finalità di ricerca scientifica e storica o finalità statistiche;

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

In sintesi, a seguito dell'introduzione del Gdpr, il diritto "all'oblio", nato dalla giurisprudenza delle corti nazionali e sovranazionali, trova una legittima collocazione e si configura come un diritto rafforzato e assistito da garanzie ulteriori rispetto a quelle previste dall'art.7 comma 3, lettera b), del Cdp, in particolare, la garanzia di una maggiore trasparenza nel trattamento dei dati e la possibilità di esercitare un effettivo controllo sulla circolazione degli stessi, diritto, quest'ultimo, da intendersi come piena realizzazione del principio di autodeterminazione informativa.

È, inoltre, previsto che la violazione delle norme del Regolamento dia luogo all'inflizione di sanzioni amministrative severe e corpose nonché, ai sensi dell'art 82, del diritto al risarcimento del danno in favore di chi subisca un danno materiale o immateriale. Si tratta di multe divise in due categorie: le prime prevedono a 10 milioni di euro o al 2% del fatturato, le seconde fino a 20 milioni di euro o al 4%del fatturato.

Collegato al diritto all'oblio, è poi previsto l'obbligo per il titolare del

trattamento di comunicare l'eventuale richiesta di cancellazione dei dati a tutti quelli che li stanno trattando; vale a dire gli altri titolari che trattano i dati personali cancellati, compresi "*qualsiasi link, copia o riproduzione" (* art. 17, paragrafo 2*)*[31].

Secondo gli esperti della "*privacy revolution*" quest'ultima sarebbe la vera novità del GDPR sul diritto all'oblio in quanto non solo impone al titolare del trattamento di cancellare i dati (sempre che ritenga la richiesta legittima), ma anche, "*tenuto conto della tecnologia disponibile e dei costi di attuazione*", di adottare "*misure ragionevoli, anche tecniche"* per informare della richiesta che gli è pervenuta anche gli altri eventuali titolari che stanno utilizzando i dati a lui resi pubblici.

Infatti, la stessa pubblicità del dato comporta che esso possa essere trattato da altri, che assumono così la veste di titolari[32].

Ciò configura il titolare come un intermediario necessario che ha l'obbligo di segnalare ad altri titolari di cui è a conoscenza l' istanza di cancellazione, sempre che l'interessato non si sia limitato a chiedere solo la cancellazione dei suoi dati da parte del titolare a cui si rivolge, ma domanda la cancellazione di "qualsiasi immagine, copia o riproduzione

[31] http://www.garanteprivacy.it/diritti-degli-interessati
[32] https://www.agendadigitale.eu/sicurezza/diritto-alloblio-nel-gdpr-tutte-le-novita/

dei suoi dati personali. Quindi va innanzitutto valutato l'oggetto della richiesta dell'interessato, ciononostante il titolare a cui è stata rivolta la richiesta ha solo il dovere di segnalazione, e non anche quello di accertarsi del comportamento degli altri titolari e di informare di questo l'interessato[33].

Chiaramente, anche il dovere di segnalazione trova un limite negli strumenti disponibili e nei costi di attuazione che devono essere "*ragionevoli*". L'obbligo di segnalazione può dunque variare, almeno per quanto riguarda le modalità di attuazione, anche sulla base della tecnologia a disposizione.

[33] Pizzetti F., in "Diritto all'oblio nel Gdpr, ecco tutte le novità", in www.agendadigitale.eu.

Il diritto alla portabilità dei dati

L'articolo 20 del Regolamento generale sulla protezione dei dati (RGPD) introduce il nuovo diritto alla portabilità, considerato tra i più ampi diritti individuali previsti dalla nuova disciplina sulla protezione dei dati personali.

La portabilità dei dati di carattere personale, consente agli utenti, ai dipendenti ed, in generale, a qualunque persona i cui dati sono trattati, di recuperare i propri dati personali in un formato strutturato, di uso comune, leggibile da un dispositivo automatico ed interoperabile, al fine di conservarli su un proprio supporto o un *cloud* privato in vista di un utilizzo ulteriore per scopi personali ovvero di trasferirli ad un altro titolare.

In base alle linee guida pubblicate il 13 dicembre 2016 dal Gruppo di lavoro ex art. 29[34] gli obiettivi della innovativa previsione, si riassumono nei seguenti punti:

- facilitare il più possibile il passaggio e lo scambio dei dati da un ambiente informatico ad un altro, "e*vitando fenomeni di "lock-in" tecnologico e*

[34] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6064410

promuovendo la libera circolazione dei dati all'interno dell'UE e favorendo altresì la concorrenza tra i titolari del trattamento[35]*";*

- consentire la creazione di nuovi servizi nel quadro della strategia dell'Ue per il mercato unico digitale;
- offrire la possibilità di «riequilibrare» il rapporto fra interessati e titolari del trattamento tramite l'affermazione dei diritti e di controllo spettanti agli interessati in rapporto ai dati personali che li riguardano.

L' articolo 20 paragrafo 1 indica le condizioni necessarie affinché il diritto possa essere esercitato, in particolare recita:

Articolo 20

Diritto alla portabilità dei dati (C68)

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggi- bile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

[35] https://www.tomshw.it/gdpr-cos-il-diritto-portabilita-dati-come-garantirlo

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o del- l'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del para- grafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

Con riferimento all' "*interesse pubblico*" di cui al paragrafo III dell'art. 20 e del considerando 68 del GDPR, il diritto non può essere esercitato quando il trattamento dei dati personali è necessario per l'adempimento

di un obbligo legale cui è soggetto il titolare del trattamento ovvero l'esecuzione di un dovere cui è tenuto il titolare del trattamento[36].

Il diritto non può essere esercitato quando abbia ad oggetto i dati *derivati* ed i dati *inferenziali,* vale a dire quei dati creati dal titolare sulla base delle informazioni "fornite dall'interessato". Si tratta ad esempio, dell'esito di una valutazione concernente la salute di un utente o il profilo creato nell'ambito di disposizioni in materia finanziaria e di gestione del rischio volto ad attribuire uno *score* creditizio o di ottemperare alla normativa antiriciclaggio). Ciononostante, ricorda il Gruppo dei Garanti europei, "l'interessato può sempre esercitare il "*diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali, nonché informazioni riguardanti "l'esistenza di decisioni automatizzate, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze*

[36]http://www.altalex.com/documents/news/2016/12/21/privacy-nuovo-regolamento-ue-prime-linee-guida-dei-garanti-europei

previste di tale trattamento per l'interessato", in base all'articolo 15 del RGPD (relativo al diritto di accesso)." [37]

Inoltre, non sono oggetto del diritto alla portabilità i dati anonimi. Tuttavia, un dato pseudonimo chiaramente riconducibile all'interessato (per esempio, attraverso la messa a disposizione da parte dello stesso del rispettivo elemento di identificazione) è senza dubbio soggetto all'esercizio del diritto alla portabilità.

Sono altresì esclusi i dati oggetto di un trattamento che non si fondi sul consenso o su un contratto. Per esempio, alla luce delle disposizioni del WP29, non sussiste alcun obbligo per gli istituti finanziari di ottemperare ad una richiesta di portabilità relativa a dati personali che sono oggetto di trattamento nell'ambito degli obblighi di prevenzione e accertamento del reato di riciclaggio o di altri reati finanziari; allo stesso modo, il diritto alla portabilità non si applica alle informazioni di contatto di natura professionale che siano trattate nel contesto di relazioni d'impresa, se tale trattamento non si fonda sul consenso dell'interessato o su un contratto di cui quest'ultimo sia parte.

[37] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb display/docweb/6058842 - pg.11 -

Pertanto, il diritto alla portabilità può essere esercitato se i dati personali sono stati forniti in modo consapevole e attivo da parte dell'interessato (attraverso la manifestazione preventiva del suo consenso, ad esempio i dati di registrazione – come l'indirizzo postale ed il nome utente- con la compilazione di un modulo o la stipulazione di un contratto di cui lo stesso è parte) ovvero sono diventati oggetto di trattamento a seguito di attività da lui svolte, quali la fruizione di un servizio o l'utilizzo di un dispositivo (si pensi ai dati personali osservati e registrati, attraverso i *cookies*, sulla base delle attività svolte online da parte dell'utente come quelli generati dalla cronologia di navigazione su un sito web, dalle ricerche effettuate ovvero da un contatore intelligente e dagli oggetti connessi, come la frequenza cardiaca registrata da dispositivi sanitari o di fitness) e sempre che siano trattati attraverso strumenti automatizzati (sono quindi esclusi gli archivi e registri cartacei ed, in generale, ogni dato trattato mediante intervento umano.)

Al fine di garantire l'esercizio della portabilità, grava sul titolare l'obbligo, ex artt. 13 e 14 GDPR, di informare gli interessati dell'esistenza del diritto in questione. Qualora i dati siano raccolti direttamente presso l'interessato, l'informativa deve essere fornita "nel momento in cui i dati personali sono ottenuti", se, invece, i dati personali non sono stati

ottenuti direttamente dall'interessato, il titolare deve fornire l'informativa nei termini previsti dal RGPD, in particolare, ai sensi dell'articolo 14, paragrafo 3, entro un termine ragionevole e comunque non superiore a un mese dall'ottenimento dei dati, in occasione della prima comunicazione con l'interessato ovvero al momento della comunicazione dei dati a terzi.

Ai sensi degli artt. *de quo* l'informativa dovrà essere *"concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro"* .

Inoltre, ogni titolare sarà obbligato ad informare gli utenti della possibilità di esercitare il diritto alla portabilità prima della chiusura di un account o del termine di un trattamento (al fine di non perderli definitivamente).

Ad ogni modo, l'esercizio del diritto alla portabilità dei dati non pregiudica nessuno degli altri diritti dell'interessato, che può, per esempio:

- continuare a fruire del servizio offerto dal titolare anche dopo un'operazione di portabilità;

- esercitare il diritto di cancellazione, ai sensi dell'art. 17 del regolamento.

Quando tecnicamente possibile, è altresì ammessa la possibilità che, su richiesta espressa dell'interessato, il titolare del trattamento trasmetta direttamente i dati personali dell'utente all'azienda concorrente. (paragrafo 2, Art.20 GDPR),

È dunque prioritario per i titolari del trattamento impostare un processo che permetta di rispondere in modo efficace alle richieste di trasferimento dati.

La *fattibilità tecnica* prevista ex art 20 deve essere valutata caso per caso in rapporto alla situazione specifica; in linea generale, si ritiene che il passaggio diretto tra titolari debba avvenire solo quando sia possibile garantire una comunicazione sicura tra i sistemi ed il destinatario dei dati sia tecnicamente in grado di ricevere quanto trasmesso.

Dal punto di vista pratico, gli esperti del settore si sono già interrogati in ordine alle modalità di selezione e di trasmissione dei dati.

I problemi sono tutt'altro che banali. In primo luogo, bisogna escludere che i dati diversi da quelli forniti dall'utente siano oggetto dell'obbligo di trasmissione. Si tratta dei dati frutto di una rielaborazione da parte del titolare del trattamento o, ancora, di quelli relativi a segreti industriali,

ad informazioni riservate e sulle quali l'azienda detiene diritti di proprietà intellettuale.

In secondo luogo, è necessario considerare che se questa categoria di dati dovesse inopportunamente essere trasmessa, il primo titolare darebbe un vantaggio ad un proprio concorrente senza che questi non ne avesse diritto e, soprattutto, in assenza di previsione dal diritto alla portabilità.

A titolo esemplificativo, dovranno "*essere rese portabili le liste di brani musicali ascoltati tramite un servizio di streaming musicale, mentre dovranno essere esclusi tutti i dati che sono derivati o dedotti dal titolare del trattamento dai dati personali forniti dall'interessato, ad esempio quei dati prodotti da un algoritmo attraverso un'attività di profilazione".*[38]

Dunque è necessario che i titolari del trattamento si dotino di un sistema di *data managment* che riesca ad avere accesso alle diverse banche dati dell'azienda per selezionare adeguatamente i dati da trasferire. Per estrarre dai *database* solo alcune parti dal *set* di dati, i Garanti consigliano l'utilizzo di una messaggistica sicura (server SFTP o WebAPI

[38] https://www.privacyitalia.eu/diritto-alla-portabilita-dei-dati-le-novita-del-gdpr/6526/

sicuri[39]) ovvero la creazione di sistemi che consentano di scaricare autonomamente le informazioni e di trasmetterle direttamente ad un diverso titolare, ad esempio tramite un'interfaccia di programmazione di applicazioni (API - interfaccia di programmazione di applicazioni) o, ancora, di mettere a disposizione dell'interessato un servizio di deposito e memorizzazione dei dati. Gli esperti sottolineano la necessità di consentire altresì la trasmissione, insieme ai dati, della maggiore quantità possibile dì metadati, per proteggere la semantica specifica delle informazioni.

Inoltre, ai sensi dell' art. 20, paragrafo 4 ed in base al considerando 68 del RGPD, *"qualora un certo insieme di dati personali riguardi più di un interessato, il diritto di ricevere i dati personali non deve pregiudicare i diritti e le libertà degli altri interessati in ottemperanza del regolamento*". Pertanto, se i dati oggetto della richiesta di portabilità contengono informazioni personali riferite a terzi, l'interessato richiedente potrà ottenerli soltanto nella misura in cui rimangano nella sua esclusiva

---

39 il server SFTP è un programma che permette di accettare connessioni in entrata e di comunicare con un client attraverso il protocollo FTP, vale a dire un protocollo per la trasmissione di dati che garantisce che due software in esecuzione su diverse macchine possano comunicare efficacemente; WebApi è uno strumento che permette di il dialogo tra dispositivi Bluetooth direttamente da Chrome;

disponibilità e siano utilizzati esclusivamente per finalità personali o domestiche.

Si pensi alla richiesta di portabilità rivolta ad un servizio di posta elettronica ove il titolare dovrebbe trasmettere all'interessato l'intero contenuto del registro dei messaggi in entrata e in uscita, o ad un conto corrente bancario ove sono registrate sia le operazioni del titolare del conto, sia quelle svolte da altri soggetti che abbiano, per esempio, effettuato un bonifico a favore del titolare del conto. Ai sensi del paragrafo IV dell'art.20, i dati portabili dovranno essere utilizzati dal solo interessato per contattare i terzi suddetti, oppure per disporre fini personali, come la creazione di un registro delle operazioni compiute dall'interessato sul suo conto corrente bancario.

Peraltro, una volta che l'interessato ha recuperato, per ragioni personali, i propri dati personali da un sistema online, il rischio che gli stessi siano conservati in sistemi meno sicuri di quelli di partenza è molto alto. Al fine di evitare questo rischio, l'interessato (responsabile nell' individuare ed adottare le misure idonee a garantire la sicurezza dei dati personali nel proprio sistema) dovrebbe essere sensibilizzato dal titolare mediante l'indicazione di formati, strumenti di crittografia ed altre misure di sicurezza idonee.

Redazione: redazione@giuricivile.it

Inoltre, il WP29 raccomanda ai titolari di predisporre una procedura di autenticazione che consenta di verificare che chi richiede (e riceve) i dati sia effettivamente l'interessato. Ciò non significa necessariamente dover adottare complessi strumenti di identificazione, in quanto può già essere considerato sufficiente, ad esempio, fornire il nome utente e la password, quando il trattamento è effettuato in relazione ad un account utente.

I legislatori ed i garanti europei non hanno dettato prescrizioni specifiche circa le modalità di trasmissione, lasciando una certa discrezionalità ai diversi *players* del mercato. La soluzione idonea a tutti i contesti non è univoca, ciò che è fondamentale è che il trasferimento avvenga in modo sicuro perché il soggetto che lo effettua ne è responsabile sino a quando i dati non sono presi in carico dal soggetto che li riceve.

In definitiva, dovranno essere sviluppati standard di mercato in considerazione dei diversi settori merceologici e, una volta ricevuti i dati, il nuovo titolare dovrà valutare se ha la legittimazione giuridica per poterli trattare, quindi se deve cancellare parte dei dati che gli sono stati trasmessi perché eccessivi rispetto a quelli che ha la possibilità di trattare.

Il Gdpr non fornisce indicazioni circa il formato in cui i dati devono essere trasmessi: ciascun titolare dovrà premurasi di utilizzare il formato più adeguato ad assicurare la portabilità dei dati stessi a seconda del settore specifico di attività e della richiesta interoperabilità, chiaramente, l'utilizzo di un formato standard consente ad un sistema italiano di comunicare con uno estero e viceversa. I garanti europei raccomandano che, qualora non vi siano formati di impiego comune in un determinato settore di attività o in un determinato contesto, i titolari dovrebbero fornire i dati personali utilizzando formati aperti di impiego comune (per esempio: XML).

Per superare questo gap tecnico, alla luce delle raccomandazioni del gruppo dei garanti, sarebbe opportuno "i*nstaurare forme di collaborazione tra i produttori e le associazioni di categoria, affinchè venga sviluppato un insieme condiviso di standard e formati interoperabili che permettano di rispettare i requisiti previsti dal gdpr per realizzare il diritto alla portabilità."*[40]

[40] https://www.tomshw.it/gdpr-cos-il-diritto-portabilita-dati-come-garantirlo

Secondo fonti ufficiali[41], la Commissione Europea sta finanziando delle iniziative di ricerca con l' obiettivo di trovare standard per l'interoperabilità da diffondere in Europa. Si discute altresì della possibilità che la Commissione Europea conferisca un mandato specifico alle ESO (European Standardisation Organizations) per sviluppare uno standard armonizzato a livello europeo. Tuttavia, ad oggi, una tale richiesta ufficiale non è stata ancora formulata.

Con riferimento alla tempistica per ottemperare a una richiesta di portabilità, l'articolo 12, paragrafo 3, dispone che il titolare fornisce le "*informazioni relative all'azione intrapresa"* dall'interessato "*senza ingiustificato ritardo*" e comunque "*entro un mese dal ricevimento dalla richiesta*" ovvero, in casi di particolare complessità, entro il termine massimo di tre mesi, purché l'interessato venga informato delle motivazioni di tale proroga entro un mese dal ricevimento della richiesta iniziale. Inoltre, le linee guida evidenziano l'opportunità di indicare la tempistica normalmente applicabile alla gestione delle richieste di portabilità informandone gli interessati.

[41] https://www.agendadigitale.eu/cittadinanza-digitale/diritto-alla-portabilita-dei-dati-personali-ecco-come-funzionera/

In presenza degli impedimenti indicati dallo stesso Regolamento, come ad esempio in caso di trattamento connesso all'esercizio di pubblici poteri, la richiesta dell'interessato potrà essere respinta dal titolare del trattamento.

Qualora sussistano ostacoli di natura tecnica, giuridica, o finanziaria, il titolare può altresì evitare o rallentare la trasmissione. In ogni caso, il diniego dovrà essere espresso entro il termine massimo di un mese dalla ricezione della richiesta e dovranno essere indicati all'interessato

i motivi del rifiuto e la possibilità di presentare reclamo all'autorità di controllo ovvero di ricorrere all'autorità giudiziaria. In caso di reclamo, opererà un'inversione dell'onere della prova di talchè sarà compito del titolare dimostrare la legittimità del proprio diniego.

In ogni caso, l'art. 12 vieta al titolare di addebitare oneri all'interessato per la fornitura dei dati personali, salvo dimostrare il carattere manifestamente infondato o eccessivo delle richieste "in particolare per il loro carattere ripetitivo [42]".

Una volta che i dati siano stati correttamente trasmessi, sarà compito del titolare ricevente garantirne la conformità al GDPR, in particolare che

[42] http://ec.europa.eu/justice/data-protection/index_en.htm

i dati a lui forniti siano *pertinenti* e *non eccedenti* rispetto al nuovo trattamento svolto, che l'interessato sia stato informato con chiarezza delle finalità di tale nuovo trattamento e, più in generale, che siano rispettati tutti i principi in materia così come fissati dal regolamento[43].

In ordine alla non eccedenza dei dati, le linee guida contemplano, a titolo esemplificativo, la possibilità che l'istanza di portabilità sia rivolta ad un servizio di posta elettronica via web; in questo caso, se la richiesta ha il solo fine di consentire all'interessato il recupero dei messaggi di posta elettronica inviandoli ad una piattaforma di archiviazione, il nuovo titolare non potrà né dovrà` trattare le informazioni di contatto dei soggetti con cui l'interessato ha scambiato messaggi.

Dunque, allorchè il titolare originario abbia adottato idonee misure dirette a ridurre i rischi della portabilità, le responsabilità in merito ai futuri trattamenti graveranno sul nuovo titolare ovvero sullo stesso interessato.

Qualora il trattamento dei dati oggetto della richiesta di portabilità sia affidato ad un responsabile, il contratto stipulato con quest'ultimo ai

---

[43] WP242 ALLEGATO – Domande frequenti
http://194.242.234.211/documents/10160/5184810/Allegato+al+documento+WP242+–+FAQ.pdf

sensi dell'articolo 28 del RGPD deve prevedere l'obbligo di assistere "*il titolare del trattamento con misure tecniche e organizzative adeguate (...) nel dare seguito alle richieste di esercizio dei diritti dell'interessato*". Pertanto, il titolare è tenuto a implementare procedure specifiche, in collaborazione con gli eventuali responsabili del trattamento, al fine di rispondere a richieste di portabilità.

In presenza di contitolari del trattamento, le responsabilità attribuite a ciascun contitolare con riguardo alla gestione delle richieste di portabilità dovranno essere specificate con chiarezza in uno strumento contrattuale[44].

In considerazione della portata del diritto *de quo* e della dimensione assunta dai dati nell'economia globale, ci si è chiesto se il diritto alla portabilità possa rappresentare un vantaggio per il business delle aziende.

Secondo gli operatori del settore, in un' epoca in cui i dati sono un *asset* di immenso valore, il diritto alla portabilità rappresenta un importante strumento di competitività: le aziende, soprattutto quelle di recente costituzione, recuperando i gap di *history* di dati dei nuovi clienti ed

[44] http://194.242.234.211/documents/10160/5184810/Linee-guida+sul+diritto+alla+portabilità+dei+dati+-+WP+242.pdf

incentivandoli a trasmettergli i propri dati (ad esempio, offrendogli particolari incentivi in cambio dell'esercizio della portabilità dei propri fornitori) possono tracciare un profilo dei propri utenti dettagliato, quindi offrire un servizio sempre più *customizzato* .

Un esempio concreto di recupero di dati personali su un dispositivo nella propria disponibilità in vista di un successivo utilizzo personale, è rappresentato dal *social network* Facebook che, tramite la sezione "impostazioni" della pagina, offre la possibilità agli utenti di scaricare una copia dei propri dati e creare un archivio dati in un file zippato. Si tratta della cronologia delle conversazioni avute in chat, dei messaggi inviati e ricevuti, del numero della carta di credito utilizzata per fare acquisti dall'app, e delle ricerche effettuate sulla piattaforma. In totale, il tracciamento dei dati raggiunge 70 categorie.

Da ciò si evince come sin dall'iscrizione Facebook conservi e si alimenti delle nostre tracce digitali.

A tal proposito, Claudio Agosti, fondatore di Hermes (Centro per la trasparenza e i diritti digitali in rete) commentando la portata del nuovo diritto ha sostenuto che "*non c'è alcuna garanzia del fatto che i dati, anche se trasmessi all'interessato, non vengano poi utilizzati dagli algoritmi dei big data per capire meglio l'utente e la società a lui*

circostante, perchè una volta che i dati vengono presi sono, in realtà, permanenti. Ci sono infiniti livelli di "copia per motivazione tecnologica o di analisi" che impongono di essere realisti e considerare che una volta che il dato è stato fornito è andato perso"[45].

Ciò trova conferma nelle Faq in ordine alla portabilità a cui risponde il Garante ove si afferma che *"la portabilità non comporta la cancellazione automatica dei dati conservati nei sistemi del titolare e non incide sul periodo di conservazione previsto originariamente per i dati oggetto di trasmissione a seguito dell'esercizio del diritto alla portabilità."* [46] . In ogni caso, è fatta salva la possibilità per l'interessato di esercitare il diritto di cancellazione, senza che il titolare possa procrastinare o negare tale diritto facendo valere l'esercizio del diritto alla portabilità.

[45] http://www.intoscana.it/it/dettaglio-video/la-protezione-dei-dati-dalla-portabilita-al-senso-etico/

[46] WP242 ALLEGATO – Domande frequenti http://194.242.234.211/documents/10160/5184810/Allegato+al+documento+WP242+–+FAQ.pdf

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

Una nuova figura di garanzia di tutela dei dati: il Responsabile Dati personali

Tra le più attese e significative novità introdotte dal Regolamento Generale sulla protezione dati, in particolare dall'art.37 RGPD, spicca un soggetto manageriale: il *Data Protection officer* (DPO), cosi definito nella dizione anglosassone, tradotta come Responsabile della protezione dei dati nel nostro ordinamento (RPD). Al riguardo preme da subito segnalare che la parola "Responsabile" non deve trarre in inganno, in quanto configura un soggetto con funzioni e compiti diversi rispetto al Responsabile del trattamento[47] di cui all'art.4 punto 8 GDPR.

Si tratta di una figura chiave nell'ambito del trattamento automatizzato dei dati personali con il compito di promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, nonché di sorvegliare l'osservanza del Regolamento e di altre disposizione dell'UE degli Stati Membri relative a,la protezione dei dati (Art.39 let.b).

Continua, invece, a gravare sul responsabile del trattamento la messa in atto delle "*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato*

[47] Art.4 punto 8 "persona o organismo che tratta dati personali per conto del titolare del trattamento.

conformemente al presente regolamento" (articolo 24, paragrafo 1). La *ratio* della disciplina risiede nella presunzione legislativa per cui nessuno meglio del responsabile può individuare sistemi di protezione e metodiche adeguate a garantire la sicurezza dei dati.

Il RPD è altresi tenuto ad informare e fornire consulenza al titolare, al responsabile ed ai loro dipendenti in merito alla disciplina di protezione dei dati, nonché alla realizzazione dell'inventario ed alla tenuta di un registro dei trattamenti che gli consenta di disporre di un quadro complessivo dei trattamenti dei dati personali svolti all'interno dell'azienda.

Come segnalato in dottrina, la figura del RPD non è una novità assoluta, infatti, nonostante non fosse contemplata dalla direttiva 95/46, in molti Stati membri la nomina di un DPO costituiva già prassi consolidata. E' il caso della Germania o, ancora, dell'Inghilterra dove ha assunto e mantiene il nome di "privacy officer".

La disciplina che definisce ruoli, funzioni e competenze del RPD è collocata nel Capo IV del Regolamento, in particolare negli articoli 38 e 39 che recitano:

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

Articolo 38

Posizione del responsabile della protezione dei dati

1. Il titolare del trattamento e il responsabile del trattamento si assicurano che il respon- sabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabi- le della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica.

3. Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.

4 Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.

5. Il responsabile della protezione dei dati è tenuto al segreto o alla riservatezza in merito all'adempimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri.

6. Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi.

Articolo 39

Compiti del responsabile della protezione dei dati

1. Il responsabile della protezione dei dati è incaricato dei seguenti compiti:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del tratta- mento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la forma- zione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35;

d) cooperare con l'autorità di controllo;

e) fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

2. Nell'eseguire i propri compiti il responsabile della protezione dei dati considera debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo.

Nonostante le precisazioni di carattere normativo, il RPD rimane una figura professionale controversa, fortemente voluta in seno alla Commissione europea, ed i cui compiti e responsabilità, non sono particolarmente chiari, specialmente con riferimento ai rapporti da questo intrattenuti con altre soggetti in ambito privacy.

In particolare, i primi commentatori del Regolamento hanno segnalato come il RPD, anche se dotato di adeguati strumenti tecnici ed organizzativi, non possa essere l' unico garante della tutela dei dati all'interno dell'azienda, soprattutto se complessa.

Per garantire il rispetto del Regolamento è, quindi, necessario che siano previsti in suo supporto altri soggetti con cui creare un flusso di reportistica in grado di prevenire eventuali trattamenti illeciti dei dati, in primis il *data breach.*

Il riferimento è ai responsabili interni del trattamento che, anche se non espressamente richiamati dal Regolamento "rivivono" attraverso lo stesso e ne danno attuazione.

Si tratta di persone, preferibilmente diverse da dirigenti con posizioni strategiche, che svolgono un effettivo controllo all'interno dell'azienda e che, pertanto, già sanno come avviene il trattamento dei dati.

La nomina di figure ausiliarie rispetto al RPD è quindi indispensabile.

Allo stesso modo, è importante che venga definito un sistema di *reporting* trimestrale, semestrale o, se sufficiente, anche annuale, che consenta al RPD di fungere da collettore di informazioni, quindi, di monitorare il continuo trattamento dei dati da parte dell' azienda.

La reportistica consente al RPD di non limitarsi ad un controllo meramente interno all'azienda, ma di esternalizzarlo e porlo in essere anche al di fuori di essa, creando un sistema di monitoraggio continuo, non solo formale ma anche sostanziale idoneo a dimostrare, anche in futuro e nell'ottica del principio dell'*accountability*, che l'azienda abbia adottato tutte le misure tecniche ed organizzative adeguate per il corretto trattamento dei dati da parte della stessa.

A conferma di ciò, gli esperti del settore hanno ritenuto la nascita di questa figura come funzionale al soddisfacimento del principio di *accountability* che tutte le Pubbliche Amministrazioni, compresi gli Enti pubblici Economici, sono chiamate a rispettare.

Dal punto di vista contenutistico, il principio di cui si discute consiste nella responsabilizzazione degli enti nella gestione della propria organizzazione in modo tale da garantire la piena conformità del

trattamento ai principi sanciti nel regolamento e alla legislazione degli stati membri, oltre che un approccio *risk based* che tenga conto dei rischi connessi.

Il principio della responsabilizzazione si differenzia dall'altro di comune radice di "responsabilità" . In questa dicotomia che risiede uno degli aspetti principali della riforma: mentre, ai sensi della Direttiva 95/46, l'accento cadeva sull'adempimento formale e sulle conseguenze della violazione, ora l'enfasi è posta sull'effettività ed efficacia dei comportamenti assunti e sulla prevenzione, anche attraverso la cd *privacy by design*[48], degli abusi.

In base al RGPD la nomina del RPD è obbligatoria per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino, su larga scala, categorie particolari di dati (vale a dire dati sensibili).

[48] La nozione di *privacy by design* si fonda sull'obiettivo di curare al massimo la sicurezza fin dalla progettazione, onde evitare di dover intervenire ex post quando il danno è già stato fatto.

Il WP29 ha chiarito che per autorità pubblica ed organismo di diritto pubblico, di cui non si rinviene alcuna definizione nel Regolamento, s'intendono le autorità nazionali, regionali e locali ma anche che, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico.

Non sono incluse nella nozione in esame gli organismi privati incaricati di funzioni pubbliche o che esercitino pubblici poteri in merito alle quali, tuttavia, sebbene non esista un obbligo di nomina del DPO, la stessa viene raccomandata dal Gruppo di lavoro, in quanto nello svolgimento della loro attività, quasi sempre, lasciano al singolo un margine ristretto, se non nullo, di decisione in ordine al trattamento dei propri dati personali. Si pensi al settore delle infrastrutture stradali, dei trasporti pubblici, delle forniture idriche ed elettriche. In questi casi, se nominato, le attività del RPD si estendono, a tutti i trattamenti svolti, compresi quelli che non sono connessi all'espletamento di funzioni pubbliche o all'esercizio di pubblici poteri quali, per esempio, la gestione di un *database* del personale.

Con riferimento alle "*attività principali del titolare del trattamento o del responsabile del trattamento*" di cui all'art. 37, paragrafo 1, lettere b) e c) RGPD, si riporta il considerando 97 che afferma che esse "riguardano le

sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria". Si tratta quindi delle operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento.

Il gruppo di lavoro impone un'interpretazione non restrittiva della nozione ricomprendendo anche i casi in cui il trattamento, nonostante non rappresenti il *core business* dell'azienda, si configura come inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento. E' il caso, ad esempio, dell'attività di un ospedale il cui *core* business consiste nella prestazione di assistenza sanitaria, impossibile da espletare in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne consegue che gli ospedali sono tenuti a nominare un RPD.

Anche la nozione di *"larga scala"* non trova espressa definizione nel Regolamento. Sulla base delle considerazioni degli esperti, si può ipotizzare che con tale espressione si faccia riferimento al trattamento di dati da parte di un motore di ricerca per finalità pubblicitarie; ovvero dei fornitori di servizi telefonici o al trattamento dei dati relativi ai clienti di

una compagnia assicurativa, o ancora, di geolocalizzazione per finalità statistiche.

A supporto di tali riflessioni il considerando 91, in proposito, chiarisce che "i trattamenti su larga scala mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato".

Non sono da considerarsi trattamenti su larga scala quelli posti in essere dal singolo professionista sanitario ed aventi ad oggetto i dati relativi ai propri pazienti né, per le medesime ragioni, il trattamento di dati personali relativi a condanne penali dell'assistito posto in essere dal suo avvocato.

Sarebbe comunque opportuno individuare standard idonei a specificare in termini più chiari cosa debba intendersi per larga scala in ordine alle classi di trattamento più comuni.

Per colmare queste lacune, sono intervenute le raccomandazioni del Gruppo di lavoro che individua nei fattori di seguito elencati elementi utili per stabilire se un trattamento sia qualificabile come effettuato su larga scala. In particolare:

- il numero di soggetti interessati dal trattamento;

- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

- la durata, ovvero la persistenza, dell'attività di trattamento;

- la portata geografica dell'attività di trattamento.

In ordine al concetto di *monitoraggio regolare e sistematico* degli interessati si rinvia al Considerando 24 che ricomprende nella categoria tutte le forme di tracciamento e profilazione di internet per finalità pubblicitarie .

Tuttavia, il tracciamento online va considerato solo come uno dei possibili esempi di monitoraggio del comportamento degli interessati.

Per fornire un esempio concreto di un monitoraggio "continuo ovvero ripetuto a intervalli costanti e svolto nell'ambito di una strategia, di un sistema o comunque predeterminato, organizzato o metodico" il Gruppo di lavoro fa riferimento ai trattamenti posti in essere mediante programmi di fidelizzazione o, ancora, attraverso l'utilizzo di telecamere a circuito chiuso.

La nomina del RPD spetta al titolare del trattamento, al responsabile del trattamento o anche ad entrambi a seconda dei criteri relativi all'obbligatorietà, (già visti) contemplati dal Regolamento.

Può accadere infatti che il secondo e non il primo sia obbligato a nominare un RPD. E' il caso, ad esempio, di un'azienda a conduzione familiare che si serve di un responsabile del trattamento la cui attività principale consista nella fornitura di servizi di tracciamento degli utenti del sito web dell'azienda. In questo caso, sarà il secondo e non il primo a svolgere, complessivamente, un'attività di trattamento su larga scala. Ne consegue che il responsabile dovrà nominare un DPO, mentre l'azienda in quanto tale non sarà obbligata alla nomina.

Il Regolamento contempla altresì l'ipotesi della designazione di un unico RPD per più organismi a condizione che sia dagli stessi "facilmente raggiungibile" sia fisicamente all'interno dello stabile ove operano i dipendenti, sia attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione. La raggiungibilità è prevista allo scopo di consentire al RPD, in quanto punto di contatto, la comunicazione tra gli interessati e di collaborare con le autorità di controllo. Per ragioni analoghe a quelle anzidette i dati di contatto del RPD devono essere resi secondo modi e termini previsti dal RGPD.

I dati di contatto del RPD comprendono tutte le informazioni che consentono agli interessati e all'autorità di controllo di raggiungere

facilmente il RPD. Si tratta, infatti, del recapito postale, del numero telefonico dedicato e dell' indirizzo dedicato di posta elettronica.

Più autorità pubbliche o organismi pubblici, possono, ai sensi dell'articolo 37, III par., tenuto conto della loro struttura organizzativa, delle dimensioni dell'azienda ed a seguito di un'adeguata valutazione circa la capacità di adempiere alle funzioni assegnate, designare un unico RPD.

Ai sensi dell'articolo 38 del RGPD, iI RPD deve essere coinvolto in tutte le questioni riguardanti la protezione dei dati personali attraverso comunicazioni tempestive ed adeguate da parte del titolare e del responsabile del trattamento.

A tal fine il RPD deve partecipare: alle valutazioni d'impatto sulla protezione di dati (DPIA, nell'acronimo inglese. – in particolare, esprime il proprio parere circa l'opportunità di condurre una DPIA e sul metodo con cui procedere); alle riunioni del management di alto e medio livello; ai confronti finalizzati all'adozione di decisioni che impattano sulla protezione dei dati. E' altresì previsto che il RPD venga tempestivamente consultato ogni qual volta si verifichi una violazione di dati o altro incidente.

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

Il titolare del trattamento o il responsabile del trattamento devono fornire al RPD, in proporzione al trattamento svolto, "tutte le risorse necessarie per assolvere i suoi compiti, consentire l'accesso ai dati personali e *per mantenere la propria conoscenza specialistica .*

Pertanto, dovranno essere forniti al RPD un supporto attivo da parte del *senior management* (per esempio, a livello del consiglio di amministrazione con cui mantiene un contatto diretto) e tempo sufficiente per l'espletamento dei suoi compiti. Al riguardo, è consigliabile che venga definito in percentuale il tempo lavorativo destinato alle attività di RPD, in particolare quando svolge anche altre funzioni. Gli devono essere altresì fornite adeguate infrastrutture nonché un riconoscimento ufficiale a livello aziendale (attraverso la comunicazione del suo ruolo al personale) ed una formazione permanente, mediante la partecipazione a corsi di formazione su materie attinenti alla protezione dei dati e ad altre occasioni di professionalizzazione (forum in materia di privacy, workshop, ecc.);

L'articolo 38 fissa alcune garanzie essenziali per consentire ai RPD di operare in modo indipendente e con un grado sufficiente di autonomia all'interno dell'organizzazione, anche qualora si tratti di un dipendente dell'azienda. A tale riguardo, il considerando 97 precisa che i RPD

"*dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente*"). Pertanto, il RPD non deve ricevere istruzioni sull'approccio da seguire né tantomeno essere sottoposto ad un controllo gerarchico che limiti la sua autonomia decisionale.

Ad ogni modo, come anticipato, il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e, pertanto, se assumono decisioni incompatibili con il RGPD e con le indicazioni fornite dal RPD, quest'ultimo dovrebbe avere la possibilità di manifestare e far attestare il proprio dissenso .

Per garantire l'autonomia e l'indipendenza del RPD è previsto, ex art. 38, paragrafo III, che non possa essere *rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti*". È sufficiente la mera minaccia di una penalizzazione per configurare l'ipotesi *de qua*. Le penalizzazioni di cui si discute non concernono solo la possibilità di un licenziamento o di una riduzione dello stipendio, ma anche altre situazioni, come il blocco delle progressioni di carriera, o la mancata concessione di incentivi rispetto ad altri dipendenti. Viceversa, il rapporto con il RPD sarebbe

legittimamente interrotto se sussistessero ragionevoli motivi, come gravi violazioni deontologiche.

Strettamente connesso agli obblighi di indipendenza è l'assenza di conflitti di interesse prevista ex art. 38, paragrafo 6, al RPD . Qualora il RPD sia nominato all'interno dell'azienda, il gruppo WP29 raccomanda vivamente di individuare le qualifiche e le funzioni incompatibili con quella di RPD, di prevedere i casi di conflitto di interessi e di redigere regole interne per prevenire il conflitto.

Il responsabile della protezione dei dati personali è individuato sulla base del possesso di un'approfondita conoscenza della normativa, delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative del settore merceologico in cui è chiamato ad operare.

Non sono richieste specifiche attestazioni formali ed iscrizioni in appositi albi.

In particolare, il RPD *"deve poter offrire, con il grado di professionalità adeguato alla complessità del compito da svolgere, la consulenza necessaria per progettare, verificare e mantenere un sistema organizzato di gestione dei dati personali, coadiuvando il titolare nell'adozione di un complesso di misure (anche di sicurezza) e garanzie adeguate al contesto in cui è chiamato a operare. Deve inoltre agire in piena indipendenza*

(considerando 97 del Regolamento UE 2016/679) e autonomia, senza ricevere istruzioni e riferendo direttamente ai vertici."[49]

Nella nota inviata a un'azienda ospedaliera, l'Ufficio del Garante, ricorda anche che "*nella selezione sarà poi opportuno privilegiare soggetti che possano dimostrare qualità professionali adeguate alla complessità del compito da svolgere, magari documentando le esperienze fatte, la partecipazione a master e corsi di studio/professionali (in particolare se risulta documentato il livello raggiunto). Gli esperti individuati dalle aziende ospedaliere, ad esempio, in considerazione della delicatezza dei trattamenti di dati effettuati (come quelli sulla salute o quelli genetici) dovranno preferibilmente vantare una specifica esperienza al riguardo e assicurare un impegno pressoché esclusivo nella gestione di tali compiti."* Il RPD può essere un dipendente aziendale, non in conflitto d'interessi, nominato mediante specifico atto di designazione, o un soggetto esterno che operi in base ad un contratto di servizi

L'atto di designazione ovvero il contratto, dovranno indicare espressamente i compiti attribuiti al RPD, le risorse che gli vengono assegnate, nonché ogni altra utile informazione in rapporto al contesto di

[49] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8036793

riferimento.

Più in generale, nell'esecuzione dei propri compiti, il responsabile della protezione dei dati personali (interno o esterno) deve ricevere supporto adeguato in termini di risorse finanziarie, infrastrutturali e, ove opportuno, di personale. A tal fine, nelle realtà organizzative di medie e grandi dimensioni, il responsabile della protezione dei dati personali, da individuarsi comunque in una persona fisica, può essere supportato anche da un ufficio.

Il responsabile della protezione dei dati personali esterno all'azienda può essere anche una persona giuridica (v. il punto 2.4 Linee guida), salvo individuare in modo chiaro una sola persona fisica che funga da punto di contatto con gli interessati e l'Autorità di controllo.

Nell'ottica del nuovo Regolamento, quest'ultima mantiene inalterato il suo ruolo, primario e centrale, di controllo ma riveste altresì quello di guida efficace, *"quasi un educatore nel difficile passaggio alla responsabilizzazione".* [50]

[50] http://www.mondoprivacy.it/blog/regolamento-europeo-privacy/principio-accountability-significato-funzione-educatrice/

In ultimo, un interessante quesito, sorto in occasione delle riflessioni di Monica Perego, docente qualificato da Tuv Italia per il Master Privacy Officer di Federprivacy, durante la VI edizione del Privacy Day Forum[51]:

il Dpo è oggetto ad un'attività di Audit?

Il Regolamento non dice nulla in merito ai controlli da effettuarsi su questa figura, limitandosi ad affermarne l'autonomia ed a vietare che sia sottoposta ad istruzioni.

Secondo l'esperta privacy, premesso che l'audit su tutti i processi aziendali è uno strumento di garanzia del nostro sistema, un controllo sulla qualità dell'ampia attività svolta dal RPD e sui processi a cui ha preso parte è da considerarsi imprescindibile, viceversa si tratterebbe di una figura autoreferenziale.

Per risolvere eventuali conflitti, la soluzione potrebbe risiedere nell'affidare l'audit sul RPD ad un soggetto esterno all'organizzazione o ad un soggetto non coinvolto direttamente nelle attività a carico del RPD. Dal punto di vista temporale, si raccomanderebbero due tipi di controllo. Il primo diretto a valutare lo stato di avanzamento delle misure che sono state definite dal pacchetto privacy ed un secondo, da espletarsi una

[51] https://www.youtube.com/watch?v=vjybFlBrsg8

volta che il meccanismo è entrato in regime, volto a verificare che le attività che sono a suo carico (art 39) siano effettivamente svolte.

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

Capitolo III

La Datacrazia

Il presente capitolo ha il fine di evidenziare le implicazioni giuridiche e sociali delle impattanti novità di un mondo, il nostro, ove i dati rappresentano il carburante dell'economia di mercato ed il loro trattamento, attraverso la vendita a terzi per profilare gli utenti e raggiungere al meglio i propri target, costituisce il modello di business delle compagnie più ricche del mondo.

Nella realtà della Data Economy la tutela dei dati conservati e trasferiti dai Big del web rappresenta un obiettivo di interesse primario per i singoli e la collettività.

Tecnologia e democrazia

Le responsabilità di Facebook nel "caso Cambridge Analytica", le tutele offerte dal nuovo Regolamento ed i rischi per la democrazia

Alla luce delle recenti rivelazioni dei quotidiani statunitensi *Guardian* e *New York Times* che, grazie a Christopher Wylie, giovane informatico ex dipendente dell'azienda di consulenza e marketing online

Cambridge Analytica, hanno mostrato al mondo come, tramite un. app'[52], l'azienda abbia profilato più di cinquanta milioni di utenti, appare opportuno soffermarsi sulla dimensione economica e sociale che i dati hanno assunto nella società odierna.

Il "caso Cambridge Analityca" è interessante per diverse ragioni. Bisogna soffermarsi "sull'incapacità" di Facebook di tenere sotto controllo i dati che gli utenti gli "affidano" e sulla tutela che il nuovo Regolamento offre, sulle implicazioni che l'uso dei dati può avere a livello sociale nonché politico ed, in ultimo, sull'inconsapevolezza dell' utente della sempre più elevata profilazione a cui è esposto, a causa dei contenuti, commenti, reazioni (like) ed ogni altro tipo di traccia digitale che lascia sul web.

Il padre del più importante e diffuso social network del web, Mark Zuckeberg ha, dopo tre giorni di silenzio, pubblicato il post di seguito riportato per scusarsi con gli utenti dell'accaduto.

[52] L'app. consisteva in un gioco a cui l'utente partecipava rispondendo a delle domande che hanno poi consentito la creazione di un identikit digitale. Si trattava di un mezzo per accumulare dati ufficialmente per fini scientifici. Dei 50 milioni di utenti profilati solo 270 mila avevano dato il consenso per l'utilizzo dei propri dati da parte dell'app.

"Abbiamo la responsabilità di proteggere i vostri dati, se non ci riusciamo, non vi meritiamo". (We have a responsibility to protect your data, and if we can't then we don't deserve to serve you).

Alla luce di ciò, la domanda sorge spontanea: il padre di Facebook è parte o vittima dell'operazione Cambridge Analytica?

Forti perplessità sulla sua innocenza sono sollevate da Jonathan Albright, direttore di ricerca presso il Tow Center for Digital Journalism, che denuncia un legame datato e forte tra Facebook e Alexander Kogan, matematico ideatore dell' app 'mydigitallife', e che sostiene: "*questo problema è parte di Facebook e non può essere scisso come un caso sfortunato di abuso: era una pratica standard e incoraggiata. Facebook sta letteralmente correndo verso la costruzione di strumenti che hanno aperto i dati dei propri utenti ai partner di marketing e ai nuovi business verticali*"[53].

Stando alle dichiarazioni rilasciate al giornale La stampa, nutre gli stessi dubbi Steven Livingston, professore alla School of Media and Public Affairs e alla Elliott School of International Affairs della George

53 https://it.businessinsider.com/tutto-quello-che-non-torna-nelle-scuse-di-mark-zuckerberg-a-partire-dal-numero-di-volte-che-gli-e-toccato-scusarsi/)

Washington University, che afferma: «*Bisogna tener conto che Facebook registra tutti i dettagli della nostra attività sulla piattaforma: quello che facciamo, ma anche quello che non facciamo, dove siamo e con chi siamo. Il social network è costruito così, quindi è difficile sostenere che siano vittime, il loro modello di business è vendere informazioni agli inserzionisti, e più sono precise più valgono*[54]».

La questione non è nuova e già da diversi anni si discute di come i servizi forniti dal web, apparentemente gratuiti, richiedano come corrispettivo informazioni sull'identità di chi ne usufruisce.

La "scoperta" del potere dei dati risale al 2007, quando due ricercatori dell'Università di Cambridge, David Stillwell e Michal Kosinski hanno messo a punto una app. per Facebook, myPersonality, in grado di tracciare la personalità degli utenti. In sostanza, si tratta di un modo nuovo, originale, di usare la psicometria, ovvero studiare la personalità di qualcuno quantificandola e rintracciando anche le più velate sfumature della sua persona e delle sue abitudini.

Una vera e proprio miniera d'oro per il marketing, e non solo.

---

54 http://www.lastampa.it/2018/03/25/tecnologia/news/il-caso-facebook-cambridge-analytica-pu-diventare-un-problema-anche-per-la-ricerca-scientifica-bisUklorlOndGeNYH0NDwN/pagina.html

"*La psicometria applicata ai social media ha cambiato tutto*", afferma Paul-Olivier Dehaye, matematico belga, esperto di big data, fondatore della startup svizzera PersonalData.IO che assiste gratuitamente chi vuole riavere il controllo dei propri dati sul web. «*Guardate dove sta andando la società: verso un capitalismo digitale, che offre sempre più servizi online, e verso la personalizzazione estrema di tali servizi. La psicometria ha messo insieme queste due tendenze. E adesso viene usata non solo per vendere telefonini o aspirapolveri ma anche per scatenare reazioni, per forgiare dibattiti e manipolare opinioni.*"

Il ricorso alla psicometria da parte di aziende come Cambridge Analytica , secondo alcuni esperti del mondo della politica, ha portato all'elezione del Presidente statunitense Trump e, ancora, all'uscita del Regno Unito dall'unione Europea .[55]

Alla luce delle disarmanti considerazioni e del già citato GDPR, preme chiedersi se questo sia in grado di proteggere da casi, come quelli anzidetti, di manipolazione lesivi per la democrazia.

[55] https://it.businessinsider.com/facebook-gate-la-politica-e-la-pubblicita-al-tempo-dei-big-data/

In relazione alla vicenda Brexit, essendo stati coinvolti cittadini europei, ai sensi dell'art 3 paragrafo 2 del Regolamento[56] relativo all'ambito territoriale che stabilisce l'applicabilità dello stesso ai trattamenti dei dati personali degli interessati che si trovano nell'Unione, anche se effettuati da un titolare o responsabile stabilito al di fuori del territorio europeo, la nuova disciplina è applicabile.

Con riferimento all'art 13[57] ed in particolare alla possibilità per gli sviluppatori di comunicare i dati raccolti a terzi, è richiesto che vi sia un consenso espresso che non solo manca nelle vicende di cui si discute, ma che la gran parte dei *social login*[58] attualmente presenti nel web neanche

---

56 Art.3.2 *"Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*
a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato."

57 *Articolo 13* Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato**:**
1. *In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:*
f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

58 Si tratta di uno strumento che consente di accedere ad un servizio offerto da un'applicazione di terze parti attraverso il proprio account social. L'autenticazione

contempla, limitandosi unicamente ad indicare a quali dati presenti sul social network l'app. ha accesso, senza che venga data un'informativa completa sulle finalità di trattamento.

Si consideri, inoltre, che la vicenda riguarda dati appartenenti ad una particolare categoria, vale a dire quelli relativi alle opinioni politiche degli interessati, per i quali, ai sensi rispettivamente degli artt. 9[59] e 35[60] del Regolamento, sono richiesti: l'acquisizione del consenso

presso la piattaforma di terze parti avviene attraverso i dettagli relativi all'utente conservati e forniti dalla piattaforma social scelta per il login.

[59] *Art. 9* Trattamento di categorie particolari di dati personali
1. 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.
2. Il paragrafo 1 non si applica se si verifica uno dei seguenti casi:
a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati persona- li per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1.

[60] *Art. 35* Valutazione d'impatto sulla protezione dei dati
Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del tratta-mento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'artico- lo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

preventivamente espresso da parte della persona a cui si riferiscono ed una valutazione d'impatto da parte della società produttrice.

In sua difesa Facebook ha sostenuto che non si è trattato di un *data breach*, ma di una "mera" violazione della policy privacy (ossia delle regole adottate dal social network).

Comprendere se nella nozione di *data breach* possa o meno rientrare l'uso illecito dei dati così come poc'anzi raccontato appare fondamentale ai fini dell'applicazione della disciplina.

Infatti, se configurato come una "violazione dei dati personali" ai sensi dell'art 33 GDPR, grava sul titolare l'onere di notificare, entro 72 ore dal momento in cui ne è venuto a conoscenza, la suddetta violazione all'autorità di controllo competente, nonché agli interessati, qualora la violazione, come in questo caso, possa comportare un *"rischio elevato per i diritti e le liberta fondamentali delle persone*" (art.34).

In definitiva, la comunicazione di un *data breach* si configura come un importante strumento di tutela fornito dalla nuova disciplina che consente ai destinatari di avere contezza delle violazioni dei dati e di porre in essere le misure necessarie ad attenuare le conseguenze derivanti dal protrarsi del trattamento illecito. Pertanto, dal punto di vista giuridico, per smentire la difesa di facebook e di ogni futuro

soggetto analogo, sarebbe auspicabile estendere la nozione di *data breach* anche alle ipotesi in cui il Titolare sia a conoscenza di un trattamento illecito dei dati personali che egli ha conferito a terzi.

Una soluzione in tal senso potrebbe essere sviluppata sulla base delle linee guida del 3.10.2017 del Gruppo ex.art 29 relative alla notifica delle violazioni dei dati personali[61] che chiariscono che per *data breach* debba intendersi un incidente di sicurezza che può comportare "violazione di confidenzialità" in cui si verifica un accesso o una distribuzione accidentale e non autorizzata di dati personali.

A ciò si aggiunga che, ai sensi del Regolamento, in caso di *data breach* e del mancato rispetto dell'obbligo di notifica, l'autorità di controllo può applicare sanzioni amministrative ex articolo 83, il cui importo può arrivare fino a 10 milioni di euro o, se superiore, al 2% del fatturato totale annuo dell'esercizio precedente.

È evidente che le sanzioni costituiscono un importante deterrente e che, in generale, il nuovo Regolamento rappresenti un'importante conquista per la riservatezza dei dati dei cittadini europei.

[61] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8050516

Al momento il *patron* del colosso Usa invitato dalla commissione britannica cultura digitale e media per rispondere a domande sullo scandalo ha declinato l'invito, offrendo di mandare al suo posto il chief technology officer di Facebook, Mike Schroepfer, e il chief product officer, Chris Cox.

Lo stesso invito è stato inoltrato dal Presidente dell'Europarlamento, Tajani.

Si rimane quindi in attesa degli esiti giuridici della vicenda e, riprendendo le parole del Garante europeo Giovanni Buttarelli, si invita a riflettere sulla "*crescente"pervasività degli algoritmi basati sui nostri dati personali nelle nostre vite e sull'impatto che questi hanno nei nostri processi decisionali democratici*. Il Garante europeo, inoltre, aggiunge che "*il rischio di manipolazione dei consensi elettorali potrebbe estendersi alle prossime tornate elettorali: le elezioni europee dell'anno prossimo sono un importante test per tutti noi. Non siamo qui per allarmarvi, ma il problema è reale e urgente".*

Ad alimentare le preoccupazioni in ordine alla manipolazione degli utenti attraverso l'utilizzo improprio dei loro dati, si riporta il quesito formulato, nel 2016, durante la conferenza annuale di Facebook: *"e se poteste scrivere direttamente dal vostro cervello?"*

Si tratterebbe di una vera e propria rivoluzione tecnologica messa in atto attraverso la realizzazione di un sistema collegato alla mente umana capace di tradurre i nostri pensieri in messaggi digitando più di 100 parole al minuto. L'obiettivo sarebbe quello di codificare gli input del cervello umano, bypassando la tastiera e facendoli arrivare direttamente sugli schermi dei dispositivi connessi.

Regina Dugan, capo dipartimento Hardware Facebook, specifica che non si tratterebbe di una decodificazione universale, ma dei soli pensieri che si sceglie di condividere.

Ad ogni modo, si pensa che nel giro di pochi anni questo sistema possa essere reso operativo e che leggere nel pensiero potrà non essere più fantascienza.

Un dato preoccupante se si considera che in molti hanno visto nel discorso di fine anno di Zuckemberg, diretto ai Millenial di Harward, la sua discesa in campo da politico.

Ipotesi fattasi poi più concreta all'inizio del 2018 quando ha invitato i propri seguaci a chiedere al Congresso americano di lottare contro i cambiamenti alle politiche di immigrazione degli Stati Uniti introdotti lo scorso anno da Donald Trump o, ancora, quando si è espresso in merito al reddito di cittadinanza, individuato come unica soluzione in un futuro

dominato da una tecnologia automatizzata che eliminerà migliaia di posti di lavoro[62].

Per concludere ed evidenziare la dimensione di un fenomeno dirompente come quello della profilazione degli utenti non solo per finalità commerciali, ma anche in chiave elettorale, e del ruolo dei Big del web nella società odierna, si riportano le dichiarazioni rilasciate dal Garante italiano, Antonello Soro: "*"Stiamo vivendo un cambiamento epocale per le nostre democrazie, che ci porta verso una feudalizzazione della società. Il rischio è che il potere di induzione, sociale prima che politico, dei colossi della rete sia tale da superare il potere degli Stati nell'orientamento e nella raccolta del consenso. Se così fosse, potrebbero esercitare un grande potere persuasivo nei confronti di tutto il mondo".*

Con il potere informativo che converge verso un solo destinatario", cioè le media company come Facebook, *"si sta creando una nuova geografia dei poteri, che tende a cambiare la natura delle democrazie moderne"*. Secondo il Garante della Privacy, l'affaire Facebook-Cambridge Analytica, è parte di *"un processo ineluttabile: attraverso la sempre maggiore conoscenza delle nostre propensioni, questi soggetti sono in grado di*

[62]https://tech.fanpage.it/mark-zuckerberg-a-favore-del-reddito-di-cittadinanza-l-unica-soluzione-nel-mondo-dei-robot/

consigliarci sia il prodotto da comprare sia il partito da votare. Nel gioco democratico il voto dei cittadini traduce in una scelta elettorale lo stato di consapevolezza, che si ha in quel momento, del mondo in cui vive. E se questa scelta è figlia di una lettura quotidiana e completa della realtà, allora possiamo parlare di libertà. Se invece è figlia di un meccanismo di conoscenza passiva, parziale, settoriale, con una spinta a farci sapere solo quello che è più vicino alle nostre aspettative, allora il percorso elettorale è diverso da quello che dovrebbe esprimere una democrazia compiuta"[63].

L'inconsapevolezza degli utenti come fonte di ricchezza dei Big del web e strumento di sorveglianza di massa dei governi

Opere letterarie come il Panopticon ed il Grande Fratello del romanzo 1984, elaborate da "visionari" del mondo letterario, hanno anticipato le dinamiche dei nostri tempi, omettendo solo l'inaspettato: oggi sono gli stessi sorvegliati a condividere, senza giudizio né cognizione dei rischi, "pezzi della propria identità" .

L'ideatore di Facebook durante un'intervista rilasciata ai media statunitensi, ha dichiarato che, al principio, quando ad Harvard espose ai

[63] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/8053813

suoi amici l'idea della piattaforma che avrebbe rivoluzionato il mondo, gli venne chiesto perché mai credeva che la gente avrebbe condiviso in Rete informazioni che la riguardasse. È chiaro che, è bastato poco più di un decennio per rivoluzionare la società e rendere quasi incomprensibili le ragioni di un simile interrogativo.

Oggi il web è tappezzato di tracce digitali lasciate da utenti che, con più o meno consapevolezza, si espongono a continui pericoli.

La combinazione delle attuali tendenze sociali, *in primis* il quotidiano utilizzo di mezzi di moltiplicazione dei rischi come i social network, con le nuove tecnologie (si pensi ai *weareable dispositive*) hanno cambiato il modo in cui le persone interagiscono con i dispositivi e con il mondo esterno.

I vantaggi di un sistema connesso e digitalizzato sono potenzialmente infinti e indiscutibili; l'internet delle cose (IoT) sta entrando nelle nostre auto e nelle nostre case, cambiando il nostro modo di vivere.

Gli algoritmi sono in grado di proporci scelte musicali o cinematografiche in perfetta linea con le nostre preferenze e di individuare altre persone altrettanto appassionate con cui poter stringere amicizia.

Ma, a detta di chi scrive, è necessario riflettere ed informare; il più delle volte l'utente non conosce le illibertà a cui è esposto e non è conscio della raccolta selvaggia ed incontrollata che viene fatta dei suoi dati.

Quanti km percorri ogni giorno? Cosa ne pensi di quella rassegna teatrale? Hai mai visitato Berna?

Ogni giorno l'utente risponde ad interrogativi di ogni genere posti da interlocutori di cui non sa nulla, alimentando l'asimmetria informativa e, di conseguenza, i profitti dei giganti della Rete che fanno della disinformazione degli utenti il loro modello di business più produttivo.

Inoltre, il monopolio del controllo digitale esercitato dai "nuovi" protagonisti dei mercati consente l'esercizio di un potere di influenza imparagonabile, per incidenza e diffusione, ad altri tipi di strumenti.

La chiamano "datacrazia". Si tratta di un nuovo ordine sociale basato sull'analisi e la raccolta dei dati attraverso dispositivi connessi. Tra questi, in prima fila, c'è lo smartphone che, ampiamente diffuso nelle società sviluppate, consente di accedere ad informazioni personali che vanno ben oltre quelle contenute nei nostri documenti identificativi ufficiali .

Sempre più spesso, l'istallazione di *cookies* e l'uso di metodi alternativi come il *fingerprinting* consentono di tracciare i profili dei propri utenti e

di offrirgli soluzioni commerciali confacenti alle loro esigenze ed ai loro gusti.

Le nostre abitudini di navigazione sono diventate un bene diffuso e disponibile; la moneta di scambio per l'accesso ai servizi "gratuiti" della Rete.

Le attuali tendenze sociali ("posto quindi sono") ed il calo esponenziale dei costi di *storage*[64] si riflettono sul valore delle nostre informazioni determinandone, in linea con la teoria economica secondo cui la disponibilità di un bene si riflette sul valore che gli viene attribuito, la riduzione.

Una ricerca di mercato stima che il 38% degli intervistati di età compresa tra i 18 ed i 34 anni scambierebbe volentieri il proprio consenso al trattamento dei dati personali per un abbonamento settimanale alla metro[65].

Questo scambio iniquo consente la raffinata profilazione di chi naviga, dando luogo a facilitazioni per l'utente ma anche ad un'insopportabile limitazione della sua capacità di autodeterminazione.

---

[64] Secondo il Dossier Tg2 del 7.5.2017 "Valle dei Robot", nel 2012 sono stati prodotti più dati dei 5 mila anni precedenti e la gestione e conservazione di questo oceano di informazioni avviene attraverso "le case dei dati", vale a dire magazzini *cloud* in grado di gestire le memorie di utenti sparsi ovunque.

[65] http://www.report.rai.it/dl/Report/puntata/ContentItem-0de6de4e-6351-4aad-ab94-96b1672402ac.html

Gli input che continuamente riceviamo, mediante i *banner* pubblicitari dei motori di ricerca e dei social che utilizziamo, condizionano le nostre scelte più di quanto pensiamo.

A tal proposito un forte allarme è stato lanciato dal Presidente dall'Autorità Garante della Privacy, Prof. Antonello Soro, secondo cui "*dobbiamo chiederci quante delle nostre decisioni siano in realtà fortemente condizionate dai risultati che un qualche algoritmo ha selezionato per noi e ci ha messo davanti agli occhi. Un libro, un certo viaggio, una clinica cui affidare la salute, un investimento dei risparmi, la scelta di un dipendente da assumere, un giudizio politico, la stessa fiducia nei confronti di una persona appena incontrata, della quale chiediamo subito informazioni cliccando sui motori di ricerca e la cui affidabilità siamo pronti a misurare su quanto appreso in rete*."

Con riferimento al controllo sui dati on-line, un sondaggio condotto da Eurobarometro nel 2016 mostra che l'81% dei cittadini europei non ha contezza dei dati che li riguardano presenti in Rete.

L'incapacità dell'interessato di mantenere il controllo sul flusso di informazioni accresce l'asimmetria informativa, consentendo ai monopolisti dell'economia digitale di intensificare il monitoraggio dei comportamenti in Rete. Si instaura, quindi, un circolo vizioso di cui

beneficiano pochi Big a danno di cittadini sempre più trasparenti e vulnerabili.

Il deficit culturale ed educativo da cui è affetta la società è tra le principali cause del business dei programmatori del web che, conoscendo le abitudini di navigazione dell'utente e, in particolare, la poca attenzione che questo presta nella gestione dei suoi dati, richiedono ingiustificatamente informazioni prive di funzionalità rispetto al servizio per il quale sono cedute.

Tra i tanti, si segnala una richiesta di accesso ai dati riferita all'applicazione torcia, scaricabile da un comune smartphone. Con l'installazione dell'app. si autorizza il fornitore a conoscere la nostra posizione quindi, potenzialmente, di geolocalizzarci anche quando non utilizziamo l'app. in questione.

Al fine di segnalare la poca attenzione che gli utenti prestano alle condizioni contrattuali, si richiama altresì l'esperimento sociale messo a punto da Peter Warren, Direttore di Future Intelligence, attraverso l'istallazione nel centro della capitale britannica di una rete wi-fi.

Dagli studi è emerso che, per accedere gratuitamente ad internet, le persone non hanno remore a sottoscrivere condizioni di utilizzo che

implichino la cessione del proprio primo genito, o ancora, la vendita della propria anima per utilizzare un gioco on-line.

Le deduzioni che se ne traggono non sono meramente sociali, con riferimento alle abitudini negative degli utenti, ma anche giuridiche.

I contratti e le relative clausole sono troppo spesso lunghi e poco chiari e tra le tante pagine dell' accordo il cliente si limita a cercarne solo una: l'ultima, per apporre un click ed accettare un'intrusione, di portata più o meno ampia, nella propria sfera privata.

È chiaro che tali scelte scaturiscono dal mancato rispetto dei principi di trasparenza e chiarezza nella redazione delle condizioni dei termini contrattuali da parte dei fornitori dei servizi.

Il dato è da esaminare attraverso la contestualizzazione del fenomeno in una realtà ove i soggetti che si occupano di implementare, distribuire e gestire i dati che forniamo sono tanti e diversi. Spesso le applicazioni immesse sul mercato sono offerte da singoli che non sono in gradi di rispettare le garanzie nazionali ed europee previste a tutela dei dati detenuti, normalmente conservati in *cloud*.

Al di là dell'abuso di richiesta di permessi tramite le app., un altro esempio di come la captazione dei dati possa avvenire anche in assenza

di dispositivi connessi è offerto dai totem pubblicitari installati nelle principali stazioni ferroviarie italiane.

La scoperta è stata fatta da un ingegnere informatico che ha spiegato come la videocamera di alcuni schermi misuri il grado di attenzione prestata dal consumatore, le sue caratteristiche e le più probabili preferenze d'acquisto.

Il sospetto è che i dati raccolti vengano venduti alle agenzie di marketing per proporre gli *advertising* più appropriati, per capire quanto siano efficaci le loro campagne pubblicitarie o per mettere a punto nuovi spot.

Al riguardo, è intervenuto il Garante della Privacy sostenendo che *"sebbene il sistema attuale non consenta il riconoscimento facciale dei passanti, né il loro monitoraggio o tracciamento, i passanti che guardano le pubblicità proiettate sui totem dovranno essere informati sulla presenza di una telecamera che analizza le loro reazioni in quanto, anche se per un brevissimo lasso di tempo, prima della immediata sovrascrittura delle immagini, effettua comunque un trattamento di dati personali."*[66] Ulteriore prova delle conseguenze sociali dell'uso della tecnologia è la notizia dei nuovi strumenti di giustizia messi a punto nei Paesi Bassi.

[66] Garante della privacy doc. web n. 7496252.

GiuriCivile – Rivista di Diritto e Giurisprudenza civile
Fondatore, Direttore e Coordinatore: Avv. Gabriele Voltaggio

Redazione: redazione@giuricivile.it

Nel civilissimo stato del Nord Europa la polizia si avvale dei dati forniti dalla società titolare del marchio tomtom per multare i trasgressori del codice della strada.

Il Governo di Singapore, Citta-Stato con il più alto tasso di smartphone al mondo, non fa mistero circa l'utilizzo dei big data per fini di ordine pubblico. In particolare sono soggetti al controllo digitale il traffico dei veicoli in circolazione, la pulizia delle strade e tutte quelle azioni rilevanti per il benessere dei cittadini, tra queste primeggiano quelle potenzialmente pericolose per la società.

Oltre alle evidenti illibertà, il rischio è che la crescita esponenziale del controllo governativo darà luogo anche a problemi sociali relativamente allo sviluppo umano che, a causa dell'autocensure generate da un simile ordine sociale, riceverà un'inevitabile frenata.

Le persone, sentendosi perennemente controllate, si conformeranno agli standard sociali reprimendo ogni tipo di impulso distintivo e creando una generale omologazione che oscurerà la diversità, caratteristica insita nel concetto di umanità.

Al fine di arginare ed evitare simili scenari la diffusione e l'implementazione della cultura e dell' etica digitale sembrano essere gli

strumenti, oltre a quelli normativi, più potenti ed incisivi a cui possiamo affidare la tutela della nostra riservatezza.

Come suggerisce Francesco Nicodemo, esperto di comunicazione e innovazione digitale ed autore della "Disinformazia: la comunicazione al tempo dei social media", è la scuola a dover insegnare ai cittadini di domani a leggere il web, a far comprendere i rischi che Internet comporta rispetto alla privacy ed a dover dare priorità all'alfabetizzazione informatica, la *digital literacy.*

Solo con una maggiore consapevolezza da parte del cittadino del funzionamento del sistema tecnologico-economico-politico-culturale dentro il quale vive, è possibile costruire politiche e norme che possano conciliare i nuovi modelli di business e l'uso governativo dei dati con il rispetto delle sue libertà. In quest'ottica, il progressivo definanziamento della scuola e delle università in molti Paesi, compresa l'Italia, non fa ben sperare, ma questo è solo un motivo in più per continuare a lavorare per una formazione migliore e per una società fatta di cittadini più consapevoli.