CAMMINO DIRITTO
Rivista di informazione giuridica
https://rivista.camminodiritto.it

I DATI SENSIBILI AI TEMPI DEI SOCIAL NETWORK E DEL GDPR.

E' indubbio che la nostra sia un'epoca caratterizzata dai paradossi e dai rapidi mutamenti ed è proprio in questo incerto contesto che si è avuta l'emanazione del General Data Protection Regulation con la direttiva UE 2016/679 che ha trovato attuazione recentemente. Perché nell'epoca in cui ognuno con uno smartphone può condividere ogni istante della sua vita, la "riservatezza" è, invero, un diritto ancora fortemente rivendicato.

di **Simona Rossi**
IUS/13 - DIRITTO INTERNAZIONALE
Articolo divulgativo - ISSN 2421-7123

Direttore responsabile
Raffaele Giaquinto

Pubblicato, Sabato 5 Gennaio 2019

CamminoDiritto.it
ISSN 2421-7123

Sommario: 1. Il diritto alla riservatezza. – 2. La genesi del D.lgs. 196/2003. – 3. Internet, i social network ed il caso Facebook/ Cambridge Analytica. – 4. L'introduzione del GDPR.

1. Il diritto alla riservatezza.

E' proprio oggi, nell'epoca dei social network, dei mass media e della condivisione sfrenata, che sembra esservi stato il "rinascimento" del diritto alla riservatezza, sempre più rivendicato. Alla luce di un fenomeno sociologico qual è la necessità (quasi morbosa!) di condivisione della propria sfera privata, e della cui analisi non intendo di certo occuparmi in questa sede, è interessante approfondire la "riscoperta" del diritto alla privacy anche alla luce dei recenti avvenimenti.

Il diritto alla riservatezza è intrinsecamente connesso al riconoscimento dei diritti della personalità e rappresenta la consacrazione del diritto di ciascun soggetto alla propria "sfera privata" e che, in virtù del collegamento con la salvaguardia dei diritti inviolabili della personalità costituzionalmente garantiti, si configura come un bene giuridicamente protetto.

Tuttavia, va osservato, che la "consacrazione" di tale diritto non è stata automatica bensì la giurisprudenza, fino agli anni '50, sosteneva non si potesse ravvisare la sussistenza di un diritto alla riservatezza[1]; nel corso degli anni, però, inizia a consolidarsi un mutamento di tale solido orientamento, dapprima con una tiepida apertura in considerazione del diritto assoluto alla personalità[2], con l'approdo al pieno riconoscimento della "privacy" negli anni '70 in cui la S.C. riconobbe "il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico".[3]

Alla luce di tali considerazioni, è evidente come la "riservatezza" non rappresenti un diritto a sé stante bensì risulti indissolubilmente connesso a tutta una serie di diritti, tanto da configurarsi come strumentale alla tutela di diritti quali l'immagine, la personalità e l'onore, soprattutto al fine di evitare che determinate notizie conferenti la sfera più privata siano oggetto di diffusione a mezzo dei mass media e ciò indipendentemente dalla veridicità o meno di quanto eventualmente diffuso e della lesività delle notizie. Si tratta, quindi, di una tutela che prescinde da tali circostanze e si connota come salvaguardia della libertà dell'individuo a poter mantenere la "riservatezza" sugli aspetti più intimi e personali della propria vita.

Ovviamente, dinanzi ad una tutela (in teoria) così astringente si pone il problema del

CamminoDiritto.it
ISSN 2421-7123

bilanciamento con altri diritti quali, ad esempio, il diritto alla cronaca che rappresenta una delle espressioni di quella "libertà di manifestazione del pensiero" garantita e tutelata dall'art. 21 della nostra Costituzione.

Al fine di contemperare i contrapposti interessi, la giurisprudenza si è impegnata a tracciare le "linee guide" affinché il diritto alla cronaca fosse esercitato nel rispetto della tutela della riservatezza. Difatti, si è giunti alla conclusione di considerare lecita l'informazione giornalistica quando, pur riportando fatti e condotte riconducibili alla sfera privata, vi sia un interesse pubblico e che i dettagli della vicenda siano riportati nella loro essenzialità.[4] In tal modo, si è stabilito che "la pubblicazione dei dati personali o dell'immagine senza il consenso dell'interessato, è legittima nell'esercizio dell'attività giornalistica, laddove si conformi ai limiti del diritto di cronaca"[5].

Ritengo, inoltre, di dover accennare a quello che si pone come uno dei più recenti diritti derivati dal diritto alla riservatezza e che, anch'esso, si "scontra" con il diritto alla cronaca: il diritto all'oblio. Indubbiamente un diritto "recente" e che sicuramente nasce dall'esigenza di tutelarsi dinanzi al mondo del web e che dovrebbe garantire l'individuo a che non siano diffusi precedenti pregiudizievoli per il suo onore e, quindi, una tutela dal protrarsi delle conseguenze connesse all'essere stati coinvolti in una vicenda di cronaca. Un diritto ad essere "dimenticati", la cui esigenza deriva dalla constatazione per cui ciò che è nella rete vi resta per sempre.

Questo nuovo diritto pone la possibilità che un fatto di cronaca torni ad essere privato quando, dopo esser stato conosciuto dal pubblico, perda alcuna utilità nel pubblico interesse. Pertanto, tale diritto, che ha trovato una regolamentazione dapprima con il Regolamento (UE) 2016/679 del Parlamento europeo e successivamente col recente GDPR, consente all'interessato di ottenere la cancellazione dei dati personali senza ritardo a meno che la diffusione di tale informazioni non sia necessaria al fine di esercitare il diritto alla cronaca ed all'informazione[6].

E' giusto, in ogni caso, evidenziare come queste premesse valevoli per qualunque soggetto possano essere "riconsiderate" qualora si tratti di un personaggio pubblico: è, difatti, evidente che l'equilibrio tra diritto all'informazione ed alla riservatezza risulti, per tali soggetti, differente. Vien da sé che rispetto alle persone note o che esercitino funzioni pubbliche, vi siano spazi più ampi per la diffusione di informazioni personali che possano avere rilievo in merito al carattere pubblico dell'attività svolta da questi.[7]

2. La genesi del D.lgs. 196/2003.

Il diritto alla riservatezza riguarda, ovviamente, soprattutto la diffusione dei propri dati

CamminoDiritto.it
ISSN 2421-7123

sensibili (e non soltanto la diffusione di notizie a mezzo stampa) ed è in epoca moderna che si è avvertita, maggiormente, la necessità di porre strumenti di tutela in tal senso.

Bisogna osservare come inizialmente, per la tutela della riservatezza, non vi fosse una normativa d'uopo prevista bensì si doveva far ricorso soltanto alla giurisprudenza (in particolare quella della Corte di Cassazione); tuttavia, con l'evolversi della società si è sentita l'esigenza di provvedere in tal senso così da disciplinare gli aspetti legati alla protezione e diffusione dei dati sensibili. L'impulso alla creazione di una normativa ad hoc fu data dalla direttiva europea 95/46/CE del 1995 che prevedeva la necessità di tutelare il trattamento dei dati personali delle persone fisiche e, pertanto, venne emanata la legge 31 dicembre 1996 n. 675, entrata in vigore nel maggio 1997. Con tale previsione normativa si è avuto un primo, importantissimo, passo per la tutela dei dati personali: infatti, venivano previsti una serie di obblighi di riservatezza nonché la previsione di una strumentazione idonea a garantire la segretezza dei dati raccolti, la cui diffusione veniva vietata salvo che espressamente consentita o prevista a norma di legge ma soprattutto si ebbe l'istituzione del "Garante per la protezione dei dati personali". Organo cui venivano affidati una serie di compiti riconnessi alla protezione dei dati personali come vigilare affinché i trattamenti siano effettuati nel rispetto delle norme di legge (con possibilità di vietare, anche d'ufficio, i trattamenti illeciti).

A tale normativa, nel corso degli anni, si affiancarono numerose altre disposizioni tanto da crearsi una stratificazione tale da far assurgere la necessità di riordinare quel "caos normativo" in un testo unico: così si ebbe la promulgazione de "codice per la protezione dei dati personali" (c.d. codice della privacy) con il D. Lgs. n. 196/2003. Suddetto testo unico, che riunisce tutta la normativa in materia, e che introdusse una serie di nuove garanzie per i cittadini, provvedendo, altresì, a semplificare gli adempimenti disposti per la tutela e protezione dei dati personali prevedendo disposizioni in merito al "trattamento" di tali dati ed in particolare circa la loro raccolta, elaborazione e diffusione, si pone essenzialmente come una "razionalizzazione" della normativa in materia.

Obiettivo primario resta, incontestabilmente, evitare che si abbia il trattamento dei dati senza il consenso dell'avente diritto ovvero in modo da recargli un qualche pregiudizio, bilanciando i contrapposti esigenti di colui che è titolare di tali dati e colui che, invece, per varie esigenze li raccoglie; a tal fine, oltra alla previsione della modalità di raccolta e le caratteristiche dei dati, venivano previsti una serie di obblighi in capo a chi raccoglieva o trattava tali dati, con conseguente riconoscimento di responsabilità in capo a questi per violazioni di legge e con la comminazione di sanzioni.

E' bene anche specificare, così come avviene all'art. 4 del D.Lgs. 196/2003, cosa si intenda per "dati sensibili": sono considerati tali qualunque dato che possa rilevare

CamminoDiritto.it
ISSN 2421-7123

l'origine razziale od etnica; opinioni politiche e convinzioni religiose o filosofiche; l'adesione a partiti ovvero ad associazioni di stampo religioso nonché notizie circa lo stato di salute o la vita sessuale.

Tali dati, ai sensi dell'art. 11, debbono essere trattati secondo correttezza, liceità ed in osservanza al principio di finalità, ed è inoltre chiaro che il trattamento dei dati deve essere ispirati a principi come la trasparenza in ogni fase. Con la nuova normativa, si ha anche l'introduzione del concetto di "trattamento leale" (con riferimento, ad esempio, agli istituti bancari che quando vi fu l'introduzione della normativa sulla privacy chiedevano ai propri clienti un ampissimo consenso sul falso presupposto per cui, in mancanza, non sarebbe stato possibile effettuare qualsivoglia operazione bancaria) ed, ovviamente, si evidenzia come il trattamento debba sempre avvenire in modo lecito e nel rispetto del principio di finalità. In riferimento a quest'ultimo aspetto, si evidenzia come i dati personali raccolti al fine dell'erogazione di un determinato servizio possa essere utilizzato esclusivamente per tale scopo.[8]

In ogni caso, pur con delle critiche (per es. con riguardo alla discussione in merito al richiamo all'art. 2050 c.c. per i danni derivanti dalla diffusione non autorizzata dei dati sensibili previsti dall'art. 15 comma 2), si può osservare come nel panorama europeo tale testo unico risulti essere il primo tentativo di dare organicità a tale disciplina.

3. Internet, i social network ed il caso Facebook/ Cambridge Analytica.

Se si parla di "dati personali" nel 2018 non si può non far riferimento ad internet che rappresenta, ormai, un immenso "raccoglitore" dei dati degli utenti della rete. Per questo motivo si è reso necessario prevedere una regolamentazione anche per quanto concerne i dati raccolti dal web. A chi non è capitato di aprire una pagina internet e trovarsi il banner che chiede il consenso per l'utilizzo dei cookies? Ebbene, quel banner che a molti potrebbe sembrare tedioso rappresenta, invero, un ulteriore strumento di tutela posto nei confronti dell'utente. Difatti i cookies http altro non sono che file di informazioni che vengono utilizzati dai siti web al fine di memorizzare il computer dell'utente internet nel corso della navigazione e poter così identificare chi ha già visitato il sito: orbene, con l'art. 112 del D.Lgs. 196/2003 entrato in vigore il 3 giugno 2015, che ha recepito la Direttiva 2009/136/CE in materia di "e-privacy", è stato previsto l'obbligo per i gestori dei siti web di informare e chiedere esplicito consenso all'utente (appunto mediante l'utilizzo dei banner che compaiono all'apertura di una pagina internet)[9].

Tuttavia i rischi riconnessi alla riservatezza dei propri dati riguarda soprattutto i cd. social network: si è avuto modo di illustrare i principi che ispirano la tutela del trattamento dei dati previsti dal D.Lgs. 196/2003 ma è palese che quando si tratta di social sorgono non

CamminoDiritto.it
ISSN 2421-7123

pochi problemi (basti pensare alla possibilità di "condividere" i contenuti così che una foto può giungere anche a soggetti a noi estranei).

Se prendiamo in esame, ad esempio, la nota piattaforma Facebook, si evidenziano una serie di rischi legati alla salvaguardia della privacy; si pensi alla circostanza per cui con l'iscrizione a tale social si rientra nei risultati dei motori di ricerca, senza che venga prestato espresso consenso, con la conseguenza che nome ed immagini "postate" possono essere alla mercé anche di soggetti non iscritti a tale community. Del resto, quando ci si iscrive ad un social, anche se si presta il consenso al trattamento dei dati, non se ne han ben chiare le finalità.

Particolarmente delicata risulta, poi, essere la posizione dei minori tanto è vero che la giurisprudenza di recente si è pronunciata sul merito della condivisione di foto minori per mezzo della piattaforma facebook, stabilendo che "l'inserimento di foto di minori sui social network costituisce un comportamento potenzialmente pregiudizievole per essi in quanto ciò determina la diffusione delle immagini fra un numero indeterminato di persone, conosciute e non", ragion per cui è necessario vi sia il consenso di entrambi i genitori[10].

Ma, altrettanto delicata nonché controversa, risulta essere il commercio illegale dei dati raccolti da tali piattaforme. E' assurto all'onore delle cronache la recente vicenda che vede coinvolta propria la nota piattaforma Facebook e la società di analisi Cambridge Analytica in merito all'acquisizione dei dati di oltre 50mila utenti. La Cambridge Analytica attraverso la raccolta dei dati in merito ai "mi piace" degli utenti ed ai post maggiormente commentati e l'elaborazione di tali informazioni, crea modelli ed algoritmi così da misurare i comportamenti e la personalità e sviluppare una pubblicità personalizzata per ogni utente. In particolare, l'Università di Cambridge elaborò un'applicazione di nome "thisisyourdigitallife" che offriva un servizio di previsione del comportamento sulla base dell'attività online e, attraverso tale app, cui si accedeva mediante login di Facebook, ha raccolto oltre 50 milioni di dati dai profili facebook poi condivisi con la predetta Cambridge Analytica. Dunque da un'applicazione nata per indagine e ricerca per il settore commerciale è stata applicata alla politica per svolgere indagini e ricerca sulle preferenze degli elettori. E' evidente che ciò contrasta con il diritto alla riservatezza (che come si è evidenziato ricomprende anche le opinioni politiche) ed è in questa prospettiva che assume una rilevanza notevole l'emanazione del recentissimo GDPR.

4. L'introduzione del GDPR.

L'ultima "rivoluzione" in materia di protezione dei dati è rappresentata dall'importante

CamminoDiritto.it
ISSN 2421-7123

riforma europea in materia di privacy, ossia l'introduzione del GDPR con cui si mira ad avere una regolamentazione uniforme in tutta Europa.

Dunque, bisognerà apportare delle modifiche alla disciplina fornita dal nostro ordinamento in materia: l'obiettivo cui sembra orientarsi la Commissione parlamentare speciale impegnata in tal progetto, sembra essere l'implemento delle novità introdotte dal Regolamento europeo pur mantenendo in essere l'impianto del testo unico delineato dal D.Lgs. 196/2003 anche nell'ottica di una più agevole transizione. Bisogna considerare che, infatti, mentre le norme del Regolamento contiene l'enunciazione di principi direttamente applicabili (si pensi al diritto dell'interessato ad avere informazioni, accesso ai dati ed a richiederne la rettifica e/o cancellazione), le altre norme necessitano l'intervento del legislatore nazionale.

Dal 25 maggio 2018, comunque, il Gdpr risulta pienamente applicabile con le sue importanti novità quali: il concetto di "data protection by design", il principio di "accountability", e la previsione della figura del Data Protection Officer (cd. DPO) da parte del responsabile e del titolare del trattamento.

Il principio di "privacy by design e by default" in base al quale il titolare del trattamento (che deve essere specificamente individuato) deve adoperarsi per porre in essere tutte le misure, sia tecniche che organizzative, per garantire che i dati raccolti siano trattati nel rispetto dei principi del corretto trattamento dei dati e, quindi, col ricorso soltanto ai dati personali che risultino necessari per la specifica finalità di trattamento.

Altro principio introdotto è il cd. "principio dell'accountabiliy" (ossia della "responsabilizzazione") che riguarda il titolare del trattamento (sia che si tratta del professionista che di aziende ovvero pubbliche amministrazioni) il quale, oltre a dover porre in essere tutte le misure necessarie a garantire la sicurezza dei dati raccolti, è tenuto, qualora accerti la violazione dei dati, a darne tempestiva comunicazione (entro 72 ore) all'autorità competente, salvo il caso in cui dimostri che la violazione dei dati non comporti alcun rischio né per i diritti né per le libertà delle persone fisiche.

Infine, assolutamente meritevole di nota, è l'introduzione della necessità della designazione del cd. Data Protection Officer (DPO) che rappresenta il "responsabile della protezione dei dati" (nomina obbligatoria per le strutture che vantano oltre 250 dipendenti e che si occupano di monitoraggio su larga scala ovvero per le autorità pubbliche) ed il cui ruolo non si limita a "vigilare" sulla protezione dei dati bensì svolge quasi il ruolo di "counsel" affinché lo sviluppo del business avvenga sempre nell'ottica di garantire la sicurezza dei dai raccolti.

CamminoDiritto.it
ISSN 2421-7123

Un ruolo "cruciale", pertanto, nell'ambito della nuova fisionomia della protezione dei dati delineata dal Gdpr eppure con riguardo alle competenze che questo debba possedere vi sono non pochi dubbi (ad esempio se debba trattarsi di un tecnico specializzato in tecniche informatiche con conoscenze giuridiche) anche tenuto conto della possibilità che questo ruolo può essere rivestito sia da un soggetto outsourcing ma anche da un soggetto "interno"[11].

Si tratta, in ogni caso, di una figura nuova (ed innovativa) che, nonostante i dubbi sugli aspetti tecnici, riveste una notevole importanza.

Note e riferimenti bibliografici

[1] "Nell'ordinamento giuridico italiano non esiste un diritto alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona; pertanto non è vietato comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto." Così la S.C. con la significativa pronuncia n. 4487 del 1956. [2] "Sebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito ed ove non sussista per la natura dell'attività svolta dalla persona e del fatto divulgato un preminente interesse pubblico di conoscenza" così Cass. 20 aprile 1963 n. 990. [3] "Il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti)" così la S.C. con la considerevole pronuncia n. 2129 del 1975 con cui si ebbe (finalmente) il pieno riconoscimento del diritto alla riservatezza quale diritto previsto e tutelato dal nostro ordinamento. [4] La S.C., con una delle pronunce più recenti sul tema, ha stabilito che "in tema di trattamento dei dati personali, il giornalista può diffondere dati personali anche senza il consenso dell'interessato, purché nei limiti del diritto di cronaca «e, in particolare, quello 12 dell'essenzialità dell'informazione rispetto a fatti di interesse pubblico» (art. 137, comma 3, del Codice) e demandando la disciplina di alcuni aspetti della materia al codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica di cui all'allegato A.1 del Codice" (così Cass. civ. Sez. III Ord. n. 13151 del

CamminoDiritto.it
ISSN 2421-7123

2017). Va inoltre sottolineato che in tema di tutela alla riservatezza, soprattutto con riguardo al diritto di cronaca, dei limiti sono stati previsti anche con l'introduzione del Codice deontologico dei Giornalisti. [5] Così il Tribunale di Ferrara con la pronuncia del 01.09.2016. [6] La S.C. a tal proposito ha stabilito, con l'ordinanza n. 6919 del 2018, che "in tema di diritto alla riservatezza, dal quadro normativo e giurisprudenziale nazionale (artt. 2 Cost., 10 c.c. e 97 della l. n. 633 del 1941) ed europeo (artt. 8 e 10, comma 2, della CEDU e 7 e 8 della c.d. "Carta di Nizza"), si ricava che il diritto fondamentale all'oblio può subire una compressione, a favore dell'ugualmente fondamentale diritto di cronaca, solo in presenza dei seguenti specifici presupposti: 1) il contributo arrecato dalla diffusione dell'immagine o della notizia ad un dibattito di interesse pubblico; 2) l'interesse effettivo ed attuale alla diffusione dell'immagine o della notizia (per ragioni di giustizia, di polizia o di tutela dei diritti e delle libertà altrui, ovvero per scopi scientifici, didattici o culturali); 3) l'elevato grado di notorietà del soggetto rappresentato, per la peculiare posizione rivestita nella vita pubblica del Paese; 4) le modalità impiegate per ottenere e nel dare l'informazione, che deve essere veritiera, diffusa con modalità non eccedenti lo scopo informativo, nell'interesse del pubblico, e scevra da insinuazioni o considerazioni personali, sì da evidenziare un esclusivo interesse oggettivo alla nuova diffusione; 5) la preventiva informazione circa la pubblicazione o trasmissione della notizia o dell'immagine a distanza di tempo, in modo da consentire all'interessato il diritto di replica prima della sua divulgazione al pubblico" [7] Così il Garante della Privacy nella Relazione annuale al Parlamento del 2004-05. [8] M. Gobbato, "Danni da trattamento illegittimo dei dati personali", HALLEY Editore, 2007, pp. 16-21. [9] E. Marchisio, "La "cookie law" italiana", Key editore, 2015, pp. 21 e ss. [10] Così il Tribunale di Mantova con la decisione del 19.10.2017. [11] D. Stella, "Il Data Protection Officer: nomina, tipologie, ruolo e compiti" su "Quotidiano – Pluris" del 15.11.2017.
