Euroconference
Centro Studi Forense

Digital & Law
Department

ADEGUAMENTO PRIVACY: PIÙ PROFESSIONALITÀ MENO FORMALITÀ

COPIA OMAGGIO

GRUPPO EUROCONFERENCE S.P.A.
Via E. Fermi, 11
37135 Verona

Sito internet: www.euroconference.it
mail: editoria@euroconference.it

Realizzazione editoriale
Editing e impaginazione: Erica Cestaro

Edizione ottobre 2018

INDICE

Editoriale

Adeguamento Privacy: più professionalità meno formalità

di Andrea Lisi[*]

1. GDPR e Decreto di Adeguamento: traccia definitiva

Dopo un lungo periodo di incubazione, è stato adottato il Decreto di adeguamento (D.Lgs. 101/2018) della normativa nazionale al Regolamento europeo in materia di protezione dei dati personali (GDPR). Il testo è stato pubblicato sulla Gazzetta Ufficiale del 4 settembre, ed è entrato in vigore il 19 settembre. Finalmente, si potrebbe esclamare!

La confusione però, non sembra essersi placata e lo *storytelling* imbastito negli ultimi mesi non ha aiutato a fare chiarezza, contribuendo, semmai, a diffondere le aspettative verso il "miracolo della certificazione", osannata in diversi congressi e workshop di settore.

Il GDPR nasce per rispondere a precise esigenze di certezza giuridica, armonizzazione e maggiore semplicità delle norme riguardanti il trattamento dei dati personali delle persone fisiche. Si tratta di una risposta, necessaria e urgente, alle sfide poste dagli sviluppi tecnologici e dai nuovi modelli di crescita economica, tenendo conto delle esigenze di tutela dei dati personali e di chiarezza dovuta agli addetti ai lavori, soprattutto in termini di responsabilizzazione e, in particolare, per quanto concerne il ruolo dei titolari del trattamento (che in Italia hanno forse risentito maggiormente del cambiamento tecnologico, rispetto al resto dell'Europa).

Il tanto atteso D.Lgs. 101/2018, in stato neonatale, conferma le misure di semplificazione per le micro, piccole e medie imprese, per le quali dovrà tuttavia esprimersi il Garante per la protezione dei dati personali, promuovendo modalità semplificate di adempimento degli obblighi del titolare del trattamento.

[*] Avvocato, Coordinatore del Digital&Law Department dello Studio Legale Lisi, Presidente ANORC Professioni

2. Garante Privacy: approccio responsabile

Adesso tutto è pronto per avviare il percorso di adeguamento normativo (se mai non fosse stato ancora intrapreso), pur nella consapevolezza che la piena applicazione delle norme contenute nel novellato Codice privacy richiede, per diversi aspetti, l'intervento del Garante per la protezione dei dati personali, titolare di nuovi e determinanti poteri di *soft law*: il suo arduo compito, in questa fase di *assessment* della normativa nazionale, risiede nel fornire un corretto orientamento sia rispetto alle principali novità introdotte dal Decreto, che ai principi applicabili al trattamento dei dati personali.

In quest'ottica, come ormai sappiamo bene, la nuova disciplina introduce il principio di "responsabilizzazione" (cd. accountability), che attribuisce direttamente ai titolari del trattamento il compito di assicurare e comprovare l'applicazione dei principi enucleati all'articolo 5 del GDPR, determinando la necessità da parte del Garante di introdurre linee guida rispetto alle priorità da mettere in atto, soprattutto per le PA meno resilienti e con grandi flussi di dati personali da gestire[1].

3. L'Italia dello "stato di grazia": questa volta non funziona

Come noto, tra i criteri direttivi da seguire, ai sensi dell'articolo 13 della L. 163/2017 (Legge di delegazione europea 2016-2017), al fine di uniformare il quadro normativo nazionale alle disposizioni del Regolamento 2016/679/UE, era compreso anche quello di "*adeguare, nell'ambito delle modifiche al Codice della privacy, il sistema sanzionatorio penale e amministrativo vigente alle disposizioni del Regolamento (UE) con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità della violazione delle disposizioni stesse*".

Sul punto, è il caso di ribadire che **il D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018 è pienamente applicabile dal 19 settembre 2018, apparato sanzionatorio compreso**. Precisazione tanto ovvia, quanto necessaria, a giudicare dalla **fantasiosa convinzione**, tuttora fomentata da interpreti improvvisati e fuorvianti titoloni, **sulla presunta sospensione delle sanzioni nei primi otto mesi di applicazione del nuovo Codice privacy**.

[1] Alle Amministrazioni pubbliche, tra l'altro, il Garante ha indicato gli interventi da avviare con assoluta priorità, sintetizzandoli in tre punti fondamentali:
1. **Designare il Responsabile della protezione dei dati – RPD** (artt. 37-39), garantendone il diretto coinvolgimento in tutte le questioni che riguardano la protezione dei dati personali, sin dalla fase transitoria, per garantire la qualità del risultato del processo di adeguamento in atto.
2. **Istituire il Registro delle attività di trattamento** (art. 30) quale esito della fase di ricognizione dei trattamenti svolti e delle loro principali caratteristiche. La ricognizione, come ribadito dal Garante, "*sarà l'occasione per verificare anche il rispetto dei principi fondamentali (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per impostazione (privacy by design e by default, art. 25)*".
3. **Notificare le violazioni dei dati personali** (cd. data breach) e dare "*pronta attuazione delle nuove misure relative alle violazioni dei dati personali*" (artt. 33 e 34), "*tenendo in particolare considerazione i criteri di attenuazione del rischio indicati dalla disciplina e individuando quanto prima idonee procedure organizzative per dare attuazione alle nuove disposizioni*".

Questa **famigerata sospensione di otto mesi** (da alcuni definita "stato di grazia") di cui si è tanto parlato e scritto prima che il decreto di adeguamento al GDPR venisse finalmente pubblicato in Gazzetta Ufficiale, è stata, effettivamente, suggerita da Camera e Senato, nei rispettivi pareri sullo schema di Decreto di adeguamento, invitando il Governo a valutare "*la possibilità che il Garante, in una fase transitoria, in ogni caso non inferiore a 8 mesi, successiva all'entrata in vigore del decreto legislativo, non irroghi sanzioni alle imprese, ma disponga ammonimenti o prescrizioni di adeguamento alla nuova disciplina*".

Raccomandazione, questa, **mai tradotta in atto** nella redazione del testo definitivo del Decreto (né, peraltro, sarebbe stato diversamente ipotizzabile, data l'**evidente antinomia** di una eventuale sospensione delle sanzioni rispetto al GDPR, che è fonte sovraordinata al diritto nazionale).

Ad alimentare l'equivoco, peraltro, ha contribuito l'ambigua formulazione dell'articolo 22 del D.Lgs. 101/2018 che, al comma 13, dispone: "*per i primi otto mesi dalla data di entrata in vigore del presente decreto, il Garante per la protezione dei dati personali tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento (UE) 2016/679, della fase di prima applicazione delle disposizioni sanzionatorie*".

La sospensione evidentemente non c'è e le sanzioni amministrative saranno applicate senza alcuna esenzione.

Ciò che si raccomanda al Garante, nei primi otto mesi dall'entrata in vigore del Decreto di adeguamento, è, piuttosto, **l'impiego di un criterio di bilanciamento nella graduazione delle sanzioni amministrative**, attenuandone, eventualmente, la severità, nella misura in cui il disvalore della violazione risulti attenuato dalla complessità del percorso di adeguamento della propria organizzazione al nuovo quadro normativo in materia di protezione dei dati personali. **Un percorso che dovrà essere, comunque e necessariamente, avviato, senza ulteriori indugi.**

In materia di sanzioni amministrative, **fermo l'apparato sanzionatorio definito dall'articolo 83 del GDPR**, ovviamente intatto, il Decreto di adeguamento ha **introdotto ulteriori ipotesi di soggezione alle sanzioni di cui all'articolo 83, paragrafi 4 e 5, del Regolamento,**[2] **puntualmente elencate all'articolo 166 del novellato Codice privacy**, dando attuazione al margine di autonomia normativa posta in capo agli Stati membri dall'articolo 84 dello stesso Regolamento.[3]

[2] Rispettivamente, **fino a 10 milioni di euro,** o per le imprese, **fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore (par. 4) e **fino a 20 milioni di euro**, o per le imprese, **fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente**, se superiore (par. 5).

[3] L'articolo 84 del GDPR prevede, in particolare, che "*Gli Stati membri stabiliscono le norme relative alle altre sanzioni per le violazioni del presente regolamento in particolare per le violazioni non soggette a sanzioni amministrative pecuniarie a norma dell'articolo 83, e adottano tutti i provvedimenti necessari per assicurarne l'applicazione. Tali sanzioni devono essere effettive, proporzionate e dissuasive*".

Vengono abrogati, invece, i restanti articoli del Codice privacy in materia di violazioni amministrative: sul punto, si segnala l'articolo 18 del D.Lgs. 101/2018, che individua un **percorso agevolato per la definizione dei procedimenti sanzionatori** riguardanti le violazioni di cui agli articoli 161, 162, 162-*bis*, 162-*ter*, 163, 164, 164-*bis*, comma 2, 33 e 162, comma 2-*bis*, del Codice, **pendenti "***alla data di applicazione del Regolamento UE*" (25 maggio 2018) e **non ancora definiti con ordinanza-ingiunzione**. [4]

Con riferimento alle **sanzioni penali,** escluse dal perimetro regolatorio del GDPR, che demanda il pertinente potere normativo agli Stati membri [5] – il Decreto di adeguamento è intervenuto sull'impianto sanzionatorio del Codice privacy **modificando**, in modo più o meno sostanziale, la maggior parte degli illeciti vigenti, al fine di assicurarne la compatibilità con il Regolamento UE, **abrogando l'articolo 169** del Codice, relativo alle misure di sicurezza e **introducendo due nuove fattispecie di reato** (articolo 167-*bis* "*Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala*" e articolo 167- *ter* "*Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala*").

4. DPO-RTD: la transizione al digitale *by design e by default*

Nell'ambito delle serie di azioni, a cui il Governo intende dare corso, per la trasformazione digitale della Pubblica Amministrazione, affinché sia da supporto alla crescita digitale dell'Italia, riveste particolare importanza l'individuazione delle figure di responsabile per la transizione al digitale.

Apre così la circolare n. 3 del 1 ottobre 2018, firmata dal Ministro per la pubblica amministrazione – Sen. Avv. Giulia Bongiorno, ribadendo l'obbligatorietà per tutte le pubbliche amministrazioni di dotarsi di un Manager specializzato per la transizione digitale (RTD), una figura di livello apicale, in grado di coordinare e gestire la *governance* della transizione al digitale - intesa come attività di indirizzo, coordinamento e correlata responsabilità - collocandosi alle dirette dipendenze dall'organo di vertice politico - o amministrativo- dell'ente (ai sensi dell'articolo 17, commi 1-*ter* e 1-*sexies* del CAD).

La volontà del Legislatore è di attivare la realizzazione di servizi pubblici rivisitati, pienamente integrati con le nuove tecnologie, evitando la giustapposizione di queste ultime alle esistenti forme di organizzazione (in prevalenza di matrice analogica). **Ovviamente RTD e DPO devono tra loro "parlarsi" e incidere insieme sui progetti di innovazione digitale delle PA italiane.**

[4] In argomento, si rinvia alle indicazioni operative contenute nelle FAQ sulla definizione agevolata delle violazioni in materia di protezione dei dati personali, predisposte dal Garante per la protezione dei dati personali per chiarire nel dettaglio la portata applicativa dell'art. 18 D.Lgs. 101/2018.

[5] Oltre al già richiamato art. 84, crf. il Considerando n. 149 del GDPR, per cui "*Gli Stati membri dovrebbero poter stabilire disposizioni relative a sanzioni penali per violazioni del presente regolamento, comprese violazioni di norme nazionali adottate in virtù ed entro i limiti del presente regolamento*".

A proposito di DPO, va ricordata l'introduzione dell'obbligo di nominare un **Responsabile della protezione dei dati per i trattamenti effettuati dalle autorità giudiziarie**, anche in relazione ai trattamenti di dati personali effettuati nell'esercizio delle loro funzioni (articolo 2-*sexiesdecies* Codice privacy).

E proprio in merito alla figura del DPO, è doveroso richiamare **la sentenza del TAR Friuli Venezia Giulia n. 287/2018,** che ha con autorevolezza affermato il principio della non obbligatorietà (e oseremmo dire superfluità) delle **certificazioni per svolgere questa delicata funzione**, sottolineandone la necessaria competenza anche in ambito giuridico. Ma il DPO, giova ricordarlo, è una funzione che deve avere **forti caratteristiche di multidisciplinarietà** per presidiare ogni aspetto dei trattamenti di dati personali svolti dal Titolare o dal Responsabile, assicurando competenza e professionalità in ambiti diversi ed eterogenei.

5. La premessa che conclude: "Trasparenza"

A conclusione del quadro ora tratteggiato, è possibile individuare un unico filo conduttore: **il principio di trasparenza**, conclusione che ha più il senso della premessa.

La parola d'ordine da seguire, ancor prima della *accountability*, della *privacy by design* e *by default* che costituiscono ormai le parole chiave del martellante *storytelling* di ogni convegno o seminario in materia - è la **trasparenza**. **Effettuare una rigorosa, efficace e trasparente mappatura di tutti i trattamenti di dati afferenti alla propria organizzazione, siano essi svolti direttamente dal Titolare o affidati all'esterno, costituisce, infatti, il presupposto necessario di ogni azione di *assessment*** e principio cardine di ogni processo di cambiamento.

Il "nuovo" Codice privacy - Breve rassegna delle novità

di Enrico Pelino[*]

Il 19 settembre scorso è entrato in vigore l'ormai attesissimo D.Lgs. 101/2018, che ha novellato il Codice privacy (D.Lgs. 196/2003) per adeguarlo al Regolamento europeo in materia di protezione dei dati personali.
L'occasione dunque è utile per tracciare un primo quadro delle principali novità. Necessari limiti di spazio limiteranno questa breve rassegna ad alcuni temi.

1. Reclamo e segnalazione

Prevedibilmente, e opportunamente, è stato eliminato il ricorso al Garante, assorbendolo concettualmente nel rimedio reclamo, del quale è fissata la durata massima in nove-dodici mesi. Il termine non è esente da perplessità circa la sua compatibilità con la disciplina europea. Vero infatti che il Regolamento non prescrive termini di durata, tuttavia all'interprete è autorizzata dall'articolo 78.2 GDPR qualche deduzione in merito a una tempistica decisamente più breve.

Viene mantenuto lo strumento della segnalazione, ma con un profilo applicativo in parte mutato.

2. Dati sulla salute

Spicca rispetto al passato, ed è certamente positivo, l'eliminazione del consenso per il trattamento dei dati sulla salute in ambito sanitario.

La misura era particolarmente attesa, ma non scontata: la possibilità di deroga concessa dall'articolo 9.4 GDPR al legislatore nazionale avrebbe potuto essere anche declinata nel senso di mantenere la base giuridica nel consenso, come in precedenza.

Le strutture sanitarie potranno dunque cessare di accumulare attestazioni di manifestazione del consenso e liberare risorse ed energie per altre attività.

La norma di riferimento è oggi l'articolo 2-*septies* Cod. priv., che prevede un sostanziale coinvolgimento del Garante, chiamato a definire misure di garanzia dell'interessato, soggette a revisione biennale, previa consultazione pubblica.

*Avvocato, co-fondatore Grieco Pelino Avvocati, membro consiglio Direttivo Anorc Professioni.

3. Autorizzazioni generali

Una parte non marginale della disciplina era contenuta in passato nelle autorizzazioni generali del Garante, emanate ai sensi dell'oggi abrogato articolo 40 Cod. priv.

Questo strumento ha avuto notevoli pregi, rappresentando anche un terreno di affinamento concettuale per il giurista. E con il Regolamento?

Non tutto è perduto: la disciplina transitoria introdotta dall'articolo 21, D.Lgs. 101/2018 onera il Garante di un'attività di selezione e aggiornamento delle prescrizioni contenute delle autorizzazioni generali, da condurre anche attraverso una consultazione pubblica. Questo vaglio è ovviamente ammesso solo entro gli spazi di precisazione nazionale o di deroga consentiti dal Regolamento.

4. Allegati al Codice privacy

Non sono stati affrontati dalla riforma ma, per così dire, "messi in frigorifero" e lasciati alla futura selezione del Garante secondo due procedimenti diversi. Le ragioni per le quali questa porzione della normativa è stata risparmiata dalla riforma sono riconducibili, in parte, alla circostanza che si tratta di testi prodotti in seguito all'interlocuzione dell'Autorità di controllo con vari soggetti anche istituzionali, non coinvolgibili nei tempi stretti di una novella giunta per così dire "*in limine litis*".

Comunque, non si possono sottacere motivi di rammarico per quello che appare uno dei maggiori passaggi incompiuti della novella, anche perché in quegli allegati si annidano talvolta soluzioni ormai incompatibili con la disciplina europea (ma anche con il "nuovo" Codice privacy), che andrebbero probabilmente disapplicate. "Probabilmente": qui infatti il giurista opera su un terreno insidioso, lontano dalla certezza del diritto che in una materia già così complessa dovrebbe essere garantita.

5. Perimetrazione stretta del diritto nazionale presupposto

Il diritto nazionale e il Regolamento europeo registrano numerose intersezioni reciproche, ad esempio nell'area rimessa alle deroghe nazionali (*in primis* articolo 23 e Capo IX GDPR). Tuttavia, il terreno in cui l'intersezione è più ricca e complessa è certamente quello del diritto "presupposto", vale a dire delle disposizioni nazionali sulle quali le norme europee necessariamente poggiano.

Si prenda l'articolo 6.1.c) GDPR, trattamento in adempimento di un obbligo di legge: il contenuto dell'obbligo di legge è fornito non solo dal diritto europeo, ma da quello diritto nazionale, dunque sarà tendenzialmente diverso in Italia, Spagna o Francia.

Stesso discorso per l’articolo 6.1.e) GDPR. Anche in questo caso il giurista dovrà andare a verificare la normativa nazionale *extra*-privacy applicabile.

Piace ricordare che il considerando 41 GDPR introduceva, com’è noto, una nozione di diritto nazionale molto ampia ed evoluta, ispirata a un approccio di *common law*. Sono tali infatti anche disposizioni diverse da norme primarie, dunque, è da ritenere, le circolari applicative, le faq ministeriali, le prassi e perfino gli orientamenti consolidati del Garante o gli approdi fermi della Cassazione. L’importante è che il diritto nazionale sia chiaro e preciso nella formulazione e prevedibile nell’applicazione.

La riforma del Codice privacy tuttavia ha annullato quasi completamente questa apertura, riducendo il diritto nazionale “presupposto”, almeno in un’ampia serie di casi, alla sola legge o al regolamento, quest’ultimo unicamente nei casi previsti dalla legge.

Qual è la conseguenza? Un restringimento delle basi giuridiche richiamabili: sia di quelle generali dell’articolo 6 GDPR, (cfr. articolo 2-*ter* Cod. priv.) sia di quelle particolari dell’articolo 9 (cfr. articolo 2-*sexies* Cod. priv.). Sono prevedibili non poche difficoltà applicative e revisioni di informative, di procedure e, in molti casi, anche dei registri del trattamento.

6. Autorizzazione preliminare

Il Regolamento europeo all’articolo 36.5 permette al Legislatore nazionale una specifica deroga alla regola della consultazione preventiva solo eventuale. È infatti possibile, per trattamenti riconducibili all’esecuzione di un compito di interesse pubblico, rendere obbligatoria l’autorizzazione preliminare del trattamento da parte del Garante.

L’Italia, nel contesto di un piano di deroghe già molto intenso, ha ritenuto qui di cogliere un’ulteriore occasione di deroga, reintroducendo un istituto che, molto alla lontana, ricorda l’ormai abrogata verifica preliminare, cfr. l’attuale articolo 2-*quinquies* *decies* Cod. priv..

7. Diritto di controllo ad effetto *post-mortem*

Costituisce una delle novità più interessanti. Com’è noto infatti i poteri di controllo della persona fisica sui propri dati personali cessano con la morte. Il Codice privacy prevedeva sì l’esercizio di diritti sulle informazioni del deceduto, ma da parte di terzi per interessi attuali loro riconducibili. Non solo questi strumenti, di indubbia utilità pratica, sono stati mantenuti anche con la riforma, ma ne sono stati aggiunti altri del tutto inediti. Oggi l’interessato può infatti conferire mandato a terzi per l’esercizio dei

suoi diritti *post-mortem* e può perfino vietare il trattamento di suoi dati *post-mortem* da parte dei terzi che vi sarebbero legittimati.

Il divieto si applica ai servizi della società dell’informazione (un contesto dunque molto ampio) e presenta profili non solo di interesse pratico ma anche di grande stimolo su un piano teorico. Cfr. nuovo articolo 2-*terdecies* Cod. priv..

8. Residui di concezione “consenso-centrica”

Terminiamo questa breve rassegna con un motivo di insoddisfazione. Il “vecchio” Codice ruotava attorno al consenso (almeno per i soggetti privati): unica base giuridica, derogabile in una serie di ipotesi tassative. Il Regolamento, ma già per la verità la Direttiva 95/46, è invece ispirato al diverso criterio dell’equipollenza delle basi giuridiche. Spiace allora notare che la novella di adeguamento non abbia sempre fatto un lavoro di pulitura e che qua e là affiorino resti, ormai archeologici, di una concezione “consenso-centrica”. La questione non è teorica, ma pratica. Questi residui confondono infatti l’interprete e rendono talvolta incerto il dettato normativo.

Le limitazioni dei diritti degli interessati

di Michele Iaselli[*]

Come noto il Regolamento UE n. 2016/679 sulla protezione dei dati personali (GDPR) riconosce dagli articoli 15 a 22 tutta una serie di diritti a favore degli interessati nei confronti del titolare e del responsabile del trattamento che rappresentano una delle principali novità della normativa comunitaria molto attenta a tutelare le ragioni dell'interessato. Lo stesso articolo 23 del GDPR, però, sottolinea che il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti di cui agli articoli da 12 a 22 e 34, nonché all'articolo 5, qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica per salvaguardare tutta una serie di interessi considerati primari e che nell'ottica del principio del pari grado vanno preferiti alle ragioni dell'interessato.

L'articolo 2, D.Lgs. 101/2018, con il quale il nostro paese ha adeguato la propria normativa nazionale al GDPR, introducendo l'articolo 2-undecies nel codice in materia di protezione dei dati personali (D.Lgs. 196/2003) ritorna sull'argomento cogliendo l'opportunità fornita dallo stesso Legislatore comunitario e chiarisce che i diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto:

a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio;
b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive;
c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria;

[*] Avvocato, esperto privacy, Presidente Associazione Nazionale per la Difesa della Privacy (ANDIP)

f) alla riservatezza dell'identità del dipendente che segnala ai sensi della L. 179/2017, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio. In quest'ultimo caso è chiaro il riferimento al whistleblowing che di recente ha trovato riconoscimento nel nostro ordinamento con la legge sopra menzionata.

La norma specifica che nei casi elencati ad eccezione dell'attività delle Commissioni parlamentari i diritti sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del GDPR. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi evidenziati nella disposizione in esame.

In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160 del Codice. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale.

Con riferimento, poi, ai trattamenti di dati personali effettuati per ragioni di giustizia nell'ambito di procedimenti dinanzi agli uffici giudiziari di ogni ordine e grado nonché dinanzi al Consiglio superiore della magistratura e agli altri organi di autogoverno delle magistrature speciali o presso il Ministero della giustizia, l'articolo 2-*duodecies* introdotto sempre dal D.Lgs. 101/2018 nel rispetto di quanto sancito dall'articolo 23, paragrafo 1, lettera f), del Regolamento, evidenzia che l'esercizio dei diritti e l'adempimento degli obblighi di cui agli articoli da 12 a 22 e 34 del Regolamento possono, in ogni caso, essere ritardati, limitati o esclusi, con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, nella misura e per il tempo in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, per salvaguardare l'indipendenza della magistratura e dei procedimenti giudiziari.

Si tratta di una disposizione che ha la stessa ratio di quella precedente e che assume una rilevanza autonoma in considerazione della delicatezza della materia che però si ricorda è già oggetto di una specifica normativa (D.Lgs. 51/2018) con la quale il nostro paese ha recepito la Direttiva comunitaria n. 2016/680.

L'articolo 2-*duodecies* precisa che si intendono effettuati per ragioni di giustizia i trattamenti di dati personali correlati alla trattazione giudiziaria di affari e di controversie, i trattamenti effettuati in materia di trattamento giuridico ed economico del personale di magistratura, nonché i trattamenti svolti nell'ambito delle attività ispettive su uffici giudiziari. Le ragioni di giustizia, naturalmente, non ricorrono per l'ordinaria attività amministrativo-gestionale di personale, mezzi o strutture, quando non è pregiudicata la segretezza di atti direttamente connessi alla trattazione giudiziaria di procedimenti.
Probabilmente questa disposizione avrebbe trovato una sistemazione più organica nello stesso D.Lgs. 51/2018, o quanto meno sarebbe stato opportuno un richiamo a questa normativa di recepimento.

Price discrimination e protezione dei dati personali: possibili scenari

di Carmine Trovato[*]

Con l'espressione *price discrimination* si intende quella strategia di prezzi per la quale beni o servizi identici o simili tra loro vengono venduti, da parte di uno stesso fornitore, a prezzi differenti e maggiori del loro costo marginale[6].

In tali casi il prezzo di un bene non è definito dai suoi costi di produzione e commercializzazione, ma da quanto il consumatore è disponibile a spendere per acquistarlo (propensione al consumo o prezzo di riserva).

Quanto più un'impresa è in grado di individuare con precisione tale propensione al consumo, tanto più ampia sarà la capacità di definire una strategia personalizzata attraverso la quale vendere lo stesso prodotto a più consumatori applicando a ciascuno un prezzo differente[7].

Sotto tale prospettiva, il tema del trattamento dei dati personali assume un'importanza decisiva per ogni titolare che intenda estrarre valore dalle informazioni raccolte. Le nuove tecnologie stanno rivelando un potenziale senza precedenti nel rendere sempre più specifiche e precise le suddivisioni in *cluster* ai quali applicare differenziazioni di prezzo. La propensione al consumo di un determinato bene da parte di un potenziale acquirente può essere sempre più agilmente dedotta dalla conoscenza dei suoi comportamenti *online* e *offline*.

Quali rischi comportano tali strategie per le libertà e i diritti delle persone?

Prendendo in considerazione uno scenario tipo, è possibile affermare che vi sono gruppi di soggetti disposti a pagare prezzi differenti per lo stesso bene. Alcuni di loro attribuiranno invece al prodotto il valore 0, esprimendo così la corrispondente propensione al consumo poiché il bene è di scarso interesse, oppure poiché il potenziale acquirente è un soggetto incapiente. Quest'ultima categoria di consumatori resterà per così dire "fuori dal gioco" essendo esclusa dall'area di ottimizzazione del venditore; non userà ad esempio una clinica privata ma la sanità pubblica, non pagherà la benzina perché non ha la

[*] Avvocato, esperto privacy

[6] Krugman; *Paul R.; Maurice Obstfeld., Economies of Scale, Imperfect Competition and International Trade. In International Economics - Theory and Policy*, VI, 2003, p. 142.

[7] Per citare alcuni tra i tanti esempi possibili di applicazione di tali pratiche, si pensi ai biglietti aerei il cui prezzo cambia a seconda del preavviso con il quale vengono acquistati. Ancora, all'interno di molti e-commerce, il *conversion* rate misura il numero di utenti del sito che si trasformano in clienti acquistando un prodotto. Ogniqualvolta il tasso diminuisce al di sotto di un valore determinato, il prezzo dei beni viene automaticamente adeguato al fine di stimolare la domanda.

possibilità di acquistare una macchina usufruendo così del servizio di trasporto pubblico. Di tali individui si prenderà dunque cura lo Stato attraverso il Welfare.

Semplificando, si possono individuare tre categorie di soggetti che entrano a far parte del gioco:

1. L'impresa che, attraverso le informazioni raccolte sulle preferenze dei consumatori, mira a massimizzare i ricavi;
2. I soggetti disposti ad acquistare il bene ad un prezzo più elevato di quello fissato dall'impresa utilizzando quella capacità di spesa non ancora aggredita (che d'ora in avanti chiameremo «*surplus*»);
3. Coloro che non entrano nel gioco e dei quali si prende cura lo Stato attraverso il servizio pubblico finanziato da quella frazione del surplus con il quale i soggetti che hanno capacità di spesa pagano le tasse.

Cosa succederebbe dunque se l'impresa conoscesse la propensione al consumo di un soggetto per ogni singolo bene? Cosa accadrebbe, ad esempio, se l'azienda farmaceutica sapesse che un individuo ha un bisogno impellente di una determinata medicina?

In questo caso, l'impresa potrebbe massimizzare i propri ricavi aggredendo quel surplus che viene in parte utilizzato per l'acquisto di beni e, in altra parte, per il pagamento delle tasse.

Ad oggi, non ci troviamo ancora di fronte ad un utilizzo intensivo di tali pratiche di *price discrimination* e, nella maggioranza dei casi, il prezzo praticato ad una pluralità di consumatori per il singolo bene è il medesimo.

La difficoltà principale riscontrata dalle imprese nell'attuazione di tali strategie risiede nel reperimento dei dati personali degli utenti. Stiamo tuttavia entrando in un'epoca in cui la produzione dei dati aumenta ogni anno[8] in modo esponenziale consentendo parallelamente una maggiore disponibilità e circolazione di quello che è stato definito il «*nuovo petrolio*»[9].

Per effetto dei *Big Data*, dell'*Internet of Things* e della commoditizzazione dell'informazione, potrebbe dunque configurarsi una nuova forma di *lock-in* determinata dal fatto che i dati renderanno manifesto il contesto nel quale l'interessato vive e consentiranno alle imprese di estrarre il corrispondente surplus in misura maggiore rispetto a quanto sarebbe accaduto in una condizione di assenza di informazioni e di cose decontestualizzate. È infatti plausibile pensare che il consumatore difficilmente rinuncerà

[8] *Gantz J.; Reinsel D., Extracting Value from Chaos, libro bianco finanziato da EMC-IDC, disponibile online. Lyman P.; Varian H.R., How Much Information?,* 2003, disponibile *online*. Secondo tali studi si stima che dalla nascita del computer fino al 2006 siano stati prodotti approssimativamente 180 *esabyte* di dati, mentre il totale è cresciuto fino a più di 1600 *esabyte* nel solo periodo che è intercorso tra il 2006 e il 2011.

[9] L'espressione è riportata in WORLD ECONOMIC FORUM, *Personal Data: the emergence of a new asset class,* 2011 p. 5.

all'acquisto del bene, proprio perché questo è stato specificamente valutato dall'impresa come necessario per il suo paniere.

L'aggressione del surplus da parte dell'impresa potrà comportare una costrizione per il consumatore ad essere più produttivo per poter acquistare altri beni e dunque una riduzione del proprio tempo libero, oppure, più verosimilmente, un'aggressione della parte di surplus utilizzata per finanziare il welfare e sussidiare i soggetti più bisognosi.

Dunque, da un trattamento dei dati personali non accompagnato da una redistribuzione del gettito fiscale, potrebbe derivare un mancato soddisfacimento dei bisogni primari per un numero molto ampio di soggetti proprio a causa dell'erosione della componente sociale da parte delle imprese.

Tuttavia, il processo di gestione dei *Big data* non è un processo esclusivamente verticale, ovvero non sono le sole imprese a conoscere le preferenze dei consumatori, ma gli stessi consumatori che si confrontano tra loro[10]. Un potenziale acquirente potrebbe ad esempio trovarsi a pagare lo stesso bene più di un altro soggetto e constatare immediatamente di essere stato vittima di una discriminazione e opporsi a questa forma di profilazione aggressiva. Tale elemento di opposizione è spesso sottovalutato, ma potrebbe rappresentare il principale ostacolo a queste strategie di mercato.

Il confronto tra interessati si configura come tutela ulteriore rispetto a quelle giuridica e tecnologica presenti nel GDPR e può portare alla reazione nella misura di un mancato acquisto del bene imponendo al titolare del trattamento di rimuovere tale discriminazione[11].

È dunque possibile per un'impresa aumentare i propri ricavi attraverso il trattamento dei dati personali senza per questo limitare i diritti e le libertà delle persone fisiche?

L'obiettivo di sistema che l'impresa si potrebbe porre per valorizzare il proprio database è quello di lavorare per spostare verso l'alto la curva della domanda e, in tal senso, i dati e la contestualizzazione sono quanto di più utile ci sia.

In sostanza, se l'aumento del valore del bene è dato da un reale riscontro dell'utilità per il consumatore, lo stesso avrà una percezione positiva di tale strategia e sarà maggiore la probabilità che anche i soggetti che restavano fuori dal gioco perché non interessati al prodotto, optino per rientrarvi e acquistarlo in quanto rispondente ad una loro utilità[12].

[10] A tal proposito, basti pensare ai fenomeni dei rating o delle recensioni.

[11] Così è avvenuto nel 2000 quando Amazon, dopo aver aumentato il prezzo di alcuni DVD ai soli utenti che si erano dimostrati più interessati, è stato costretto a porgere le scuse e a bloccare la sperimentazione dopo che gli stessi avevano manifestato apertamente un chiaro disappunto per quanto accaduto.

[12] Si pensi alle tecnologie che monitorano l'utilizzo degli oggetti acquistati, per poi suggerire il momento in cui si sta per verificare un guasto o la necessità di una revisione, o ancora, ai sistemi di geolocalizzazione installati nelle autovetture che avvertono autonomamente il servizio di soccorso in seguito ad un incidente stradale, riducendo così in misura significativa i rischi per l'incolumità della persona.

Una piena valorizzazione dei dati personali potrebbe essere raggiunta non tanto attraverso l'aggressione al surplus, quanto piuttosto dallo sfruttamento della loro capacità di aumentare la domanda.

L'obiettivo da un punto di vista economico della *privacy by design*[13] è quello di effettuare una contestualizzazione del bene che consenta di estrarre l'informazione dai dati, ma di lasciare fuori la persona poiché, come dimostrato, questa si opporrebbe ad una limitazione della propria libertà personale.

> «Il fatto che privacy e Big data non appaiano come contendenti, ma come 2 alleati per garantire la protezione dei dati personali e, la valorizzazione dei dati, è presupposto di stabilità per l'affermarsi dei benefici innegabili che deriveranno dai Big data»[14].

Dunque, difendere la privacy della persona assume un valore di difesa della collettività e, in particolare, individuare soluzioni che configurino come accettabile un determinato trattamento di dati personali effettuando una previa valutazione per i rischi e le libertà delle persone fisiche, potrebbe comportare il duplice effetto di consentire una massimizzazione dei ricavi da parte delle imprese, garantendo tuttavia il rispetto delle regole in materia di protezione dei dati personali.

[13] Cfr. Art 25 par.1, Regolamento Europeo 2016/679: *"Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects".*

[14] D'Acquisto G.-Naldi M., op.cit., p.23.

Social marketing e *social spam* fra diritto alla protezione dei dati personali e casistica concreta

di Luca Christian Natali[*]

1. Il fenomeno del social marketing e del social spam

Al fine di svolgere un discorso consapevole e corretto, tanto sul paino teorico quanto sul piano concreto, occorre anzitutto definire il concetto di "*social marketing*".

A parte le particolari possibili sfumature semantiche, in sostanza, per "*social marketing*" potremmo convenzionalmente intendere l'attività promozionale veicolata tramite i *social network* cioè l'invio di comunicazioni promozionali effettato nel contesto del social (per esempio, inviando messaggi promozionali in bacheca o nella chat degli utenti social, oppure (o anche in aggiunta) l'invio di siffatte comunicazioni a dati di contatto (indirizzi e-mail; numeri di telefono) reperiti sui *social*.

Tale attività di per sé può considerarsi un'attività economica lecita, persino meritevole in ottica di utilità sociale, e comunque, potremmo dire, fisiologica nell'ambito dell'economia di mercato, e tanto più nell'ambito dell'economia digitale, considerate l'economicità e la diffusione del mezzo social. La medesima contribuisce all'attuazione della libertà di circolazione dei dati, che è anch'esso obiettivo fondamentale dell'UE proprio perché rilevante presupposto per lo sviluppo economico.

Tuttavia, il *social marketing* può trasformarsi in attività "patologica "sotto il profilo privacy, qualora fuoriesca dai binari della normativa in materia di protezione dei dati. Ed è allora, solo allora, che va qualificata come "*social spam*".

> Ferma restando la mancanza di una specifica disciplina dedicata, a tale tipologia di trattamento non può essere applicato troppo rigidamente il Codice privacy (D.Lgs. 196/2003), soprattutto tenendo conto della peculiare funzione dei social network, che sono sinonimo di condivisione **volontaria** e circolazione di idee, conoscenze, foto, contatti, gusti, hobbies, e quindi di numerosi tipi di dati personali.

* Dottore di ricerca in Diritto Civile Scuola Sant'Anna di Pisa; dottore di ricerca in diritto del lavoro presso l'Università Cattolica di Milano.
Si ripropongono con questo contributo alcune riflessioni formulate dall'Autore in occasione del seminario tenuto per Euroconference a Vicenza il 4 luglio 2018. Tali opinioni s'intendono formulate a titolo meramente personale e non impegnative in alcun modo per l'amministrazione di appartenenza.

Con questa espressa consapevolezza, l'Autorità ha provato a dare definizione e disciplina al *social marketing*, con le ***Linee guida in materia di attività promozionale e contrasto allo spam*, 4 luglio 2013** [doc. web 2542348].

Ebbene, come osserva il Garante, il c.d. "social spam" consiste in un insieme di attività mediante le quali lo spammer veicola messaggi e *link* attraverso le reti sociali *online*.

Un primo grave problema è che spesso tale attività viene svolta al di fuori, e quindi in violazione, dei fondamentali principi di informativa e consenso degli interessati.

Un secondo grave problema è che tali comunicazioni spesso, a dispetto dei contenuti apparentemente commerciali, possono nascondere intenti fraudolenti e truffaldini (v. fenomeni del *phishing*, ossia …, o dello *smishing,* che è fenomeno analogo al *phishing*, ma svolto tramite sms), o anche veri e propri tentativi di hackeraggio, mediante *virus i*nformatici e *trojan horses,* destinati a distruggere i sistemi operativi dei destinatari.

Va considerato poi anche un terzo problema: l'indiscriminato e spesso inconsapevole impiego dei propri dati personali da parte degli utenti nell'ambito dei *social network*, tanto più, come si è già evidenziato, rispetto a profili di tipo "aperto".

Questo impiego si presta alla commercializzazione o ad altri trattamenti dei dati personali a fini di profilazione e marketing da parte di società terze che siano partner commerciali delle società che gestiscono tali siti oppure che "approfittino" della disponibilità di fatto di tali dati in *Internet*. Inoltre, essendo i *social network* reti sociali tra persone reali, lo *spam* in questo caso può mirare a catturare l'elenco dei contatti dell'utente interessato mirato per aumentare la portata virale del messaggio.

Al riguardo, l'Autorità anzitutto ricorda che l'agevole rintracciabilità di dati personali in *Internet* (quali numeri di telefono o indirizzi di posta elettronica) non autorizza a poter utilizzare tali dati per inviare comunicazioni promozionali automatizzate senza il consenso dei destinatari.

Riguardo a tale tipo di *spam*, si fa presente che i messaggi promozionali inviati agli utenti dei *social network* (come Facebook), in privato come pubblicamente sulla loro bacheca virtuale, sono sottoposti alla disciplina del Codice, e, in particolare, agli articoli 3, 11, 13, 23 e 130.

La medesima disciplina, stabilisce il Garante nelle citate Linee Guida, è applicabile ai messaggi promozionali inviati utilizzando strumenti o servizi sempre più diffusi tipo Skype, WhatsApp, Viber, Messanger, etc.. Per questi, si ricorda il rischio di proliferazione dello spam dato che, come peraltro indicato nelle relative condizioni di servizio, tali strumenti talora comportano la condivisione indifferenziata di tutti i dati personali presenti negli *smart-phone* e nei *tablet* (quali rubrica, contatti, sms, dati della navigazione *internet*) o comunque la possibilità di accesso della società che li fornisce

alla lista dei contatti e-mail o alla rubrica presente sul telefono mobile dell'utente per reperire e/o conservare tali dati personali.

Per gli utenti il rischio di ricevere spam, e in particolare il c.d. "spam mirato", basato sulla profilazione dei dati disponibili *on line*, è senz'altro aggravato dalla diffusione di piattaforme tecnologiche che prevedono l'integrazione dei diversi servizi resi (nonché dei relativi profili) consentendo ai loro gestori di pervenire ad una conoscenza sempre più approfondita ed analitica degli utenti, a cui indirizzare messaggi diversificati sulla base dei gusti rilevabili su molteplici applicazioni.

Se da una parte questa nuova pratica può agevolare il rapporto commerciale tra produttore e consumatore, riducendo per il primo i costi di marketing e per il secondo i costi di ricerca del prodotto, tuttavia può causare all'interessato che viene profilato a dispetto della sua volontà, o perlomeno senza adeguata consapevolezza, oltre alla ricezione dello spam, anche la compressione della sua libertà di fruizione dei servizi della società dell'informazione.

Ciò premesso, ferma restando la liceità dei messaggi a scopo meramente personale, si possono individuare, secondo l'Autorità Garante, **alcune ipotesi** paradigmatiche.

Una **prima ipotesi** è quella in cui l'utente riceva, in privato, in bacheca o nel suo indirizzo di posta e-mail collegato al suo profilo *social*, un determinato messaggio promozionale relativo a uno specifico prodotto o servizio da un'impresa che abbia tratto i dati personali del destinatario dal profilo del *social network* al quale egli è iscritto.

Una **seconda ipotesi**, individuata nelle menzionate Linee Guida, è quella in cui l'utente sia diventato "*fan*" della pagina di una determinata impresa o società oppure si sia iscritto a un "gruppo" di *follower* di un determinato marchio, personaggio, prodotto o servizio (decidendo così di "seguirne" le relative vicende, novità o commenti) e successivamente riceva messaggi pubblicitari concernenti i suddetti elementi.

Orbene vediamo ora la disciplina applicabile il Garante.

> Nel primo caso, osserva l'Autorità, il trattamento sarà da considerarsi illecito, a meno che il mittente non dimostri di aver acquisito dall'interessato un suo consenso preventivo, specifico, libero e documentato ai sensi dell'articolo 130, commi 1 e 2, del Codice.
>
> Nel secondo caso, l'invio di una comunicazione promozionale riguardante un determinato marchio, prodotto o servizio, effettuato dall'impresa a cui fa riferimento la relativa pagina, può considerarsi lecita se dal contesto o dalle modalità di funzionamento del *social network,* anche sulla base delle informazioni fornite, può evincersi **in modo inequivocabile** che l'interessato abbia

> in tal modo voluto manifestare anche la volontà di fornire il proprio consenso alla ricezione di messaggi promozionali da parte di quella determinata impresa.

Occorre fin d'ora osservare come tale disciplina individuata dal Garante risulti compatibile, anzi in armonia, con il dettato del Regolamento generale europeo di cui si dirà di seguito (v. par. 3), che evidenzia, per poter configurare il valido consenso degli interessati, la necessità di una inequivocabile manifestazione di volontà.

Riprendendo il citato caso (secondo), tuttavia, se invece l'interessato si cancella dal gruppo, oppure smette di "seguire" quel marchio o quel personaggio, o comunque si oppone ad eventuali ulteriori comunicazioni promozionali, il successivo invio di messaggi promozionali sarà illecito, con le relative conseguenze sanzionatorie. Come ricorda il Garante, comunque resta salva la possibilità, talora fornita dai *social network* ai loro utenti, di bloccare l'invio di messaggi da parte di un determinato "contatto" o di segnalare quest'ultimo come *spammer*.

> In base a quanto ricordato dal Garante, nell'ipotesi dei "contatti" (i c.d. "amici") dell'utente, dei quali spesso nei social *network* o nelle comunità degli iscritti ai servizi di cui sopra, sono visualizzabili numeri di telefono o indirizzi di posta elettronica, l'impresa o società che intenda inviare legittimamente messaggi promozionali dovrà aver previamente acquisito, per ciascun "contatto" o "amico", un consenso specifico per l'attività promozionale.

2. Caso pratico di social marketing: provvedimento del 21 settembre 2017

In tema di social marketing, emerge lo specifico **provvedimento adottato il 21 settembre 2017** nei confronti di una società operante nell'ambito dei servizi *on line* [doc. web n. 7221917], con il quale il Garante ha affrontato una delle prime istruttorie riguardanti anzitutto il fenomeno del social *marketing*.

Nell'occasione, l'Autorità ha evidenziato che, se un indirizzo e-mail è presente su un *social network*, ciò non significa che possa essere utilizzato liberamente per qualsiasi scopo, poiché, per inviare proposte commerciali, è sempre necessario il consenso dei destinatari.

L'intervento del Garante ha preso spunto da un'articolata segnalazione di una società di consulenza finanziaria, lamentante l'invio di numerose e-mail promozionali indirizzate alle caselle di posta elettronica di alcuni suoi promotori senza che questi avessero dato alcun consenso al trattamento dei loro dati.

Dagli accertamenti, svolti presso la società dall'Autorità in collaborazione con il Nucleo Speciale Privacy della GdF, è emerso che la raccolta degli indirizzi di posta elettronica per l'invio delle proprie

comunicazioni promozionali avveniva anche attraverso i *social*, quali in particolare Linkedin, ove la società sanzionata è risultata avere fra i propri contatti alcuni intermediari finanziari della società segnalante.

Il Garante, anche sulla base delle Linee guida del 4 luglio 2013, che hanno disciplinato in via generale, fra i vari aspetti di protezione dei dati, anche il fenomeno del "*social spam*", ha quindi ritenuto illecito il trattamento degli indirizzi di posta elettronica. Infatti, come statuito nel provvedimento in questione, i dati reperiti sui *social network* e, più in generale, presenti *on line*, non possono essere utilizzati liberamente, a pena di violazione, anzitutto, dei principi di finalità e liceità del trattamento (potremmo aggiungere).

Non è stata ritenuta la tesi sostenuta dalla società secondo la quale l'iscrizione a un *social network* implica un consenso all'utilizzo dei dati personali per l'attività di *marketing*. Tale finalità non è stata ritenuta compatibile con le funzioni, potremmo dire naturali e tipiche dei *social network* che sono preordinate alla condivisione di informazioni e allo sviluppo di contatti professionali, e non alla commercializzazione di prodotti e servizi. Tesi peraltro affermata anche dal Gruppo *ex* articolo 29, secondo il quale l'iscrizione a un servizio presente sul *web* non comporta la legittimità del trattamento dei dati personali da parte di altri partecipanti alla medesima piattaforma ai fini dell'invio di informazioni commerciali.

Oltre alla contestazione amministrativa già effettuata dal Nucleo Speciale per il trattamento senza il necessario consenso, l'Autorità si è riservata di contestare, alla società autrice delle comunicazioni promozionali indesiderate, anche la violazione dell´obbligo di rilascio dell´informativa. Alla medesima società è stato anche prescritto di modificare il modello di richiesta di consenso presente sul sito, in modo che risulti chiaro lo svolgimento di finalità promozionali.

3. La necessaria valorizzazione dei nuovi principi del regolamento UE anche nel settore e-privacy

Con riferimento alle comunicazioni elettroniche, e in particolare a trattamenti potenzialmente notevolmente invasivi, come quelli svolti mediante i *social network*, è senz'altro auspicabile l'espressa valorizzazione, anche nel regolamento *e-privacy* in corso di definizione al quale è demandato il compito di ridisciplinare il settore in questione, di alcuni principi individuati già dal nuovo Regolamento UE, come peraltro quest'ultimo auspica espressamente[15].

[15] Cfr. considerando 173.

Non va trascurato che, a nuova concezione di privacy, sempre più ricca di diritti e facoltà di vario contenuto a favore del lavoratore interessato (si pensi ai nuovi diritti all'*oblio* e alla *portabilità* dei dati), dovrebbe (*rectius:* deve) corrispondere, simmetricamente, una diversa posizione giuridica in capo ai *data controller*, che si deve necessariamente arricchire e rafforzare di nuovi obblighi e responsabilità.

In questo senso, dovrebbero stabilirsi espressamente anche con riferimento alle comunicazioni elettroniche i nuovi principi, quali quello di *accountability*, ossia il principio di "autoresponsabilità" dei *data controller*, che, come è stato definito da autorevole dottrina (Modugno), è la "capacità di render conto" degli adempimenti e dei controlli in materia, anche tramite la relativa necessaria documentazione, prima ancora e a prescindere da un'eventuale (successiva) attività di controllo da parte del Garante.

Inoltre, proprio in base all'applicazione di tali principi, a partire da quello di *accountability*, e per espressa previsione del regolamento generale europeo con riguardo alla generalità dei titolari del trattamento, non sarà più possibile limitarsi ad adottare misure minime di sicurezza, prestabilite dal legislatore nazionale in un apposito testo tecnico (qual è famigerato allegato B al Codice anche in base all'articolo 33 del medesimo), ma occorrerà, indefettibilmente, adottare tutte le misure idonee da individuarsi in base alla previa valutazione da effettuarsi, caso per caso, in rapporto ai rischi specificamente individuati[16], con la possibilità, tuttavia, di ricorrere all'adesione a specifici codici di condotta oppure a schemi di certificazione per attestare l'adeguatezza delle misure di sicurezza adottate.

Tuttavia, occorre, al contempo, ricordare quale sia l'ambito oggettivo del GDPR, dal quale risulta escluso il settore delle comunicazioni elettroniche in vista dell'approvazione di una specifica disciplina di settore, la futura "*direttiva e-privacy*", per i citati trattamenti di dati personali nell'ambito dei *social network).* Nelle more, per tale trattamento di dati, la normativa europea di riferimento rimane la Direttiva 2002/58/UE, con le sue successive modifiche. Conseguentemente, parte del Codice (titolo X "comunicazioni elettroniche": articolo 121 ss.) e del *corpus* provvedimentale del Garante, incluse, solo ad esempio, le Linee Guida per posta elettronica e *internet* del 10 marzo 2007 [doc. web n. 1387522] e le menzionate Linee Guida in materia di *spam,* attenendo al settore della comunicazioni elettroniche e non risultando incompatibile con la disciplina eurounitaria, parrebbe ancora vitale, anche a seguito (dal 25 maggio scorso) della piena operatività della disciplina eurounitaria.

Al contempo, tuttavia, si può ritenere necessario implementare, sulla base di tale generale modello europeo, alcuni fondamentali adempimenti, quali quelli dell'informativa e del consenso. Sicché l'informativa resa agli utenti dei SSN dovrà contenere, tassativamente, tutti gli elementi dell'articolo 13

[16] Come previsto dall'articolo 32 GDPR.

GDPR (compresi i riferimenti al diritto alla portabilità; al diritto di reclamo presso il Garante e all'Autorità giudiziaria; ai tempi di conservazione dei dati raccolti). Inoltre, il consenso al trattamento dovrà essere acquisito con formulazione "inequivocabile", vale a dire con una manifestazione di volontà chiara, certo ed oggettivo, e dovrà essere documentato (o documentabile), in armonia con il menzionato fondamentale obbligo di *accountability*.

Il principio di *accountability*: la silente rivoluzione nella protezione dei dati

di Vincenzo Colarocco[*]

Uno dei pilastri fondamentali del Regolamento Europeo 679/2016 per la protezione dei dati personali (GDPR) è il principio di *accountability* che sta rivoluzionando l'approccio nei riguardi della *data protection*.

Il *Working Party* 29 (WP29) con il parere 3/2010 ha rappresentato, già nel luglio del 2010, come i principi e gli obblighi dell'Unione europea in materia di protezione dei dati siano spesso applicati in modo insufficiente cagionando di fatto una lesione dei diritti degli interessati. Ed infatti se la protezione dei dati non fosse diventata **parte integrante** delle pratiche e dei **valori condivisi** di un'organizzazione e se le relative responsabilità non fossero state espressamente ripartite, il rispetto effettivo delle norme in materia di protezione dei dati sarebbe stato messo notevolmente a rischio e gli incidenti in questo settore sarebbero inevitabilmente continuati.

Proprio per questa ragione, il WP29 ha avanzato una proposta concreta per l'introduzione di un principio di responsabilità che richiede ai titolari del trattamento di mettere in atto misure adeguate ed efficaci per garantire il rispetto dei principi e degli obblighi stabiliti nella direttiva. La *ratio* è quella di passare "dalla teoria alla pratica", garantire la certezza del diritto, pur ammettendo, al tempo stesso, una certa flessibilità, sì da consentire la determinazione delle misure concrete da applicare in funzione dei rischi connessi al trattamento dei dati, avuto riguardo delle differenti tipologie degli stessi.

Dunque, sul solco tracciato dal WP29 il GDPR con il Considerando 74 ha, sin da subito, precisato l'opportunità di stabilire la **responsabilità generale del titolare** del trattamento per qualsiasi utilizzazione di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci **dimostrando la conformità** delle attività di trattamento con il Regolamento. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche.

* Avvocato, esperto privacy

A ciò si aggiunga che il **principio di *accountability* è trasversale** all'intero impianto normativo del GDPR, basti pensare all'articolo 5 par. 2 ove,

> *"Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo (responsabilizzazione)"*

e all'articolo 24 par. 1:

> ***"****Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".*

Dunque, il Regolamento **rovescia la prospettiva** della disciplina in materia di protezione dei dati personali in quanto **tutto** il nuovo quadro normativo è prevalentemente incentrato sui doveri e sulla responsabilizzazione del **titolare** del trattamento, il quale determina le finalità e i mezzi del trattamento, nonché le misure di sicurezza ed ha **maggiore discrezionalità** nel decidere come conformarsi alle disposizioni del GDPR, pur avendo **l'onere di motivare** le ragioni a supporto di tali decisioni dimostrandone la conformità al Regolamento.

Ulteriore forza propulsiva del principio dell'***accountability*** è data dall'applicabilità dello stesso **a tutti i soggetti** che trattano dati personali e non solo al titolare del trattamento, ma anche al responsabile (articoli 28.1 ("*garanzie sufficienti*"), al *Data Protection Officer* (articolo 37.5 "*conoscenza specialistica della materia e delle prassi*"), alle persone autorizzate o designate (articolo 39.1.b "*formazione e sensibilizzazione del personale*"). Ed è proprio in questa ottica che si riesce a passare "dalla teoria alla pratica", garantendo la **concreta applicabilità** della protezione dei dati personali, riducendo sostanzialmente i rischi connessi al trattamento e alla tipologia di dati trattati. Del resto il principio di *accountability* ben potrebbe tradursi anche nel principio di **consapevolezza** secondo il quale ogni individuo conosce i rischi ed i diritti propri della società dell'informazione o meglio della società *data driven*.

Proprio in tale ottica il principio di *accountability* permea tutta la struttura del GDPR, sì da coinvolgere anche la **revisione dei processi**, ed infatti il titolare deve riesaminare ed aggiornare le misure adottate rivalutando anche la valutazione di impatto almeno quando insorgono variazioni del rischio e, insieme

al responsabile, assicurare su base continua riservatezza, integrità, disponibilità, resilienza dei sistemi tecnologici.

A ciò si aggiunga che la protezione dei dati personali, intrinsecamente dinamica, stante la stretta correlazione con le nuove tecnologie, ha la sua chiave di volta nel **rischio** per i diritti e le libertà dell'interessato, da intendersi a mero titolo esemplificativo come:

- perdita del controllo dei dati personali; limitazione di diritti; discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie;
- decifratura non autorizzata pseudonimizzazione; pregiudizio alla reputazione; compromissione del segreto professionale; qualsiasi altro danno economico o sociale significativo alla persona fisica, etc..

> Dunque, il principio di *accountability* può esser soddisfatto attraverso gli strumenti necessari idonei a mettere in pratica misure efficaci come le procedure per garantire l'identificazione di tutte le operazioni di trattamento dei dati e per rispondere alle richieste di accesso, lo stanziamento di risorse e la designazione di persone responsabili per l'organizzazione della conformità della protezione dei dati, la gestione dinamica del registro dei trattamenti.

In **conclusione**, lo sviluppo di nuove tecnologie e la costante globalizzazione dell'economia e della società hanno condotto ad una proliferazione di dati personali raccolti, selezionati, trasferiti o altrimenti conservati. I rischi connessi a tali dati, pertanto, si sono moltiplicati.

L'aumento sia dei rischi sia del valore dei dati personali in sé determina la necessità di rafforzare il ruolo che il titolare del trattamento, adottando un **approccio proattivo** e **dinamico,** è chiamato ad individuare e ad applicare mediante **misure** appropriate, **concrete** ed **efficaci**, al fine di realizzare i risultati richiesti dal GDPR.

Tutto ciò attraverso la creazione di **cultura** e consapevolezza all'interno della propria realtà.

Privacy in azienda: ripensare il modello organizzativo per minimizzare i costi e creare valore aggiunto

di Ludovica De Benedetti[*]

Il Regolamento Generale sulla Protezione dei Dati (GDPR) è pienamente in vigore in tutta Europa da diversi mesi. Per garantire la conformità alla nuova normativa, le organizzazioni hanno dovuto affrontare costi anche molto elevati. Questi costi potrebbero essere ridotti e potrebbero essere massimizzati i benefici derivanti dal trattamento di dati personali, attraverso un'adeguata divisione dei compiti.

Partiamo da un presupposto: nominare un DPO e delegargli l'attività di adeguamento alla nuova normativa è un approccio che si pone in contrasto con il dettato del GDPR per due ragioni. La prima è di natura pratica: se il DPO si deve occupare di tutte le attività di adeguamento alla normativa, spesso con scarse risorse, non può riuscire a svolgere le attività proprie della sua funzione quali la gestione delle richieste degli interessati o la sorveglianza sulla corretta gestione dei dati. La seconda è di natura giuridica: al DPO che, in base a quanto stabilito dal GDPR, è una figura (anche) di controllo, deve essere garantita l'indipendenza rispetto all'ente controllato. Se gli fossero demandate tutte le attività legate all'adeguamento e mantenimento degli obblighi previsti dal Regolamento, controllore e controllato finirebbero per coincidere.

Un DPO, da solo, soprattutto nelle realtà più ampie e complesse, non potrebbe gestire in modo efficiente tutti gli obblighi previsti dal GDPR. È allora particolarmente importante pensare ad un diverso modello organizzativo che possa venire incontro alla triplice esigenza di garantire l'indipendenza e l'effettività del ruolo del DPO, garantire l'efficienza nell'utilizzo dei dati e abbattere, quanto più possibile, i costi di adeguamento alla nuova normativa.

Al fine di raggiungere tali finalità risulta fondamentale procedere in due direzioni: da un lato prevedere una suddivisione ragionata dei compiti e delle responsabilità, dall'altro creare meccanismi che permettano una visione d'insieme dei trattamenti effettuati ed un continuo dialogo fra tutti i soggetti che trattano dati all'interno di un'organizzazione.

* (Privacy Professional, Consulente e Formatrice)

Quattro sono le azioni che, se integrate fra loro, possono aiutare un'organizzazione a raggiungere i massimi risultati per quanto riguarda l'adempimento degli obblighi privacy e un utilizzo efficiente dei dati:

1. la creazione di un ufficio che affianchi il DPO;
2. la riorganizzazione aziendale;
3. la creazione di un comitato privacy;
4. il coinvolgimento del DPO in tutte le attività afferenti al trattamento di dati personali.

La prima azione, la creazione di un ufficio dedicato (che, per semplicità, chiameremo Ufficio) che affianchi il DPO nello svolgimento dei suoi compiti, serve a garantire a quest'ultimo un supporto effettivo per lo svolgimento dei suoi compiti. A tale fine è fondamentale un'approfondita conoscenza della realtà aziendale in cui si opera ed è necessario creare una sinergia fra anima giuridica e tecnica per analizzare i possibili rischi sottesi ad un trattamento di dati personali. All'interno dell'ufficio devono, allora, coesistere più professionalità: giuristi, informatici, ingegneri, professionisti in ambito *risk management*; inoltre una parte dei membri dell'Ufficio dovrebbe essere scelta fra i dipendenti interni all'azienda (Ufficio Legale, *IT Security*).

La creazione di un Ufficio Data Protection non risolve, però, il problema dell'indipendenza del DPO (controllore e controllato continuerebbero a coincidere). Inoltre delegare tutti gli adempimenti privacy al DPO e al suo Ufficio non è una soluzione efficiente: ogni ente è suddiviso in aree funzionali (Ufficio Legale, *Marketing*, Credito). Ognuna di tali aree effettua determinati trattamenti di dati che possono, dunque, essere conosciuti in modo approfondito solo da chi lavora quotidianamente all'interno dell'area stessa. Solo questi ultimi soggetti, hanno la possibilità di tenere costantemente sotto controllo le particolarità ed inefficienze dei trattamenti operati e, di conseguenza, posso proporre soluzioni pratiche per garantire performance migliori per l'azienda.

È allora consigliabile ripensare i vecchi modelli organizzativi aziendali e prevedere una ripartizione dei compiti di *data protection* a livello delle singole aree funzionali richiedendo al responsabile di ogni area di coordinare le attività di *data protection* e di individuare i soggetti (uno o più anche in base alla complessità dell'area), fra coloro che lavorano con lui, che, in base alla conoscenza dei trattamenti ed al tempo a disposizione, possano operare quali punti di riferimento privacy. I referenti scelti dovrebbero adempiere operativamente a quanto previsto dal GDPR e interfacciarsi sia con il DPO, sia con il proprio responsabile di area, riferendo a entrambi la propria attività. In tal modo, è garantito un controllo costante e diffuso sull'adempimento degli obblighi privacy e si una divisione dei ruoli fra controllore

(DPO) e controllato (Titolare del trattamento) in quanto le attività operative di *data protection* non verrebbero effettuate dall'Ufficio del DPO, ma da soggetti interni al titolare stesso.

Abbiamo, inizialmente, detto che oltre a un'efficiente divisione dei compiti è necessario muoversi anche in una seconda direzione: garantire un dialogo fra tutti i soggetti che trattano dati personale nello stesso ente. La ragione sta nel fatto che raramente i trattamenti di dati personali si esauriscono in un singolo dipartimento e per tale ragione, può non essere sufficiente che ogni area tratti i dati nel modo più corretto perché il trattamento finale garantisca i risultati migliori all'azienda.

Attraverso la condivisione delle "*best practices*" e la partecipazione del DPO si possono garantire modalità di utilizzo dei dati più efficienti e conformi a quanto richiesto dalla normativa. Per garantire questo dialogo e migliorare le performance aziendali sarebbe utile prevedere una struttura di raccordo collettiva che possa valutare le problematiche connesse ai diversi trattamenti, individuare collegialmente le migliori modalità per affrontarle e prendere decisioni sulle questioni più impattanti per l'organizzazione, come la notifica agli interessati di un data *breach* o la decisione di procedere ad una consultazione preventiva all'Autorità.

Infine bisogna tener presente che il DPO rimane una figura di importanza fondamentale e non solo perché in alcuni casi la sua nomina è obbligatoria, ma soprattutto per la possibilità che ha di ad evitare inefficienze comunicative, aiutando le funzioni di business ad estrarre valore dai dati raccolti e trattati. A tal fine il DPO deve sempre mantenere una visione ampia e globale delle attività di trattamento di dati personali che si svolgono nella realtà in cui opera attraverso un dialogo costante con i responsabili e i referenti di ogni area che devono tenerlo aggiornato sull'attività che svolgono riguardante i trattamenti di dati e devono richiedere la sua consulenza in tutti i casi in cui ritengano necessario il suo supporto (formazione specifica, risposte agli interessati, valutazioni di impatto, violazioni dei dati, uso di nuove tecnologie).

In conclusione, è importante comprendere come il GDPR non debba essere visto solo come un costo per le organizzazioni, ma anche come un'opportunità. La nuova normativa richiede una maggiore conoscenza e consapevolezza riguardo alle modalità con cui si trattano dati personali. E proprio questa consapevolezza si può rivelare un'inestimabile risorsa, permettendo un utilizzo più efficiente dei dati e performance, anche economiche, migliori. Perché ciò sia possibile, però, come visto, sono necessari due fattori: una ragionata condivisione e suddivisione di compiti e responsabilità che permetta un controllo, aggiornamento e verifica costante e diffusa dei trattamenti e delle loro possibili inefficienze e un dialogo fra tutte le parti che trattano dati che garantisca una condivisione delle migliori soluzioni e pratiche e una risoluzione più efficiente delle problematiche legate ai trattamenti.

Risk assessment e DPIA

di Pasquale Di Gennaro[*]

Uno degli elementi di maggiore novità introdotti dal Regolamento (UE) 2016/679 sulla protezione dei dati, è la previsione che i titolari del trattamento predispongano una valutazione di impatto (DPIA–Data protection impact assessment o anche PIA–Privacy impact assessment) ogni qual volta un trattamento presenti rischi elevati per i diritti e le libertà delle persone fisiche. Per determinare se debba essere predisposta la DPIA per uno specifico trattamento, e cioè per accertare se i rischi siano elevati, è implicitamente necessario effettuarne una stima. Il processo di stima del rischio è noto come risk assessment, ed è un elemento propredeutico all'avvio di qualunque trattamento. Se all'esito di una prima valutazione il rischio dovesse risultare elevato, il processo stesso dovrà essere formalizzato e documentato in una Valutazione di impatto, e ne costituirà una parte fondamentale.

1. La protezione dei dati e il rischio

Il concetto di proporzionare le misure di sicurezza tecnico-organizzative ai *rischi* per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali, non è nuovo nella storia della *data protection*. Infatti, già il Codice italiano in materia di protezione dei dati personali[17], appena novellato dal D.Lgs. 101/2018 prescriveva, prima di tale ultimo intervento normativo, oltre alle misure di sicurezza *minime* l'adozione di misure di sicurezza cosiddette *idonee* che tenessero conto dei rischi peculiari al trattamento. Nel caso in cui il trattamento avesse presentato un *rischio specifico*, il Codice disponeva con l'articolo 17, il ricorso all'istituto della *verifica preliminare* (o *prior checking*) da presentare al Garante affinché potesse prescrivere misure speciali adatte a mitigare i rischi peculiari di quel trattamento. Il nuovo D.Lgs. 101/2018, con l'articolo 27, ha abrogato sia gli articoli riguardanti le misure di sicurezza minime e idonee, sia quelli riguardanti il *prior checking*. Tale modifica è stata resa necessaria per adeguare il Codice al GDPR e deriva dal fatto che per il GDPR le misure di sicurezza devono essere sempre proporzionate alle specificità di ciascun trattamento. Difatti, il Regolamento non prevede misure di sicurezza *minime* e puntuali[18], ma individua gli *obiettivi* di sicurezza. E prescrive che i titolari partendo dalla valutazione del rischio insito nel trattamento, lo mitighino individuando responsabilmente misure

[*] Già Funzionario direttivo presso il Garante per la protezione dei dati personali

[17] D.Lgs. 196/2003.

[18] Anche la pseudonimizzazione e la cifratura di cui all'articolo 32, par. 1, lettera a) vanno intese come mere tecniche di ausilio al conseguimento degli obiettivi di confidenzialità, integrità e disponibilità. Ma non misure minime.

e accorgimenti adeguati, diminuendo così la possibilità che i dati siano oggetto di violazioni di sicurezza. Il Regolamento oltre a fissare gli obiettivi di sicurezza definisce anche uno schema metodologico per perseguirli. Tale schema, che potremmo definire come *"risk based approach*", consiste pertanto nel salvaguardare gli obiettivi di protezione dei dati individuando e mitigando i rischi propri di ciascun trattamento. L'approccio orientato alla valutazione del rischio (*risk based approach*), insieme al principio di responsabilitazione (*accountability*[19]) costituiscono l'ossatura stessa del Regolamento.

2. La scelta delle misure guidata dal rischio

Il *risk based approach*, cioè l'adozione da parte dei titolari di un approccio basato sulla valutazione del rischio propedeutica all'avvio di ciascun trattamento, è così importante per il Regolamento che il termine "rischio" compare ben 75 volte nel testo, in varie espressioni. E tra le varie espressioni, quella che forse più efficacemente palesa la *ratio* dell'articolo 35, relativo alla "Valutazione d'impatto sulla protezione dati", risalta all'articolo 24 sulla responsabilità del titolare, laddove dispone che il titolare tenga "conto [...] dei *rischi aventi probabilità e gravità diverse* per i diritti e le libertà delle persone fisiche [...]". La valutazione dell'impatto che un trattamento può avere sui diritti e sulle libertà, non può prescindere dall'individuazione dei rischi e dalla stima della loro *probabilità e gravità*. Ma cos'è, dunque, un "rischio"? E in cosa consiste la sua valutazione (*risk assessment*)?

3. Cosa si intende per "rischio"

Nonostante il Regolamento citi il termine "rischio" più di 70 volte, non ne fornisce una definizione formale. L'Agenzia europea Enisa[20] nel suo glossario *on-line* sul *risk management* riprende la definizione generica ISO/IEC PDTR 13335-1, qui riformulata e semplificata per calarla nel contesto della protezione dati[21]:

> Rischio:
> con il termine "rischio" si intende la possibilità che una minaccia riesca a sfruttare le vulnerabilità insite in un sistema informativo per il trattamento di dati personali, causando danni agli interessati e all'organizzazione.

[19] Termine che in inglese sintetizza una dimensione soggettiva e una oggettiva della responsabilità: sento il peso della responsabilità derivante dalla fiducia che hanno riposto in me i miei clienti quando mi hanno affidato i loro dati personali, ma devo essere in grado di dimostrare di trattare tali dati responsabilmente. Ad esempio predisponendo la DPIA.
[20] *European Union Agency for Network and Information Security.*
[21] Per un approfondimento, si veda la definizione di "rischio" nella ISO/IEC 27000:2018 che ha assorbito e sostituito la ISO/IEC 13335

La definizione su riportata chiarisce un aspetto fondamentale: il rischio associato al trattamento dei dati personali ha una duplice dimensione: la prima relativa ai rischi per i diritti e le libertà degli interessati dal trattamento dei propri dati; la seconda relativa ai titolari (e responsabili) che si avvalgono di quei dati nell'ambito delle loro attività di impresa. Il GDPR focalizza l'attenzione sui rischi derivanti dai trattamenti per le persone fisiche. Tuttavia, se i rischi per gli interessati non sono opportunamente mitigati ne consegue un aumento del rischio d'impresa. In effetti, i danni derivanti per l'impresa non sono solo le possibili sanzioni motivate dalla *legal un-compliance*. Nella società dell'informazione, infatti, i dati personali sono un *asset* per le imprese, un patrimonio strategico da valorizzare e difendere costruito con fatica e solo dopo aver guadagnato la fiducia dei propri utenti. Si intuisce, pertanto, che le conseguenze per l'impresa derivanti dalla violazione della confidenzialità del proprio patrimonio aziendale, o dalla distruzione anche solo parziale di tale patrimonio, vanno ben oltre l'obbligo di inviare al Garante la notifica di *data breach* (articolo 33 del Regolamento), ma hanno a che fare con danni per l'impresa di natura patrimoniale e d'immagine. Assume dunque primaria importanza l'attività di prevenzione mirata a gestire e contenere i rischi (*risk management*) che parte proprio dalla loro individuazione e stima*:* il *risk assessment*.

4. Il *risk assessment*

L'individuazione e la stima dei rischi connaturati a uno specifico trattamento sono un'attività complessa. Complessa perché richiede un bagaglio di conoscenze multidisciplinari e di esperienze notevole. Oltre che di una conoscenza approfondita del contesto operativo. Tale complessità può essere utilmente gestita partendo proprio dal *rendere consapevoli*. Infatti, la consapevolezza dell'importanza del *risk management* nel processo di adeguamento al GDPR è già un traguardo importante che può influenzare produttivamente l'atteggiamento e la propensione alla collaborazione del vertice decisionale e degli altri *stakeholder* nell'organizzazione. La successiva individuazione e valutazione dei rischi andrà conseguita tenuto conto anche della dimensione e della complessità della realtà in cui si è chiamati ad operare. In realtà più articolate il *risk assessment* è certamente un processo che richiede la sinergia dei vari dipartimenti aziendali, legali e tecnici, e risulterà più efficace se conseguito in maniera sistematica e strutturata, avvalendosi di una metodologia. Ad esempio, Enisa ha recentemente pubblicato un *Handbook on Security of Personal Data Processing*[22] rivolto alle piccole e medie imprese che introduce una metodologia di valutazione del rischio e ne esemplifica l'applicazione discutendo alcuni trattamenti

[22] https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

ricorrenti. Nel caso delle micro-imprese si può comunque trarre beneficio dalle esemplificazioni Enisa, perché sono un valido ausilio a una pre-valutazione del rischio che consenta di determinare se lo scenario allo studio richieda o meno il ricorso ad una metodologia più strutturata. Un ulteriore utilissimo strumento sono le indicazioni del gruppo ex articolo 29[23], riportate in particolare nella *opinion WP* 248, che fornisce dei criteri per individuare i trattamenti ad elevato rischio e delle esemplificazioni che consentono di inquadrare la rischiosità di alcuni trattamenti "tipo" e comprendere laddove sia necessario o meno procedere con la predisposizione della Valutazione di impatto sulla protezione dati (DPIA).

5. Conclusioni

La gestione del rischio è una delle novità più importanti del GDPR, ma anche forse la più difficile da illustrare e da padroneggiare, perché reca in sé un cambio di mentalità: il passaggio dalla *legal compliance,* in particolare delle misure di sicurezza, intesa come una *check list* da smarcare, vecchio retaggio delle misure minime di sicurezza ormai superate; alla *legal compliance* come un obiettivo di adeguatezza delle misure di sicurezza tecniche e organizzative da perseguire con un metodo guidato dal rischio intrinseco, il *risk based approach*, che necessita dell'individuazione e della stima dei rischi come elementi propedeutici e necessari alla loro mitigazione. Il modo più efficace di conseguire gli obiettivi di protezione dei dati personali, ovvero di protezione delle persone *e* dell'impresa, è infatti *prevenire* i danni grazie all'efficace *mitigazione* dei rischi connaturati all'utilizzo dei dati personali. Dati che, nell'era dell'informazione completamente digitale, sono esposti alle molteplici e mutevoli minacce del cyberspazio.

[23] Sostituito dal Comitato europeo per la protezione dei dati, EDPB - European Data Protection Board

La decisione di adeguatezza nei trasferimenti dei dati extra UE

di Andrea Passano[*]

In una società tecnologica, dematerializzata e fluida quale quella moderna è sempre più frequente che i dati siano un flusso e che, nel corso del loro trattamento, circolino anche al di fuori dell'unione europea. Si pensi ad esempio ad un dato gestito e conservato in cloud, ove magari non si ha neppure certezza sul luogo in cui lo stesso si trovi.

Il criterio principale previsto dal GDPR affinché possa effettuarsi un trasferimento di dati al di fuori dell'Unione è la previa adozione, da parte della Commissione, di una decisione di adeguatezza, come previsto dall'articolo 45.

La Commissione, quindi, dovrà verificare se, nel contesto extra europeo, il livello di protezione dei dati è "adeguato", ovverosia equivalente a quello previsto dal GDPR. Nella valutazione la Commissione prende in considerazione una serie di criteri, elencati all'interno del Regolamento, quali lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti, e altri.

Le decisioni di adeguatezza, inoltre, non sono statiche ma soggette ad un riesame periodico per valutarne la rispondenza con lo status attuale della legislazione extra UE.

Nel caso in cui la Commissione decida che un paese terzo o un'organizzazione internazionale non garantiscono più un livello adeguato di protezione, il trasferimento di dati personali dovrà considerarsi vietato, a meno che non siano presenti altre garanzie adeguate indicate nel GDPR.

Acclarata l'importanza delle decisioni di adeguatezza va segnalato un recente intervento del WP 29 (ora European Data Protection Board) in merito. (il contributo è disponibile al seguente link http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).

Il gruppo di lavoro puntualizza una serie di elementi che devono essere presenti nello stato od organizzazione internazionale al fine di poter garantire un livello di protezione adeguato dei dati. Tale elemento acquista pertanto una grande rilevanza in quanto consente di fornire una maggior precisione

[*] Avvocato, esperto privacy

alle indicazioni contenute nell'articolo 45. Inoltre, consente anche ai soggetti extra Ue di avere delle linee guida da seguire per poter ottenere un parere positivo dalla Commissione.

I requisiti per la decisione di adeguatezza vengono suddivisi fra principi basilari il cui rispetto va sempre garantito, principi aggiuntivi più specifici per alcune tipologie di trattamento e, infine, procedure e meccanismi che devono essere presenti nello stato o organizzazione internazionale.

Quanto al primo gruppo si specifica che, basilarmente, il soggetto terzo deve essere fornito o comunque soggetto ad una normativa per la tutela dei dati. Non è necessario che la stessa sia del tutto speculare al GDPR, tuttavia deve racchiuderne i fondamenti ed i principi cardine. In secondo luogo devono essere sempre garantiti l'indicazione chiara della base del trattamento, la limitazione dell'uso dei dati per il tempo e per lo scopo per cui sono stati raccolti e l'utilizzo dei soli dati necessari evitando trattamenti di dati ultronei rispetto agli scopi prefissati.

Deve poi essere garantito un trattamento sicuro, che includa anche una protezione nei confronti dell'uso illecito, non autorizzato, delle perdite e della distruzione dei dati.

Viene poi richiesto che venga resa una informativa chiara, concisa, trasparente ed intellegibile dagli interessati i cui dati vengono trattati, salvo i casi in cui sia necessario, ad esempio per finalità di pubblica sicurezza, non fornire tale informazione.

Sul punto appare necessario effettuare una precisazione.

> La mancata informativa agli interessati per finalità ad esempio di ordine pubblico potrebbe costituire una agevole scappatoia per stati esteri in cui viga un regime differente da quello democratico. Ecco allora che assume rilievo l'indicazione preliminare, contenuta nell'articolo 45, per cui la Commissione deve tenere conto anche dello stato di diritto vigente. Appare infatti evidente che un regime totalitario difficilmente possa ottenere una decisione di adeguatezza anche se magari dotato di una normativa sulla protezione dei dati che però, nei fatti, viene ignorata per perseguire finalità antidemocratiche.

Procedendo con l'analisi il WP 29 segnala che deve essere fornito (con modalità che possono variare di caso in caso) un diritto di accesso, rettifica, cancellazione ed opposizione al trattamento dei dati. Anche in questo caso si possono richiamare le osservazioni effettuate per il punto precedente in tema di eccezioni per scopi di ordine pubblico.

Quanto al secondo gruppo di requisiti, quelli relativi a casi speciali, il WP 29 specifica che nel caso in cui si trattino dati particolari (ai sensi degli articoli 9 e 10 GDPR), è necessaria la presenza di una tutela

rafforzata per tutto il trattamento, a partire da una richiesta corretta di consenso al fino alla gestione tecnica del dato con misure di sicurezza aggiuntive.

Analogamente, una tutela rafforzata deve essere garantita nel caso in cui il trattamento avvenga per scopi di natura prettamente commerciali, quali la vendita diretta, ovvero nel caso in cui sia posto in essere per il tramite di un procedimento automatizzato. Nel primo caso si richiede che sia sempre garantita all'interessato la possibilità di modificare e rivedere il conferimento e l'utilizzo dei propri dati; nel secondo viene ritenuto necessario un consenso rafforzato, specie nel caso in cui dal trattamento automatizzato possano derivare degli effetti significativi sulla vita dell'interessato. L'esempio fornito è quello della profilazione, ad esempio bancaria in tema di erogazione di mutui e agevolazioni.

Il WP 29 specifica poi che una decisione di adeguatezza deve tenere in considerazione anche la presenza di procedure e soggetti terzi in grado di garantire il rispetto dei principi sopra indicati. Anche se naturalmente i mezzi che lo stato o l'organizzazione internazionale adopera possono differire da quelli previsti dal GDPR, si ritiene che vi siano alcuni punti fondamentali da utilizzarsi quali parametro per valutare l'adeguato livello di protezione dei dati.

In primo luogo si richiede che vi sia (almeno) un'autorità di supervisione competente ed indipendente. Nell'esercizio delle sue funzioni l'autorità dovrà agire con completa imparzialità ed indipendenza senza richiedere né accettare istruzioni da altri soggetti. Dovrà altresì essere fornita di tutti i poteri necessari per poter svolgere il compito assegnatole.

Strettamente correlato con la presenza di una valida autorità di settore, si richiede che chi è materialmente incaricato di effettuare l'attività di controllo sia un soggetto con un elevato grado di conoscenza della materia e preparazione specifica. Naturalmente tale dato si coniuga con l'*accountability*, ovvero sia la capacità dei controllori di garantire ed essere in grado di dimostrare il rispetto della normativa sulla tutela dei dati nell'attività svolta.

Infine si ritiene necessario che, al fine di garantire un livello di protezione dei dati equivalente a quello europeo, sia garantita all'interessato la possibilità di avere rimedi legali per far valere i propri diritti in modo rapido, efficace e senza costi proibitivi.

> In conclusione si può affermare che con il proprio contributo il WP 29 ha fornito preziose indicazioni che potranno essere utilizzate dalla Commissione nella sua attività di valutazione, anche e soprattutto alla luce delle rinnovate prospettive indicate dal GDPR.