ISSN 2039-6651
anno 2020 numero 56

MISCELLANEA INGV

Gli enti di ricerca e la protezione dei dati personali: una introduzione al GDPR

ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA

56

REGISTRAZIONE AL TRIBUNALE DI ROMA N.174 | 2014, 23 LUGLIO

ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA

ISSN 2039-6651
anno **2020** numero **56**

MISCELLANEA INGV

Gli enti di ricerca e la protezione dei dati personali: una introduzione al GDPR

Lucio Badiali

INGV | Istituto Nazionale di Geofisica e Vulcanologia, Amministrazione Centrale

Accettato 31 luglio 2020 | *Accepted 31 July 2020*
Come citare | *How to cite* Badiali L., (2020). Gli enti di ricerca e la protezione dei dati personali: una introduzione al GDPR. Misc. INGV, 56: 1-40, https://doi.org/10.13127/misc/56

In copertina Il rompicapo del GDPR | *Cover Solving the GDPR puzzle*

56

The makers of the Constitution conferred the most comprehensive of rights and the right most valued by all civilized men — the right to be let alone.

Justice Louis D. Brandeis
(in Olmstead v. United States, landmark supreme court ruling, 1928)

INDICE

Introduzione

Da una ricerca sulla *privacy* [Kaspersky, 2020] è emerso che il 69% degli italiani è preoccupato per la propria *privacy* e ha dichiarato per questo motivo di aver provato a cancellare le proprie informazioni private dai siti web o dai social media. A tal riguardo, prosegue il report, che il 50% degli utenti italiani non ha saputo come fare e che il 12%, sempre degli utenti italiani, ha raccontato che i propri dati personali o le informazioni sulla propria famiglia sono diventati di dominio pubblico senza il loro consenso.
La fase di *smart working*, inoltre, ha portato un ravvivato interesse nei riguardi della disciplina della *privacy*. Sono infatti arrivate molte più richieste di chiarimenti ai Responsabili della Protezione dei Dati (o come si usa più spesso, in inglese, DPO: *Data Protection Officer*) in merito ad operazioni di trattamento di dati personali ed alla loro legittimità. Un *vademecum* minimo può dunque tornare utile a decodificare alcune informazioni che ci riguardano.
La normativa è articolata ed unica ma, nel dettaglio, ogni ente o azienda ha delle particolarità che portano ad accentuare alcuni punti rispetto ad altri: un ente di ricerca (d'ora in poi EPR) e una azienda sanitaria possono avere differenti sensibilità al riguardo.
Lo scopo di questo lavoro è duplice: fornire da un lato le regole del gioco della cosiddetta *privacy*, le quali si trovano principalmente nel recente GDPR[1] [GDPR, 2016], così da iniziare a giocare una partita che riguarda tutti, non solo dentro l'ente ma pure nella società come cittadini e, dall'altro informare e formare ufficialmente i dipendenti dell'ente come richiesto con precisione dal più ampio obbligo previsto dall'articolo 32 del GDPR perché, come recita, chiunque: "abbia accesso a dati personali non tratti tali dati se non è istruito". La formazione aziendale in ambito *privacy* è necessaria per rendere sia i soggetti autorizzati che gli incaricati consapevoli dei trattamenti di dati personali che svolgono quotidianamente e anche per limitare i rischi di sanzioni. Come si vedrà, sono davvero pochi i casi in cui si sfugge dal ricoprire un ruolo nella filiera della *privacy*. Prima o poi si gioca un ruolo nel "trattamento dei dati personali": non bisogna essere necessariamente in una amministrazione o in una segreteria per trattare dati personali, si può anche partecipare alla gestione di un progetto per giocare la partita. Già nell'introduzione, senza averci fatto caso, sono stati usati dei termini che hanno una valenza normativa, non solo nel linguaggio ordinario. Alla fine del lavoro sarà più chiaro che col GDPR si è dato avvio ad una vera propria nuova prassi cui conformarsi a livello europeo.
L'*app* IMMUNI è un tema caldo al tempo del Covid-19: viola o meno la *privacy* del cittadino? Chi crede che la *privacy* in situazioni di emergenza diventi un dettaglio trascurabile o un'inutile perdita di tempo, ha una concezione della riservatezza ancora "burocratica" ed un po' datata, tipica dell'Ottocento-Novecento. La *privacy* non è un insieme di formalismi e norme strumentali che frenano lo sviluppo digitale della società. Seguendo le attuali normative, come si vedrà, è possibile fare (quasi) tutto a "norma di legge" senza pensare a inutili violazioni o intromissioni nella vita privata. Sull'*app* il Garante Privacy si è pronunciato affermando che il "sistema di *contact tracing* prefigurato non appare in contrasto con i principi di protezione dei dati personali" [Garante, 2020] ma bisogna seguire le norme che stiamo per approfondire.
Anche l'atto di prendere la temperatura all'ingresso del luogo di lavoro diventa lecito - solo se - si seguono le regole del gioco (che vanno conosciute ed applicate: prendere la misura anche se solo di temperatura, può costituire un trattamento di dati personali illecito e pertanto sanzionabile).

Keywords GDPR, Accountability, DPO

[1] Si consideri il termine GDPR in modo banalizzato come "la nuova legge sulla Privacy". Al cap. 2 primo capoverso verrà spiegato in maggior dettaglio.

1. *Privacy* o protezione dei dati personali?

Il concetto di *privacy* inteso come *the right to be let alone* [Warren and Brandeis, 1890] non è certamente tipico dei paesi mediterranei che hanno una tradizione giuridica differente da quella anglosassone. Ciò fa intuire perché ancora oggi in Italia si possa considerare, a torto, la *privacy* un diritto sacrificabile. Il concetto formalizzato di *privacy* nasce negli USA e si fa risalire al celebre articolo di S. Warren e L. Brandeis pubblicato nella prestigiosa Harvard Law Review nel 1890 che applicava il principio di riservatezza anche alla sfera personale estendendo una precedente decisione presa dalla *High Court of Chancery* britannica nel caso Prince Albert contro Strange del 1849, in cui oggetto del contendere era un vantaggio economico tratto dalle raffigurazioni della regina Vittoria e del principe consorte Albert [Tomsett, 1848].
Oggi la *privacy* non è più, o meglio non è più soltanto, il diritto ad essere lasciati in pace. È la protezione di ciò che si riferisce al cittadino nella sua duplice identità, fisica e digitale. Tutto ciò che lo riguarda, o può identificarlo, è dato personale. La nuova normativa "protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali" [GDPR, 2016] e tratta di "norme relative alla libera circolazione di tali dati", e della "libera circolazione dei dati personali nell'Unione" (*ibid.*).
Non più mera riservatezza vecchio stampo: la *privacy* e la protezione dei dati personali c'entrano ogni giorno di più con la possibilità di trovare e mantenere un lavoro, con il diritto di circolare, fare impresa, col poter votare liberamente alle elezioni, avere una propria opinione senza che questa possa essere usata contro la persona stessa, ecc.
Come regola del gioco, bisogna sempre ricordare che la protezione dei dati personali deve essere sempre bilanciata con la libertà di espressione, il diritto di critica e cronaca, il diritto a essere informati. I trattamenti di dati con queste finalità non soggiacciono a tutte le norme in materia di protezione dei dati personali o comunque hanno alcune particolari esenzioni a favore (per es. l'attività giornalistica).

2. Il GDPR e la *privacy*

Il precedente paragrafo virgolettato riassume il primo articolo della nuova legge che è il Regolamento EU 679/2016, noto come GDPR (*General Data Protection Regulation*) e che sostituisce la precedente Direttiva dalla quale nacque il celebre Testo Unico della *privacy* (il d.lgs. 196/2003 o T.U.). Il GDPR, composto da 99 articoli e 173 Considerando[2], in realtà, non parla mai di *privacy* bensì di dati personali, della loro protezione e del loro muoversi con tutte le tutele nel mercato comune.
Il GDPR non è una "successiva modificazione e integrazione" del vecchio testo unico. Un Regolamento europeo, fonte di diritto derivato, è un atto legislativo vincolante che deve essere applicato in tutti i suoi elementi nell'intera Unione europea e questo si applica a tutti i cittadini senza mediazione ulteriore dello Stato. In un primo momento si pensò di abrogare del tutto il precedente testo unico, perché il Regolamento è di per sé sufficiente. Poi, per mantenere i risultati degli anni precedenti, si è proceduto in modo diverso: novellando il d.lgs. 196/2003 con il d.lgs. 101/2018 [D.LGS., 2018]. In breve, sono stati abrogati quasi tutti gli articoli al suo interno e si sono allineati quelli che non contraddicevano il Regolamento con le sue nuove disposizioni.
Un punto importante del GDPR è che vale ovunque nello spazio dei paesi membri europei e si applica anche alle imprese straniere che devono adeguarsi alla normativa quando trattano dati di soggetti residenti all'interno dell'Unione. Uno degli scopi del GDPR, a lungo termine, è il

[2] Considerando o motivazione, è in modo conciso la norma essenziale dell'articolato, senza riprodurne o parafrasarne il dettato. Racconta e spiega il senso delle norme usando una forma differente.

contribuire a ripristinare la fiducia e l'equità tra società e utenti (interessati o consumatori) in un mondo guidato sempre più dai dati. Il GDPR è un regolamento di protezione dei dati con una portata molto estesa e sta servendo da modello per le normative future. È stato preso come esempio per conformità dal *California Consumer Privacy Act* (CCPA) e anche il Regno Unito (dove vige ancora il GDPR) sta preparando un nuovo disegno di legge sulla protezione dei dati che seguirà gli stessi requisiti del GDPR, così che si applichino le stesse regole europee in futuro dopo la sua uscita dall'Unione.

3. I dati personali ed il loro trattamento

L'art. 4 del GDPR recita:

1. «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
2. «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

La società dell'informazione ha mutato il rapporto tra cittadini, amministrazioni e aziende. Ognuno possiede un *doppelgänger* - il suo doppio digitale - nella parallela società "virtuale". Il mondo pervasivo e sempre presente, l'*online*, generato dalla tecnologia è un'appendice della realtà primaria, dove l'entità, che sia il privato, l'azienda o l'amministrazione, vive una vita aumentata ed iperrelazionata. Un dato, o meglio un insieme di dati, dopo esser stati analizzati e processati possono restituire informazioni coerenti e permettono di eseguire inferenze e previsioni. In campo scientifico la cosa assume immediatamente un senso. Da questo punto di vista un dato personale altro non è che un dato come un altro: la tutela, la cura ed il trattamento per un dato deve essere la stessa a prescindere dalla sua origine. Un dato, in qualunque accezione, è come una traccia d'oro dentro una miniera. Il dato personale, in aggiunta, porta con sé una possibile identità ed un intero universo legato alla persona ma la sua gestione non è differente da un qualunque altro dato portatore di significato ed importanza. Le tecniche e la letteratura sulla gestione dei dati valgono ancora in questo contesto. Questo dettaglio non andrebbe trascurato in enti di ricerca che sono abituati già a trattare dati, a verificarne la qualità e a proteggerli. In un ente è facile riconoscere i trattamenti in ottica GDPR. L'analisi del cartellino delle presenze, la preparazione di una busta paga, la gestione delle trasferte, l'analisi del traffico di rete ascrivibile a un dipendente o dei visitatori a un sito web, ecc. Un dato personale è comunque un concetto dinamico da riferirsi sempre al contesto. Se un'informazione è isolata ed innocua e pare non sia in grado di portare all'identificazione di un individuo, il fatto che questa informazione possa essere utilizzata per l'identificazione tramite incrocio con altri dati ne determina comunque la natura di dato personale.
A volte è la Giustizia per mezzo di sentenze a definire un dato personale, come per esempio l'immagine di una persona costituisce dato personale [CASS.13663/16, 2016], trattandosi di dato immediatamente idoneo a identificare una persona a prescindere dalla sua notorietà.
Il precedente testo unico sulla *privacy* parlava di dati personali così delicati che il loro trattamento

doveva ricevere una cura più attenta. Erano i dati noti come sensibili. Con il GDPR ora sono dati particolari (art. 9: trattamento di categorie particolari di dati personali) e sono quei dati personali che "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale". È vietato trattare sia quelli che i "dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". Divieto superabile, come si vedrà in seguito, se l'interessato ha prestato il proprio consenso esplicito per finalità specifiche o se il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato). Il trattamento è possibile in caso sia necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso. Se il trattamento si rende necessario per motivi di interesse pubblico, e in special modo nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute, il divieto può decadere.
Vale come sempre la regola che se i dati personali sono resi manifestamente pubblici dall'interessato nulla vieta di trattarli.

4. Identificazione e identificabilità della persona

Tutelare il dato personale significa tutelare l'insieme dei diritti collegati all'identità personale. Come regola generale, un dato si considera personale quando consente l'identificazione dell'individuo oppure se riesce a descriverlo in modo tale da identificarlo permettendo di acquisire ulteriori dati sulla persona stessa. La tutela è sia sul dato che sul meccanismo che porta ad una maggiore conoscibilità: entrambi sono ugualmente tutelati. Per identificazione, quindi, si intende la possibilità di distinguere la persona sia da qualsiasi altro soggetto sia all'interno di una categoria. Non serve ottenere un alto grado di identificazione perché il dato sia assoggettato a tutela: "identificabile" è la persona che può essere "identificata" anche mediante il riferimento ad ulteriori elementi. Il dato personale, dunque, diventa un concetto dinamico da contestualizzare. Se pure, una singola informazione non potesse immediatamente portare all'identificazione di qualcuno, il fatto stesso che quella può usarsi insieme ad altri dati, ne determina lo stesso la natura di dato personale.
Si arriva all'identificabilità mediante incrocio di informazioni che inizialmente sembravano poco correlate. La tecnologia tramite di *Machine Learning*, inoltre, incrementa molto le capacità di correlazione ed identificabilità fino all'ottenimento di profili automatici.
Un esempio aiuta a chiarire. Oggi, non occorre che l'informazione sia in grado di individuare fisicamente la determinata persona. Una azienda di pubblicità, tra le varie tecniche di tracciamento per identificare singolarmente un individuo in mezzo a tanti navigatori online, punta al suo browser (o al suo dispositivo digitale) col quale naviga in rete. Anche questi dati (*cookie*, *fingerprint*, IP, ecc.) rientrano perciò nei dati personali. La Corte di Giustizia europea ha definito espressamente l'indirizzo IP (*Internet Protocol*) come dato personale, pure in riferimento all'IP dinamico nella sentenza "Breyer contro Germania" [CURIA, 2016]. L'account di un servizio *online* è sicuramente un dato personale, in quanto consente di identificare univocamente una persona, così come la mail, il nickname. In generale, il GDPR include espressamente nei dati personali gli identificatori online, geolocalizzazione compresa. In prima battuta, il fatto che l'IP sia considerato dato personale impedisce ad una azienda di ottenere dall'ISP (fornitore di accesso ad Internet) il nominativo di un soggetto che ha scaricato file piratati online. Lo stesso è impedito, sempre in prima battuta, al datore di lavoro nei riguardi del dipendente. Bisogna arrivare ad una "seconda battuta", con cautele e garanzie, per poter operare in tal senso.

5. Quando il GDPR non si applica

La Corte dei diritti dell'uomo ha affermato che non esiste una netta separazione tra vita privata e vita professionale[3] in relazione ai dati personali, dunque le informazioni riguardanti la vita professionale e pubblica di una persona sono dati da tutelare. Tuttavia, se necessario l'autorità giudiziaria può accedere ai dati personali come espresso nell'art. 2.2.d[4]. *Il presente regolamento non si applica ai trattamenti di dati personali: effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse.*
Ma anche il trattamento eseguito da una persona fisica per l'esercizio di attività a carattere esclusivamente domestico o privato è escluso dal campo di applicazione materiale (la c.d. *household exclusion provision*). Per interpretare l'art. 2.2.c torna utile il Considerando 18: *Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.* Chiunque, se vuole, può liberamente esporre i suoi dati personali sui social e ne è responsabile.
Resta, ovviamente, una più stringente responsabilità al gestore del social. Su questo rapporto, ad es., si è innestato il caso Cambridge Analytica.

6. Il principio dell'accountability

La regola più importante del gioco riguarda la figura a capo di tutto, il Titolare del trattamento, che qui compare solo accennata e viene specificata in seguito. Il Regolamento ha un principio cardine che è tipico in sistemi *common law* anglosassoni: l'*accountability*. Una chiara affermazione di questo principio è riecheggiata in Senato durante l'audizione del 7 giugno 2018 durante la discussione sulle modifiche del previgente testo *privacy* in ottica GDPR: "*… vanno anzitutto individuati i princìpi sui quali si fonda il Regolamento. Uno dei più importanti tra questi – forse il principio dei princìpi – è l'Accountability (art. 24). Principio che introduce una sorta di rivoluzione copernicana nella legislazione europea di settore, segnando il passaggio da un modello prescrittivo e formalistico ad un modello di responsabilità/rendiconto e di sostanziale protezione dei dati. Si abbandona, così, una tecnica di regolazione delle condotte basata sull'elencazione dettagliata delle prescrizioni per il trattamento e sulla determinazione delle relative sanzioni di una individuazione del bene da proteggere, dello scopo da perseguire, della tutela dei dati da garantire. Ecco il passaggio al principio-responsabilità: spetta al titolare del trattamento il compito di individuare modalità, garanzie e limiti del trattamento dei dati in coerenza con i princìpi e le disposizioni del regolamento. Il titolare, dunque, anziché conformarsi ad una serie di regole imposte dall'esterno (e il cui rispetto formalistico non è detto che garantisca la tutela effettiva del dato), deve adottare una condotta proattiva, idonea a dar prova in concreto (rendicontare) delle misure giuridiche, organizzative, tecniche adottate al fine di assicurare una piena attuazione del Regolamento*" [Punzi, 2018].
È dunque l'*accountability* un principio di responsabilità dove si è pronti a rispondere in prima persona delle scelte tecniche ed organizzative, e come vedremo, con sanzioni davvero elevate. Non è né il principio della trasparenza amministrativa che ha assunto per la prima volta una

[3] Per es. vd. sentenza 16 dicembre 1992 Niemietz contro Germania, serie A 251 B.

[4] Anche quando non espressamente riportato, il riferimento dell'articolo è sempre il GDPR.

forma tangibile con la promulgazione della Legge 241/90 né quello ascrivibile all'art. 97 della Costituzione. Nell'art. 24 del GDPR c'è il portatore di un diritto, l'interessato, e colui che lo deve garantire, il Titolare del trattamento (figure che vedremo meglio tra poco). Non esiste il rivolo delle responsabilità delegate cui è abituato il dirigente dello Stato, la ricerca affannosa di capire dove il trattamento ha avuto problemi, ritardi o una eventuale falla.
Se volessimo tentare una analogia con l'azione amministrativa, potremmo dire che se questa non fosse del tutto efficace ed efficiente – segno di un buon equilibrio tra risorse impiegate, obiettivi prefissati e risultati conseguiti, ovvero proprio l'obiettivo di una Pubblica Amministrazione - e fossimo in uno degli altri tre possibili casi - efficace ma non efficiente; efficiente ma non efficace; inefficace ed inefficiente - non ci sarebbe dialettica nei confronti dell'Autorità Garante e/o con la Giustizia: la sanzione per il Titolare potrebbe raggiungere i 20 milioni di euro o il 4% del fatturato.
L'*accountability* è quindi la capacità di poter rendicontare dimostrando ex post di aver fatto il meglio possibile non basandosi sulle sole norme ma tenendo conto degli standard che offre il particolare momento storico. È un concetto dinamico che cerca di continuo nuove forme attraverso le prassi, le *best practice* del momento aggiornandole di volta in volta e cercando costantemente la migliore efficienza del sistema. I principi generali del trattamento di dati personali sono all'articolo 5 paragrafo 2 che richiede al titolare di rispettare alcuni princìpi fondamentali e di essere in grado di comprovarlo. Brevemente, questi cinque sono:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati (i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento);
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione (è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento);
- integrità e riservatezza (ne va garantita la sicurezza adeguata).

7. Le misure tecniche e organizzative

Il GDPR responsabilizza in modo esplicito. Nell'art. 32 si occupa nello specifico della sicurezza del trattamento dei dati personali: *tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*. La sicurezza va necessariamente garantita attraverso l'adozione di una serie di misure concrete.
Chi è a capo del trattamento dei dati personali deve predisporre ed attuare delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio.
Per fare questo si deve tenere debitamente conto dell'attuale stato dell'arte (della tecnologica disponibile, dei sistemi informatici, ecc.), dei costi di attuazione, della natura dei dati e dei meccanismi adottati, del campo di applicazione, del contesto e delle finalità del trattamento dei dati, oltre che del rischio per i diritti e le libertà delle persone fisiche che può essere più o meno probabile e più o meno alto a seconda di ciascun diverso contesto. L'art. 32, paragrafo 1 fornisce alcuni punti importanti:

1. *la pseudonimizzazione*[5] *e la cifratura dei dati personali;*
2. *la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;*
3. *la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;*
4. *una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

Il paragrafo 2 poi continua: *nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.*
Nulla è lasciato al caso, nulla è delegato ad altri. Il cuore dell'*accountability* non è far sì che nulla di inaspettato accada bensì di dimostrare di essere stati previdenti e consapevoli per quanto sia ragionevolmente possibile.
Le vecchie misure minime di sicurezza (come in Allegato B del d.lgs. 196/2003) erano assolutamente prescrittive e totalmente estranee al principio fondante del GDPR. Per ricordarne una assai nota, le password dovevano essere lunghe almeno 8 caratteri. Un obbligo poco utile oggi in tempi di *cyber-security*. AgID nella Circolare n. 2/2017 del 18 aprile 2017 [AgID, 2017], ne ha prodotte di nuove, più aderenti al momento e queste sono state prese come un modello per le amministrazioni. Le nuove misure sono un riferimento pratico per valutare e migliorare il livello di sicurezza e consistono in controlli di natura tecnologica, organizzativa e procedurale e utili per valutare il proprio livello di sicurezza informatica.
Il Garante dopo il recente caso INPS ha scritto: *Quella della mancanza di sicurezza delle banche dati e dei siti delle amministrazioni pubbliche è una questione che si ripropone costantemente, segno di una ancora insufficiente cultura della protezione dati nel nostro Paese* [Perilli, 2020]. Il Garante ha voluto porre l'accento non tanto, o non solo, sullo specifico caso INPS, che resta grave, ma più generale sull'attitudine che ha portato a questo ovvero che si pone da troppo tempo poca attenzione sul tema culturale della sicurezza e prevenzione dei dati personali.
I *data breach* sono gli incidenti di sicurezza successivi alle intrusioni in sistemi che contengono dati privati o riservati che, anche se per pochissimo tempo, vengono nelle mani di soggetti non autorizzati. In senso lato, non solo la divulgazione di dati personali e confidenziali è una breccia ma anche il fermo temporaneo di un servizio garantito all'utente. La perdita accidentale, il furto, l'infedeltà aziendale, l'accesso abusivo sono degli esempi di effetti legati a *data breach*. Il Titolare ha l'obbligo di notificare la violazione entro 72 ore dal momento in cui viene a conoscenza del fatto e comunque "senza giustificato ritardo". Tutta la documentazione relativa alle misure tecniche ed organizzative deve essere disponibile perché questo è un classico caso in cui sta al Titolare dimostrare di aver fatto davvero il possibile.

8. I ruoli nel GDPR

Il GDPR è un gioco con poche pedine. Le figure sono ridotte rispetto al previgente T.U. della *privacy*. Il nuovo Regolamento ha semplificato la catena di responsabilità in ambito *data protection*. Per capire come funziona la partita vediamo i ruoli.

[5] La pseudonimizzazione è una tecnica che consiste "nel trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile" (art. 4 punto 5 del GDPR).

8.1 L'interessato

L'interessato, già introdotto come persona fisica cui si riferiscono i dati personali oggetto di trattamento, è il cittadino portatore di diritti. È colui che sta al centro del gioco ed i cui interessi e la sua libertà vanno tutelati. È il destinatario finale della tutela predisposta dall'Unione per quanto riguarda le operazioni di trattamento dei suoi dati. Tra i diritti fondamentali ci sono quello di ricevere una corretta e idonea informativa riguardante il trattamento dei suoi dati (artt. 13 e 14 del GDPR), il diritto di accesso ai dati, all'oblio, la rettifica dei dati, il diritto di limitazione e di opposizione al trattamento e il diritto alla portabilità dei dati. Inoltre, secondo l'art. 77, comma 1, *fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo* all'autorità competente. L'amministrazione troppo spesso non è consapevole dei diritti dell'interessato. Ad esempio nella dinamica del consenso come base giuridica di un trattamento, l'interessato può sempre chiedere di conoscere lo stato dei consensi che in precedenza ha fornito, come sono trattati e mantenuti. E l'amministrazione deve saper rispondere riprendendo tali consensi, mostrarli, ed in caso anche cancellarli perché, se richiesto, non siano più disponibili. Una delle domande che può mettere in crisi molte amministrazioni pubbliche da parte del suo dipendente o del cittadino in generale, è proprio nel chiedere di sapere dove sono i suoi dati, i suoi consensi e chi li sta trattando. Non è davvero cosa difficile poter arrivare a richieste di risarcimento dei danni per trattamento illecito dei dati. Il GDPR consente al soggetto interessato di tutelarsi facendo valere i suoi diritti nel caso reputi ci sia una violazione nel trattamento dei suoi dati personali. Ogni Stato dell'Unione ha una sua propria Autorità di controllo che è anche competente per la ricezione dei reclami su eventuali violazioni del Regolamento (come pure delle norme nazionali) in materia di protezione dei dati. L'Autorità di controllo nazionale per il nostro paese è il Garante per la protezione dei dati personali cui l'interessato propone un reclamo, ovvero un atto circostanziato in cui si denuncia la presunta violazione delle disposizioni in materia di protezione dei dati personali. È un atto che può essere proposto senza particolari formalità basta che contenga l'indicazione dei fatti e delle circostanze relative, delle disposizioni che si presumono violate e dell'istante in cui sono accaduti. Al reclamo può seguire una fase istruttoria come pure un eventuale procedimento amministrativo a seguito del quale possono essere adottati vari provvedimenti, ad esempio, il blocco del trattamento o l'adozione di misure al fine di rendere il trattamento conforme alla normativa.

8.2 Il Titolare del trattamento

Nel punto più alto della filiera della protezione dati, come già anticipato, si trova il Titolare del trattamento (nell'originale, il *Data Controller*) ovvero *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali* (art. 4. par. 1, n. 7 GDPR). In sostanza il Titolare è chi tratta i dati senza ricevere alcuna istruzione da altri, colui che decide il "come" e il "perché" devono essere trattati i dati. Il Titolare del trattamento, dunque, non è chi gestisce i dati, ma chi decide motivi e modalità del trattamento. Ed è proprio il Titolare colui che è soggetto al descritto principio di *accountability*. Tornando all'analogia del gioco, se la partita finisse male, lui perderebbe e risponderebbe più di tutti gli altri.
Il Titolare è responsabile giuridicamente del rispetto degli obblighi di legge (nazionale e internazionale) in materia di protezione dei dati personali. È lui che risponde dell'adozione delle misure tecniche e organizzative adeguate per garantire la tutela dei diritti dell'interessato, garantisce che i dati non siano persi, alterati, distrutti, trattati in modo illecito. Al Titolare spetta, con la nuova norma europea, anche la redazione del "Registro dei trattamenti" (descritto in

seguito) e la formazione del personale. Sempre a lui è in carico la documentazione delle eventuali violazioni dei dati personali, e lui deve spiegare motivando le circostanze, le conseguenze e i provvedimenti adottati per porvi rimedio. Al Titolare sta anche un ulteriore importante compito: la nomina del Responsabile della Protezione dei Dati (il DPO) e la sua comunicazione ufficiale all'Autorità Garante nazionale.
Nel settore pubblico, quale ricade un EPR, Titolare del trattamento è l'ente nel suo complesso (l'istituto, il ministero, l'ente pubblico, l'associazione, ecc.). Nel nostro caso questo si specifica come la figura che ha potere di rappresentanza, appunto il legale rappresentante che è il presidente pro tempore (mentre in un ministero potrebbe essere il ministro). Si ha, quindi, una duplice gerarchia che ad un capo vede il Titolare-presidente per la protezione dei dati, ed il direttore generale-datore di lavoro (che dipende dal CdA e dal Presidente) per la gestione dei rapporti di lavoro e la realizzazione degli obiettivi.

8.3 Il Responsabile del trattamento

Il Responsabile del trattamento (o *Data Processor* nella versione originale del GDPR) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR). È un soggetto - distinto dal Titolare - cui il Titolare si affida e al quale delega l'esecuzione di alcuni compiti. Questo nuovo Responsabile deve essere in grado di fornire garanzie tali da assicurare il rispetto delle disposizioni sul trattamento dei dati personali, prima tra tutte la tutela dei diritti dell'interessato. Su questo punto la responsabilità del Titolare è molto alta e se uno cerca bene, trova negli enti figure, più spesso individuate in società, che andrebbero nominate Responsabili. Il Titolare del trattamento risponde della gestione effettuata dal Responsabile per i compiti che gli affida e perché è lui che lo sceglie dopo aver attentamente valutato che presenti le garanzie sufficienti in termini di conoscenza della materia, affidabilità e risorse, così da attuare le misure tecniche e organizzative che soddisfano i requisiti del GDPR (Considerando 81). Tra i compiti del Titolare c'è quello di valutare il rischio del trattamento che pone in essere per mezzo dei vari Responsabili. Il Titolare deve quindi poter sempre sindacare le decisioni del Responsabile per non trovarsi in situazioni spiacevoli da giustificare di non conformità alle leggi. Anche il precedente testo del 2003 prevedeva una figura di responsabile che poteva essere "interno" alla società (per noi, all'interno dell'ente). Con il GDPR questo non è più possibile. Il principio di *accountability* carica il peso della responsabilità sul Titolare solamente. L'escamotage di creare un Responsabile che dipende in modo subordinato dal Titolare si configura in una mancanza di libertà di movimento per il Responsabile stesso ed una via di uscita nello scarico di responsabilità per il Titolare. Un Responsabile ha senso, dunque, solo se esterno nel rapporto con l'ente che lo nomina. Internamente le responsabilità, nell'accezione *privacy*, non si scaricano mai, tuttavia è possibile delegare alcune funzioni, come vedremo poi, grazie alle novità introdotte col d.lgs 101/2018 [D.LGS., 2018]. Il GDPR richiede espressamente un contratto o atto giuridico per nominare un Responsabile del trattamento. Questo contratto è definito tecnicamente *Data Protection Agreement* (DPA). Il DPA disciplina quale sia l'esecuzione dei compiti del Responsabile e contiene le indicazioni relative alle materie indicate al comma 3 dell'art. 28, tra cui la natura, la durata e le finalità del trattamento, la tipologia dei dati oggetto del trattamento, le misure tecniche e organizzative adeguate e necessarie ad assicurare il rispetto delle indicazioni ricevute dal Titolare. Il DPA ha il fine di suddividere in modo chiaro compiti e responsabilità tra i soggetti attivi del trattamento dati (Considerando 79). Il DPA è fondamentale perché il Responsabile è tenuto a rispondere dei danni qualora non si sia attenuto alle indicazioni del Titolare e non abbia adempiuto gli obblighi presenti nel DPA. Dalla teoria alla pratica: siamo in grado di individuare nelle nostre attività un possibile Responsabile ogni volta che si contrattualizza una fornitura di servizi all'ente. Se la società che eroga il servizio per l'ente,

o per suo nome e conto, tratta dati personali in possesso dell'ente, deve necessariamente essere nominata Responsabile del trattamento. Serve un addendum al contratto, il DPA, per la nomina con ben specificati i compiti e come vanno eseguiti. Una società, per esempio, che fornisce un servizio su *Cloud* o di posta elettronica si configura come Responsabile del trattamento (ma anche un contratto con un gestore di connettività, ISP per es.). Il Titolare che sceglie la società, la rende Responsabile. Deve essere, secondo il Regolamento, pienamente consapevole delle capacità e delle misure tecniche e organizzative offerte. Si può, e in realtà si dovrebbe sempre, anche nel contratto, proporre degli audit per verificare che la società esterna sia conforme alle norme e ai compiti richiesti. Ovvero, nulla osta che il Titolare investa il suo personale del compito di intervistare e verificare la conformità della ditta che offre servizi all'ente che rappresenta. Vale la pena spendere qualche riga in più e descrivere meglio il tema del rapporto tra Titolare e Responsabile. In un ente che offre servizi grazie anche a società terze il Responsabile deve "intervenire per conto" del Titolare il che significa che ne serve gli interessi. Da punto di vista giuridico questo fa riecheggiare il concetto di mandato. La designazione a Responsabile del trattamento va ricondotta all'istituto del mandato come negli artt. 1703 e seguenti del codice civile. Ricordiamo che l'art. 1708 prevede che il mandato comprende non soltanto gli atti per cui è stato conferito ma pure quelli che sono necessari al loro compimento. È un atto di autonomia con natura negoziale per cui si attua una distribuzione di compiti e una suddivisione delle competenze (e per questo, anche di responsabilità). La designazione a Responsabile del trattamento è da considerarsi valida a condizione che risulti da un atto scritto recante data certa e che il responsabile sia in possesso dei requisiti di professionalità ed esperienza richiesti alle specifiche funzioni attribuite. Il GDPR risulta, dunque, armonico pure con la normativa nazionale. Si può riprendere e specificare un caso di esempio per gli enti come il nostro in cui ritroviamo questa figura nell'inquadramento della nomina di Responsabile in un contratto di appalto, nell'ambito di un incarico per la realizzazione e manutenzione di un sistema informatico o anche di un *outsourcing* di servizi. Immaginiamo un prodotto realizzato da una società per la nostra amministrazione e che magari stiamo usando in questo momento. I difetti del sistema informatico non conforme al GDPR ricadono nel tema delle garanzie come previsto nell'art. 1668 cod. civile: i "difetti dell'opera". Il Responsabile del trattamento, ai sensi dell'articolo 82 GDPR, "risponde per il danno causato …" ma solo se non ha adempiuto gli obblighi specificatamente diretti a lui dal Titolare. Se tale previsione non era nel contratto né nella lettera di nomina di Responsabile allora la valutazione della responsabilità della violazione seguirà i principi ordinari relativi alla imputabilità (colpa o dolo) e della conseguente responsabilità. In ottica GDPR nel caso di una violazione degli obblighi, cosa comporta e in cosa si differenzia dall'ordinario? il Responsabile è passibile di una sanzione amministrativa pecuniaria che ammonta fino a 10 milioni di euro o fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore (art. 83, par. 4 GDPR).
Il suggerimento agli enti e alle loro amministrazioni è quindi di valutare bene i contratti (anche quelli posti in essere prima del GDPR) e basarli su una seria valutazione del rischio che può generare il trattamento dei dati. Il Titolare, è bene ricordarlo ancora, può sempre valutare tramite audit e conferme ulteriori che il Responsabile sia adeguato al compito. Un Titolare può, in qualunque momento, eseguire la valutazione delle misure tecniche ed organizzative, la validità delle nomine ad amministratore di sistema ecc. (meglio far presente questa prerogativa nel contratto stesso).

8.4 Contitolari e autonomi titolari di trattamento

La figura del Contitolare (*Joint Controller*) si trova nell'art. 26 al comma 1: *allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive*

responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni. La Corte di Giustizia europea[6] ha stabilito che Titolare del trattamento è anche chi decide delle finalità e dei mezzi del trattamento solo parzialmente, e che non è necessario che tutti i Titolari abbiano accesso a tutti i dati. Ovviamente in tal caso la ripartizione di responsabilità non è uguale tra i diversi Titolari. Può capitare di trovare queste figure in un grosso progetto europeo dove i vari partner possano essere individuati come Contitolari.
Se una figura, invece, di fatto determina in modo autonomo le finalità ed i mezzi del trattamento dei dati personali ricevuti dal proprio "cliente", e decide e pone in atto, sempre in maniera autonoma, le più adeguate misure tecniche, organizzative e di sicurezza, per garantire l'elevato livello di tutela dei dati adeguato al rischio, questa si configura come Titolare autonomo (*Independent Data Controller*). In questo modo, non si instaura un rapporto di contitolarità sui dati personali che sono usati da entrambi i soggetti, in quanto ciascuno si assume pienamente tutte le responsabilità conseguenti. Per esempio, il medico competente è un autonomo Titolare[7], unico legittimato a trattare i dati sanitari dei lavoratori per le finalità indicate dalla legge di settore. O, come si vedrà successivamente, anche Google a volte è Titolare autonomo (quando non è Responsabile).

8.5 Il soggetto designato

Abbiamo già visto che all'interno di un ente la responsabilità non si delega e che dunque è un errore nominare un Responsabile interno (alcune amministrazioni, purtroppo, cadono ancora in questo fraintendimento, finché non lo si fa presente). Tuttavia, alcune funzioni – non le responsabilità – possono essere delegate. L'art 2-quaterdecies del decreto legislativo 101/2018 [D.LGS., 2018] ha introdotto la definizione di "soggetto designato". In "Attribuzione di funzioni e compiti a soggetti designati" troviamo, testualmente: *Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità. Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità*. Ricordiamo che il previgente testo unico è stato novellato abrogando tutto ciò che contraddice il GDPR e rimodulando quello che è compatibile. E che l'*accoutability* è il principio fondante che non può essere messo in discussione (e questa è la vera ragione per cui un responsabile interno non può più esserci). Nella relazione illustrativa al decreto si spiega che questo aiuta a mantenere funzioni e compiti che venivano assegnati in passato evitando di stravolgere la *governance* della protezione dei dati personali. Tecnicamente un soggetto designato può essere interpretato come una figura apicale che, con delega del Titolare, definisce gli incaricati e i loro compiti. Sarebbe invero assai difficile per es. per un Titolare - presidente di un ente - con un migliaio di dipendenti conoscere i nomi e le attività di tutti quelli che trattano dati. Per conseguire la conformità normativa il Titolare potrebbe (in verità, dovrebbe sempre...) far eseguire un *assessment* della sua organizzazione, verificare lo stato dei dati personali e dei relativi trattamenti, dei rischi associati, oltre che delle misure tecniche per migliorare la situazione verso il rischio minimo. Per far questo i soggetti designati ed il Titolare (anche col supporto del DPO e del suo ufficio, solo se richiesto) mappano l'organizzazione, definiscono i compiti ed il personale e si assicurano che tutti siano formati per l'attività da espletare.

[6] Sentenza del 29 luglio 2019, caso 40-17 Fashion ID.

[7] Risposta del Garante (prot. 9593 del 19 marzo 2019) al quesito posto dalla Società Italiana Medici del Lavoro-SIML.

Qualche esempio preso dal mondo reale. Il responsabile degli affari del personale può essere individuato come un "soggetto designato". Il suo ufficio, lui compreso, tratta i dati dei dipendenti, ferie, malattie ecc. ed è dunque costituito da incaricati del trattamento. Il Titolare-presidente potrebbe non sapere bene chi-fa-cosa e se sono state impartite le istruzioni a norma di legge. Insieme al soggetto delegato e con chi si occupa della protezione dati può riuscire a definire un organigramma *privacy* e predisporre le lettere di incarico, le informative e capire quanto le misure tecniche ed organizzative sono adeguate al compito.

8.6 Incaricati e Amministratori di Sistema

Il Regolamento non definisce espressamente la figura dell'incaricato - come era espressamente definito nella legge del 2003 all'art. 4, comma 1, lett. h: "la persona fisica autorizzata a compiere le operazioni di trattamento dal titolare o dal responsabile" - ma neppure la evita perché fa un generico riferimento a "persone autorizzate al trattamento dei dati sotto l'autorità diretta del Titolare o del Responsabile" (art. 4, n. 10 GDPR). Questa figura è la persona che effettua materialmente le operazioni di trattamento sui dati personali. L'autorizzato opera alle dipendenze del Titolare (o del Responsabile, se nominato). Sempre per tenere fede al principio dell'*accountability* è fondamentale fornire agli autorizzati le istruzioni operative (art. 29 GDPR), gli obblighi relativi alle misure di sicurezza e la formazione. Altrimenti anche in presenza di formali designazioni, queste non avrebbero alcun valore. L'incaricato, ovviamente, deve attenersi senza interpretazioni alle istruzioni ricevute, e non ha alcuna autonomia (altrimenti si convertirebbe in un ulteriore Titolare). È importante che quanto prima un'amministrazione nomini i suoi incaricati per poter funzionare (si immagini il lavoro di una sua qualunque segreteria dove i dati personali sono trattati ogni giorno).
Un particolare autorizzato al trattamento è il c.d. Amministratore di Sistema (AdS), la cui figura nasce prima del codice *privacy* e definito come "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione" (art. 1, comma 1, lett. c d.P.R. 318/1999). È stato poi specificato nel provvedimento del Garante del 27 novembre 2008 e modificato nel 2009[8] come "una figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengano effettuati trattamenti di dati personali, compresi i sistemi di gestione delle basi di dati, i sistemi software complessi quali i sistemi ERP utilizzati in grandi aziende e organizzazioni, le reti locali e gli apparati di sicurezza, nella misura in cui consentano di intervenire sui dati personali" e vengono "considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi". La figura è implicitamente richiamata nel GDPR per le sue competenze tecniche, quando al Titolare del trattamento (o al Responsabile, se nominato) spetta il compito di mettere in atto le misure tecniche per garantire il livello di sicurezza adeguato al rischio come descritto nell' art. 32, quali la cifratura dei dati personali, il loro tempestivo ripristino in caso di incidenti fisici o tecnici e le verifiche periodiche delle misure tecniche ed organizzative adottate – che lasciano intendere una necessaria partecipazione di personale esperto nella gestione informatica dei dati personali. Gli incaricati del trattamento, come anticipato, sono la struttura portante di qualunque amministrazione, EPR compresi. Chiunque acceda al contenuto di dati personali è per sua natura un incaricato del trattamento - e deve essere necessariamente autorizzato, formato e con delle

[8] Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008) (così modificato in base al provvedimento del 25 giugno 2009).

istruzioni puntuali da seguire. Chi opera al protocollo, chi prepara gli stipendi, chi nell'ufficio del personale ha accesso ai dati del dipendente ecc. Anche un OIV, Organismo Interno di Vigilanza, necessita di autorizzazione[9]. Idem per un ufficio disciplinare. La normativa non discrimina né esclude nessuno nella filiera della protezione dei diritti e delle libertà fondamentali.
Un dipendente che lavora su un elaboratore, con permessi non di semplice utente ma come amministratore e che accede a dati personali, è un incaricato evoluto ovvero un AdS. Nella nostra realtà, un AdS può essere un dipendente che amministra il *workflow* o il protocollo. Chi amministra un database con dati personali, un web server o dispositivi di *networking*, è sempre un AdS. I tecnici dei servizi informativi amministrano la rete informatica e i suoi dispositivi, dove passano dati personali, non necessariamente anagrafici (basta un IP anche dinamico o un MAC address associati ad un individuo anche se per un periodo di tempo limitato) e tramite i quali si possono tracciare le attività durante il lavoro: sono tutti chiaramente AdS. Quei dati possono essere potenzialmente usati per misurare come lavora un dipendente, dove accede e per quanto tempo. In molti casi per scoprire cosa accade o per superare delle possibili contestazioni, torna utile lo strumento del log server dove vengono registrati in modo immutabile i *log* di sistema dei dispositivi. Già nel 2008 il garante presentò un provvedimento sugli Amministratori di Sistema e di come registrare i log su piattaforme che li rendessero immodificabili così che le registrazioni valessero come prova in caso di problemi. Un sistema di log raccoglie gli eventi che accadono all'interno della rete e sui diversi sistemi di sicurezza. Oggi i dispositivi sono più evoluti, noti come SIEM (*security information and event management*) e offrono la possibilità di fornire report inerenti ai dati raccolti, rispondendo alle esigenze di *data protection*, *incident response*, *compliance* e di analisi *forensic*. Un simile sistema è utile tanto all'AdS quanto al Titolare. Segue che anche gli AdS vanno quanto prima nominati come deve essere fatto per gli incaricati, dotati di istruzioni chiare e formati. In caso di una richiesta di *log* di attività da parte sia del Titolare che del datore di lavoro, magari legata ad una indagine o attività difensiva dell'ente, è importante far trovare gli AdS già nominati e preparati per evitare che accedano ai sistemi senza copertura di legge. La gestione della sicurezza, specialmente quella informatica, è di particolare importanza nella *data protection*. Il DPO (figura che vedremo subito dopo) deve avere conoscenze di sicurezza informatica per potersi interfacciare con i responsabili IT del Titolare così da poter comprendere e verificare le tecniche e le *policy* di sicurezza sul tema ed essere in grado di consigliare.
Quanto descritto per soggetti autorizzati, incaricati e amministratori, va fatto per tutti gli uffici. Non è un atto facoltativo: è un obbligo di legge. Una amministrazione può continuare a disattendere ma consapevole di prestare il fianco a segnalazioni e prepararsi a risponderne nelle sedi opportune (anche citata per danni).

8.7 Il Responsabile della Protezione dei *Dati o Data Protection Officer*

Il Responsabile della Protezione dei Dati (artt. da 37 a 39 GDPR), più spesso indicato come DPO per evitare confusioni con altre figure responsabili, è l'evoluzione della figura del *privacy officer* prevista dalla precedente Direttiva europea 95/46. In alcuni paesi erano già attivi, come in Germania dagli anni '70 (*Datenschutzbeauftragter*) o negli USA (*Chief Data Officer*) dalla fine degli anni '90 dello scorso secolo.

[9] Il Garante per la protezione dei dati personali, su sollecitazione dell'Associazione dei Componenti degli Organismi di Vigilanza ex D.Lgs. 231/2001, ha espresso il suo parere sulla qualificazione soggettiva ai fini privacy degli OdV, definendoli "soggetti autorizzati (artt. 4, n.10, 29, 32 par. 4 GDPR)". Doc. 12 maggio 2020 con prot. u. 17347 dell'Ufficio del Garante. In assenza dell'OIV, l'onere di attestazione è stato attribuito all'Organismo di Vigilanza (OdV) istituito a seguito dell'approvazione del Modello Organizzativo (ex dlg.s 231/2001) secondo quanto indicato dall'ANAC nella delibera 1134/2017 ("all'organo interno di controllo reputato più idoneo ovvero all'Organismo di Vigilanza", cfr. pag. 29 della delibera A.N.A.C. n.1134/2017 [ANAC, 2017].

La designazione del DPO mostra il nuovo approccio del GDPR centrato sulla responsabilizzazione e finalizzato all'attuazione del Regolamento da parte del Titolare (o del Responsabile) del trattamento. Il ruolo del DPO non è di tutelare gli interessi del Titolare del trattamento, che è uno dei compiti del suo ufficio legale, bensì tutelare i dati personali e supportare il Titolare nella politica di *data protecion* (ed anche nel rispondere agli interessati su questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti). Il DPO non è dunque una figura operativa o esecutiva ma consulenziale del Titolare e di controllo al tempo stesso[10].

Il regolamento suggerisce che possieda un'adeguata conoscenza delle normative sulla gestione dei dati personali come pure delle tecnologie informatiche e di sicurezza e sia in grado di dare supporto nell'analisi dei rischi associati al trattamento. Da norma, deve adempiere alle proprie funzioni in piena autonomia ed indipendenza. Non deve avere conflitti di interesse ovvero non deve trovarsi in grado di influenzare le scelte adottate in materia di trattamento dei dati, ragione per cui i garanti nazionali seguendo WP29 hanno prodotto delle "Linee guida sui responsabili della protezione dei dati", WP243, hanno specificato che il ruolo non può venir affidato a particolari responsabili di altri uffici. Ma neppure ad altre figure quali *compliance*, *risk management* e *internal audit*: l'autorità per la protezione dei dati belga ha sanzionato un'azienda per 50.000 euro, rilevando irregolarità riguardanti il conflitto di interessi del DPO proprio su questo aspetto perché ricopriva simili cariche. Per garantire l'autonomia del DPO, l'articolo 38 del GDPR chiede al Titolare del trattamento che si assicuri che il DPO non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. Il DPO non può per legge, inoltre, essere penalizzato o rimosso dal titolare per l'adempimento dei propri compiti. Il DPO, se richiesto, consiglia il Titolare con dei pareri. Il GDPR ed il Garante italiano ricordano poi al titolare che deve fornire le risorse umane e finanziarie per poter svolgere al meglio il suo compito. Suggerimento importante visto che, ricordiamolo ancora, il Titolare del trattamento risponde in prima persona per le scelte (anche le avesse delegate ad altri) ed il DPO è una risorsa solo se viene messo in condizione di supportarlo. L'art. 38 al comma 1 specifica chiaramente che il Titolare assicura che "il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali". Il GDPR non è solo un insieme di norme quanto piuttosto una prassi e quindi l'attività del DPO è pratica e funzionale.

Uno dei *leitmotiv* ricorrenti della protezione dei dati personali è l'implementazione di misure tecniche ed organizzative adeguate al rischio ed il DPO fornisce una verifica ed una regia per il Titolare e per l'azienda per raggiungere la *compliance* normativa. Aiuta ad avere contezza delle nuove tecnologie rilevanti in ambito di trattamenti di dati personali e può rendere consapevoli se la resilienza delle infrastrutture dell'ente e la loro sicurezza sono ben assicurate, e questo da un punto di vista terzo (rispetto a punti di vista *executive* di chi tali misure deve invece progettarle ed attuarle ed il cui parere sarebbe comunque soggettivo). Per come è stato pensato il Regolamento, la protezione dei dati deve essere vista come una occupazione che riguarda tutti in un ente. Il DPO ha una funzione di verifica e controllo se richiesto, ma non è la figura che prepara le informative, i consensi e gli addendum ai contratti. Il trattamento dei dati è a capo di chi, appunto, li tratta e che deve avere la consapevolezza e la sensibilità di sapere cosa e perché lo fa. Il DPO ed il suo ufficio è a supporto di questa attività non può e non deve sostituirsi a nessuno, per il principio di indipendenza e terzietà come per quello di *accountability*, ma senza far mancare l'aiuto se richiesto per far raggiungere l'operatività degli uffici.

La figura del DPO è un nuovo ruolo valido in tutta Europa che ne permette una mobilità senza pari tra i vari paesi dell'Unione. Tale ruolo non è sempre obbligatorio. Il Regolamento prevede

[10] Un DPO non ha una dipendenza gerarchica in quanto è legato al solo Titolare. La dipendenza, in caso di DPO interno è solo amministrativa e non funzionale altrimenti salterebbe il principio fondante del GDPR su cui il ruolo è disegnato. Se dipendesse gerarchicamente da un responsabile si trasformerebbe in una figura subordinata senza più la richiesta indipendenza ed autonomia.

l'obbligo di designazione del *Data Protection Officer* sicuramente in tre casi (e negli altri casi, sta alla sensibilità del Titolare avvalersi o meno di un DPO perché adeguarsi al GDPR è, in ogni caso, obbligo di legge). Per grandi linee i tre casi sono i seguenti:

1. se "il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico";
2. per i soggetti privati, nell'ipotesi in cui "le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala";
3. "nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10".

L'introduzione della figura del DPO ci permette di approfondire la definizione di "autorità pubblica" e di "organismo pubblico" che nel GDPR non è direttamente definita. I documenti del Gruppo di lavoro Articolo 29[11] ricordano che queste sono non solo "le autorità nazionali, regionali e locali [...] a seconda del diritto nazionale applicabile» ma pure che la nozione potrebbe ricomprendere "tutta una serie di altri organismi di diritto pubblico"[12]. I concetti di "ente pubblico" e "organismo di diritto pubblico" si trovano prima ancora nell'art. 2, paragrafi 1 e 2, della Direttiva 2003/98/CE [Direttiva, 2003], relativa al riutilizzo dell'informazione del settore pubblico. Ai sensi di tale disciplina, per "ente pubblico" devono intendersi "le autorità statali, regionali o locali, gli organismi di diritto pubblico e le associazioni formate da una o più di tali autorità oppure da uno o più di tali organismi di diritto pubblico". Per "organismi di diritto pubblico" si intendono tutti quegli enti che siano stati:

- istituiti per soddisfare specificatamente bisogni d'interesse generale aventi carattere non industriale o commerciale, quanto meno in via prevalente;
- dotati di personalità giuridica;
- che presentino, inoltre, almeno uno dei seguenti tratti sintomatici: il finanziamento dell'attività, la soggezione al controllo di gestione, oppure la designazione di più della metà dei componenti degli organi di amministrazione, di direzione o di vigilanza da parte dello Stato, di enti pubblici territoriali o di altri organismi di diritto pubblico.

Un'ultima considerazione. Una pubblica amministrazione moderna oggi si fonda su tre nuove figure chiave che, se ben utilizzate e valorizzate, ne accelerano lo sviluppo e l'efficienza: il DPO, il responsabile per la transizione digitale ed il responsabile della trasparenza amministrativa (e della prevenzione della corruzione) che sempre più spesso collaborano strettamente perché hanno molti punti di contatto.

9. La base giuridica del trattamento

Un trattamento di dati personali per essere lecito deve avere una giustificazione come fondamento. La base giuridica è ciò che legalmente autorizza un trattamento. Senza una base legale, il trattamento dei dati è formalmente illecito (e dunque sanzionabile). Valutare quale sia la base giuridica più adatta in relazione al trattamento che si intende porre in essere, prima ancora che il trattamento inizi, è proprio uno degli obblighi del Titolare. Non è quindi libero di scegliere la base giuridica che preferisce, ma deve rispettare le condizioni previste dal GDPR in relazione alle caratteristiche di ciascuna di quelle indicate nell'art. 6. E, come, effetto del principio

[11] Il Gruppo dell'articolo 29 per la tutela dei dati (Article 29 Working Party o WP29) era un organismo consultivo indipendente formato delle autorità nazionali di vigilanza e protezione dei dati. Ora trasformato nell'EPDB (vedi dopo).

[12] WP29 - WP243 rev. 01, p. 6, nota n. 12.

di *accountability*, deve essere sempre in grado di dimostrare la correttezza della scelta fatta. Grazie al GDPR, oggi non è più centrale il consenso fornito dall'interessato quanto invece la prospettiva di controllo del dato per cui l'interessato deve sempre sapere se i suoi dati sono usati, e come, in modo da proteggerlo dai rischi che il trattamento può provocare.
Ogni base giuridica obbedisce a specifiche condizioni con diverse conseguenze sui diritti della persona. Ce ne sono sei e lasciamo direttamente la parola al Regolamento.
1) Consenso. Il consenso dell'interessato autorizza il trattamento dei dati e deve essere legato ad una ben precisa finalità (ovvero specifico). Quando il trattamento è basato su consenso, il Titolare fornisce l'informativa e garantisce la portabilità dei dati. Le autorità di protezione incoraggiano a superare la precedente abitudine alla richiesta del consenso perché ritenuta troppo forte, molte volte non giustificata e troppo spesso l'informativa allegata non corrispondente alle reali necessità del caso. Con il GDPR il consenso deve essere una *extrema ratio*, da prendere in considerazione solo se nessuna delle altre giustificazioni è applicabile, del tutto diverso da quello che accadeva con il d.lgs. 196/2003. Come anticipato, il consenso è come una forma di contratto da rispettare. Quando l'interessato chiede di conoscere dove si trova il suo dato personale, chi lo gestisce e in caso se vuole modificarlo o cancellarlo, l'amministrazione deve prontamente agire e rispondere. Il consenso per essere ritenuto valido deve seguire una manifestazione di volontà e deve essere "libera" (art. 4 paragrafo 1, numero 11 GDPR). È fondamentale, quindi, che, se si sceglie come base giuridica il consenso, questo possa essere liberamente rifiutato, e questo non deve produrre conseguenze negative per l'interessato.
2) Adempimento di obblighi contrattuali. Il trattamento è lecito quando è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso. Un caso chiaro per le amministrazioni, tra cui gli EPR: nella partecipazione ad un concorso non si può non inviare documenti con i propri dati personali. Sia nella fase iniziale concorsuale, che è tecnicamente "precontrattuale", sia nell'atto successivo in cui si firma il contratto che introduce alla presa di servizio: non serve firmare il consenso ma basta solo l'informativa. Non avrebbe senso negare il consenso al trattamento dei dati necessari alla partecipazione ad un concorso cui siamo noi stessi interessati. L'amministrazione in quel momento diventa custode del dato personale. L'informativa diventa fondamentale. Per esempio, è necessario far sapere che esiste un incaricato del trattamento ed essere più che sicuri delle misure tecniche che proteggono i dati personali.
3) Obblighi di legge cui è soggetto il Titolare del trattamento. Questo obbligo deve soddisfare quattro condizioni:

- deve essere definito dalla legge europea o nazionale di uno Stato membro a cui è soggetto il titolare del trattamento;
- tali disposizioni legali devono stabilire un obbligo imperativo di trattamento dei dati personali, sufficientemente chiaro e preciso;
- tali disposizioni devono definire le finalità del trattamento;
- tale obbligo deve essere imposto al titolare del trattamento e non alle persone interessate dal trattamento.

Nel caso di trattamento dei dati necessario per l'adempimento di obblighi derivanti da legge, regolamento o normativa comunitaria non occorre il consenso, non si deve garantire la portabilità dei dati, ma occorre fornire un'informativa, in cui indicare la base giuridica del trattamento. In questo caso la finalità è specificata dalla legge.
4) Interessi vitali della persona interessata o di terzi. Il trattamento è ammesso quando è necessario per la salvaguardia degli interessi vitali dell'interessato (o di un'altra persona fisica). Per es., se l'interessato si trova nell'incapacità fisica di prestare il consenso. Si può utilizzare come base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione. In

questo caso non occorre il consenso ma occorre fornire l'informativa.
5) Legittimo interesse prevalente del Titolare o di terzi cui i dati vengono comunicati. Se il trattamento è necessario per il perseguimento dei legittimi interessi del Titolare o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. Anche qui non occorre un consenso ma si deve fornire l'informativa che indica la base giuridica del trattamento. Il legittimo interesse del Titolare può essere la sicurezza dei beni aziendali e costituisce la base giuridica del trattamento dei dati purché siano bilanciati i diritti tra il titolare e l'interessato.
6) Interesse pubblico o esercizio di pubblici poteri. La base giuridica si applica per il trattamento effettuato dalle autorità necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. È la norma giuridica (legge, regolamento o decreto) che deve indicare i compiti, e quindi l'interesse pubblico. Vale pure per le organizzazioni private che svolgono compiti di interesse pubblico.

10. L'informativa

In base alla finalità, il Titolare deve fornire agli interessati, prima del trattamento, le relative informazioni necessarie (art. 12 GDPR). L'informativa è una comunicazione rivolta al cittadino col fine, appunto, di informarlo, prima ancora che diventi interessato (cioè prima che inizi il trattamento), sulle finalità e le modalità. È una condizione non tanto, o non solo, del rispetto del diritto individuale ad essere informati quanto uno dei doveri del Titolare che ha l'obbligo di assicurare la trasparenza e la correttezza dei trattamenti dalla fase di progettazione, e deve essere in grado di comprovarlo in qualunque momento, secondo il principio dell'*accountability*.
L'informativa non deve essere un trattato lungo e complesso. Si richiede che abbia una forma coincisa, chiara, facilmente accessibile ed intellegibile per l'interessato (Considerando 39), eventualmente anche utilizzando immagini o icone. L'informativa va resa per iscritto o con altri mezzi (anche elettronici, come per es., la posta elettronica). Se richiesto dall'interessato, l'informativa va data oralmente ma è preferibile fornirla in forma tale da provarne l'esistenza e per consentire alle autorità di vigilanza di verificarne la completezza e correttezza. Molte amministrazioni interpretano male il concetto di "oralità" perché è sempre necessario sapere che esiste un originale da controllare e verificare (sia dall'interessato che dall'autorità in sede di ispezione) specie se l'informativa è raccontata da incaricati di una società che opera come Responsabile (questo accade per esempio con le società di vigilanza che devono operare secondo un contratto di responsabilità nel perimetro dell'ente di un Titolare ed usano proprio personale per trattare dati e fornire informative. Attenzione, al riguardo, perché, ad esempio in tempo di Covid-19, anche prendere un dato di temperatura da parte di incaricati di società esterna richiede un DPA con la società Responsabile).
Una violazione in materia di informazione agli utenti può avere come conseguenza l'indagine da parte dell'Autorità di controllo che può portare ad avviare una azione per il risarcimento del danno contro il Titolare del trattamento.
Quando si richiede il consenso dell'interessato, l'informativa è anche condizione di legittimità (ovvero è la modalità per cui il consenso è valido). L'informativa ha lo scopo di rendere valido un consenso quando questo è base giuridica del trattamento.
L'informativa è estremamente importante anche in relazione al recente Jobs Act [Jobs, 2015]. La disciplina dei controlli a distanza in ambito lavorativo deve bilanciare due interessi. Uno è l'interesse certamente legittimo, del datore di lavoro (nel verificare il corretto utilizzo degli strumenti di lavoro) e l'altro è l'interesse del lavoratore che le informazioni raccolte tramite tali strumenti (di potenziale controllo su di lui ed il suo operato) vengano trattate in maniera tale da

non ledere diritti e dignità. Sussiste un interesse legittimo del datore di lavoro al trattamento dei dati acquisiti per esigenze connesse all'organizzazione dell'attività produttiva, alla sicurezza sul lavoro e alla tutela del patrimonio aziendale. Ma il trattamento deve essere il più possibile proporzionale alle finalità legittimamente perseguite. Una volta correttamente individuati gli "strumenti di lavoro" forniti dal datore di lavoro al lavoratore, l'amministrazione ha l'obbligo - fondamentale - di garantire al dipendente una corretta informativa sulle modalità d'uso ed i potenziali controlli per ciascuno strumento di lavoro (anche in questo caso in forma concisa, trasparente, comprensibile per l'interessato e facilmente accessibile ex art. 13 GDPR). L'accordo sindacale non comporta la mancanza di informativa o una informativa incompleta o fatta male. La corretta illustrazione delle finalità del trattamento, in caso di contenzioso, verrà portata nell'eventuale giudizio a seguire, per dimostrare la valutazione della proporzionalità tra controlli posti in essere e le finalità del trattamento. La valutazione di legittimità dell'eventuale controllo (classico esempio, una sanzione disciplinare basata su elementi le cui prove sono state raccolte attraverso tali controlli) va letta sia dalla prospettiva del GDPR che di quella dell'art. 4 dello Statuto dei Lavoratori.

11. Cookie ed ePrivacy

L'informativa ci porta naturalmente a parlare dei cookie e di come vanno annunciati. La stretta relazione tra web e dati personali è uno dei temi più ricorrenti tra le richieste di chiarimenti ai DPO. La protezione della *privacy* riguarda anche i siti web con cui ormai non si può più non interagire e questa vale per tutti i siti con utenti nella UE. Non c'è solo il GDPR da considerare ma anche i pareri del Working Party e dei vari garanti. Esiste, inoltre, un'ulteriore normativa oltre al Regolamento che tratta dell'uso dei cookie e del monitoraggio da parte dei siti ed è la Direttiva ePrivacy[13], che dovrebbe essere a breve abbandonata in favore del Regolamento ePrivacy in dirittura di approvazione definitiva. Il suo campo di applicazione è sempre la protezione dati ma nel settore delle comunicazioni elettroniche. La sua portata va dall'immagazzinamento di informazioni mediante cookie all'invio di comunicazioni commerciali. Le disposizioni della Direttiva ePrivacy hanno una natura speciale e dunque prevalgono su quelle generali del GDPR per quei trattamenti che specificamente attengono alla materia delle comunicazioni elettroniche (come i dati relativi al traffico, quelli relativi all'ubicazione ed appunto, i cookie). Secondo il GDPR l'uso dei cookie può comportare un "controllo del comportamento" anche quando si tratta di cookie statistici anonimi. Come regola, per impostazione predefinita meglio bloccare i cookie prima di ottenere il consenso esplicito. Nelle FAQ rese disponibili sul tema ad ottobre 2018, il Garante nazionale ha ricordato che per l'installazione dei cookie tecnici non occorre il consenso degli utenti, bastando dare l'informativa ex art. 13 GDPR se non effettuano tracciamento e se sono strettamente necessari al funzionamento dei servizi richiesti dall'utente. Il Titolare del sito deve però fornire l'informativa semplificata e richiedere il consenso all'uso dei cookie di profilazione[14]. Un'informativa si può impostare su due livelli. Nel momento in cui l'utente accede al sito web (sulla home page o su altra pagina), deve comparire un banner contenente la prima informativa breve con espressa la richiesta di consenso all'uso dei cookie, oltre ad un link per accedere alla informativa estesa dove l'utente può reperire informazioni più dettagliate sui

[13] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002 Gazzetta ufficiale n. L 201 del 31/07/2002 pag. 0037 - 0047, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

[14] "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica" (art. 4 GDPR). L'uso di *Machine Learning* su dati personali.

cookie scegliendo bene quali specifici cookie autorizzare, e quali no.
Riguardo ai cookie di "terzi" si ricordi che solitamente non sono "strettamente necessari" all'utente che visita il sito web poiché sono connessi a un servizio distinto da quello "esplicitamente richiesto" dall'utente. Gli obblighi di informativa e consenso gravano anche sulle "terze parti" ma il Titolare del sito, quale intermediario tecnico tra queste e gli utenti, è obbligato a inserire nella informativa estesa i link aggiornati alle informative e ai moduli di consenso delle terze parti stesse.
È utile ricordare a questo punto che l'acquisire il consenso con lo *scroll*, ovvero sulla prosecuzione della navigazione all'interno della medesima pagina web, è considerato in linea con i requisiti di legge se questo è chiaramente indicato nella informativa (questo significa che esiste un evento, registrabile e documentabile presso il server del gestore del sito di prima parte) e si qualifica come azione positiva dell'utente.
Rivediamo meglio ed estendiamo i risultati di quanto detto finora. È obbligatorio fornire una *policy* sui cookie che contenga le informazioni su come interagiscono con le attività degli utenti, cioè gli interessati, che accedono ad un sito web, così che si possa scegliere di non accettare alcuni cookie o, se necessario, modificare le loro impostazioni in relazione a quelli in uso. Si può scegliere se incorporare la *policy* sui cookie come una sezione della *policy* privacy generale (la classica informativa del sito web) o averne una dedicata proprio a questo proposito.
L'informativa sulla *privacy* è un documento, per es. una pagina sul sito web, in cui sono descritti tutti i metodi e le finalità delle attività di trattamento dei dati sul sito, insieme ai moduli di contatto, informazioni, le mailing list, riferimento del DPO, ecc. I cookie sono stati considerati un potenziale rischio per la *privacy* dal momento che permettono di tracciare, archiviare e condividere il comportamento degli interessati, i visitatori del sito. In fondo, i cookie operano "di nascosto" e spesso i Titolari stessi del sito web, che delegano la gestione e l'amministrazione a figure ben precise (amministratori di sistema, web in questo caso specifico) non sanno nemmeno loro quali siano i cookie in funzione sul sito di cui loro sono i reali responsabili dal punto di vista giuridico (i Titolari o i Responsabili del trattamento, non gli amministratori. Attenzione però: il Titolare potrebbe rifarsi nei confronti degli amministratori).
La *policy* sulla *privacy* - l'informativa web - può essere statica perché può variare poco nel tempo ma i cookie utilizzati su un sito web sono per loro natura dinamici e possono cambiare spesso. Per questa ragione la *policy* sui cookie utilizzati può essere separata, per poter essere regolarmente aggiornata, così che le informazioni siano accurate in ogni momento. È una declinazione in campo web dell'*accountability* del Titolare e bisogna dare agli utenti la possibilità di accettare o rifiutare. Il Titolare non deve dimenticare che in caso di problemi risponde lui per il lavoro dei suoi amministratori. La *policy* sui cookie deve poter dare informazioni, almeno, su:

- quali tipi di cookie sono impostati;
- per quanto tempo persistono nel browser dell'utente;
- che dati tracciano;
- quale sia il loro scopo (es. funzionalità, prestazioni, statistiche, ecc.);
- dove sono inviati i dati e con chi sono condivisi;
- in che modo poter rifiutare i cookie e come modificare successivamente lo stato dei cookie.

Come regola semplice, quando i dati acquisiti dai cookie sono strettamente funzionali alla erogazione del servizio (cookie di preferenza, cookie di sessione, *load balancing* ecc.) o servono solo per fini statistici - ma gestiti direttamente dal sito del Titolare e non da una terza parte - e in formato anonimizzato come Google Analytics, non occorre il consenso dell'utente, basta la sola informativa. Quando, invece, i cookie acquisiscono dati che permettano la profilazione dell'utente diventa necessaria l'acquisizione del consenso, che va tenuto come dimostrazione di azione consapevole dell'interessato (è una sorta di comportamento concludente). In tali casi, è bene predisporre un link di rimando ad un documento indipendente contenente tutti i dettagli

relativi ai cookie utilizzati e le modalità per esprimere il consenso (e le politiche per la modifica e la cancellazione relativa). L'obbligo di acquisire il consenso preventivo e informato degli utenti solo per i cookie utilizzati per finalità diverse da quelle meramente tecniche si trova nell'art. 1, comma 5, lett. a), del D.lgs. 28 maggio 2012, n. 69[15] [D.LGS., 2012]. Brevemente una lista di casi pratici per i siti web che possono tornare utili.

Se un sito web non permette la registrazione degli utenti, e non ne tratta i dati, l'informativa *privacy* non serve. Occorre però verificare bene se i siti web acquisiscano comunque informazioni (anche dati personali) tramite i server sui quali sono ospitati. L'informativa è, invece, sempre dovuta ogni qual volta vi sia una raccolta e trattamento dei dati (tra cui per es. indirizzi IP, mail) degli utenti (per es. nella compilazione di moduli). È altresì dovuta anche quando il consenso dell'interessato non è richiesto, oppure quando l'interessato è tenuto obbligatoriamente per legge a fornire i dati.

Se il sito permette la registrazione degli utenti, ma i dati vengono usati solo per fini del sito medesimo (ad es. mailing list ma non per l'invio di proposte commerciali ecc.), occorre solo l'informativa *privacy* (in genere da collegare al modulo di registrazione per consentirne la consultazione), ma non è necessaria la raccolta del consenso.

Invece, se il sito permette la registrazione degli utenti e raccoglie dati anche a fini promozionali e pubblicitari, compreso la trasmissione a terzi, occorre l'informativa *privacy* e il consenso deve essere espresso con accettazione separata dell'informativa.

Vale la pena, a questo punto, fare anche un rapido accenno a Google ed al suo rapporto con il GDPR dato l'uso che ne facciamo come fruitori/interessati o come Titolari/utilizzatori. Con l'avvento del Regolamento il Titolare del trattamento non è più Google Inc. bensì Google Ireland Limited, stabilito in Irlanda[16]. Questa modifica ha permesso di evitare tutte le problematiche legate al trasferimento dei dati al di fuori dello spazio giuridico europeo normate nel GDPR. Quando Google offre dei servizi, per es. DoubleClick, Ad Exchange, AdMob, AdSense, ecc., ai suoi clienti per il loro propri siti web, questi si configurano come Titolari del trattamento e nei contratti sono chiamati i *Publisher*. Google dal canto suo, si comporta invece da un autonomo Titolare (*Independent Data Controller*). Sono entrambe le parti che definiscono la politica di uso dei dati, infatti Google deve essere libera di poter far elaborare i dati ai suoi prodotti (il trattamento) per fornire le informazioni, le statistiche, la visualizzazione grafica, filtri e previsioni ecc., che il Titolare vuole estrarre dagli strumenti messigli a disposizione. Non potrebbe essere altrimenti: Google non obbliga all'uso di questi strumenti che hanno diversi scopi. In questo caso, per tali *tool*, occorre inserire nel sito l'informativa *privacy*, raggiungibile con un link visibile in tutte le pagine, e specificare che il sito usa i cookie di Google per raccogliere informazioni anche a fini di profilazione (che è a carico di Google). Va quindi raccolto il consenso per i cookie tramite il banner con l'informativa breve con l'avviso che il sito usa cookie di terzi a fini di profilazione anche per fornire pubblicità.

Con strumenti quali Google Analytics (GA), Attribution, Data Studio, invece, Google opera quale Responsabile del trattamento (ed infatti nel contratto essa stessa si qualifica quale *Data Processor*) dei dati gestiti dal servizio. Google ha preparato già il necessario DPA come un emendamento al contratto (è parte delle impostazioni account) dove informa gli utenti che utilizzano il servizio e che è abbinabile ad altri servizi di annunci e profilazione. Per utilizzare il servizio senza annunci pubblicitari, si deve procedere all'anonimizzazione di Analytics, con blocco dell'incrocio dei dati tra i vari servizi.

[15] In attuazione delle direttive 2009/136/CE [Direttiva, 2009], in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE [Direttiva. 140, 2009] in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori [Regolamento, 2004].

[16] Sede in Gordon House Barrow Street Dublin 4.

12. Un moderno mito metropolitano: il disclaimer privacy

Prima di abbandonare il tema delle informative nel campo delle comunicazioni elettroniche, vale la pena parlare del *disclaimer*. Molti nel corpo della mail in fondo inseriscono un avvertimento che, in caso la mail per "sbaglio" giungesse a chi non ne è il destinatario deve cancellarla subito, e seguono strane richieste. Una forma potrebbe essere questa: *le informazioni contenute nella presente mail ed eventualmente nei suoi allegat, sono di carattere confidenziale e riservato. Sono destinate ad uso esclusivo del destinatario ed ogni divulgazione, copia, distribuzione o riferimento è proibito e può essere considerato illegale. Se tale messaggio è stato ricevuto per errore, il mittente deve esserne prontamente avvisato ed il messaggio deve essere distrutto, compreso ogni allegato presente.* Ovviamente, se una mail arrivasse per "sbaglio" a qualcuno, lo sbaglio sarebbe del mittente che non ha controllato. Il destinatario non ha ovviamente alcun obbligo legale al riguardo. Può leggerla, allegati compresi e conservarla quanto vuole senza avvisare. Questa storia che sfiora la *privacy*, ha a che vedere più con le leggende metropolitane, tipo il coccodrillo bianco che esce dalle fogne di New York. Sono state elaborate fantasiose teorie al riguardo. Verosimili alcune, ma decisamente non vere. Tali *disclaimer* iniziano sempre con riferimenti letterali al d.lgs. 196 del 2003 e ora molte si aggiornano al GDPR, quindi troviamo una data di nascita per il mito. Così forte il mito che diventa storia: il mittente sente ormai di doverlo inserire quanto il destinatario si aspetta di trovarlo. Dal punto di vista normativo, non c'è alcun obbligo sull'inserimento di questi testi, mi si passi il termine, "esoterici", e per di più la loro utilità legale è inesistente. Alcuni trovano un'origine nella - decisamente - cattiva interpretazione delle "linee guida del Garante per posta elettronica e internet" [G.U., 2007], in particolare nel punto 5.2. Lì, però, il Garante dice altro ed inoltre la sicurezza e la riservatezza che voleva portare nella gestione delle comunicazioni via mail non fu mai finalizzata (consigliava all'azienda, per esempio, che al dipendente fossero forniti due account, di cui uno per fini personali oltre a quello prettamente istituzionale). Qualcuno ha voluto trovare l'origine nell'articolo 616 del codice penale, secondo cui "*chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o sopprime, è punito, se il fatto non è preceduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa*". Questo caso sarebbe analogo al ricevere la corrispondenza cartacea. L'analogia non regge del tutto: sulla busta ci sarebbe scritto il nome di un'altra persona rispetto a chi l'ha ricevuta. Nel nostro caso è invece il mittente ad aver commesso l'errore ed il ricevente è proprio quello: se nella mail sono contenuti dati personali, giuridicamente responsabile sarebbe chi li ha inviati non chi li ha ricevuti. Ovviamente, se il destinatario rivelasse pubblicamente il contenuto di una mail - che in teoria non avrebbe dovuto ricevere - sempre per l'articolo 616 "*se il colpevole, senza giusta causa, rivela, in tutto o in parte, il contenuto della corrispondenza, è punito, se dal fatto deriva nocumento ed il fatto medesimo non costituisce un più grave reato, con la reclusione fino a tre anni*". In questo caso non sta al mittente ricordare al destinatario, anche se errato, che si sta compiendo una violazione di legge nella divulgazione. Dato che vale la presunzione di conoscenza della legge - *ignorantia legis non excusat* - a che servirebbe allora il *disclaimer*? Cosa si può fare o meno con una mail viene stabilito dalla legge, non da un *disclaimer*. Che sia presente o no una formula legale, una preghiera o una maledizione azteca, non fa alcuna differenza. Se non c'è nessun obbligo legale a inserire un *disclaimer* come questo, allora perché lo fanno in tanti? L'emulazione virale ha fatto porre la stessa domanda alla rivista The Economist in un servizio del 2011: *Legal disclaimers. Spare us the e-mail yada-yada. Automatic e-mail footers are not just annoying. They are legally useless* [The Economist, 2011]. Secondo il periodico britannico il motivo è molto più semplice di quanto si possa pensare: qualche società cominciò a farlo, qualcuna copiò, poi qualcun'altra ancora, e così via da allora. Considerato da quanto tempo la cosa gira, il fenomeno virale è più resistente del Covid-19.

13. Registro dei trattamenti

Uno dei principali elementi di *accountability* richiesti al Titolare, previsto nell'articolo 30 GDPR, è la tenuta del registro dei trattamenti. Il registro che va tenuto sempre aggiornato, serve a dimostrare una corretta gestione dei trattamenti perché ne permette una valutazione e una ricognizione, e va esibito all'autorità di controllo (il Garante) o all'autorità ispettiva in caso di verifiche.
Il registro deve permettere di identificare i soggetti coinvolti nel trattamento dei dati, le categorie dei dati trattati, lo scopo che hanno i dati, chi accede agli stessi, a chi vengono comunicati, tempo di conservazione e stato della loro sicurezza, ecc. In fondo, il registro permette sia una analisi del rischio che una corretta pianificazione dei trattamenti. È un documento vivo, pronto ad essere aggiornato quando necessario. La tenuta può essere cartacea ma è preferibile sia elettronica (esistono dei software ideali per la gestione sempre aggiornata del registro): semplifica la manutenzione e gestione del documento. Spesso le amministrazioni cadono nell'errore di preparare un registro e lo lasciano morire così. Per una amministrazione pubblica, il registro è un documento amministrativo per cui è possibile farne richiesta di accesso.

14. *Privacy by design* e *privacy by default*

Con l'entrata in vigore del nuovo Regolamento, sono stati introdotti due nuovi concetti legati a rendere sicuro un trattamento: *privacy by design* - la protezione dei dati fin dalla progettazione - e *privacy by default* - la protezione per impostazione predefinita (ex art. 25). Queste due tecniche sono necessarie al Titolare che ha l'obbligo di adottare le misure di sicurezza richieste nel GDPR prevedendo, fin da subito, i rischi che possono incontrare per la tutela dei dati personali. Il concetto *by design* non è altro che un concetto di prevenzione rischi: prevenire i problemi nella fase iniziale, di progettazione del sistema di trattamento, è meglio che correggerli poi quando potrebbe essere tardi. Un approccio basato sulla misurazione di responsabilità del Titolare (o del Responsabile) ha il vantaggio di essere flessibile e adattabile al mutare delle esigenze e degli strumenti tecnologici che si possono sfruttare nel particolare momento in cui si progetta il trattamento.
Il Considerando 76 introduce il tema della valutazione del rischio: *la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato*.
Il principio di *privacy by default* stabilisce che si trattino solo i dati personali nella misura sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Quindi, in un trattamento non si deve ricorrere all'utilizzo di ulteriori dati senza motivi specifici. Per es. se per un riconoscimento basta solo verificare un documento, la copia del documento, se non esistono necessità di legge, non va fatta.

15. La Valutazione d'Impatto sulla Protezione dei Dati

Lo strumento principale con cui il titolare effettua l'analisi dei rischi derivanti dai trattamenti posti in essere è la valutazione di impatto del trattamento o DPIA, *Data Protection Impact Assessment*. Tale onere è posto a carico del Titolare che così elabora una valutazione preventiva (ovvero: prima di iniziare il trattamento) delle conseguenze che un trattamento sui dati ha sulle libertà e i diritti degli interessati. Ove necessario, anche il Responsabile del trattamento assiste il Titolare,

fornendo le necessarie informazioni. Il Titolare deve consultarsi col DPO il quale ha il compito di fornire, se richiesto, un parere in merito alla valutazione di impatto e sorvegliarne lo svolgimento. Per il principio di *accountability*, la valutazione del rischio deve condurre il Titolare a decidere, in piena autonomia, se esistano rischi elevati legati al futuro trattamento. Se non ci sono rischi, potrà procedere oltre. In caso contrario, se valutasse la presenza di rischi per le libertà e i diritti degli interessati, avrà l'obbligo di determinare le misure specifiche richieste per attenuare o eliminare i rischi. Nel caso non si riuscissero a trovare misure idonee a cancellare o minimizzare il rischio, il Titolare potrà consultare l'Autorità di controllo. L'Autorità interviene solo successivamente alle valutazioni del Titolare, indicando le ulteriori misure da implementare, e se necessario, potrà ammonire o vietare il trattamento. Il Titolare dovrà comunque giustificare le proprie valutazioni e rendicontarle nel registro dei trattamenti. Il paragrafo 9 dell'art. 35 prevede la possibilità che il Titolare consulti gli interessati coinvolti per valutazioni sull'eventuale invasività del trattamento. Qualora la decisione del Titolare si discosti dall'opinione degli interessati, occorre motivare. Secondo le norme, il Titolare dovrebbe documentare anche le motivazioni della mancata consultazione degli interessati.
Esistono casi in cui la DPIA è ineludibile. La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano solo un rischio o un rischio elevato. Casi in cui è obbligatoria è quando i trattamenti sono effettuati nell'ambito del rapporto di lavoro con l'uso di sistemi tecnologici come i sistemi di videosorveglianza e di geolocalizzazione da cui deriva la possibilità di effettuare un controllo a distanza dell'attività del lavoratore. Anche se i trattamenti vengono realizzati con l'uso di tecnologie innovative come IoT, sistemi di intelligenza artificiale, utilizzo di assistenti vocali *online* attraverso lo scanning vocale e testuale, monitoraggi effettuati da dispositivi indossabili come per esempio, gli *smartwatch* o gli stessi smartphone attraverso i software di assistenza e comando vocale; i tracciamenti di prossimità come ad es. il *wi-fi tracking*. Esistono al proposito dei criteri individuati che aiutano a decidere. Il Titolare deve considerare se i trattamenti sono valutativi, se le decisioni automatizzate possono produrre effetti significativi per es. finalizzati ad assumere "decisioni che producono effetti giuridici", se il monitoraggio è sistematico e sicuramente nel caso di dati particolari o dati di natura estremamente personale, nuove soluzioni tecnologiche o organizzative o che producono asimmetrie nei diritti (ovvero, quando l'interessato diventa una figura debole rispetto al Titolare) e difficoltà nell'esercizio dei diritti: serve una DPIA. Un esempio chiaro può essere il seguente: in un ente si immagina l'uso di un sistema di telecamere per monitorare il comportamento di guida sulle strade. È evidentemente un monitoraggio sistematico con uso innovativo tramite una applicazione che fornisce soluzioni tecnologiche od organizzative.

Una DPIA contiene almeno:

- la descrizione sistematica dei trattamenti previsti, la finalità del trattamento, compreso l'interesse legittimo perseguito dal titolare;
- la valutazione della necessità e proporzionalità del trattamento in relazione alla finalità;
- la valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi, incluse le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Esempi di impatto che una violazione dei dati personali può comportare verso gli interessati, per esempio, sono:

- impatto finanziario (dati di accesso a conti correnti, credenziali carte di credito);

- impatto reputazionale, compromissione di opportunità di lavoro;
- furto di identità.

La mancata esecuzione di una DPIA nei casi in cui è necessaria (ex art. 35, paragrafi 1, 3 e 4), o l'esecuzione in maniera errata di tale valutazione (articolo 35, paragrafi. 2 e da 7 a 9) o la mancata consultazione dell'Autorità di controllo quando richiesto (articolo 36, paragrafo 3, lettera e.), possono comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di euro (oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale importo sia superiore). Il principio di *accountability* richiede al Titolare di porsi - almeno - il problema. Se neppure se lo pone, ricade nella situazione peggiore della sanzione. Dunque, riassumendo, sempre meglio che il Titolare in caso di dubbio si confronti col DPO, descriva il trattamento, ne valuti la necessità e la proporzionalità, e contribuisca a gestire i rischi per i diritti e le libertà delle persone valutando i rischi e le misure per affrontarli.
Un caso pratico di DPIA è quella della già introdotta *app* IMMUNI. All'*app* di *contact tracing* anti-COVID19 servirà una valutazione d'impatto sulla protezione dei dati perché con il Regolamento oggi è un obbligo di legge previsto dal diritto dell'Unione. La DPIA è lo strumento per analizzare i rischi per i diritti e le libertà delle persone e i rischi legati alla sicurezza cyber perché il suo utilizzo comporta il monitoraggio dei cittadini. Si è affermato che l'efficacia con la *app* si ottiene se viene utilizzata da almeno il 60% della popolazione e questa quantità non può non essere definita "massiva" in ottica GDPR. Gli esperti del tavolo tecnico del governo hanno il compito di individuare i profili di compatibilità con i principi costituzionali e con quelli relativi alla protezione dei dati personali. È necessario determinare le misure tecniche, giuridiche e organizzative da adottare per mitigare i rischi connessi all'uso. Sappiamo che la DPIA è un onere posto direttamente a carico del Titolare del trattamento che in questo caso è lo Stato stesso, assistito dal Responsabile del trattamento, la Bending Spoons, che gli fornisce tutte le necessarie informazioni. I passi a norma di legge dovrebbero essere i seguenti: prima di avviare il sistema di tracciamento, va approvata la norma adeguata che costituirà la base giuridica ex artt. 2-ter/2-sexies Codice Privacy ed artt. 6.1.c)-e) e 9.2.g)-i) GDPR. In questa fase, nell'ambito dell'adozione della base giuridica, si dovrebbe svolgere una DPIA generale, allegandola alla norma, ex art. 35 punto 10 GDPR. La DPIA porta con sé le ragioni delle azioni previste dallo Stato. Mentre il contratto di designazione a Responsabile esterno ex art. 28 GDPR dovrebbe contenere le indicazioni sull'uso dei dati e come evitare qualsiasi ipotesi di riuso dei dati acquisiti.

16. Potere sanzionatorio dell'Autorità

Il Garante è una Autorità di controllo che non può essere condizionata da nessun altro potere, men che meno dal potere politico. Il Garante segue i commi 4-6 dell'art. 83 del GDPR per valutare l'opportunità di una sanzione e del suo ammontare. Tra gli elementi che deve valutare per la sanzione, troviamo questo elenco:

- natura, gravità e durata della violazione;
- carattere doloso o colposo della violazione;
- misure adottate per attenuare il danno subito dagli interessati;
- grado di responsabilità del titolare o responsabile del trattamento;
- eventuali precedenti violazioni;
- grado di cooperazione con l'Autorità di controllo;
- categorie di dati personali interessate dalla violazione;
- modalità in cui l'Autorità di controllo ha preso conoscenza della violazione;
- eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso tra cui,

ad esempio, l'eventuale beneficio finanziario conseguito o le perdite evitate quale conseguenza della violazione.

Il Regolamento prevede due fasce di massimo edittale: 10 milioni di euro, o per le imprese il 2 % del fatturato mondiale totale annuo dell'esercizio precedente e 20 milioni di euro, o per le imprese il 4 % del fatturato mondiale totale annuo dell'esercizio precedente. Queste ultime sono per violazioni gravi legate all'inosservanza dei principi di base del trattamento, come per es. le condizioni relative al consenso, o ai diritti degli interessati. In ogni caso le sanzioni, almeno in primo ordine, devono essere considerate un'arma dissuasiva non una punizione definitiva che porti una società al fallimento. Le sanzioni secondo il Regolamento sono amministrative ma ha lasciato ai singoli paesi la possibilità anche di una rilevanza penale secondo il codice novellato. Sono sanzionati penalmente, per esempio, il trattamento illecito dei dati e la comunicazione e la diffusione illecita di dati personali oggetto di trattamento su larga scala come pure l'acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala.
Come caso reale, in base alle sue facoltà il Garante ha recentemente sanzionato ENI Gas e Luce per 11 milioni e 500 mila euro e TIM per 27 milioni e 800 mila euro. Ed ha avvisato – o meglio intimato - l'INPS di rimediare al recente *data breach* chiamando le persone coinvolte e illustrando i pericoli connessi alla diffusione dei loro dati. La sanzione, in caso contrario, potrebbe raggiungere i 20 milioni di euro.
Tra i vari compiti, il Garante ha anche quelli di indagine come pure il diritto di correggere il comportamento del Titolare (o anche del Responsabile) tramite avvertimenti, ammonimenti, ingiunzioni e divieti (*ius corrigendi*).

17. Il Comitato europeo per la protezione dei dati

L'*European Data Protection Board*, EDPB o Comitato europeo per la protezione dei dati, è un organismo consultivo indipendente composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati più un rappresentante della Commissione, e sostituisce il Gruppo di lavoro articolo 29 (Working Party Article 29 o WP29). Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni. Il suo compito è garantire il principio di congruità e coerenza, ovvero, tramite decisioni a maggioranza semplice, assicura che le autorità di controllo nazionali seguano interpretazioni comuni della normativa europea in materia così da evitare vie diverse all'applicazione del GDPR.

Fra i compiti definiti nell'art. 70 troviamo:

- assicurare l'applicazione corretta del regolamento fatti salvi i compiti delle autorità nazionali di controllo;
- fornire consulenza alla Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione;
- pubblicare linee guida, raccomandazioni e prassi al fine di promuovere l'applicazione coerente del regolamento e sulle materie previste;
- esaminare, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, ogni questione relativa all'applicazione del regolamento;
- fornire alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale;
- mantenere il registro elettronico, accessibile al pubblico, delle decisioni adottate dalle autorità di controllo e dalle autorità giurisdizionali su questioni trattate nell'ambito del meccanismo di coerenza.

Inoltre, se la decisione di un'Autorità di controllo capofila viene contestata da altra Autorità di controllo, è l'EDPB a fungere da tribunale di ultima istanza.

18. Il *corpus* sulla protezione dati personali

L'insieme generale delle regole europee sulla protezione dei dati personali non si ferma al GDPR. Al Regolamento 2016/679 si aggiunge la Direttiva 2016/680 del Parlamento europeo e del Consiglio d'Europa sui trattamenti di pubblica sicurezza (Direttiva relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, introduce la regolamentazione delle protezione delle persone fisiche con riferimento al trattamento dei dati da parte delle autorità a fini di prevenzione, investigazione e repressione di reati). Questa unifica le norme sulla cooperazione delle forze di polizia e in materia di giustizia e regolamenta il trattamento dei dati da parte delle autorità di polizia anche con lo scopo di realizzare uno scambio di informazioni più efficiente tra le autorità. Il recepimento statale in l'Italia, è avvenuto col d.lgs. 18 maggio 2018, n. 51[17].
È utile ricordare a questo punto che esiste una ulteriore legge europea in tema *privacy*. la n. 167 del 2017[18]. Questa modifica la disciplina della *privacy* in tema di responsabile del trattamento - art. 28, co. 1, lett. a - riutilizzo dei dati per finalità di ricerca scientifica o per scopi statistici - art. 28, co. 1, lett. b, e *data retention* del traffico telefonico e telematico - art. 24. L'articolo 24, in particolare, impone agli operatori di comunicazione (i c.d. *provider*) la conservazione dei dati di traffico telefonico e telematico per 72 mesi. Un ente che abbia la sua propria rete di connettività e che si comporti come ISP è sottoposta a tale obbligo[19].
Ulteriore tassello, infine, è il Regolamento UE 2018/1725 (101 articoli introdotti da 89 considerando) che stabilisce le norme relative alla *protezione delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organi dell'Unione, nonché norme relative alla libera circolazione dei dati personali tra tali istituzioni e organi o verso altri destinatari stabiliti nell'Unione*. Una sorta di GDPR ma nell'ambito delle istituzioni dell'Unione. Al Garante Europeo per la Protezione Dati, EDPS viene affidato il compito di sorvegliare l'applicazione del regolamento a tutti i trattamenti effettuati da un'istituzione o un organo dell'Unione. Come già accennato mentre si descriveva la *policy* sui cookie, il *framework* sulla protezione dei dati personali potrà dirsi completato con l'emanazione del Regolamento ePrivacy sulla vita privata e le comunicazioni elettroniche che sostituirà la Direttiva 2002/58/CE [Direttiva, 2002] già emendata, specie in riferimento proprio al consenso per i cookie, dalla Direttiva 2009/136/CE [Direttiva, 2002].

19. Progetti europei e protezione dati personali: il caso *e-SHAPE*

Il Regolamento sta diventando una componente integrante anche nei progetti europei. Un esempio è e-SHAPE. *EuroGEO Showcases: Applications Powered by Europe*, *e-SHAPE*[20], è una

[17] La nuova normativa ha sostituito quella presente nei titoli I e II della seconda parte del previgente Codice Privacy, dedicati al settore giudiziario e ai trattamenti da parte delle forze di polizia.

[18] LEGGE 20 novembre 2017 n. 167 - Legge europea 2017. Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea – Legge europea 2017. (17G00180) (GU Serie Generale n.277 del 27-11-2017).

[19] Il nostro Istituto sta per equipararsi ad un ISP con un proprio piano di indirizzi IP come *autonomous system* (AS).

[20] Progetto H2020 Grant Agreement 820852.

iniziativa di 54 tra istituti di ricerca, università ed aziende[21] tra cui INGV, CNR, CNRS, CMCC, DLR, ecc. ed è il contributo europeo a GEOSS (*Global Earth Observation System of Systems*) che conta 27 applicazioni pilota divise in 7 aree tematiche legate al pianeta. All'interno del progetto è stato lanciato il network dei DPO di tutti i partner, coordinato dal DPO di ARMINES. Scopo dell'iniziativa è assicurare che i dati acquisiti e gestiti da e-SHAPE siano conformi al GDPR. La Commissione ha identificato il trattamento dei dati personali tra i temi più delicati del progetto ed ha richiesto un ulteriore Work Package con diversi *deliveralbles* per coprire il tema del "*personal data processing in scientific implementation as well as several ethics issues*". Per l'ultimo tema ha espressamente chiesto la nomina di un *Ethics and Data Advisor*[22] esterno. Nei *deliverables* sono presenti le procedure sui consensi informati, le procedure di sicurezza nel trattamento dei dati e le problematiche relative al passaggio dei dati verso paesi fuori dell'Unione. Uno dei compiti del nuovo WP7, *Ethics requirements*, insieme alla *External and Personal Data Advisor* è stato preparare un *Personal Data Risk Assessment* (PDRA) da riempire a cura di tutti i DPO.

Conclusioni

Un ente di ricerca (come una società) non sfugge alla normativa. È una amministrazione pubblica e deve dimostrare di conformarsi alla legge.
Dopo un primo approccio alla tematica, già in poche pagine, si può intuire cosa ci possiamo aspettare sia quando siamo sul posto di lavoro che nella società come cittadini portatori di un diritto. Per esempio, possiamo iniziare a fare più attenzione alle informative che ci mostrano o ai consensi che ci richiedono, sapere come e perché i nostri dati vengono trattati e da chi.
Riprendiamo, come esempio ed esercizio, i modi in cui un Titolare giustifica un trattamento e noi come possibili interessati o suoi autorizzati, cosa ci dobbiamo aspettare. La scelta della base giuridica, che legittima un trattamento, spetta sempre al Titolare e lui deve tener conto che deve essere conforme a quanto previsto dal Regolamento. Questo significa che il Titolare non è libero di scegliere a suo piacere il fondamento di legittimità del trattamento. Deve rispettare le condizioni previste dal GDPR ed essere sempre in grado di dimostrare la correttezza della scelta fatta. Ma quanto è consapevole un Titolare e quanto delega un compito indelegabile sotto il profilo della responsabilità? Immaginiamo di essere all'ingresso di un'azienda o di un ente di ricerca, pronti ad entrare. Ci viene proposto prima un modulo però. C'è la richiesta di firma di un consenso informato o una presa visione dell'informativa? C'è una norma o un decreto alla base, oppure dobbiamo contrattare e dare un consenso altrimenti l'accesso è negato? Chi prende il consenso, dipende dal Titolare direttamente o è dipende da una società esterna e questa, è stata nominata Responsabile? Magari, siamo anche sottoposti ad una misura di temperatura, rimanendo sempre in tema Covid-19. Cosa è corretto trovare? Uno non vale l'altro.
Esiste ancora oggi il rischio di muoversi come se le norme sulla protezione dei dati personali non fossero leggi da rispettare ma leggi di serie B. La *privacy* è una prassi e dovrebbe riflettersi in uno stile che porta ad essere attenti, come interessati e come Titolari. Il dato va protetto. Una volta che il dato è uscito dal radar della protezione, è fuori controllo. Si deve iniziare ad avere attenzione anche nelle cose minime, neppure un nome e cognome su un foglio va sottovalutato. Si insiste su questo perché ancora, oggi troppo spesso, i Titolari delegano i compiti a chi non ha capito che il d.lgs. 196/2003 è superato ed abbandonato, rischiando un trattamento di dati personali illecito.
Una amministrazione deve valutare con cadenza periodica se è in regola, e poter sempre rispondere positivamente in ambito protezione dati, tanto all'Autorità quanto ad un interessato,

[21] https://e-shape.eu/index.php/team

[22] Mrs Anne Demoisy, della Rhizome S.A., esperta di tema *Horizon 2020 ethics and data protection expert*.

che le è noto chi-fa-cosa, con quali istruzioni e a quali livelli di sicurezza fino alla gestione di un *data breach*. Si può iniziare a verificare, accertandosi, se esiste:

- la nomina, per gli uffici ed il relativo personale, a "soggetti delegati" e incaricati così che siano autorizzati al trattamento;
- la mappa delle misure organizzative e tecniche (sicurezza informatica compresa);
- il Registro dei trattamenti e, se presente, che sia rivisto e aggiornato;
- e chiedere, nel dubbio, una valutazione al DPO relativamente alla correttezza delle procedure.

Vale la pena porsi anche la domanda se il personale è stato preparato ad un eventuale controllo o ispezione. Il Garante usa un nucleo della Guardia di Finanza. Gli autorizzati al trattamento, sono pronti ad un incontro a sorpresa?
In alternativa, se la situazione iniziale non è chiara, va fatto necessariamente un *assessment* e prevedere degli audit periodici.

Il lavoro è solo introduttivo ma si intuisce che le attività da svolgere in base alla normativa anche se sono complesse, sono di facile realizzazione. Basta procedere con conoscenza e costanza.

Bibliografia

ANAC, (2017). *Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici*. Determinazione n. 1134 del 8/11/2017 pubblicata nella Gazzetta Ufficiale - Serie Generale n. 284 del 5 dicembre 2017.

AgID, (2017). *Circolare n. 2/2017 del 18 aprile 2017*. In G.U. Serie Generale n.103 del 05-05-2017.

CASS.13663/16, (2016). CORTE SUPREMA DI CASSAZIONE SEZIONE SECONDA CIVILE Sent., (ud. 19/04/2016) 05-07-2016, n. 13663.

CURIA, (2016). Corte di Giustizia Seconda Sezione, Causa C582/14. *Rinvio pregiudiziale – Trattamento dei dati personali – Direttiva 95/46/CE – Articolo 2, lettera a) – Articolo 7, lettera f) – Nozione di "dati personali" – Indirizzi di protocollo Internet – Conservazione da parte di un fornitore di servizi di media online – Normativa nazionale che non consente di prendere in considerazione l'interesse legittimo perseguito dal responsabile del trattamento*, 19 ottobre 2016.

Direttiva 2002/58/CE, (2002). In Gazzetta ufficiale delle Comunità europee ISSN 0378-7028, L 201 45o anno 31 luglio 2002.

Direttiva 2003/98/CE, (2003). In Gazzetta ufficiale n. L 345 del 31/12/2003, pag. 0090 – 0096.

Direttiva 2009/136/CE, (2009). *In materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche*. In Gazzetta ufficiale dell'Unione europea ISSN 1725-258X, L 337 52o anno 18 dicembre 2009.

Direttiva 2009/140/CE, (2009). *In materia di reti e servizi di comunicazione elettronica*. In Gazzetta ufficiale dell'Unione europea ISSN 1725-258X, L 337 52o anno, 18 dicembre 2009.

D.LGS, (2012). *DECRETO LEGISLATIVO 28 maggio 2012, n. 69 Modifiche al decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali in attuazione delle direttive 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche, e 2009/140/CE in materia di reti e servizi di comunicazione elettronica e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorita' nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori*. (12G0090) In GU Serie Generale n.126 del 31-05-2012.

D.LGS, (2018). *DECRETO LEGISLATIVO 10 agosto 2018, n. 101 Disposizioni per l'adeguamento*

della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). (18G00129) In GU Serie Generale n.205 del 04-09-2018.

The Economist, (2011). *Legal disclaimers. Spare us the e-mail yada-yada. Automatic e-mail footers are not just annoying. They are legally useless.* Sezione Business edizione 7 aprile 2011 – Redazione.

Garante, (2020). *Parere sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da COVID-19* - 29 aprile 2020. Registro dei provvedimenti n. 79 del 29 aprile 2020 (doc. web n. 9328050).

GDPR, (2016). Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE - Regolamento Generale sulla Protezione dei Dati - *General Data Protection Regulation* in Gazzetta ufficiale dell'Unione europea ISSN 1977-0707, L 119 59° anno 4 maggio 2016.

G.U., (2007). *Linee guida del Garante per posta elettronica e internet*. In G.U. n. 58 del 10 marzo 2007.

Tomsett J., (1848). *Sketches of Her Majesty's Household.* – In Royal Collection Trust-Her Majesty Queen Elizabeth II 2014.

Jobs Act, (2015). *DECRETO LEGISLATIVO 15 giugno 2015, n. 81 Disciplina organica dei contratti di lavoro e revisione della normativa in tema di mansioni* (in GU Serie Generale n.144 del 24-06-2015 - Suppl. Ordinario n. 34 e s.m.i.).

Kaspersky, (2020). *Global Privacy Report. Defending digital privacy: taking personal protection to the next level*. In www.kaspersky.com/blog/global-privacy-report-2020.

Perilli P., (2020). *Garante privacy su sito INPS, "Subito accertamenti, intanto chiudere falla", Dichiarazione di Antonello Soro, Presidente del Garante per la protezione dei dati personali*. Adnkronos. Reperibile anche sul sito del Garante per la Protezione dei Dati Personali come doc. web 9304360.

Punzi A., (2018). *L'adeguamento della disciplina sulla protezione dei dati personali al Regolamento (UE) 2016/679*. In *Le posizioni espresse dagli auditi.* Documentazione per l'esame di Atti del Governo pubblicato da Servizio Studi del Senato della Repubblica Dossier n. 18/1 e da Camera dei Deputati Dip. Giustizia Atti di Governo n. 22/1.

Regolamento (CE) n. 2006/2004, (2004). *Sulla cooperazione tra le autorità nazionali responsabili dell´esecuzione della normativa a tutela dei consumatori*. Gazzetta ufficiale dell'Unione europea ISSN 1725-258X, L 364 47o anno 9 dicembre 2004.

Warren Samuel D., Brandeis Louis D., (1890). *The Right to Privacy. Harvard Law Review*. Vol. 4, No. 5., pp. 193-220, Dec. 15, 1890.

Note sull'autore

Lucio Badiali, Primo Tecnologo, DPO di INGV

Studi:
Laurea in Fisica specializzazione in Cibernetica.
Ph.D. internazionale in Novel Physics Methodologies, con tesi su modelli predittivi tramite Machine Learning.
Master di II livello in Giurisprudenza in protezione dei dati personali - sotto l'egida dell'Autorità Garante della Protezione dei Dati Personali.
Laurea in Scienze Politiche con specializzazione sul diritto della privacy.

Certificazioni:
DPO UNI 11679:2017
SCH73 CEPAS
ISO Certified 17024 Bureau Veritas DPO0022

Affiliazioni:
Membro di ASSODPO
Membro di EADPP European Association of Data Protection Professionals
Membro di IAPP International Association of Privacy Professionals

QUADERNI di GEOFISICA

ISSN 1590-2595 http://istituto.ingv.it/it/le-collane-editoriali-ingv/quaderni-di-geofisica.html/

I QUADERNI DI GEOFISICA (QUAD. GEOFIS.) accolgono lavori, sia in italiano che in inglese, che diano particolare risalto alla pubblicazione di dati, misure, osservazioni e loro elaborazioni anche preliminari che necessitano di rapida diffusione nella comunità scientifica nazionale ed internazionale. Per questo scopo la pubblicazione on-line è particolarmente utile e fornisce accesso immediato a tutti i possibili utenti. Un Editorial Board multidisciplinare ed un accurato processo di peer-review garantiscono i requisiti di qualità per la pubblicazione dei contributi. I QUADERNI DI GEOFISICA sono presenti in "Emerging Sources Citation Index" di Clarivate Analytics, e in "Open Access Journals" di Scopus.

QUADERNI DI GEOFISICA (QUAD. GEOFIS.) welcome contributions, in Italian and/or in English, with special emphasis on preliminary elaborations of data, measures, and observations that need rapid and widespread diffusion in the scientific community. The on-line publication is particularly useful for this purpose, and a multidisciplinary Editorial Board with an accurate peer-review process provides the quality standard for the publication of the manuscripts. QUADERNI DI GEOFISICA are present in "Emerging Sources Citation Index" of Clarivate Analytics, and in "Open Access Journals" of Scopus.

RAPPORTI TECNICI INGV

ISSN 2039-7941 http://istituto.ingv.it/it/le-collane-editoriali-ingv/rapporti-tecnici-ingv.html/

I RAPPORTI TECNICI INGV (RAPP. TEC. INGV) pubblicano contributi, sia in italiano che in inglese, di tipo tecnologico come manuali, software, applicazioni ed innovazioni di strumentazioni, tecniche di raccolta dati di rilevante interesse tecnico-scientifico. I RAPPORTI TECNICI INGV sono pubblicati esclusivamente on-line per garantire agli autori rapidità di diffusione e agli utenti accesso immediato ai dati pubblicati. Un Editorial Board multidisciplinare ed un accurato processo di peer-review garantiscono i requisiti di qualità per la pubblicazione dei contributi.

RAPPORTI TECNICI INGV (RAPP. TEC. INGV) publish technological contributions (in Italian and/or in English) such as manuals, software, applications and implementations of instruments, and techniques of data collection. RAPPORTI TECNICI INGV are published online to guarantee celerity of diffusion and a prompt access to published data. A multidisciplinary Editorial Board and an accurate peer-review process provide the quality standard for the publication of the contributions.

MISCELLANEA INGV

ISSN 2039-6651 http://istituto.ingv.it/it/le-collane-editoriali-ingv/miscellanea-ingv.html

MISCELLANEA INGV (MISC. INGV) favorisce la pubblicazione di contributi scientifici riguardanti le attività svolte dall'INGV. In particolare, MISCELLANEA INGV raccoglie reports di progetti scientifici, proceedings di convegni, manuali, monografie di rilevante interesse, raccolte di articoli, ecc. La pubblicazione è esclusivamente on-line, completamente gratuita e garantisce tempi rapidi e grande diffusione sul web. L'Editorial Board INGV, grazie al suo carattere multidisciplinare, assicura i requisiti di qualità per la pubblicazione dei contributi sottomessi.

MISCELLANEA INGV (MISC. INGV) favours the publication of scientific contributions regarding the main activities carried out at INGV. In particular, MISCELLANEA INGV gathers reports of scientific projects, proceedings of meetings, manuals, relevant monographs, collections of articles etc. The journal is published online to guarantee celerity of diffusion on the internet. A multidisciplinary Editorial Board and an accurate peer-review process provide the quality standard for the publication of the contributions.

Coordinamento editoriale e impaginazione
Francesca DI STEFANO, Rossella CELI
Istituto Nazionale di Geofisica e Vulcanologia

Progetto grafico e impaginazione
Barbara ANGIONI
Istituto Nazionale di Geofisica e Vulcanologia

Istituto Nazionale di Geofisica e Vulcanologia
Via di Vigna Murata, 605
00143 Roma
tel. +39 06518601

www.ingv.it

ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA