“L’analisi dettagliata e puntuale effettuata da Rosario Imperiali con riferimento ai principali accadimenti nazionali e internazionali avvenuti nel 2019 in tema di data protection evidenzia nitidamente, da un lato, un passaggio epocale in corso e, dall’altro, un assestamento continuo di obblighi e diritti che l’interprete deve cercare di chiarire al fine di consentire un adeguamento che sia sostanziale e non solo – o non più – formale.”

“La grande novità, e Imperiali questo aspetto l’ha colto sin dall’inizio, è che ormai la data protection dovrebbe essere vista come un *corpus iuris* europeo, tanto più in un momento in cui la “politica” della protezione dei dati in Italia sta attraversando un momento di grande crisi (con i ritardi nella nomina del nuovo Collegio e le vicende di Governo degli ultimi anni che hanno reso il quadro italiano più fragile di quello di altri Paesi).”

Rosario Imperiali viene comunemente considerato un punto di riferimento nel mondo della privacy, per l’interessante mix che lo contraddistingue: il rigore interpretativo correlato a quel pragmatismo operativo che gli deriva dalla sua militanza aziendale.

Dal 2012, raccoglie i suoi interventi settimanali di commento e di informazione sulla protezione dei dati personali, in un volume che vuole essere una sorta di “giornale di bordo” di quanto di interessante si è registrato nel corso dell’anno in questo ambito.

In questo modo Rosario intende fornire un supporto tempestivo e dettagliato per muoversi a proprio agio tra i numerosi e variegati profili di questa materia: un appuntamento che si ripete ogni anno.

ROSARIO IMPERIALI

ANNUARIO 2019

PROTEZIONE DATI

PROTEZIONE DATI

ANNUARIO 2019

ROSARIO IMPERIALI

Segui
Rosario Imperiali
su

Rosario Imperiali

Ros_Imperiali

RosarioImperiali

dptel.imperialida.com

Copyright © 2019 Rosario Imperiali

Studio Legale Imperiali
Milano

Prefazione

L'analisi dettagliata e puntuale effettuata da Rosario Imperiali con riferimento ai principali accadimenti nazionali e internazionali avvenuti nel 2019 in tema di data protection evidenzia nitidamente, da un lato, un passaggio epocale in corso e, dall'altro, un assestamento continuo di obblighi e diritti che l'interprete deve cercare di chiarire al fine di consentire un adeguamento che sia sostanziale e non solo – o non più – formale.

Passando in rassegna le quasi trecento pagine e le centinaia di pronunce, documenti ed eventi giuridici e politici commentati, si noteranno, già dall'indice, alcuni "grandi temi" che, a nostro avviso, spiccano in un quadro che è in piena trasformazione e che, in molti casi, sta ancora cercando una sua identità.

Il primo è, in generale, quello della corretta applicazione dell'idea di accountability, che è probabilmente la novità centrale del GDPR soprattutto in confronto a un quadro più che ventennale disegnato dalla Direttiva Madre che ci aveva abituato, invece, a un approccio più "latino" (o normativo/prescrittivo) rispetto all'approccio anglosassone, più libero.

Nella pratica, ad esempio, non è facile allontanarsi dall'idea di misure minime di sicurezza, imposte per legge, che erano previste dalla normativa precedente, per tratteggiare, di contro, su un foglio bianco le misure di sicurezza adeguate. In tal caso, una corretta interpretazione dello stato dell'arte, dei costi di attuazione, del "peso" del trattamento e di un'analisi del rischio diventano essenziali.

Si noti, però, che il tema delle misure di sicurezza è soltanto una parte dell'idea generale di accountability, che contiene principi ancora più ostici, a volte, da mettere a fuoco. Me ne sovvengono due, che nel libro di Rosario Imperiali sono più volte citati: il delicato rapporto tra titolare e responsabile (e i confini labili tra i due soggetti) e il concetto "astratto" (e per certi versi immateriale) della data protection by design/by default.

Il primo punto si sta rivelando problematico anche nella pratica, e non solo da un punto di vista teorico: il rifiuto da parte di un responsabile esterno di contrattualizzare (o anche solo negoziare) la sua posizione nei confronti del titolare può portare a un *vulnus* in quella stessa idea di accountability che, spesso, più che la forma di responsabilizzazione prende il significato di "dover rendere conto" di ogni scelta effettuata.

Il secondo aspetto, la data protection by design, è altrettanto nebuloso: come si dovrebbe operare per far sì che in una società o in un ente si "possa respirare" l'idea di privacy e di protezione del dato soprattutto nell'uso degli strumenti informatici? Spesso occorre non solo un mutamento informatico/tecnologico ma, anche, culturale.

Un secondo aspetto importante di questo "commentario" all'anno di data protection che si sta chiudendo è la costante attenzione agli aspetti, e agli accadimenti, internazionali.

La grande novità, e Imperiali questo aspetto l'ha colto sin dall'inizio, è che ormai la data protection dovrebbe essere vista come un *corpus iuris* europeo, tanto più in un momento in cui la "politica" della protezione dei dati in Italia sta attraversando un momento di grande crisi (con i ritardi nella nomina del nuovo Collegio e le vicende di Governo degli ultimi anni che hanno reso il quadro italiano più fragile di quello di altri Paesi).

A mio avviso, oggi l'attenzione internazionale deve comprendere sicuramente l'attività delle autorità di controllo degli altri Paesi, che dal 26 maggio 2018 hanno iniziato a sanzionare e a stabilire i primi principi di applicazione pratica delle nuove regole (con conseguenti sanzioni).
Il panorama internazionale è, ora, piuttosto fluido: alcuni Paesi non avevano una tradizione di sanzioni in tema di protezione dei dati, e si sono trovati, con il GDPR, a dover inaugurare un'era giuridica nuova.
Altre, e penso a Francia, Austria, Germania, UK, Polonia e Spagna, si sono invece immediatamente attivate, anche con sanzioni di decine o, addirittura, centinaia di milioni di Euro, per sensibilizzare immediatamente la società su questo cambio epocale nella protezione dei dati dei cittadini.
Infine, ultimo ma non ultimo, il libro di Rosario Imperiali è attento, mese dopo mese, al problema di armonizzazione tra la nuova normativa europea e il quadro giuridico italiano.
Si vedano le parti, assai interessanti, che riguardano le "vecchie" (*absit iniuria verbis*) autorizzazioni generali (con un lavoro certosino di identificazione di quelle "compatibili", o meno, con il nuovo quadro) e, soprattutto, i codici di condotta e le certificazioni, che sono due tra i punti ancora non completamente "attuati" del Regolamento che assumeranno, a nostro avviso, un'importanza essenziale nel 2020 (anche e soprattutto in un'ottica di business).
A parte la chiarezza, la "pulizia" del testo, l'integrazione dinamica con slides e infografiche e la profondità di analisi, una cosa in particolare ho apprezzato di questo enorme lavoro di commento, coordinamento ed esposizione che Rosario Imperiali è solito fare ogni anno sul tema della data protection: il fatto che lo studioso non abbia il timore di affrontare anche le questioni più controverse e che stanno dividendo la dottrina in molti Paesi a causa di interpretazioni di alcune parti del Regolamento che non sono certo facili.
Mi hanno appassionato, ad esempio, non solo i passaggi sul già detto controverso ruolo del responsabile, ma anche quelli sul ruolo dell'OdV, la "polemica" di inizio anno tra Garante e consulenti del lavoro, l'ambito delle carte fedeltà e del marketing (che è stato, *per incidens*, oggetto di una intensa attività ispettiva nel 2019 in Italia) e il delicato rapporto tra la normativa italiana in tema di antiriciclaggio, whistleblowing e trasparenza e i principi del Regolamento.
Si tratta, in definitiva, di una guida preziosa che affronta il tema della data protection anche, e soprattutto, dal punto di vista culturale ed internazionale: due prospettive oggi indispensabili per comprendere al meglio questo passaggio epocale che stiamo vivendo.

Milano, 15 dicembre 2019

GIOVANNI ZICCARDI
Cattedra di Informatica Giuridica,
Università degli Studi di Milano

Indice

GENNAIO
1. Nuove autorizzazioni generali e regole deontologiche
2. La sfocata linea di confine tra titolari e responsabili
   Quarta puntata
3. Regole deontologiche e registro pubblico delle opposizioni
4. Molte notizie interessanti da commentare

FEBBRAIO
5. Sesta riunione plenaria dell'EDPB
6. Garante: i consulenti del lavoro sono "responsabili"
7. EDPB: un ricco programma per il prossimo biennio
8. Codici di condotta: linee guida EDPB in consultazione

MARZO
9. L'Argentina ratifica la Convenzione 108
10. Valutazione prima della DPIA
11. EDPB: l'ottava plenaria e prima panoramica dell'implementazione del GDPR
12. CGUE: l'avvocato generale su consenso e consenso cookie

APRILE
13. Passi avanti per la certificazione GDPR
14. Sanzione dell'ICO per e-mail marketing
15. Nona sessione plenaria dell'EDPB

MAGGIO
16. Necessità contrattuale come base giuridica, in consultazione pubblica
17. Ruolo privacy dell'OdV
18. Ruolo privacy dell'OdV
19. Facebook condannata dall'antitrust tedesca per la politica sui dati
20. Finalità del trattamento tra principi di liceità e basi giuridiche – Prima parte

GIUGNO
21. Clausole contrattuali tipo: deciderà la GGUE
22. Cybersecurity Act
23. Linee guida su codici di condotta ed allegati su certificazione e accreditamento
24. Approvato il codice di condotta sulle informazioni commerciali

LUGLIO

25. Eurobarometro 2019: livello di consapevolezza GDPR nella UE
26. Big dataa: indagine conoscitiva congiunta di Garante, AGCM e AGCOM
27. Valzer di sanzioni “privacy”, 12a plenaria EDPB ed altre news
28. EDPB: bozza linee guida 3/2019 su videosorveglianza Prima puntata
29. Carte fedeltà e marketing

SETTEMBRE

30. EDPB: bozza linee guida 3/2019 su videosorveglianza Seconda parte
31. Prescrizioni per dati sensibili e data breach
32. EDPB: bozza linee guida 3/2019 su videosorveglianza Terza parte
33. Approvato il codice di condotta SIC

OTTOBRE

34. Consenso libero e “a pagamento”
35. Dalla decisione Planet49 sui cookie, poche ma importanti novità
36. Accountability, fiducia e prova
37. CtEDU e videosorveglianza: chi ruba non è tutelato
38. Pubblicate le linee guida sulla necessità contrattuale

NOVEMBRE

39. Whistleblowing: importanti novità
40. Decreto di recepimento della V Direttiva antiriciclaggio Prima parte
41. EDPS: linee guida su titolare, contitolare e responsabile
42. EDPB - Linee guida 3/2018, «criterio dello stabilimento»

DICEMBRE

43. Whistleblowing: linee guida ANAC
44. “Prassi di riferimento” e simili come «meccanismi di certificazione della protezione dei dati»
45. V Direttiva antiriciclaggio e impatti data protection

Indice delle figure

Norme transitorie per autorizzazioni e provvedimenti del Garante secondo dlgs 101/2018 e provv. 13/12/18 p. 4
Autorizzazioni generali compatibili e non 5
Tabella del processo di conversione dei previgenti codici deontologici "privacy" 14
Tabella del processo di conversione dei previgenti codici deontologici "privacy" in "regole deontologiche" 16
Awareness of GDPR rules 20
Most common type of complaints 28
Sistemi volontari di conformità 45, 191
Valutazione di adeguatezza 56
Have you heard of GDPR? 135-136
Have you heard about the existence of a public authority? 137
What are the reasons why you do not usually read privacy statements? 138
How concerned are you about having complete control over the information you provide online? 139
Andamento delle notifiche data breach in ottica eIDAS 149
Videosorveglianza: Cartello indicato a titolo esemplificativo nel provvedimento 2010 del Garante 176
Videosorveglianza: Cartello indicato a titolo di esempio nelle linee guida 3/2019 dell'EDPB 177
Flessibilità normativa in favore degli Stati membri 179
Impatti "privacy" per tipo di videosorveglianza 184
Consenso: condizioni 198
Il panel dell'evento su "Data protection certification models" 210
Why be accountable 212, 213
Are sanctions really dissuasive? 212
An example: Zuckerberg and Privacy 214
Market needs trust 214
Accountability is … 215
Data protection risk management 216
Integrated risk management 217
Videosorveglianza: criteri determinativi della proporzionalità 219
Basi giuridiche 224
DPO e OdV 231 nella gestione del whistleblowing 229
Sviluppi normativi antiriciclaggio 234, 269
Titolare del trattamento: i 5 elementi della definizione 239
Ambito territoriale: criterio dello stabilimento 245
Whistleblowing: profilo normativo 252
Certificazione ai sensi del GDPR 259

I simboli sulla certificazione GDPR già presenti sul mercato ma non in linea col GDPR 263
I 3 passi della certificazione GDPR 264

1.
Nuove autorizzazioni generali e regole deontologiche

Nelle ultime settimane dell'anno trascorso la nostra ASN – il Garante privacy – ha emesso un provvedimento nel quale, provvisoriamente, si adeguano alcune autorizzazioni generali sui dati sensibili che rientrano nel perimetro di flessibilità che il GDPR riconosce agli Stati membri. Contemporaneamente, stati emessi ulteriori provvedimenti con cui si è verificata la conformità al GDPR dei Codici di deontologia e di buona condotta per i trattamenti di dati personali:

- per l'attività giornalistica;
- per scopi storici, statistici, scientifici e;
- per investigazioni difensive.

Disciplina transitoria

Sul profilo della disciplina transitoria – intercorrente tra l'applicazione del GDPR e la nuova disciplina nazionale di adeguamento – ci si è già soffermati in:

- l'Editoriale del 13/9/2018, in merito alla "Efficacia di provvedimenti e autorizzazioni del Garante, ante GDPR";
- l'Editoriale dell'11/10/2018, in tema di "Efficacia di codici deontologici, ante GDPR";
- l'Editoriale del 27/12/2018, su "È ancora legittimo trattare i dati del casellario giudiziale?".

Autorizzazioni generali

Tornando alle autorizzazioni generali adottate dal Garante prima dell'entrata in vigore del decreto di adeguamento (dlgs. n. 101/2018), il citato Editoriale del 13/9 riportava che quest'ultimo opera una distinzione tra:

1. quelle aventi ad oggetto le **materie per le quali il GDPR lascia spazio di intervento agli Stati membri** (i.e. trattamenti funzionali all'esecuzione di un obbligo legale, di un compito di interesse pubblico ovvero connessi all'esercizio di pubblici poteri o comunque inerenti libertà di espressione e informazione, accesso documentale, numero di identificazione nazionale, rapporti di lavoro, archivistica, ricerca scientifica, storica, statistica, obblighi di segretezza, contesti religiosi, di cui agli articoli 6, paragrafo 1, lettere c) ed e), 9, paragrafo 2, lettera b) e 4, nonché capo IX del GDPR);
2. quelle relative a **trattamenti diversi dai precedenti**.

Sorte delle autorizzazioni generali

In quella stessa tornata del 13/9 si indicava che Il decreto di adeguamento ha previsto la seguente disciplina transitoria per le autorizzazioni generali.

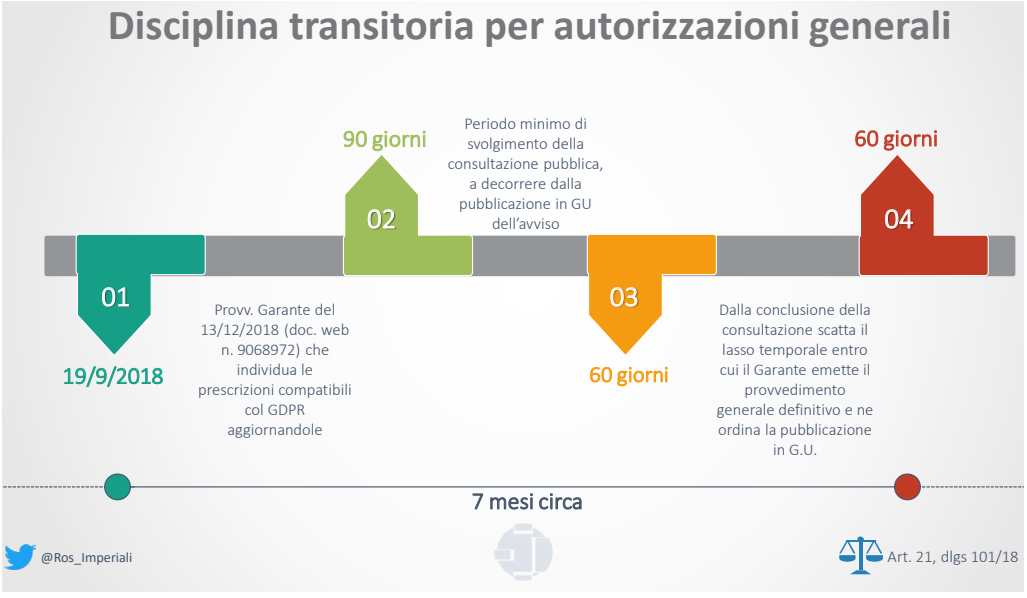
Le autorizzazioni generali di cui al punto 2. del precedente paragrafo (autorizzazioni generali emesse in relazione a materie non coperte dalla delega in favore degli Stati membri) cessano di produrre effetti dal 19/9/2018 (data di entrata in vigore del decreto di adeguamento).

Le autorizzazioni generali di cui al punto 1. (autorizzazioni generali rientranti fra le materie delegate) sono assoggettate ad una speciale procedura di verifica che potrebbe richiedere un lasso temporale della durata di circa 7 mesi (art. 21 del decreto):

- **entro 90 giorni dalla data di entrata in vigore del decreto**, il Garante sottopone a consultazione pubblica uno schema di provvedimento di carattere generale che individua le prescrizioni contenute nelle autorizzazioni generali vigenti ritenute compatibili con il GDPR, aggiornandole se necessario;

- **entro 60 giorni dall'esito del procedimento di consultazione pubblica** (la quale consultazione – in base alla regola dell'articolo 2-septies, comma 3 – dovrà svolgersi per una durata temporale non inferiore a 60 giorni), il Garante emette il provvedimento generale definitivo e ne ordina la pubblicazione in gazzetta;
- **le autorizzazioni generali** di questa categoria, di converso, ritenute dall'autorità **incompatibili col GDPR** o non incluse nel provvedimento generale citato, cessano di produrre effetti dalla data di pubblicazione dello stesso provvedimento in gazzetta (art. 21.2 del decreto);
- in relazione alle corrispondenti categorie di dati e di trattamenti oggetto delle **autorizzazioni generali compatibili col GDPR**, la pertinente disciplina sarà definita, a regime, dall'adozione delle regole deontologiche e delle misure di garanzia di cui agli articoli 2-quater e 2-septies del Codice; detto diversamente, le autorizzazioni generali compatibili col GDPR saranno sostituite – a regime – dalle regole deontologiche (art. 2-quater) e dalle misure di garanzia (art. 2-septies).

Si riporta di seguito lo schema aggiornato del processo transitorio per le autorizzazioni generali "compatibili".



Interpretazione del comma 4 dell'art. 21 dlgs 101/2018

Nella puntata richiamata del 13/9 si era data un'interpretazione del comma 4 dell'articolo 21 del decreto di adeguamento che garantiva dal rischio di vuoti normativi riguardo al perimetro di intervento delle citate autorizzazioni generali: secondo tale interpretazione, «*sino all'adozione delle regole deontologiche e delle misure di garanzia di cui agli articoli 2-quater e 2-septies del Codice*», sarebbero continuate a produrre effetti tutte le autorizzazioni generali (cioè, sia quelle compatibili che quelle incompatibili col GDPR).

È bene precisare che **tale interpretazione non è condivisa dall'Autorità**, la quale nel provvedimento che individua le prescrizioni delle autorizzazioni generali compatibili col GDPR (provv. 13/12/2018, doc. web n. 9068972), ha ritenuto che quattro delle nove autorizzazioni generali al trattamento dei dati abbiano cessato completamente i loro effetti a partire dal 19/9/2018.

Norme transitorie per autorizzazioni e provvedimenti del Garante secondo dlgs 101/2018 e provv. 13/12/18

Rif. Norma	Tipo	Efficacia	Condizioni	Cessazione efficacia	Nuovo tipo
art. 22.4 decreto	Autorizzazioni individuali	**Continuano** a produrre effetti	Se compatibili con GDPR e decreto	N/A	N/A
art. 21.1 e 21.4 decreto - provv. 13/12/18	Autorizzazioni generali (*compatibili*)	**Continuano** a produrre effetti	Secondo provv. del 13/12/2018 (doc. web n. 9068972): A.G. n. 1/2016 per i **rapporti di lavoro** A.G. n. 3/2016 per **organismi di tipo associativo e fondazioni** A.G. n. 6/2016 per **investigatori privati** A.G. n. 8/2016 per **dati genetici** A.G. n. 9/2016 per scopi di **ricerca scientifica** Sino a completamento procedura che segue: '- Garante pone in consultazione pubblica il provvedimento generale del 13/12/2018 - consultazione non inferiore a 60 gg. dalla pubblicazione dell'avviso in G.U. - Garante adotta provvedimento generale entro 60 gg. da esito consultazione	Sino ad adozione di regole deontologiche e misure di garanzie ex artt. 2-quater e 2-septies del Codice	regole deontologiche e misure di garanzia
art. 21.2 decreto - provv. 13/12/18	Autorizzazioni generali (*incompatibili*)	**Cessano** di produrre effetti	A.G. n. 2/2016 su stato di **salute e vita sessuale** A.G. n. 4/2016 per **liberi professionisti** A.G. n. 5/2016 per **diverse categorie di titolari** A.G. n. 7/2016 per **dati giudiziari**	Dal 19/9/2018 (data di entrata in vigore del dlgs 101/2018)	N/A
art. 21.3 decreto	Autorizzazioni generali (*ulteriori*)	**Cessano** di produrre effetti	Se ultronee rispetto alle materie delegate agli Stati membri	Dal 19/9/2018	N/A
art. 22.4 decreto	Provvedimenti	**Continuano** a produrre effetti	Se compatibili con GDPR e decreto	N/A	N/A

Autorizzazioni generali che hanno cessato gli effetti

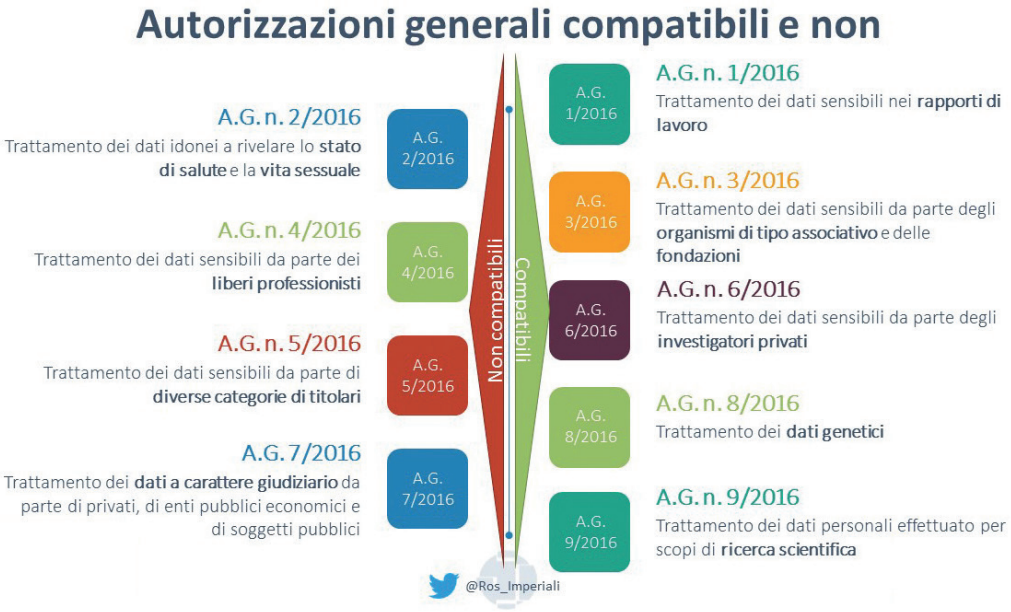
Sulla base dell'analisi di compatibilità effettuata dal Garante, le seguenti quattro autorizzazioni generali hanno cessato i loro effetti giuridici:

- **Autorizzazione generale n. 2/2016** al trattamento dei dati idonei a rivelare lo stato di **salute** e la **vita sessuale**.
- **Autorizzazione generale n. 4/2016** al trattamento dei dati sensibili **da parte dei liberi professionisti**.
- **Autorizzazione generale n. 5/2016** al trattamento dei dati sensibili **da parte di diverse categorie di titolari**.
- **Autorizzazione generale n. 7/2016** al trattamento dei **dati a carattere giudiziario** da parte di privati, di enti pubblici economici e di soggetti pubblici.

Autorizzazioni generali aggiornate

Le autorizzazioni generali ritenute compatibili col GDPR – e pertanto aggiornate – sono le seguenti:

- **Autorizzazione generale n. 1/2016** al trattamento dei dati sensibili nei **rapporti di lavoro**.
- **Autorizzazione generale n. 3/2016** al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni.
- **Autorizzazione generale n. 6/2016** al trattamento dei dati sensibili da parte degli investigatori privati.
- **Autorizzazione generale n. 8/2016** al trattamento dei **dati genetici**.
  Autorizzazione generale n. 9/2016 al trattamento dei dati personali effettuato per scopi di **ricerca scientifica**.



Validità temporanea delle autorizzazioni aggiornate

Il testo delle cinque autorizzazioni generali aggiornate viene sottoposto a consultazione pubblica prima della loro approvazione definitiva (in tal senso, si veda l'avviso pubblico di avvio della consultazione pubblica, ai sensi dell'art. 21, dlgs. 101/2018, doc. web n. 9068965).
Il provvedimento definitivo produrrà effetti fino all'emanazione delle regole deontologiche e l'adozione delle misure di garanzia previste rispettivamente agli articoli 2-quater e 2-septies del codice.

Codici deontologici previgenti

Come indicato in precedenza, l'Editoriale dell'11/10/2018, cui si rinvia, si è soffermato sulla disciplina transitoria relativa ai codici deontologici allegati al previgente codice ed al rapporto in essere tra questi e le novelle "regole deontologiche" disciplinate dal codice privacy.

Regole deontologiche

Sulla base di quanto prescritto dal decreto di adeguamento (dlgs. 101/2018, art. 20.4) il Garante ha effettuato la verifica di conformità delle disposizioni in essi contenute, rispetto al GDPR.
Le disposizioni dei precedenti codici deontologici ritenute conformi sono state ridenominate "regole deontologiche" e – secondo quanto dispone l'articolo 20 del dlgs 101/2018 – sono pubblicate dal Garante senza che siano sottoposte a consultazione pubblica, contrariamente a quanto prescritto per le "regole deontologiche" future che saranno soggette, invece, alla consultazione pubblica (art. 2-quater del codice).

Trasformazione dei "vecchi" codici in "regole deontologiche"

A seguito della citata operazione di verifica, il Garante ha emesso le seguenti regole deontologiche:

- Regole deontologiche relative al trattamento dei dati personali nell'esercizio dell'**attività giornalistica**.
- Regole deontologiche per trattamenti a **fini statistici o di ricerca scientifica**.
- Regole deontologiche per il trattamento a fini di **archiviazione nel pubblico interesse o per scopi di ricerca storica**.
- Regole deontologiche per trattamenti a **fini statistici o di ricerca scientifica effettuati nell'ambito del Sistema Statistico nazionale**.
- Regole deontologiche relative ai trattamenti di dati personali effettuati per svolgere **investigazioni difensive o per fare valere o difendere un diritto in sede giudiziaria**.

Allegazione al codice privacy

Le regole deontologiche citate saranno successivamente allegate al codice privacy mediante decreto del Ministero della giustizia.

2.
La sfocata linea di confine tra titolari e responsabili - Quarta puntata

Con questa puntata concludiamo l'esame degli elementi distintivi dei ruoli legali di titolare del trattamento e suo responsabile, ora focalizzandoci su quelle situazioni in cui la terza parte, sebbene operativamente svolga un servizio per conto del proprio committente – in deroga al criterio generale che lo vorrebbe qualificabile come responsabile del trattamento dei dati personali utilizzati allo scopo – si trovi, invece, ad assumere la posizione giuridica di titolare di un autonomo trattamento.

Sintesi

Le precedenti tornate su questo tema sono le seguenti:

- Editoriale del 25/10/2018 sulla individuazione del ruolo di titolare.
- Editoriale dell'8/11/2018 sul tema della delega di esercizio della titolarità, delle conseguenze derivanti da violazioni interne e della contitolarità.
- Editoriale del 20/12/2018 riguardo ai criteri distintivi per l'individuazione di titolare e responsabile.

Gli operatori che forniscono servizi in favore di un proprio cliente non sono sempre qualificabili come responsabili del trattamento del cliente-titolare, in quanto le sottostanti circostanze di fatto, dall'analisi di ciascun caso, talvolta denotano che i dati personali di riferimento sono utilizzati dal provider, con sostanziale autonomia decisionale. In queste situazioni, da valutare attentamente, il fornitore assume il ruolo di titolare del trattamento di dati personali che utilizza per l'erogazione del servizio di riferimento.

Fornitori titolari del trattamento di dati

Non sempre un operatore che eroga un servizio per conto del proprio cliente si qualifica come **responsabile del trattamento**, facendo scattare le pertinenti prescrizioni del GDPR. L'avvento del regolamento ha reso maggiormente evidente alcuni profili interpretativi che, in verità, risultavano già fondati durante la vigenza della direttiva 95/46/CE. La sottolineatura del GDPR alla necessaria verifica delle circostanze di fatto sottostanti, ha fatto emergere con maggiore chiarezza, rispetto al passato, quelle situazioni in cui l'appaltatore, nell'ambito del servizio che eroga in favore del cliente, utilizza comunque i dati con piena autonomia decisionale, come autonomo titolare del trattamento.

Esempio del responsabile che agisce come titolare

Quando il fornitore del servizio svolge la propria attività sui dati in sostanziale autonomia, cioè esercitando su aspetti essenziali di tali operazioni un proprio potere decisionale, esso si qualifica come titolare autonomo, nonostante eroghi un servizio nell'interesse del cliente. Questa situazione si può verificare

- a causa dell'**intrinseca natura del servizio** oppure;
- per le **specifiche circostanze attuative** dello stesso.

Il caso dei servizi professionali

Esempi del primo gruppo (**intrinseca natura del servizio**), ci vengono offerti da taluni servizi professionali, caratterizzati dall'autonomo esercizio della professione in questione: ad esempio, commercialisti, avvocati (v. esempi che seguono) trattano i dati personali in conformità ai propri

obblighi professionali e, quindi, agiranno per lo più come titolari autonomi, non potendo ricevere istruzioni dal cliente nel contesto dell'incarico per tale servizio.

L'esempio degli avvocati

Il parere wp169 del gruppo di lavoro dell'articolo 29 fa l'esempio di un avvocato che rappresenta un suo cliente davanti al giudice e – nell'ambito di tale funzione – tratta dati personali collegati al caso del cliente. «*La base legale per poter utilizzare le informazioni necessarie è il mandato del cliente. Tale mandato, tuttavia, non verte sul trattamento di dati bensì sulla rappresentanza in giudizio, attività per la quale queste professioni hanno tradizionalmente la propria base legale. Tali professioni devono quindi essere considerate come "titolari del trattamento" indipendenti per quanto riguarda il trattamento dei dati svolto nell'ambito della rappresentanza legale del cliente*». Quindi, il mandato alle liti conferito al proprio difensore non ha per oggetto il trattamento dei pertinenti dati personali (cioè la contrattualizzazione del rapporto titolare/responsabile ai sensi dell'articolo 28 GDPR), il trattamento dei dati da parte dell'avvocato ha la sua base giuridica nella disciplina legale dell'attività forense, mentre la trasmissione dei dati dal cliente al proprio difensore ha il suo fondamento nella necessità di difendere un diritto in giudizio.

Esempio dei contabili

L'esempio sui contabili, contenuto nel medesimo parere wp169, pone in buona evidenza i diversi ruoli che può assumere un professionista in corrispondenza delle diverse attività svolte.
«*La qualifica del contabile può variare a seconda del contesto. Quando fornisce servizi ai cittadini e ai piccoli imprenditori sulla base di istruzioni molto generali ("Mi prepari la dichiarazione dei redditi"), il contabile – come gli avvocati, che agiscono in condizioni analoghe e per ragioni comparabili – sarà un titolare del trattamento.*
Tuttavia, se lavora per una società, ed è vincolato alle dettagliate istruzioni del contabile interno, per effettuare, ad esempio un audit dettagliato, sarà, se non un dipendente, un responsabile del trattamento, dato che le istruzioni saranno molto chiare e il suo potere discrezionale di conseguenza limitato.». Morale: il professionista di turno ben può rivestire più ruoli data protection e la loro corretta individuazione discende – come di consueto – dall'analisi delle reali circostanze di fatto del rapporto di riferimento.

Gli organi indipendenti

Nell'esempio citato relativo ai contabili, riportato nel parere wp169, il gruppo di lavoro dell'articolo 29 fa un'altra precisazione di rilievo: «*Interviene tuttavia una riserva molto importante: quando (il contabile) ritiene di avere scoperto un'irregolarità che è obbligato a segnalare, allora, in virtù degli obblighi professionali cui è tenuto, agisce in modo indipendente in qualità di titolare del trattamento*». Si pensi, ad esempio, al caso dei revisori esterni.
Quest'ultima osservazione chiarisce l'ulteriore situazione degli organi di vigilanza interna, come ad esempio, l'attività svolta ad opera dei componenti dell'Organismo di vigilanza previsto dal decreto legislativo 231, nell'ambito del modello di vigilanza e controllo per il contrasto ai reati commessi dai propri dipendenti o consulenti. L'indipendenza del ruolo, evidente nell'esempio emblematico della gestione delle denunce volontarie (cosiddetto ***whistleblowing***), è il fondamento circostanziale di tale conclusione che vede nell'OdV un titolare autonomo del trattamento dei dati personali (rispetto all'azienda per la quale svolge il proprio ufficio) che utilizza nel corso delle conseguenti attività.

Casistiche di promiscuità di "ruoli privacy"

Il citato esempio del contabile testimonia che il ruolo assunto da un soggetto non sia necessariamente univoco in quanto l'attività svolta dal professionista per conto del cliente può essere effettuata sia in sostanziale autonomia decisionale (nel qual caso, il professionista sarà titolare autonomo) sia nel rispetto delle istruzioni impartite dal cliente sotto la sua diretta autorità (laddove il ruolo del professionista sarà quello di responsabile del trattamento dei pertinenti dati personali). Su questo versante di promiscuità di ruoli si pongono altre casistiche in cui – in tema di trattamento di dati personali – il fornitore agisce sia sotto le direttive del cliente sia nel proprio interesse.

Esempio dell'agenzia di reclutamento

Si faccia l'esempio dei "cacciatori di testa", parzialmente tratto dal parere wp169. Frequentemente, le agenzie di reclutamento cui si rivolgono le aziende per la ricerca di candidature per nuovo impiego, svolgono diversi ruoli in corrispondenza delle differenti fasi del processo di ricerca e selezione. Nella fase in cui l'*headhunter*, per svolgere l'incarico, attinge dal proprio data base e arricchisce la propria banca dati con nuove informazioni di contatto o esperienze personali acquisite nello svolgimento del mandato ricevuto, l'agenzia di reclutamento agisce come titolare di autonomo trattamento, decidendo in autonomia su finalità e mezzi d'uso dei relativi dati. Differenti sono i presupposti di fatto, invece, relativi alla fase più propriamente di selezione, quando l'agente gestisce interviste con i candidati seguendo le istruzioni dell'azienda cliente, al fine di verificarne l'attitudine a ricoprire la mansione. La gestione dei dati personali svolta dall'agente sotto l'autorità diretta dell'azienda cliente, viene effettuata in qualità di responsabile del trattamento per conto dell'azienda-titolare.

Il caso del responsabile "ultra vires"

Sulla scia dell'esempio citato in precedenza, talvolta si può assumere il ruolo di titolare del trattamento anche senza esserne consapevoli.

Il soggetto che, in astratto, sarebbe qualificabile come responsabile del trattamento, di converso, può trovarsi ad agire come autonomo titolare soprattutto in due circostanze:

1. quando **non rispetta le istruzioni ricevute** dal proprio titolare del trattamento;
2. quando, violando le prescrizioni del GDPR, **determina le finalità ed i mezzi del trattamento** [art. 28(10), GDPR].

Il parere wp169 riporta l'esempio della società MarketinZ che «*fornisce servizi di pubblicità promozionale e marketing diretto a varie imprese.*

La società GoodProductZ conclude un contratto con MarketinZ: in base a tale contratto MarketinZ fornisce servizi di pubblicità commerciale per i clienti di GoodProductZ ed è designata come responsabile del trattamento. MarketinZ, tuttavia, decide di usare la banca data dei clienti di GoodProducts per promuovere prodotti anche di altri clienti.»; questa decisione di utilizzare i dati personali acquisiti anche nel proprio interesse, rappresenta un cambio di finalità deciso in autonomia da MarketinZ che «*fa di MarketinZ il titolare del trattamento per tale operazione.*». Chiarita questa trasformazione dei ruoli, sarà poi necessario verificare se il trattamento dei dati personali svolto da MarketingZ in qualità di titolare possa considerarsi lecito alla luce degli articoli da 5 a 10 del GDPR.

Il ruolo di responsabile del trattamento connaturato al settore di attività

Nell'ambito dell'outsourcing IT e del cloud, i fornitori di servizi normalmente assumono il ruolo di responsabili del trattamento per i dati personali di pertinenza del cliente e che utilizzano al fine di erogare i rispettivi servizi.

Esempi degli Internet Service Providers

«*Un provider di servizi Internet (ISP) che fornisce servizi di hosting è in linea di principio un responsabile del trattamento per i dati personali pubblicati on-line dai suoi clienti, che si rivolgono a lui per l'hosting e la manutenzione del loro sito web. Se tuttavia l'ISP tratta ulteriormente, per scopi propri, i dati contenuti nei siti web, diventa titolare per tale specifico trattamento*».

Esempio dei fornitori di messaggistica online

Diversamente, il fornitore di servizi di messaggistica online (e-mail) – anche secondo quanto indicato dal Considerando (47) della direttiva 95/46/CE – si ritiene di norma titolare del trattamento dei dati personali supplementari, necessari per il funzionamento del servizio; mentre le persone che hanno prodotto i messaggi saranno titolari del trattamento dei dati in essi contenuti.

Rapporti di fornitura con distinta titolarità

Altre volte, nonostante la cornice di contesto sia sempre quella di un rapporto di appalto, l'analisi della sottostante situazione di fatto porta a concludere che entrambi gli operatori coinvolti siano autonomi titolari di trattamento di dati personali.

Esempio delle sperimentazioni cliniche

Nell'ambito delle sperimentazioni cliniche di medicinali – altro contesto in cui la distinzione dei "ruoli privacy" potrebbe risultare non immediata – è pur vero che «*(i)l promotore* (cioè lo sponsor, nda) *non effettua alcuna attività di raccolta diretta dei dati, né può interloquire con gli individui inclusi nella sperimentazione; compiti, questi, spettanti ai medici sperimentatori.*
Tuttavia, il promotore acquisisce (...) in diverse ipotesi i dati dei pazienti raccolti dai centri e sugli stessi effettua diverse operazioni di trattamento». Quindi, medico sperimentatore e sponsor sono entrambi titolari di autonomi trattamenti aventi come base giuridica la necessità di soddisfare un obbligo legale e la finalità di ricerca medico-scientifica.
«*D´altra parte, va rilevato che il centro non è assoggettato a vincoli di subordinazione nei confronti del promotore: accetta il protocollo concordandone con il promotore alcuni aspetti (...); esegue la sperimentazione con propria autonomia organizzativa, sebbene nel rispetto del protocollo, delle procedure operative standard e delle direttive del promotore; per l´esecuzione della sperimentazione si avvale di collaboratori che ritiene idonei ed è responsabile del loro operato*» (linee guida del Garante, doc. web n. 1533155).
Di conseguenza, il promotore ("sponsor") ed i centri di sperimentazione sono in rapporto di reciproca autonomia e si qualificano pertanto entrambi come titolari per i trattamenti di dati personali (dei pazienti) di rispettiva pertinenza o, a seconda dei casi, quali contitolari del trattamento che li accomuna.

Esempio delle società di pagamento rispetto ai rivenditori online

Un rivenditore online lavora in collaborazione con una società di pagamento per elaborare le transazioni dei clienti in quanto quest'ultima fornisce tale servizio specifico per conto del rivenditore online.

Nonostante i dati personali siano dei clienti del rivenditore e siano trasmessi alla società di pagamento in occasione delle transazioni online tra il rivenditore ed i propri clienti, il rivenditore online non ha voce in capitolo sul modo in cui il trattamento dei dati personali dei clienti viene effettuato dalla società per erogare il servizio di pagamento.

Di conseguenza, la società di pagamento è titolare del trattamento dei dati personali elaborati per i pagamenti, così come il rivenditore, a sua volta, è titolare dei dati personali dei clienti necessari per eseguire la transazione commerciale.

Altri esempi di autonoma titolarità

Gli esempi che seguono sono tratti dall'autorità di supervisione dell'Isola di Man e vengono qui riproposti perché si collocano su quella linea di confine già detta "sfumata", pervenendo alla conclusione di una duplice titolarità.

Noleggiatore d'auto e società di localizzazione dei veicoli – Una società di noleggio auto contrae un apposito contratto con una società di localizzazione di veicoli per installare dispositivi nelle proprie auto e monitorarli in modo che le auto possano essere recuperate se, anziché essere regolarmente restituite al termine del noleggio, scompaiono. Le condizioni contrattuali tra le parti specificano che la società di monitoraggio dovrebbe tracciare tutte le auto della società di noleggio e, se l'auto non è stata restituita, trasmettere i dati di localizzazione alla stessa sei ore dopo la fine del periodo di noleggio. Secondo l'autorità di controllo dell'Isola di Man l'azienda di tracciamento del veicolo – sebbene tratti i dati di localizzazione per inviare un rapporto basato su tali informazioni alla società di noleggio auto – è titolare del trattamento dei dati, perché determina in autonomia come vengono elaborati questi stessi dati personali. Mentre la società di noleggio auto non ha voce in capitolo su come funziona il sistema di localizzazione dei veicoli. Si può aggiungere che, ovviamente, la società di noleggio sarà titolare del trattamento dei dati di localizzazione così ricevuti ed utilizzati al fine di rintracciare il veicolo.

Banca e società di ricerche di mercato

Una banca incarica una società di ricerche di mercato di effettuare ricerche per suo conto. L'incarico della banca specifica il budget e richiede un sondaggio sulla soddisfazione dei suoi principali servizi di vendita al dettaglio in base alle opinioni di un campione dei suoi clienti in tutto il Regno Unito. La banca lascia libertà alla società di ricerca di determinare le dimensioni del campione, i metodi di intervista e la presentazione dei risultati.

Secondo l'autorità dell'Isola di Man, da cui abbiamo tratto l'esempio, la società di ricerca è titolare del trattamento dei dati, in quanto determina la metodologia per l'elaborazione dei dati personali di riferimento. Resta fermo che la banca rimane titolare per il trattamento dei dati personali dei propri clienti contenuti nella lista consegnata all'agenzia.

3.
Regole deontologiche e registro pubblico delle opposizioni

Nel corso di questa terza settimana di gennaio 2019 sono state pubblicate in Gazzetta ufficiale le prime regole deontologiche sulla protezione dei dati personali, oltre quella che era già avvenuta riguardo ai giornalisti – esaminate nell'Editoriale dell'11/10/2018 e di cui si è data notizia nell'Alert del 10/1/2019. La Gazzetta n. 16 del 19/1/2019 ha pubblicato, altresì, il DPR di modifica al regolamento sul funzionamento del Registro Pubblico delle Opposizioni con riguardo all'impiego della posta cartacea – già oggetto dell'Alert del 18/1/2018.

Regole deontologiche

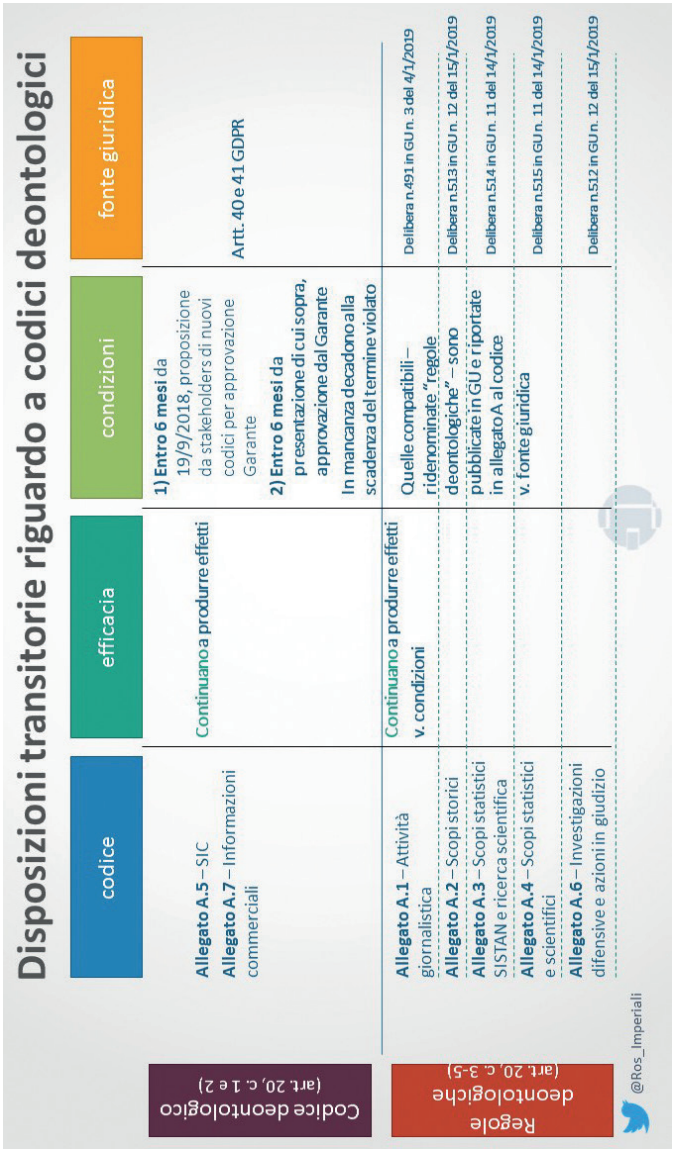


Tabella del processo di conversione dei previgenti codici deontologici "privacy".

Come evidenziato nella tabella di sopra, i previgenti codici deontologici allegati al codice privacy seguono due distinti processi di conversione – ai sensi dell'art. 20 del dlgs n. 101/2018 – nell'ambito della più generale operazione di adeguamento della disciplina nazionale al GDPR:

1. i codici SIC (già A.5) e sulle informazioni commerciali (già A.7) dovranno sottostare a specifica procedura di rinnovamento, al termine della quale saranno considerati e produrranno effetti giuridici come codici deontologici secondo gli articoli 40 e 41 del GDPR (art. 20, commi 1-2, dlgs. 101/2018);
2. sono sottoposti ad una preliminare operazione di verifica di compatibilità da parte del Garante, i restanti codici:
    a. A.1 sull'attività giornalistica;
    b. A.2 per gli scopi storici;
    c. A.3 per gli scopi statistici del Sistan e per ricerca scientifica;
    d. A.4 per gli scopi statistici e scientifici;
    e. A.6 per le investigazioni difensive e la difesa in giudizio.

Dai codici deontologici alle regole deontologiche

Con riferimento ai codici deontologici precedentemente classificati come A.1, A.2, A.3, A.4 e A.6, conclusasi positivamente la procedura (art. 20, commi 3-4, dlgs. 101/2018), le prescrizioni ritenute compatibili dall'autorità si trasformano in "regole deontologiche" – ai sensi dell'art. 2-quater del codice privacy – vengono pubblicate in gazzetta ufficiale e sono infine allegate al codice privacy in Allegato A.

Pubblicazione delle regole deontologiche in Gazzetta ufficiale

Il Garante privacy ha effettuato l'anzidetta verifica di compatibilità ed ha indicato – con proprie delibere – le pertinenti regole ritenute compatibili, richiedendone la pubblicazione in gazzetta, come previsto.

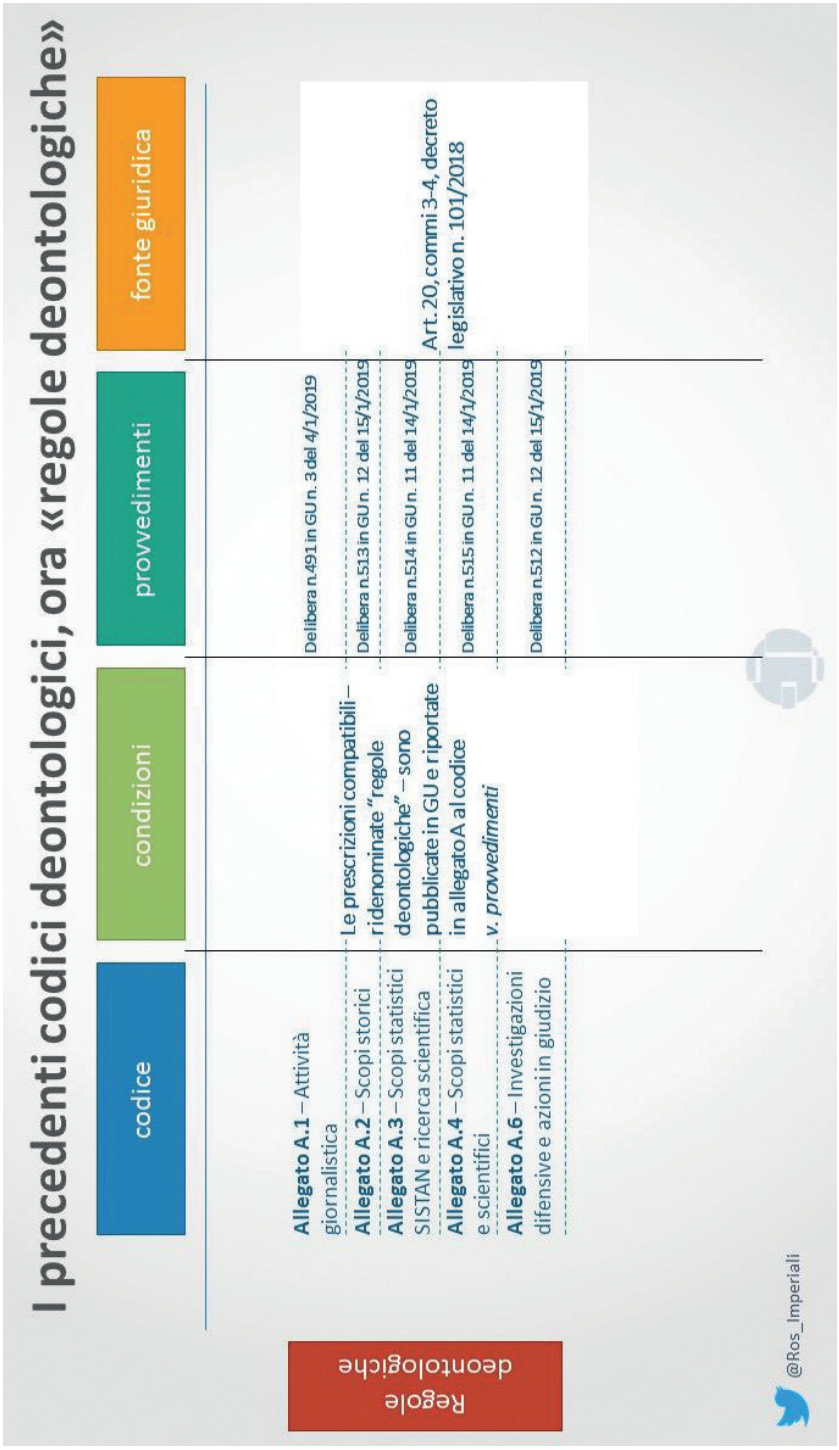


Tabella del processo di conversione dei previgenti codici deontologici "privacy" in "regole deontologiche".

La pertinente documentazione può essere reperita sulla gazzetta ufficiale come riportato di seguito:

Precedente classificazione	Delibera Garante	Gazzetta ufficiale
Allegato A.1 - Attività giornalistica	Delibera n. 491	n. 3 del 4/1/2019
Allegato A.2 - Scopi storici	Delibera n. 513	n. 12 del 15/1/2019
Allegato A.3 - SISTAN	Delibera n. 514	n. 11 del 14/1/2019
Allegato A.4 - Scopi statico scientifici	Delibera n. 515	n. 11 del 14/1/2019
Allegato A.6 - Investigazioni	Delibera n. 512	n. 12 del 15/1/2019

Sanzioni per violazioni delle regole deontologiche

Il rispetto delle regole deontologiche «*costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali*» (art. 2-quater, comma 4, codice privacy). Pertanto, la violazione delle disposizioni in esse contenute comporta l'illiceità del trattamento svolto.

Di conseguenza, sebbene l'articolo 166 del codice privacy non menzioni l'articolo 2-quater in via specifica tra le prescrizioni soggette alle sanzioni pecuniarie amministrative del regolamento, si ritiene che la violazione dello stesso rientri tra quelle sui principi di base del trattamento (cioè di liceità e correttezza) e, pertanto, sia punita con la sanzione fino a 20.000.000 di euro o, per le imprese, fino al 4% del fatturato mondiale totale annuo, se superiore; così come previsto dall'art. 83, paragrafo 5, lettera a) del GDPR.

Registro Pubblico delle Opposizioni

Si è completato il lungo iter avuto inizio con la previsione normativa con cui è stato ampliato l'ambito delle iscrizioni del RPO anche agli indirizzi postali, in aggiunta alle utenze telefoniche, per regolamentarne l'uso in campagne di direct marketing (**l. n. 124/2017**).

Il decreto del Presidente della repubblica n. 149 dell'8 novembre 2018 – pubblicato nella gazzetta ufficiale n. 16 del 19/1/2019 – ha modificato il dpr. n. 178/2010 in materia di registro pubblico delle opposizioni, al fine di dare attuazione alla nuova disciplina riguardo all'uso degli indirizzi postali pubblicati sull'elenco telefonico pubblico per attività promozionale mediante posta cartacea.

Utilizzo degli indirizzi sugli elenchi telefonici per marketing postale

Con questo passaggio, almeno dal punto di vista normativo, può darsi attuazione alla disciplina che consente di utilizzare gli indirizzi postali dei contraenti presenti sugli elenchi telefonici, cartacei o automatizzati, a disposizione del pubblico per marketing postale, a patto che tali indirizzi (e relativi dati personali) non risultino iscritti nel RPO.

Tale utilizzo, in verità, potrà avere luogo **non prima del 4 maggio 2019**, vale a dire 90 giorni successivi all'entrata in vigore delle norme del dpr (cioè il 3/2/2019, v. art. 1, comma 4, dpr n. 149/2018), in quanto la concreta realizzazione e il funzionamento del registro esteso alla posta cartacea è soggetto al medesimo periodo di decorrenza (art.1, comma 3, dpr n. 149/2018).

Consultazione del RPO e periodo di efficacia

L'operatore che intende avvalersi delle utenze telefoniche e degli altri dati personali pubblicati sugli elenchi telefonici è tenuto a consultare preliminarmente il RPO, al fine di riscontrare eventuali iscrizioni di opposizione, che sono cause ostative al contatto commerciale. La consultazione effettuata ha validità di 15 giorni riguardo all'uso delle utenze telefoniche e di 30 giorni per i trattamenti dei dati personali presenti sugli elenchi, sempre a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale mediante l'impiego del telefono o della posta cartacea (art. 8, comma 2, dpr 178/2010).

Sanzioni

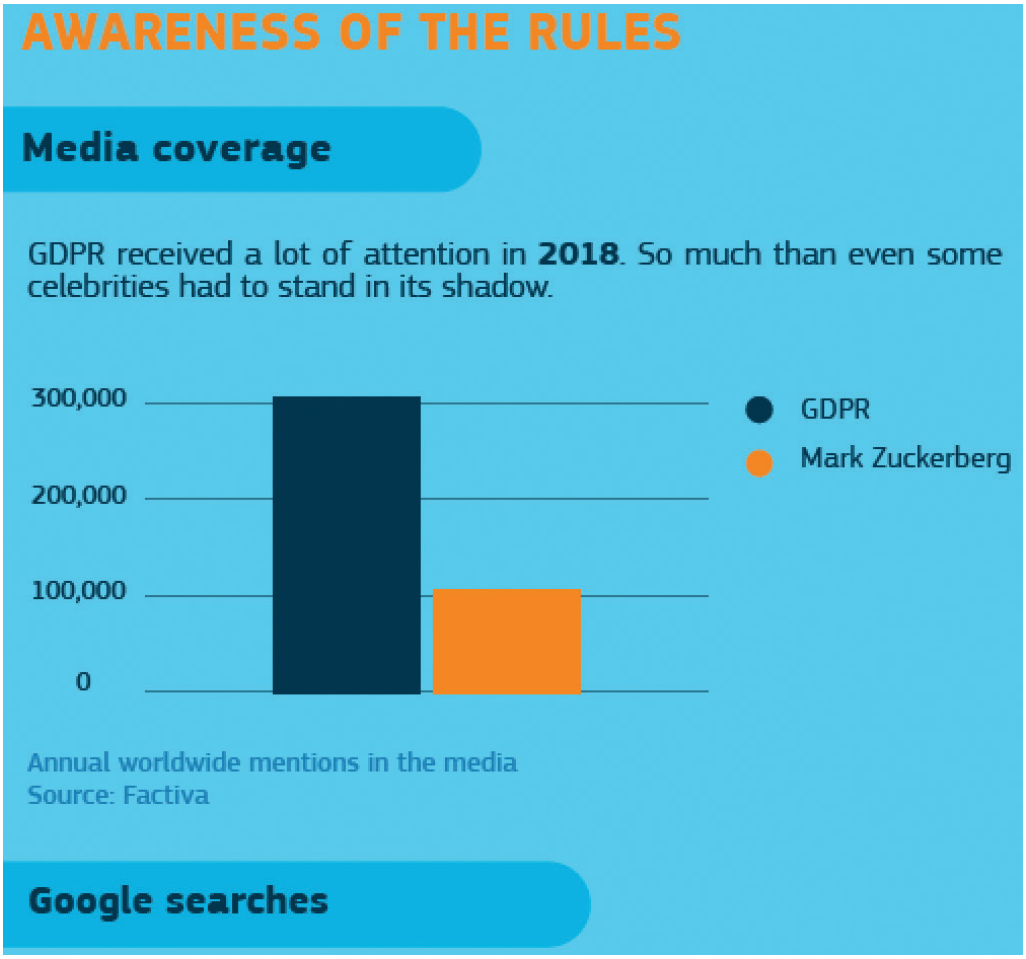
In caso di trasgressione di tali norme, poiché si vengono conseguentemente a violare le disposizioni dell'articolo 130 del codice privacy, si applicherà la sanzione pecuniaria amministrativa prevista nel massimo sino a 20 milioni di euro o sino al 4% del fatturato globale annuo, quale dei due importi risulta maggiore (art. 85, paragrafo 5, del GDPR); in applicazione di quanto disposto dall'articolo 166, comma 2, del codice privacy.

Prossimi sviluppi del RPO

A questo primo intervento di modifica del funzionamento del RPO riguardo all'uso della posta cartacea, se ne aggiungerà in futuro un successivo, volto a consentire l'iscrizione nello stesso di qualsiasi utenza telefonica, sia pubblica sia riservata, sia fissa sia mobile, come previsto dalla riforma del settore introdotta dalla legge n. 5/2018, oggetto dell'Alert del 18/1/2018.

4.
Molte notizie interessanti da commentare

Si parla molto di GDPR nel mondo, come efficacemente mostra questo diagramma tratto dall'infografica pubblicata dalla Commissione UE.
Sotto il cielo del data protection vi sono sempre notizie da divulgare o temi e decisioni da approfondire, come questa settimana ricca di novità di cui dare evidenza, in alternativa a riflessioni, come di consueto, su uno specifico argomento.



Sintesi

- La **sanzione inflitta a Google dal CNIL** ha ottenuto i primi titoli dei media.
- Eppure, agli addetti ai lavori non sarà sfuggito l'uno-due della firma del trattato commerciale **UE-Giappone**, subito seguito dal **mutuo riconoscimento del livello di adeguatezza dei due regimi** sulla protezione dei dati personali, aggiungendo in tal modo il Giappone alla *white list* dei paesi di destinazione cui viene riconosciuto il libero flusso di dati personali che partono dalla UE.
- Il Comitato (EDPB) ha pubblicato la relazione sul Secondo Rapporto Congiunto Annuale del **EU-US Privacy Shield**.

- L'ICO – l'autorità di supervisione inglese – ha rilasciato le FAQ sul dopo Brexit che indirizzano anche l'ipotesi del "no-deal".
- Sul versante interno fa notizia il **primo provvedimento del Garante in tema di violazione dei dati personali (data breach)** sotto l'egida del GDPR, interessante sotto molteplici profili.
- Il 28 di gennaio si è celebrato il primo Privacy Day del post-GDPR.

Google sanzionata per 50 milioni dal CNIL

A seguito di reclami promossi dalle organizzazioni no-profit None of Your Business ("NOYB") e La Quadrature du Net ("LQDN"), quest'ultima su mandato di 10.000 utenti, l'autorità di controllo francese ("CNIL") ha inflitto una sanzione da 50 milioni di euro a Google il 21 gennaio 2019. L'accusa è di aver effettuato trattamenti di dati personali degli utenti dei propri servizi – in particolare per pubblicità comportamentale – quando essi configurano il sistema operativo del proprio cellulare Android e creano un account Google

- rilasciando **informative poco chiare e non agevolmente accessibili** dagli utenti;
- in **assenza di una specifica base giuridica** per il trattamento dei dati e la profilazione.

CNIL e l'autorità capofila

Nel giugno 2018 il CNIL aveva coinvolto le autorità di controllo degli altri Stati membri per valutare congiuntamente quale fosse l'autorità capofila che – in base al meccanismo dello sportello unico ("one stop shop") – potesse prendere in carico questa pratica. Secondo il GDPR, l'autorità capofila – che coordina le attività delle altre autorità riguardo ad una specifica questione di rilevanza europea – viene individuata dal luogo dove si trova lo stabilimento principale del titolare del trattamento (art. 56, GDPR).

Nel caso di Google, inizialmente si era ritenuto – insieme all'autorità irlandese, in quanto in quel paese si trova il quartier generale europeo di Google LLC (cioè l'azienda statunitense casa madre che offre servizi online, con quartier generale a Mountain View in California) – che la consociata irlandese Google Ireland Limited non potesse essere considerata suo stabilimento principale nella UE. Google, dal suo canto, ha contestato questa posizione ritenendo, di converso, che lo stabilimento principale di Google LLC fosse in Irlanda e che, quindi, competente a decidere dei reclami fosse l'autorità di controllo irlandese anzichè il CNIL.

Stabilimento principale nella UE

L'argomentazione su cui si è basata la conclusione dell'assenza di uno stabilimento principale di Google LLC nella UE è stata che la consociata irlandese del gruppo risultava non esercitare alcun potere decisionale sulle operazioni di trattamento connesse al sistema operativo Android ed ai servizi forniti dalla società Google LLC.

In assenza di uno stabilimento principale – quindi del meccanismo dello "one stop shop" – il CNIL si è ritenuto competente a decidere in merito alla pratica, come qualsiasi altra autorità di controllo degli altri Stati membri, senza tuttavia ritenere necessario consultare il Comitato europeo (EDPB).

Applicabilità del GDPR

Sebbene non si è avuto modo di averne evidenza specifica, riteniamo che nel caso prospettato il CNIL sia giunto alla conclusione dell'applicabilità del GDPR nei riguardi di una società non-UE (Google LLC) sulla base di più di un profilo indicato dall'articolo 3 del regolamento; vale a dire:

- **in base al criterio territoriale [art. 3(1)]** in quanto, in ogni caso, sembrerebbe che Google LLC abbia propri stabilimenti sul territorio della UE;
- **in base al criterio del "bersaglio" [art. 3(2)]** perchè Google LLC offre servizi a individui che si trovano nella UE.

Informative carenti e di non agevole accesso

La prima contestazione sollevata a Google LLC è stata in tema di trasparenza ed informativa: molte informazioni essenziali, come le finalità per le quali i dati vengono elaborati, il tempo di memorizzazione dei dati o le categorie di dati utilizzate per personalizzare l'annuncio, sono eccessivamente dispersive, essendo collocate in vari documenti, nonché reperibili mediante il ricorso a pulsanti e collegamenti che è necessario attivare per leggere le informazioni.
In particolare, le informazioni rilevanti sono accessibili solo dopo diversi passaggi, a volte fino a cinque o sei azioni. Questo è, ad esempio, il caso in cui un utente desidera avere informazioni complete sulla raccolta dei dati per la personalizzazione della pubblicità o per la sua geolocalizzazione. Inoltre, il CNIL ha rilevato che la descrizione delle finalità (come la fornitura di servizi personalizzati in termini di contenuto e pubblicità, la sicurezza dei servizi e dei prodotti, la fornitura e lo sviluppo di servizi) e del tipo di dati trattati per tali scopi era troppo vaga, tale da non consentire agli utenti di comprendere la portata del trattamento e le connesse conseguenze. Infine, ulteriore addebito ha riguardato la mancata indicazione dei termini di conservazione per un certo tipo di dati ovvero dei criteri che avrebbero consentito agli utenti di determinarli.

Informativa multi-strato

Il caso costituisce un utile precedente come linea guida cui attenersi quando si intenda adottare la modalità dell'informativa "multi-livello" – peraltro suggerita dallo stesso Comitato (wp260 rev.01) per rendere più agevole l'accesso alle informazioni da parte degli utenti online – avendo cura di non eccedere nella stratificazione delle informazioni rilevanti col rischio di conseguire l'effetto opposto, cioè un'eccessiva laboriosità per l'utente nella ricerca di quelle di interesse.

Assenza di base giuridica

La seconda contestazione ha riguardato la base giuridica del trattamento posto in essere da Google LLC: Google – secondo il CNIL – ha fatto affidamento sul consenso degli utenti per il trattamento dei loro dati per scopi di pubblicità personalizzata.

1. Consenso non informato

Tuttavia, secondo l'autorità francese, il consenso non sarebbe stato validamente raccolto per due ragioni: in primo luogo, perché il consenso dell'utente non era sufficientemente informato. Le informazioni su questi trattamenti, diluite in diversi documenti, non avrebbero consentito all'utente di prendere coscienza, ad esempio, della pluralità di servizi, siti, applicazioni coinvolte in questi trattamenti e quindi del volume dei dati elaborati e combinati.

2. Consenso non specifico nè inequivocabile

La seconda obiezione sollevata riguardo al consenso ottenuto ha contestato che esso fosse "specifico" e "inequivocabile". Ciò in quanto sebbene fosse stato possibile per gli utenti modificare alcune delle opzioni associate al proprio account Google e configurare la scelta della visualizzazione di annunci personalizzati spuntando una casella, queste ultime risultavano già spuntate per *default*. In aggiunta, l'assenza di specificità è stata riscontrata nella circostanza che prima di creare un account, gli utenti sarebbero stati invitati ad acconsentire a tutte le operazioni di trattamento effettuate da Google, mentre il regolamento prevede che il consenso sia specifico solo se è dato distintamente per ogni finalità.

Di conseguenza, la conclusione che il consenso ottenuto doveva ritenersi invalido e che il relativo trattamento fosse privo di fondamento giuridico.

Determinazione dell'ammontare della sanzione

I principali criteri utilizzati dall'autorità francese nella determinazione della sanzione di € 50 milioni sono stati:

- Il fatto che le presunte **violazioni** si riferiscono ai principi essenziali del GDPR e sono quindi particolarmente **gravi**.
- Il fatto che le presunte violazioni siano **ancora in corso** e costituiscano continue violazioni del GDPR.
- L'importanza del sistema operativo Android nel mercato francese; e
- La **portata delle operazioni di trattamento** dei dati.

Appello

Sebbene la sanzione sia stata inflitta a Google LLC, il provvedimento dell'autorità è stato notificato a Google France SARL al fine di renderlo eseguibile. Google LLC, dal suo canto, ha già dichiarato di volerlo impugnare: entro quattro mesi dalla notifica presso il Consiglio di Stato (*Conseil d'Etat*).

Mutuo riconoscimento UE-Giappone sui reciproci sistemi data protection

Il comunicato stampa della Commissione europea ha informato in merito alla decisione adottata (e relativi allegati) circa il riconoscimento dell'adeguatezza del regime data protection vigente in Giappone, in tal modo liberalizzando il flusso di dati personali dal territorio europeo verso quel paese. Come rilevato dalla Commissione, questo è il risultato della «*procedura avviata nel settembre 2018, che includeva il parere del Comitato europeo per la protezione dei dati (EDPB) e l'accordo di un comitato composto da rappresentanti degli Stati membri dell'UE*».

Accordo di partenariato economico UE-Giappone

Le decisioni di adeguatezza integrano l'accordo di partenariato economico UE-Giappone, che entra in vigore il 1° febbraio 2019. Questo non solo crea l'area di libero scambio commerciale forse più importante a livello globale ma rappresenta una concreta testimonianza dell'affermazione secondo cui commercio e protezione dei dati personali sono tutt'altro che antagonisti ma procedono mano nella mano.

Libero flusso di dati personali UE-Giappone

Insieme alla equivalente decisione adottata dal Giappone, il libero flusso di dati personali tra i due blocchi (inclusa l'area del SEE che comprende Norvegia, Liechtenstein e Islanda) **inizia ad applicarsi a partire dal 23 gennaio 2019**. Questo significa che le aziende europee che trasmettono dati personali verso il Giappone non hanno più necessità di individuare specifiche salvaguardie per la tutela dei dati oggetto di trasferimento (come ad esempio le clausole contrattuali standard, approvate dalla Commissione) proprio in virtù di questa decisione. Analogamente, avverrà per i flussi inversi, che partono dal territorio giapponese e sono diretti verso l'area UE-SEE.

La "white list" dei paesi adeguati

Con questa decisione, la lista dei paesi oggetto di una decisione di adeguatezza (verso i quali, dunque, il trasferimento di dati personali è libero) si arricchisce di un'importante novità. Ne fanno parte ad oggi:

- Andorra;
- Argentina;
- Canada (per le organizzazioni commerciali);
- Isole Faroe;
- Giappone;
- Guernsey;
- Israele;
- Isola di Man;
- Jersey;
- Nuova Zelanda;
- Svizzera;
- Uruguay;
- USA (limitatamente al Privacy Shield).

Privacy Shield: Secondo rapporto congiunto annuale

Il Comitato europeo (EDPB) ha partecipato alla seconda revisione annuale condotta dalla Commissione UE sul Privacy Shield ed ha esaminato il secondo rapporto pubblicato dalla stessa il 19 dicembre 2018, al fine di valutare la robustezza della connessa decisione di adeguatezza dello strumento nonché della sua attuazione operativa. L'EDPB ha concentrato l'attenzione sugli aspetti commerciali Privacy Shield e sull'accesso ai dati personali trasferiti dall'UE da parte delle autorità governative ai fini dell'applicazione della legge e della sicurezza nazionale, compresi i rimedi legali disponibili per i cittadini dell'UE.

Nonostante si registrino alcuni miglioramenti rispetto ai rilievi sollevati nella prima revisione annuale il Comitato ha evidenziato il permanere di criticità.

Aspetti commerciali del Privacy Shield

Nell'ambito dei profili commerciali che riguardano il Privacy Shield, l'EDPB ha rilevato le seguenti carenze:

- una certa mancanza di supervisione nella sostanza;
- una non soddisfacente regolamentazione dei trasferimenti ulteriori;
- la tutela dei dati relativi alle risorse umane;
- il sistema del rinnovo della certificazione, suscettibile di creare confusione.

Accesso da parte delle autorità pubbliche ai dati trasferiti in USA sotto l'ombrello del Privacy Shield

In questo ambito l'EDPB rileva quanto segue:

- insoddisfacente definizione delle operazioni di raccolta ed accesso a dati personali a **fini di sicurezza nazionale** specie per quanto riguarda modalità di accesso massivo e indiscriminato;
- il diritto dei cittadini UE di promuovere **azioni di rimedio dinanzi alle corti statunitensi** deve ancora essere garantito in modo effettivo, come nel caso di **accesso da parte delle autorità di contrasto USA ai dati personali** detenuti da aziende commerciali;
- il posto di **Ombudsperson** risulta ancora **vacante** come assenti appaiono le procedure interne per la gestione dei rapporti con gli altri organi di intelligence o di controllo dell'amministrazione.

FAQ di ICO sul dopo Brexit

L'autorità inglese ha rilasciato un set di domande frequenti (FAQ) in tema di data protection riguardo al dopo-Brexit. Tra queste spiccano per interesse le seguenti risposte:

- Di regola il GDPR non trova più applicazione nel Regno Unito dopo la data di vigenza della Brexit (29/3/2019) ma, se non dovesse essere raggiunto un accordo tra le due parti, chi opera in UK dovrà comunque rispettare il Data Protection Act 2018 (la legge inglese sulla protezione dei dati personali) che non si discosta significativamente dal regolamento europeo, in quanto emessa in origine per adeguarsi al GDPR. In seguito, sono prevedibili interventi legislativi per consentire a questa norma di riferirsi al solo contesto inglese.
- Mentre la direttiva NIS continuerà ad avere applicazione nel Regno Unito, grazie alla legge nazionale di recepimento, lo stesso non varrà per il regolamento eIDAS sull'identità elettronica ed i servizi fiduciari; tuttavia il governo ha dichiarato di voler incorporare la disciplina eIDAS in una propria legge nazionale.
- I trasferimenti di dati personali dall'Inghilterra al SEE non dovrebbero subire restrizioni, ma se non si dovesse raggiungere un accordo, i trasferimenti di dati dal SEE all'Inghilterra sarebbero soggetti alla disciplina prevista dal GDPR per i paesi extra-UE.
- Le linee guida dell'ICO continueranno ad essere rilevanti per i cittadini inglesi.

Primo provvedimento del Garante sul data breach

Importante primo provvedimento del Garante privacy in materia di violazione dei dati personali, sotto l'egida del GDPR. La decisione reca la data del 13 dicembre 2018 (n. 499 doc. web n. 9076378) ma è stato reso pubblico in questi giorni.

Il caso

La questione ha riguardato un incidente di sicurezza causato da un attacco hacker contro una primaria banca nazionale, finalizzato ad acquisire le credenziali di accesso dei propri clienti ai servizi bancari online. L'attacco «*proveniente da rete anonimizzata (TOR), avente lo scopo di mascherare il reale indirizzo IP dell'attaccante*» è stato sferrato contro «*il sistema di online banking*» in più fasi diverse, «*attraverso l'utilizzo massivo di codici sequenziali per individuare quali di essi corrispondessero a REB code effettivamente esistenti (codice identificativo personale per l'accesso al sistema di on-line banking)*», al fine di captare con successo i dati identificativi dei clienti e le relative chiavi di accesso.

Esiti

Di circa 7.000 clienti sono state acquisite le password (PIN) – grazie ai tentativi andati a buon fine – mentre la violazione ha coinvolto con esiti diversi oltre 700.000 interessati.

Azioni intraprese

La banca ha provveduto a:

- adottare misure di rimedio;
- notificare la violazione all'autorità;
- bloccare «*per motivi di sicurezza le credenziali di circa 10.000 clienti*»;
- «*contattare i clienti interessati per procedere con il reset della password*»;
- pubblicare «*un comunicato sul proprio sito web*», «*non ravvisando il "rischio elevato" di cui all'art. 34 del Regolamento ed in considerazione del numero elevato di interessati*».

Obbligo di comunicazione agli interessati

L'autorità non ha convenuto con la banca circa la valutazione di rischio non elevato conseguente alla violazione in quanto:

- ha interessato «***una gran quantità di dati personali***»;
- l'acquisizione dei dati personali dei clienti «è da ritenere già ***di per sé fonte di potenziale grave pregiudizio per gli interessati***, *in considerazione dell'abitudine diffusa tra gli utenti dei servizi online di utilizzare password o PIN facilmente memorizzabili*»;
- che i dati trafugati sono «***direttamente e univocamente identificativi*** *che, alla luce delle tecnologie disponibili, possono essere utilizzati come chiavi di ricerca per individuare in rete l´interessato e conseguentemente accedere anche ad altre informazioni allo stesso riferibili (quali, a esempio, un recapito telefonico o un indirizzo di posta elettronica)*»;
- «*tali informazioni potrebbero essere utilizzate per rivolgere agli interessati* ***comunicazioni telefoniche o messaggi di phishing a scopo fraudolento***, *grazie alla conoscenza dei dati personali da parte dei soggetti terzi che hanno condotto l'attacco informatico*».

In base a tali considerazioni il Garante ha ritenuto che la banca non abbia rispettato l'obbligo di comunicazione agli interessati coinvolti [art. 34(1)] e pertanto le ha ordinato di provvedere anche in considerazione del fatto che il comunicato pubblico sarebbe risultato ambiguo in quanto «*lascia intendere che la violazione dei dati personali ha riguardato solamente*» i clienti che hanno visto bloccate le proprie credenziali di accesso.

Valutazione del rischio da violazione di dati personali

Sul profilo della valutazione del rischio il Garante ha sottolineato l'importanza che i rischi dovrebbero «***essere determinati in base a una valutazione oggettiva***» e tenere «*in* ***considerazione tanto la probabilità quanto la gravità dei rischi*** *per i diritti e le libertà degli interessati*», in proposito richiamando i considerando (75) e (76). Contestualmente è stato ricordato che le linee guida wp250 rev.01 hanno «*individuato i fattori da considerare nella valutazione del rischio – presentato da una violazione dei dati personali – per i diritti e le libertà delle persone fisiche:*

- tipo di violazione;
- natura, carattere sensibile e volume dei dati personali;
- facilità di identificazione delle persone fisiche;
- gravità delle conseguenze per le persone fisiche;
- caratteristiche particolari dell'interessato;
- caratteristiche particolari del titolare del trattamento dei dati;
- numero di persone fisiche interessate;
- *altri aspetti generali*».

Valutazione di "elevato rischio"

Sulla base di questa impostazione il Garante ha ritenuto che l'incidente in questione abbia determinato un elevato rischio per i diritti e le libertà degli interessati coinvolti a causa dei seguenti fattori:

- «***elevato numero di persone fisiche*** *a cui si riferiscono i dati personali oggetto di violazione*»;
- «***particolare qualità ed esattezza (dei dati)*** *in quanto acquisiti a seguito di identificazione certa del cliente secondo le procedure tipiche del settore bancario*»;
- «***facilità con cui è possibile identificare specifiche persone fisiche*** *direttamente dai dati personali oggetto di violazione*»;
- «*violazione dei dati personali si* è *verificata nell'ambito di un attacco informatico di*
- ***ampia portata***»;
- «***il particolare contesto (attività bancaria)*** *nel quale il titolare del trattamento, tra i maggiori gruppi bancari operanti a livello europeo, effettua il trattamento di dati personali*»;
- «***la gravità e la permanenza delle possibili conseguenze*** *per le persone fisiche che potrebbero derivare dalla violazione*».

Riserva di ulteriori provvedimenti

Da ultimo l'autorità si è riservata «*ogni altra determinazione all'esito della definizione dell'istruttoria avviata sul caso*».

28 gennaio - Il primo Privacy Day del post-GDPR

In occasione della celebrazione del Privacy Day – che quest'anno coincide con la prima del dopo-GDPR – le istituzioni europee riunite in una dichiarazione congiunta, tracciano i primi risultati della riforma divenuta, di fatto, uno standard internazionale.

«*In gioco non ci sono solo la tutela della nostra privacy, ma anche la tutela delle nostre democrazie e la necessità di garantire la sostenibilità delle nostre economie basate sui dati.*».

Obiettivo del GDPR

Uno dei principali obiettivi del GDPR «è quello di offrire un ruolo attivo alle persone, dando loro maggiore controllo su una delle risorse più preziose dell'economia moderna: *i loro dati. Per poter raggiungere questo obiettivo è indispensabile che le persone siano pienamente consapevoli dei loro diritti e delle conseguenze delle loro decisioni.*».

Primi risultati

Le autorità nazionali hanno finora ricevuto 95.000 reclami da parte dei cittadini, la vicenda Google-CNIL evidenzia che le autorità stanno già esercitando i poteri sanzionatori che sono loro attribuiti dal regolamento.

Tratto dall'infografica della Commissione UE.

Solo **cinque Stati membri** non hanno ancora provveduto ad adeguare il proprio quadro giuridico alle nuove norme europee (Bulgaria – dove la legge nazionale sarebbe alla firma del capo dello Stato – Grecia, Slovenia, Portogallo, Cechia), il mutuo riconoscimento dell'adeguatezza dei regimi data protection UE-Giappone è testimonianza di «*una chiara convergenza verso un regime di protezione dei dati moderno*» a livello globale e presto sarà accompagnata da un'analoga decisione di adeguatezza riguardo alla Corea del Sud.

5.
Sesta riunione plenaria dell'EDPB

Il 22 e 23 gennaio si è tenuta la sesta riunione plenaria dell'EDPB in cui sono stati discussi numerosi temi quali il secondo rapporto annuale su Privacy Shield, Brexit, domande e risposte sulle sperimentazioni cliniche, le liste riguardo alla DPIA, le linee guida sulla certificazione e la risposta del Comitato all'autorità di supervisione australiana sulle notifiche di data breach.

Privacy Shield

Sul tema del rapporto del Comitato riguardo alla seconda revisione annuale dell'EU-US Privacy Shield si è già detto in occasione dello scorso Editoriale del 31 gennaio.
Il Comitato ha evidenziato pregi e difetti dell'attuale intesa; **tra i miglioramenti** realizzati – rispetto alla precedente versione – in particolare sono state rilevate le azioni intraprese per adattare il processo di certificazione iniziale, l'azione di supervisione e di controllo d'ufficio, la pubblicazione delle decisioni delle corti FISA (cioè decidenti in base al Foreign Intelligence Surveillance Act cioè la legge sulla sorveglianza e l'intelligence straniera), la nomina di un nuovo Presidente e di tre nuovi membri del Consiglio per la tutela della privacy e delle libertà civili (PCLOB) e l'annuncio della nomina di un difensore civico permanente ("Ombudsperson").
Tra le preoccupazioni ancora non risolte sono state evidenziate: la mancanza di assicurazioni concrete che escludono la raccolta e l'accesso indiscriminati ai dati personali a fini di sicurezza nazionale, l'assenza di certezza della disponibilità di poteri cogenti in capo al Difensore civico per porre rimedio ad eventuali inadempienze, la permanente carenza di robustezza dei controlli (ad es. per quanto riguarda i controlli necessari per soddisfare i requisiti di trasferimenti successivi), la portata del significato dei dati sulle risorse umane e il processo di ri-certificazione al programma.
In conclusione, il Privacy Shield rimane uno strumento temporaneamente valido per la legittimazione dei flussi commerciali di dati personali tra UE e Stati Uniti, ancorchè soggetto a monitoraggio ed alle future decisioni della CGUE.

Brexit

Riguardo alla Brexit, nel citato Editoriale si è accennato delle iniziative di chiarimento assunte dall'autorità di supervisione del Regno Unito; l'EDPB, dal suo canto, ha discusso le possibili conseguenze di Brexit nell'area della protezione dei dati e della necessità di cooperazione e di scambio di informazioni tra le ASN degli Stati membri su preparativi e strumenti disponibili per trasferire i dati nel Regno Unito, una volta che il Regno Unito non farà più parte dell'UE.
In conclusione, si sta cercando di fare quanto possibile affinché il passaggio di regime – specie nell'ipotesi del "no-deal" – possa avvenire senza eccessivi traumi: tuttavia, come traspare anche dalle risposte pubblicate dall'ICO, continuano a sussistere ampi margini di incertezza per i flussi tra UE-UK e viceversa, per il dopo Brexit.

Sperimentazioni cliniche

A seguito di una richiesta della Commissione europea (DG SANTE), l'EDPB ha adottato il suo parere sulle domande e risposte sugli studi clinici. Il parere – che si incentra sulle interrelazioni fra il regolamento sugli studi clinici ed il GDPR – affronta in particolare gli aspetti relativi alle basi giuridiche nel contesto delle sperimentazioni cliniche e degli usi secondari dei dati delle sperimentazioni cliniche a fini scientifici.

Premesse

Il GDPR prevede che tra i compiti dell'EDPB vi sia quello di fornire «*consulenza alla Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione (...)*» [art. 70(1)(b)], su questa base la Commissione ha chiesto il parere del Comitato riguardo ad un proprio documento [Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR)] contenente domande e risposte sui rapporti tra i due regolamenti, quello sugli studi clinici [Regolamento (UE) N. 536/2014] e il GDPR.

Differenze tra i due regolamenti

Mentre il GDPR garantisce la protezione delle persone rispetto al trattamento dei dati personali e le norme armonizzate sulla libera circolazione di tali dati, il CTR mira a garantire un livello maggiore di armonizzazione delle norme per lo svolgimento di sperimentazioni cliniche in tutta l'UE, includendo prescrizioni sulla protezione delle persone, sul consenso informato e requisiti di trasparenza. Inoltre, mentre il GDPR è già pienamente applicativo dal 25 maggio 2018, il CTR, sebbene entrato in vigore il 16 giugno 2014, attende la pubblicazione di un avviso di conferma da parte della Commissione UE ed il decorso di un successivo semestre di transizione, prima di essere pienamente applicabile (ad oggi si stima che ciò accadrà nel 2020).

Correlazioni tra CTR e GDPR

Il CTR espressamente prevede che le prescrizioni in esso contenute vanno attuate applicando il GDPR (anche se il riferimento è alla precedente direttiva 95/46/CE, ora sostituita dal regolamento) ed il regolamento 2018/1725 per la protezione dei dati personali da parte delle istituzioni europee (anche in tal caso richiamato tramite il suo predecessore, il regolamento (EC) n. 45/2001) (si veda l'art. 93 del CTR). Dal suo canto, il GDPR fa esplicito riferimento alla normativa sugli studi clinici [Considerando (156) e (161)].

In conclusione, i due regolamenti si applicano congiuntamente ed il CTR è norma settoriale per quanto riguarda le disposizioni rilevanti sotto l'aspetto data protection, ma non può comunque contrastare col GDPR. Quindi, in attesa della piena applicazione del CTR, le domande e risposte redatte dalla Commissione costituiscono una buona base di riferimento per la conformità degli studi clinici al GDPR.

Base giuridica dei trattamenti a fini di sperimentazioni cliniche

Una prima distinzione va fatta, al riguardo, tra "uso primario" e "uso secondario": secondo l'EDPB «*tutte le operazioni di trattamento relative a uno specifico protocollo di sperimentazione clinica durante l'intero ciclo di vita, dall'avvio della sperimentazione alla cancellazione alla fine del periodo di archiviazione, devono essere intese come uso primario di dati per studi clinici*». In questo ambito, secondo il Comitato, a sua volta occorre distinguere «*le* ***operazioni di trattamento puramente connesse alle attività di ricerca*** *(...) dalle operazioni di trattamento* ***connesse agli scopi della protezione della salute****, stabilendo standard di qualità e sicurezza per i medicinali generando dati affidabili e solidi (affidabilità e sicurezza)*» (enfasi aggiunta); questa distinzione si rende necessaria in quanto «*queste due principali categorie di attività di trattamento si fondano su basi giuridiche diverse*».

Base giuridica per affidabilità e sicurezza

Secondo il Comitato, nell'ambito degli studi clinici i trattamenti di dati personali effettuati dal promotore o dallo sperimentatore che perseguono finalità di "affidabilità e sicurezza" – come sopra specificato – si fondano sulla base giuridica prevista dall'articolo 6(1)(c) (per i dati "comuni") e dall'art. 9(2)(i) (per le speciali categorie di dati) del GDPR, cioè in quanto «*il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento*» oppure «è necessario per motivi di interesse pubblico nel settore della sanità, quali (...) la garanzia di parametri *elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale*».

In conclusione, rientrerebbero nella base giuridica dell'obbligo legale ovvero dei motivi di interesse pubblico nel settore della sanità, i trattamenti di dati personali necessari per «*l'adempimento delle registrazioni e comunicazioni sulla sicurezza di cui agli articoli da 41 a 43 del CTR e gli obblighi relativi all'archiviazione del fascicolo permanente della sperimentazione clinica (25 anni ai sensi dell'articolo 58 CTR) e delle cartelle cliniche dei soggetti (che deve essere determinato dalla legge nazionale secondo la stessa disposizione). Lo stesso vale per qualsiasi divulgazione dei dati delle sperimentazioni cliniche alle autorità nazionali competenti nel corso di un'ispezione in conformità alle pertinenti norme nazionali (cfr. Articoli 77-79 CTR)*».

Base giuridica dei trattamenti per finalità di ricerca

Le restanti operazioni di trattamento connesse ad attività di ricerca nel contesto di una sperimentazione clinica – «*a seconda delle circostanze del processo e della concreta attività di trattamento dei dati*», possono fondarsi su:

- «*compito svolto nell'interesse pubblico (articolo 6, paragrafo 1, lettera e)) in combinato disposto con l'articolo 9, paragrafo 2, lettere i) o j) del GDPR*»;
- «*interessi legittimi del titolare del trattamento (articolo 6, paragrafo 1, lettera f)) in combinato disposto con l'articolo 9, paragrafo 2, lettera j) del GDPR»;*
- in circostanze specifiche, quando tutte le condizioni sono soddisfatte, «*consenso esplicito della persona interessata (articolo 6, paragrafo 1, lettera a), in combinato disposto con l'articolo 9, paragrafo 2, lettera a)) del GDPR*».

Base giuridica per usi secondari fuori dal protocollo di sperimentazione clinica

«*(S)e uno sponsor o uno sperimentatore desidera utilizzare ulteriormente i dati personali raccolti per altri scopi scientifici, diversi da quelli definiti dal protocollo di sperimentazione clinica, deve individuare un altro fondamento giuridico specifico rispetto a quello utilizzato per lo scopo principale*» senza tuttavia escludere a priori – secondo l'EDPB – la «*presunzione di compatibilità prevista dall'articolo 5, paragrafo 1, lettera b), del GDPR*»; per cui «*(p)er il momento, la presunzione di compatibilità, fatte salve le condizioni di cui all'articolo 89, non dovrebbe essere esclusa, in tutte le circostanze, per l'uso secondario dei dati delle sperimentazioni cliniche al di fuori del protocollo della sperimentazione clinica per altri scopi scientifici*».

Liste DPIA

L'EDPB ha rilasciato un parere in merito alle liste di trattamenti con potenziale rischio elevato (da sottoporre quindi a DPIA) rilasciate dalle NSA di Liechtenstein e Norvegia, cioè due dei

Paesi aderenti al SEE o EEA. Questi due pareri seguono i 22 pareri adottati durante la plenaria di settembre e i quattro pareri adottati durante la plenaria di dicembre.

Linee guida sulla certificazione

Conclusasi la consultazione pubblica, l'EDPB ha adottato la versione finale delle linee guida sulla certificazione, adottando anche un nuovo allegato (che sarà sottoposto a consultazione pubblica in tempi brevi): «*(l)e linee guida aiuteranno gli Stati membri, le autorità di vigilanza e gli organismi nazionali di accreditamento (NAB) a rivedere e approvare i criteri di certificazione ai sensi dell'art. 42 e art. 43 GDPR.*».

Risposta del Comitato all'autorità di supervisione australiana sulle notifiche di data breach

L'EDPB – dietro specifica richiesta dell'Australian Information Commissioner pervenuta nell'ottobre 2018 – ha fornito delucidazioni in merito all'obbligo di notifica delle violazioni dei dati alle autorità di vigilanza. Questa iniziativa, come sottolineato dal Comitato, evidenzia l'importanza della collaborazione internazionale sui temi della protezione dei dati personali.

6.
Garante: i consulenti del lavoro sono “responsabili”

L'ultima newsletter della nostra autorità di controllo ci informa dell'irrogazione di una sanzione di 600.000 euro per telemarketing selvaggio, dell'approssimarsi di sanzioni contro Facebook per il "caso Cambridge Analytica, a conclusione dell'istruttoria," e della risposta dell'Autorità ai quesiti formulati dal Consiglio Nazionale in merito al ruolo privacy assunto dai consulenti del lavoro. Riguardo a quest'ultimo punto, a prima vista le precisazioni del Garante privacy indirizzate al Consiglio Nazionale dei consulenti del lavoro sembrerebbero avere il solo pregio di mettere le "cose in chiaro": obiettivo non da poco – si dirà – specie avuto riguardo al contesto di incertezza giuridica che caratterizza questi tempi. Che i consulenti del lavoro, quando utilizzano i dati personali dei dipendenti dei loro clienti per effettuare i servizi cui sono professionalmente preposti, fossero da inquadrare come "responsabili del trattamento", era alquanto palese. Si potrebbe aggiungere, a mò di commento generale, che forse sarebbe stato preferibile che il Consiglio Nazionale avesse chiesto il parere del Garante, prima di emettere una propria posizione ufficiale (circolare 23 luglio 2018, n. 1150) – peraltro basata su un'interpretazione della norma chiaramente errata – anzichè successivamente, evitando in tal modo di provocare una turbativa nel settore e non solo, di cui non si sentiva affatto la necessità.

Sintesi

Come spesso accade con la lettura frettolosa dei quotidiani, fermarsi sui titoli rischia di far perdere il vero "cuore" della notizia, talvolta fatta di chiaroscuri, piuttosto che basata su affermazioni lapidarie. Ci sembra che qualcosa di analogo sia accaduto con il citato documento dell'Autorità, laddove in filigrana si possono scorgere alcune interessanti considerazioni o "passaggi" che qui vorremmo evidenziare e commentare; in particolare:

1. Spesso si attribuisce al novello regolamento conclusioni giuridiche che, viceversa, hanno origini molto più datate, in quanto il GDPR non riempie un preesistente vuoto normativo bensì esso riforma una disciplina ancora talvolta poco nota.
2. Il processo di determinazione del ruolo data protection assunto da un soggetto, non necessariamente perviene a conclusioni univoche, nel senso che lo stesso soggetto può assumere più ruoli in relazione a distinti trattamenti.
3. Prima dell'applicazione del GDPR si era soliti ritenere che la molteplicità dei trattamenti dovesse necessariamente presupporre una molteplicità di rapporti giuridici, mentre la riforma – anche tramite l'enfasi data alle basi giuridiche – ci ha insegnato che un operatore può assumere più ruoli data protection pur nell'ambito del medesimo rapporto giuridico di fornitura con una terza parte.
4. Come sottolineato nella serie di nostri precedenti interventi sulla linea di confine tra Titolari e Responsabili (si vedano gli Editoriali del 25/10/2018, 8/11/2018, 20/12/2018, e 17/1/2019), un eventuale – anche apprezzabile – margine di autonomia e correlativa responsabilità del fornitore sotto il profilo data protection, non esclude a priori una possibile collocazione di quest'ultimo come "responsabile del trattamento" del cliente-titolare.
5. I soggetti che nell'assetto organizzativo del responsabile del trattamento effettuano "senza apprezzabili margini di autonomia operazioni di trattamento" sotto la sua autorità" (art. 29) (cioè anche quelle di pertinenza del cliente-titolare), i quali sono assimilabili al ruolo di incaricati del trattamento, devono ricevere ed attenersi alle specifiche istruzioni impartite

dal medesimo responsabile; inoltre il responsabile può delegare taluni dei suoi compiti ad altri soggetti facenti parte della sua organizzazione interna, in qualità di sub-responsabili, previa autorizzazione anche generale del cliente-titolare.

Il GDPR è una riforma

Non è esaltante dover constatare che dopo ventidue anni dalla prima legge nazionale su questo tema, solo l'onda mediatica seguita alla piena applicazione del regolamento abbia suscitato l'interesse di enti, istituzioni ed imprese verso questa disciplina.

Che si trattasse di una riforma, anziché di una regolamentazione di totale nuovo conio, era alquanto palese. La stessa autorità di controllo – in uno dei suoi più felici interventi formativi a cavallo della piena applicazione del GDPR – ha pubblicato sul proprio sito istituzionale una guida all'applicazione della riforma che evidenzia, per ciascun principale profilo della disciplina, ciò che cambia rispetto a ciò che rimane come prima.

Sintomaticità del quesito formulato

Il quesito posto dal Consiglio Nazionale dei consulenti del lavoro – se letto in trasparenza – denota la originalità dell'approccio verso il tema: perchè in proposito nulla di sostanziale è cambiato con l'avvento del regolamento. Viene naturale chiedersi, pertanto, perché il quesito abbia impiegato 22 anni per essere formulato e, se si vuole, com'è possibile che dopo 22 anni un Consiglio Nazionale di una professione regolamentata possa essere pervenuto ad una conclusione interpretativa, qualificando i propri iscritti come titolari autonomi anzichè come responsabili, sulla base di argomentazioni palesemente erronee.

Prima lezione appresa

Da questa circostanza, come da altre similari, si può trarre un primo insegnamento: enti e imprese che si sono risvegliate da un torpore pluri-ventennale ed affrontano oggi la materia per la prima volta, farebbero bene ad esaminare i precedenti consolidatisi in questi anni, prima di pervenire a conclusioni affrettate e fuorvianti.

Un unico rapporto giuridico può alimentare più ruoli data protection

Granularità di analisi

Chi vive nel mondo della consulenza ben sa di doversi confrontare spesso con quesiti formulati a mò di quiz: qual è il ruolo di questo o di quello, devo richiedere il consenso o meno, e così via. Una delle maggiori "novità" originate dall'applicazione del GDPR sta proprio nella mutata granularità di approccio e di analisi, non consueta nella prassi ante-regolamento. Una granularità di analisi orizzontale che interessa quasi tutti i profili della disciplina; ad esempio, toccando anche il processo di redazione dell'informativa, generalmente vissuta altrimenti come un mero standard documentale. Il periodo post-GDPR impone, di converso, un preliminare processo di raccolta delle informazioni necessarie (ragionevolmente, dal registro dei trattamenti) ed una valutazione delle basi giuridiche sottostanti, di non sempre agevole determinazione. In aggiunta, il GDPR ci ha posto in evidenza che ogni profilo della disciplina non vive di vita autonoma bensì che ciascuno sia intrinsecamente correlato agli altri.

Basi giuridiche e ruoli soggettivi

L'esempio dell'informativa non è preso a caso, in quanto l'identificazione di titolarità e basi giuridiche sono informazioni da rendere note all'interessato nell'informativa; peraltro, l'analisi delle basi giuridiche che sono a fondamento di uno specifico trattamento, funge da spia dell'eventuale assunzione di ruoli soggettivi distinti, all'interno del medesimo rapporto giuridico, come quello che si viene ad instaurare tra il cliente ed il consulente del lavoro. Il trattamento di dati personali che si pone in essere può trovare fondamento su una o su più basi giuridiche; nel primo caso, il fornitore acquisirà generalmente un unico ruolo soggettivo, quello di titolare autonomo o di responsabile del trattamento, secondo le circostanze di fatto sottostanti. Qualora, invece, si individuassero più basi giuridiche, il fornitore potrebbe assumere distinti ruoli data protection.

Distinti ruoli DP del consulente del lavoro

A. Consulente - responsabile del trattamento

Nel caso sottoposto al parere del Garante, il consulente agisce in qualità di responsabile del trattamento per conto del cliente-titolare, quando svolge operazioni di trattamento sui dati personali dei dipendenti del cliente per erogare servizi su aspetti che rientrano nelle competenze del datore di lavoro (ad es. elaborazione e predisposizione delle buste paga, gestione dei trattamenti relativi all'assunzione e a quelli di fine rapporto, gestione degli adempimenti previsti dalla disciplina previdenziale ed assistenziale). Queste attività trovano la base giuridica in capo al titolare-cliente e, specificamente, nella necessità di eseguire il contratto di lavoro instaurato tra il cliente (datore di lavoro) ed il proprio dipendente oppure in norme di legge o di regolamento applicabili. Tali basi giuridiche sono quelle che legittimano il trattamento operato dall'azienda cliente, nel cui "cono d'ombra" trova legittimazione anche l'intervento del consulente.

B. Consulente - titolare autonomo

In parallelo, allorquando la base giuridica sarà individuata nella necessità di effettuare il trattamento per dare esecuzione al contratto sottoscritto col cliente (per le operazioni svolte sui dati personali dei propri clienti al fine di dare corso all'incarico ricevuto) il consulente del lavoro assumerà il ruolo di titolare del trattamento, in quanto in questo ambito esso esercita un autonomo potere decisionale su finalità e mezzi del trattamento.

Incaricati

Il documento dell'Autorità ribadisce che, nel quadro normativo della riforma, la figura dell'incaricato del trattamento deve ritenersi compatibile col GDPR e, in quanto tale, essa rimane in vigore. Ciò sta a significare, come avveniva prima del regolamento, che l'obbligo di impartire specifiche istruzioni a coloro che effettuano "senza apprezzabili margini di autonomia operazioni di trattamento sotto l'autorità del titolare o del responsabile (art. 29)", spetta a entrambi il titolare ed il responsabile del trattamento. Nell'esempio del rapporto tra il cliente (titolare e datore di lavoro) ed il consulente del lavoro che agisce in qualità di suo responsabile del trattamento, sarà compito anche di quest'ultimo fornire adeguate istruzioni formali ai propri dipendenti circa le modalità d'uso dei dati personali del personale del cliente, in favore del quale vengono effettuati i servizi di settore. Tali soggetti incaricati dovranno sottostare a vincoli di riservatezza per quanto attiene ai dati personali cui hanno accesso.

Sub-responsabili

Ferma restando la discrezionalità di ciascun imprenditore – sia esso titolare o responsabile del trattamento – di attribuire specifiche funzioni e compiti connessi al trattamento di dati personali a soggetti appositamente designati (v. art. 2-quaterdecies, cod. privacy) il documento dell'Autorità evidenzia un'ulteriore possibilità riguardo alle modalità di designazione di sub-responsabili.
Come noto, nella prassi si intendono con il termine di "sub-responsabili" quelle terze parti di cui eventualmente il responsabile del trattamento si possa avvalere per dare esecuzione all'incarico ricevuto dal proprio cliente in materia di protezione dei dati personali: in sostanza, essi sono sub-appaltatori che effettuano operazioni di trattamento sui dati personali di pertinenza del cliente originario (titolare).

Sub-responsabili all'interno dell'assetto organizzativo del responsabile

Il parere dell'autorità italiana fornisce evidenza di un'ipotesi di modalità di designazione del sub-responsabile che lascia qualche incertezza. Secondo quanto prospettato nel documento del Garante, sarebbe ipotizzabile per il fornitore (responsabile del trattamento) – previa autorizzazione anche generale del cliente-titolare – ingaggiare come "sub-responsabile" [ai sensi dell'articolo 28(2) e (4)], persone fisiche espressamente designate e che operano nell'ambito del proprio assetto organizzativo interno, sotto la sua diretta autorità. A tali "manager sub-responsabili" verrebbe affidata l'esecuzione di specifiche attività di trattamento per conto del titolare. Nei riguardi di costoro, quindi, troverebbe applicazione la regolamentazione prevista dal GDPR in materia di sub-responsabili [artt. 28(2)(4)].

Critiche al sub-responsabile interno

Una prima obiezione all'ipotesi del sub-responsabile "interno" discende dalla constatazione che il cosiddetto "sub-responsabile" sia un "responsabile del trattamento" a tutti gli effetti; tanto è vero che il GDPR anzichè utilizzare un termine apposito per questa figura, lo indica come "ulteriore responsabile". Il "sub-responsabile", quindi, altro non è che un "responsabile" di secondo livello. Questo implica che sul "sub-responsabile" gravano le prescrizioni e le responsabilità che il GDPR attribuisce in via diretta al "processor", nonostante che «*(q)ualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile*».

Terzietà soggettiva del sub-responsabile

Chiarito che il "sub-responsabile" è comunque un "processor", se è incontestabile che la figura del responsabile (ancorchè di primo livello) possa essere ricoperta solo da un soggetto "terzo" rispetto al titolare (tanto da ritenere non più compatibile col GDPR la figura del responsabile "interno", presente sotto l'egida del codice privacy previgente) anche quella del "sub-responsabile" dovrebbe essere "terza parte" rispetto al responsabile di primo livello. Viene in soccorso di questa tesi la prescrizione che – riguardo alla relazione tra i due responsabili (di primo e di secondo livello) – richiede la riproduzione speculare degli obblighi assunti dal responsabile iniziale nei confronti del titolare; prescrizione che sarebbe difficile attuare nei riguardi di un proprio dipendente. Recita, infatti, la norma: «*su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati*

contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3» (cioè, il responsabile iniziale).

Distribuzione di compiti nell'assetto organizzativo interno del responsabile

Il GDPR specifica che il contratto con il sub-responsabile debba prevedere l'obbligo di quest'ultimo di adottare «*in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento*». Disposizione difficilmente suscettibile di adempimento da parte di un sub-responsabile, lavoratore subordinato.

Vale ricordare, in conclusione, che ad analogo risultato si possa pervenire – senza dover necessariamente "forzare" la figura tipica del responsabile "ulteriore" – tramite la facoltà riconosciuta anche al "processor" di organizzarsi al proprio interno in autonomia, assegnando specifici compiti e funzioni a persone fisiche che agiscono sotto la sua autorità (art. 2-quaterdecies, cod. privacy). In quest'ultimo caso, avremo un unico responsabile con distribuzione di compiti e funzioni al proprio interno, senza necessità di preventiva autorizzazione del titolare.

7.
EDPB: un ricco programma per il prossimo biennio

Nella settima riunione plenaria, il Comitato europeo (EDPB) ha rilasciato il piano operativo per il prossimo biennio 2019-2020 in cui concentrerà i propri interventi maggiormente su aree più specialistiche e su nuove tecnologie in aggiunta alle consuete linee guida sul GDPR, come avvenuto sinora. In tale riunione sono anche stati adottati altri importanti documenti.

Attività dell'EDPB

Ancor più del suo predecessore – il Gruppo di lavoro dell'articolo 29 (WPArt29) – l'EDPB è un punto di riferimento centrale ed una rilevante fonte interpretativa nell'ambito della protezione dei dati personali: le sue riunioni plenarie contengono agende molto ricche e producono di solito documenti di rilievo da tenere presente nelle operazioni di conformità al GDPR; di questi, i principali saranno richiamati nella sezione "Normativa" del DPtel® associata ad una valutazione di comodo circa la loro rilevanza generale (applicando la consueta scala a stellette, di cinque livelli), che riteniamo possa essere d'ausilio per l'utente.

Programma biennale 2019-2020

Il programma biennale 2019-2020 risulta ambizioso: si compone di attività di varia natura (linee guida, pareri di coerenza, ulteriore documentazione) che può raggrupparsi nei seguenti temi principali:

- Diritti degli interessati.
- Vincolatività.
- Trasferimenti internazionali di dati.
- e-Privacy e servizi online.
- Dati finanziari e PSD2.

Diritti degli interessati

L'EDPB prevede il rilascio di linee guida sui diritti degli interessati, affrontando in maggior dettaglio i diritti di accesso, cancellazione, obiezione e limitazione al trattamento nonchè i casi di deroga. Ulteriore attività programmata avrà per oggetto il profilo dei dati personali dei minori ed il tema della disiscrizione (delisting).

Vincolatività

Fa parte del programma biennale la pubblicazione di un documento dell'EDPB sulla strategia per l'esecuzione del GDPR e di documenti di valutazione per il ricorso a strumenti di mutua assistenza e cooperazione per rendere vincolante il regolamento fuori dall'Unione. È prevista una linea guida sui poteri delle autorità di supervisione nazionali riguardo all'articolo 47 della direttiva sui dati per finalità penali (dir. 2016/680), insieme a possibili ulteriori attività riguardo ai poteri esecutivi verso titolari del trattamento in paesi terzi.

Trasferimenti internazionali di dati

In merito ai flussi esteri di dati personali, sono previste linee guida sulle certificazioni e codici di condotta GDPR come strumenti di legittimazione di tali flussi, così come sui flussi esteri tra pubbliche autorità a fini di cooperazione amministrativa (si veda, su questo, il parere 4/2019 più in basso). Sempre su questo tema vi è da aggiungere la pubblicazione definitiva – a conclusione

del periodo di consultazione pubblica – delle linee guida sull'ambito applicativo del GDPR. Un possibile intervento del Comitato potrà riguardare le interazioni tra il GDPR ed il regolamento sulla libera circolazione nella UE dei dati non-personali, sulle richieste internazionali a fini probatori e sulla interoperabilità.
In questo ambito, in ogni caso, continuerà l'attività di pareristica dell'EDPB sulle proposte di decisione delle ASN sulle clausole contrattuali standard [in base all'art. 46(2)], sulle clausole standard per responsabili [in base all'art. 28(8)] e sulle clausole contrattuali "ad hoc" per flussi transfrontalieri [in base all'art. 46(3)].

e-Privacy e servizi online

Il Comitato prevede di rilasciare un parere di coerenza sulla relazione tra GDPR e ePrivacy e linee guida sugli utenti dei social media come *target* pubblicitario, sulla videosorveglianza e sui veicoli connessi. Verrà anche approfondita l'ipotesi di necessità contrattuale come base giuridica per i trattamenti nel contesto dei servizi on line. Altre attività possibili in quest'area comprendono il lavoro sulla blockchain e l'uso di nuove tecnologie, come l'intelligenza artificiale e gli assistenti collegati ("connected assistants").

Dati finanziari e PSD2

Linee guida sono previste in merito alle interrelazioni col GDPR della direttiva di modifica sui servizi di pagamento (2015/2366 o PSD2). Altre attività possibili riguardanti la regolamentazione dei dati finanziari includono il lavoro sull'utilizzo delle carte di credito per i pagamenti a distanza e la conservazione post-transazione dei numeri delle carte, così come le fatture elettroniche e la creazione di banche dati centralizzate da parte del Ministero delle Finanze.

Bozza di intesa amministrativa nel campo del controllo dei mercati finanziari

Il Comitato ha anche pubblicato il parere 4/2019 – il primo indirizzato alla Commissione in base all'art. 64(2) – su una proposta di accordo amministrativo (AA), per i trasferimenti di dati personali tra le autorità di vigilanza finanziaria del SEE, tra cui l'Autorità europea degli strumenti finanziari e dei mercati (ESMA), e le pertinenti autorità non-UE; questo parere è stato rilasciato in base all'art. 46(3)(b) del GDPR.
Il documento oggetto del parere verrà firmato da parte delle autorità preposte al controllo dei mercati finanziari al fine di «predisporre adeguate salvaguardie per il trattamento dei dati personali nell'esercizio dei rispettivi mandati e responsabilità regolamentari»; l'EDPB ha ritenuto che l'AA garantisca garanzie adeguate quando i dati personali saranno trasferiti sulla base di questo AA ad organismi pubblici di paesi extra-SEE non coperti da una decisione di adeguatezza della Commissione europea. Con questo passo il flusso transfrontaliero di dati personali tra le autorità firmatarie dell'AA per lo svolgimento delle funzioni pubbliche cui sono preposte, sarà legittimato.

Brexit: nota informativa in caso di mancato accordo

L'EDPB ha rilasciato una nota informativa sulle conseguenze derivanti da un mancato accordo Brexit, in relazione ai flussi di dati personali dal SEE alla Gran Bretagna.
In assenza di un accordo tra l'UE e il Regno Unito (no-deal Brexit), il Regno Unito diventerà un paese terzo dalle 00:00 am CET del 30 marzo 2019. Di conseguenza, il trasferimento di dati

personali dal SEE al Regno Unito dovrà basarsi su uno degli strumenti previsti per i flussi esteri di dati dal regolamento: cioè Clausole contrattuali standard o ad hoc, Regole aziendali vincolanti (BCR), codici di condotta e meccanismi di certificazione e gli strumenti di trasferimento specifici disponibili per le autorità pubbliche.
In senso inverso, stando alle dichiarazione del governo UK, i trasferimenti di dati personali dal Regno Unito al SEE, potranno continuare liberamente anche nel caso di una Brexit senza accordo.

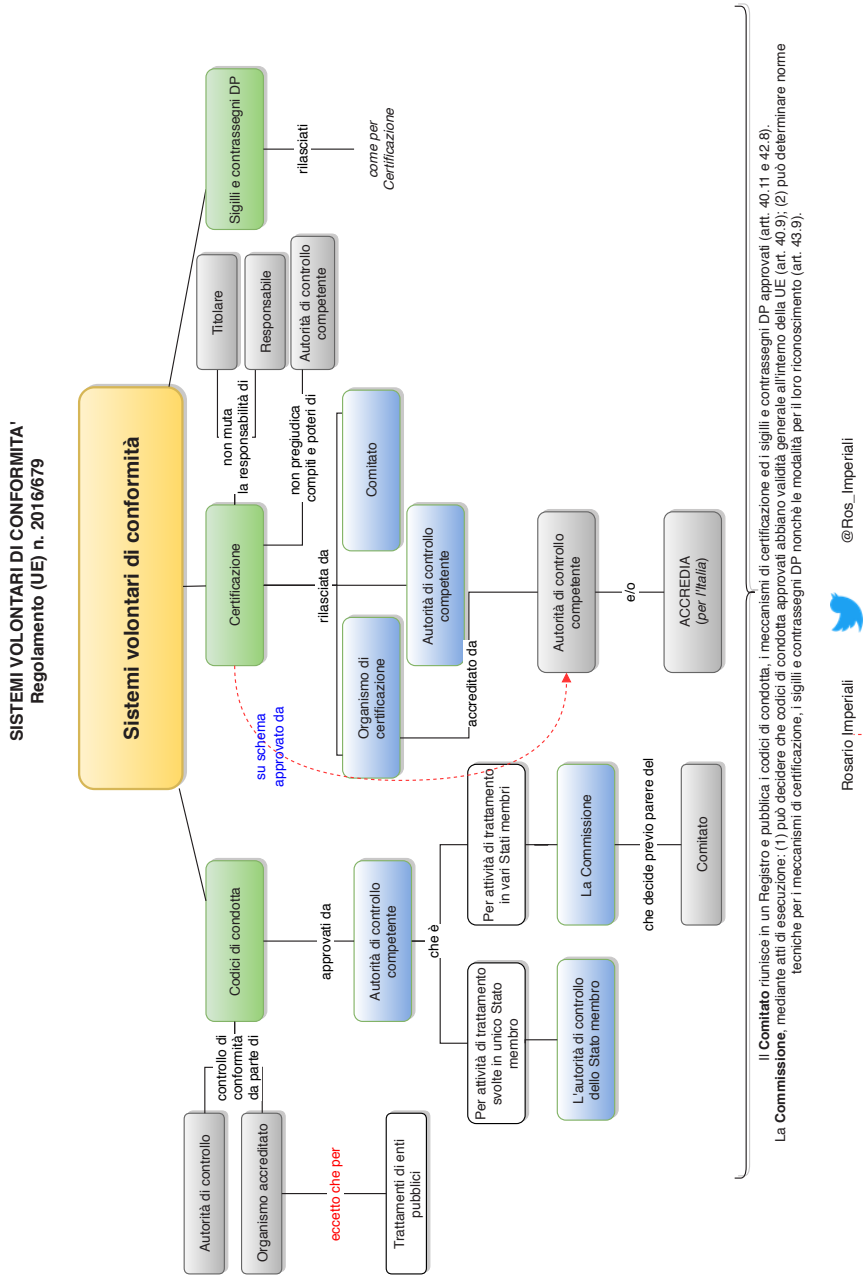
Codici di condotta: linee guida

L'EDPB ha adottato linee guida sui codici di condotta che saranno pubblicate non appena verranno ultimate le verifiche giuridiche e linguistiche sul documento; come di consueto, esse saranno sottoposte a consultazione pubblica e formeranno oggetto di analisi in una prossima tornata dell'Editoriale. Scopo delle linee guida è fornire indicazioni pratiche e assistenza interpretativa in relazione all'applicazione degli articoli 40 e 41 del GDPR. Le linee guida intendono contribuire a chiarire le procedure e le regole coinvolte nella presentazione, approvazione e pubblicazione di codici di condotta a livello sia nazionale che europeo.

8.
Codici di condotta: linee guida EDPB in consultazione

Il Comitato europeo (EDPB) ha sottoposto a consultazione pubblica – con scadenza il 2 aprile 2019 – le linee guida in materia di codici di condotta in relazione a quanto disciplinato agli articoli 40 e 41 del GDPR.

Sintesi



Obiettivo delle linee guida

Scopo delle linee guida n.1/2019 è quello di fornire orientamenti pratici e supporto interpretativo rispetto all'applicazione della disciplina in materia di codici di condotta (artt. 40-41), distinguendo sia la diversa tipologia dei codici nazionali e transnazionali sia le due fasi del processo di approvazione da parte dell'autorità di controllo (ASN) competente, consistenti in:

1. ammissibilità della presentazione della proposta di codice;
2. analisi dei suoi contenuti ed approvazione della proposta di codice.

Contenuti delle linee guida 1/2019

Le linee guida, adottate il 12 febbraio 2019 ed oggetto di consultazione pubblica fino al 2 aprile 2019, affrontano anche il tema delle modalità di accreditamento e del ruolo degli organismi di monitoraggio dei medesimi codici.

Dopo un'introduzione che ribadisce la natura dei codici di condotta ed i benefici che se ne possono trarre, le linee guida si soffermano sui criteri

- per l'ammissibilità della proposta di codice all'esame dell'ASN competente (**criteri di ammissibilità**);
- per l'approvazione finale della proposta (**criteri per l'approvazione**).

A seguire, il documento dell'EDPB descrive i processi di approvazione previsti per i:

- codici di condotta nazionali;
- **codici di condotta transnazionali** (cioè quelli che interessano più Stati membri).

Il documento si conclude con **quattro allegati** che descrivono rispettivamente:

- gli elementi distintivi dei codici di condotta nazionali da quelli transnazionali (all.1);
- le modalità di individuazione dell'autorità di controllo competente (all.2);
- la lista di controllo per la presentazione di una proposta di codice (all.3);
- il diagramma di flusso relativo all'intero processo (all.4).

Codici di condotta

I codici di condotta sono regolati dagli articoli 40 e 41 del GDPR e – come evidenziato nell'infografica sopra – rappresentano uno degli strumenti di disciplina volontaria e di accountability considerati dal regolamento. Tramite tali codici, rappresentanti ed associazioni di settore, avendo contezza delle peculiarità dei propri contesti, possono stabilire regole specifiche di protezione dei dati personali per le categorie di titolari e responsabili di riferimento, nel rispetto del GDPR; in tal modo, essi hanno l'opportunità di definire quali siano i comportamenti più appropriati – di natura legale ed etica – nel settore considerato.

Finalità dei codici di condotta

I codici di condotta offrono un'opportunità per specifici settori di affrontare questioni comuni riguardo al trattamento dei dati e di accettare regole di protezione dei dati più pratiche ed operative, personalizzate al contesto di riferimento, che soddisfino le esigenze del settore e le esigenze del GDPR. In questo modo, i codici possono contribuire a creare una maggiore armonizzazione in ambiti settoriali e colmare le lacune di armonizzazione che possono esistere tra gli Stati membri nell'applicazione della disciplina sulla protezione dei dati.

I codici di condotta possono anche rappresentare una forma di salvaguardia per i flussi di dati personali diretti verso paesi extra-UE privi di un sistema di protezione ritenuto comparabile con quello della UE, come previsto dall'articolo 40(3) del GDPR; questi ultimi, tuttavia, formeranno oggetto di specifiche linee guida dell'EDPB, ulteriori rispetto a quelle qui in commento.

Codici di condotta nazionali ed europei

Sono **codici di condotta "nazionali"** quelli che riguardano le attività di trattamento di titolari e/o responsabili le quali si realizzano all'interno di un unico Stato membro.
Di converso, si hanno **codici di condotta "transnazionali"** quando il codice di condotta adottato da un'associazione nazionale in uno Stato membro riguarda le attività di trattamento da parte dei suoi membri in diversi Stati membri, senza che esso necessariamente implichi un flusso transfrontaliero di dati personali all'interno dell'Unione.

Rilevanza dei codici di condotta

L'aderenza a un codice non garantisce di per sé il rispetto del GDPR o l'immunità per titolari/responsabili da sanzioni o responsabilità previste dal GDPR.
Diversamente dalle regole deontologiche introdotte dal novellato codice privacy (art. quater), le prescrizioni dei codici di condotta del GDPR non sono condizioni di liceità del trattamento. Ciononostante, il loro rispetto incide a vario titolo sulla valutazione di conformità dell'operato dei titolari o responsabili che vi aderiscono; l'osservanza di un codice di condotta approvato sarà un fattore preso in considerazione dalle autorità di vigilanza nel

- valutare gli aspetti relativi alla sicurezza [art. 32(3)];
- valutare l'impatto del trattamento nell'ambito di una DPIA [art. 35(8)];
- determinare l'ammontare di una sanzione amministrativa [art. 83(2)(j)].

Fasi del processo di approvazione

Le linee guida 1/2019 evidenziano due distinte fasi del complessivo processo di valutazione ed approvazione dei codici di condotta da parte dell'ASN competente:

1. fase di presentazione della proposta di codice;
2. **fase di analisi di dettaglio** dei contenuti ed approvazione del codice.

Fase 1: Criteri di ammissibilità della presentazione del progetto di codice

Affinchè un progetto di codice possa essere preso in considerazione dall'ASN competente, l'EDPB prescrive che sia dimostrato il soddisfacimento di 11 criteri.

1. **Dichiarazione esplicativa e documentazione di supporto** – le associazioni o altri enti che redigono e presentano il loro codice (detti "proprietari del codice") devono fornire una dichiarazione esplicativa e tutta la documentazione di supporto pertinente per consentire all'ASN competente di comprendere lo scopo del codice, l'ambito e il modo in cui esso faciliterà l'effettiva applicazione del regolamento (paragrafo 20).
2. **Rappresentatività -** occorre dimostrare che si sia un'associazione o un altro organismo che rappresenta categorie di titolari o responsabili del trattamento, fornendo dettagli nella presentazione per dimostrare che si sia un organo rappresentativo efficace, in grado

di comprendere le esigenze dei propri membri (es. numero o quota di iscritti, esperienza di settore dell'organo rappresentativo) (paragrafi 21 e 22).

3. **Ambito del trattamento -** definizione chiara dell'attività o del settore di trattamento e specifica dei problemi di trattamento a cui il codice è destinato ad indirizzarsi (paragrafo 23).
4. **Ambito territoriale -** identificazione dell'ambito territoriale del codice, incluso un elenco di tutte le ASN interessate (se pertinente) (paragrafo 24)
5. **Individuazione dell'autorità competente -** dettagli per giustificare l'identificazione della ASN competente (paragrafo 25).
6. **Supervisione dei meccanismi -** inclusione di meccanismi che consentono un monitoraggio efficace della conformità del codice (paragrafo 26).
7. **Organismo di monitoraggio -** identificazione di un organismo di monitoraggio e spiegazione delle modalità mediante cui si soddisfano i requisiti di monitoraggio del codice (paragrafo 27).
8. **Consultazione -** informazioni sulla portata della consultazione svolta nel procedimento di realizzazione del codice (paragrafo 28).
9. **Legislazione nazionale -** conferma del fatto che il progetto di codice è conforme alle leggi degli Stati membri (se pertinente) (paragrafo 29).
10. **Lingua -** soddisfacimento dei requisiti linguistici (paragrafo 30).
11. **Conformità al GDPR -** dettagli sufficienti per dimostrare la corretta applicazione del GDPR (paragrafi 32-41).

Fase 2: Criteri per l'approvazione del codice di condotta

Una volta superata la fase di ammissibilità – essendo risultati soddisfatti gli 11 criteri sopra indicati – la ASN competente ne informa il proprietario del codice e dà inizio alla fase di analisi dei contenuti e di approvazione della proposta di codice. Anche per questa seconda fase la ASN competente effettuerà la verifica di sussistenza dei seguenti 5 criteri di approvazione:

1. **Soddisfazione di una particolare esigenza -** la proposta di codice deve indirizzare problematiche data protection presenti nel settore considerato, fornendo soluzioni effettive e valide sia per i membri sia per gli interessati (capitolo 6.1).
2. **Facilitazione dell'effettiva applicazione del GDPR -** la proposta deve essere in grado di dimostrare di facilitare l'effettiva applicazione del GDPR nel contesto di riferimento (capitolo 6.2).
3. **Specificazione dell'applicazione del GDPR -** il progetto di codice sottoposto ad approvazione dovrà stabilire chiaramente la sua applicazione settoriale del GDPR, identificare e soddisfare i bisogni specifici di un settore in termini di conformità con la legge sulla protezione dei dati, stabilendo standard realistici e raggiungibili per tutti i membri (capitolo 6.3).
4. **Presenza di sufficienti garanzie -** al fine di mitigare i rischi riguardo al trattamento ed ai diritti e libertà degli individui (paragrafo 39).
5. **Presenza di meccanismi che consentiranno un controllo efficace -** il progetto di codice richiede l'attuazione di meccanismi adeguati per garantire che le prescrizioni in esso contenute siano adeguatamente monitorate e che siano messe in atto misure di

applicazione efficaci e significative per garantirne la piena conformità. Il progetto di codice dovrà inoltre identificare un organismo appropriato che disponga di meccanismi volti a garantire un controllo efficace della conformità al codice (ad es. audit regolari, requisiti di rendicontazione, procedure di gestione e risoluzione delle controversie chiare e trasparenti, sanzioni e rimedi concreti in caso di violazioni del codice, nonché politiche per segnalare violazioni delle sue disposizioni).

Individuazione dell'autorità di controllo competente

L'individuazione dell'ASN competente a decidere in merito ad un progetto di codice di condotta è operazione delicata in quanto essa

- sarà l'unico punto di contatto del proprietario del codice durante il procedimento di approvazione;
- gestisce la procedura di richiesta nella sua fase di cooperazione;
- accredita l'organismo di monitoraggio (se pertinente);
- agisce come supervisore nel garantire che un codice approvato sia monitorato in modo efficace.

Il GDPR non fornisce indicazioni specifiche in proposito e le linee guida evidenziano alcuni fattori orientativi da tenere in considerazione per tale determinazione, come:

- l'ubicazione della maggiore attività di trattamento o del settore;
- l'ubicazione della maggior parte di soggetti interessati dall'attività di trattamento o dal settore;
- l'ubicazione del quartier generale del proprietario del codice;
- l'ubicazione del quartier generale dell'organismo di monitoraggio proposto; o
- le iniziative sviluppate da un'autorità di vigilanza in un campo specifico.

Organismo di monitoraggio

Affinché un codice (nazionale o transnazionale) sia approvato, un organismo di monitoraggio deve essere identificato come parte del codice e **accreditato dalla ASN competente** in quanto capace di monitorare efficacemente il codice.

I proprietari del codice possono decidere di ricorrere a **organismi di controllo esterni o interni**.

Accreditamento dell'organismo di monitoraggio

L'accreditamento dell'organismo di monitoraggio – operazione diversa da quella omologa prevista per gli enti di certificazione – è di spettanza della sola ASN competente, la quale dovrà applicare i requisiti approvati dall'EDPB in base al meccanismo di coerenza (art. 63 del GDPR). Il regolamento lascia una certa flessibilità all'individuazione di questi requisiti evidenziandone solo le caratteristiche principali [art. 41(2)].

Le linee guida elenca i seguenti otto criteri:

1. **Indipendenza** - l'organismo di monitoraggio deve godere di imparzialità di funzione che può essere comprovata attraverso una serie di aree come il finanziamento dell'organismo di monitoraggio, la nomina dei membri/personale, il processo decisionale e più in generale in termini di struttura organizzativa (capitolo 12.1).

2. **Conflitto di interesse** - l'organismo di monitoraggio proposto si asterrà da qualsiasi azione che sia incompatibile con i suoi compiti e doveri (capitolo 12.2).
3. **Esperienza** - l'organismo dovrà possedere conoscenza ed esperienza per quanto riguarda la legge sulla protezione dei dati, nonché del particolare settore o attività di trattamento (capitolo 12.3).
4. **Procedure e strutture stabilite** - un organismo di monitoraggio dovrà disporre di strutture e procedure di governance adeguate che consentano di: valutare l'idoneità di titolari e responsabili ad applicare il codice; monitorare la loro conformità alle sue disposizioni; effettuare revisioni del funzionamento del codice (capitolo 12.4).
5. **Gestione trasparente dei reclami** - l'organismo di monitoraggio dovrà stabilire procedure e strutture efficaci che possano gestire la gestione dei reclami in modo imparziale e trasparente (capitolo 12.5).
6. **Comunicazione con l'ASN competente** - l'organismo di monitoraggio proposto deve consentire la comunicazione efficace di eventuali azioni da esso svolte in merito al codice, alla ASN competente e ad altre autorità di controllo (capitolo 12.6).
7. **Meccanismi di revisione** - appropriati meccanismi di revisione devono garantire che il codice rimanga rilevante e continui a contribuire alla corretta applicazione del GDPR (capitolo 12.7).
8. **Stato legale** - i proprietari del codice devono dimostrare che l'organismo di monitoraggio ha la posizione appropriata per svolgere il proprio ruolo ai sensi dell'articolo 41, paragrafo 4 ed è soggetto a sanzioni a norma dell'articolo 83, paragrafo 4, lettera c), del GDPR (capitolo 12.8).

Procedura di approvazione dei codici di condotta

Codici di condotta nazionali

L'ASN competente, ricevuta la richiesta di approvazione di un progetto di codice di condotta, effettua preliminarmente la verifica del soddisfacimento dei criteri di ammissibilità di cui si è detto sopra. **Se i criteri di ammissibilità non sono soddisfatti** il procedimento si conclude ed eventualmente occorrerà effettuare una nuova richiesta. Al contrario, **se i criteri di ammissibilità sono soddisfatti**, l'ASN competente ne dà notizia al proprietario del codice e prosegue con la fase di analisi dei contenuti del progetto. **In caso di rigetto**, il procedimento si conclude con la notifica della decisione negativa al proprietario del codice. Qualora, invece, **il progetto viene approvato**, l'ASN competente provvede alla sua registrazione e pubblicazione in base all'articolo 40(6) del GDPR.

Codici di condotta transnazionali

Il progetto di codice transnazionale viene presentato all'ASN competente che agisce come autorità principale per il procedimento di approvazione del codice.

All'atto della presentazione l'ASN competente ne dà notizia a tutte le ASN al fine di verificare quali di esse sono ASN interessate [secondo la definizione dell'art. 4(22)(a) e (b)]. **Qualora non risultino rispettati i criteri di ammissibilità**, il procedimento ha termine e l'ASN competente ne informa le altre ASN interessate.

Se, viceversa, **i criteri di ammissibilità sono soddisfatti**, l'ASN competente ne dà comunicazione ai proprietari del progetto e dà inizio alla fase di analisi dei relativi contenuti innescando la **procedura di cooperazione informale** con le altre ASN interessate; tra queste verranno individuate massimo due co-revisori che assisteranno la ASN competente nella valutazione del progetto di codice. L'ASN competente determinerà in via definitiva [art. 40(7)] se il progetto di decisione debba essere presentato all'EDPB ai sensi degli articoli 63 e 64 del GDPR.
In caso di decisione di rigetto, il procedimento cessa e le parti riceveranno conseguente notifica; se, invece, **l'ASN considera il progetto suscettibile di approvazione**, farà circolare la bozza di decisione di approvazione tra le ASN interessate per ottenerne il parere entro i successivi 30 giorni. Se la decisione è di **rimettere la questione all'EDPB**, l'ASN competente comunicherà tale decisione a tutte le ASN interessate secondo la procedura relativa ai meccanismi di coerenza. L'EDPB rilascerà un proprio parere e l'ASN competente sarà libera di mantenere o modificare la propria proposta di decisione.
Al termine del procedimento di approvazione andato a buon fine, l'EDPB raccoglierà il codice transnazionale approvato e lo renderà disponibile al pubblico insieme agli altri.

9.
L’Argentina ratifica la Convenzione 108

Oggi i riflettori della scena internazionale sono tutti per lui, il GDPR; eppure uno strumento normativo di pari importanza, in ambito data protection, è stato approvato quasi contemporaneamente alla piena applicazione del regolamento nel maggio 2018: il Protocollo di modernizzazione della convenzione del Consiglio d'Europa sul trattamento di dati personali, meglio nota come "Convenzione 108".
In questi giorni anche l'Argentina ratifica la Convenzione 108.

Consiglio d'Europa

Il Consiglio d'Europa – da non confondere con l'istituzione europea Consiglio dell'Unione europea – è un organismo internazionale, con sede a Strasburgo, sorto subito dopo il secondo conflitto mondiale, costituito in origine da 10 Paesi e che oggi vanta 47 Stati aderenti, anche non europei o a cavallo tra Europa ed Asia (come la Federazione Russa, la Turchia, l'Azerbaijan, la Georgia e l'Armenia).

Unione europea

Unione europea e Consiglio d'Europa sono entità distinte ma che condividono i valori fondamentali. Spesso su questi temi la UE prende spunto da pertinenti iniziative del Consiglio d'Europa, come è accaduto per la Convenzione Europea dei Diritti Umani firmata anche dalla UE (oltre che dai singoli 28 Stati membri dell'Unione) oppure, in tema data protection, durante i lavori preparatori della direttiva 95/46/CE che presero spunto dalla convenzione 108 del 1981.

Convenzione 108, protocollo aggiuntivo 181 e Convenzione 108+

Già nell'Alert del 24 maggio 2018, cui si rinvia, si sono fornite informazioni in merito ai documenti internazionali in tema di data protection promossi dal Consiglio d'Europa. In sintesi, la Convenzione n.108 del 1981 è il trattato internazionale sul trattamento automatizzato dei dati personali – unico strumento internazionale vincolante in materia – successivamente integrato dal protocollo aggiuntivo ETS No. 181 del 2001, in cui fu prevista l'istituzione di autorità di controllo indipendenti con compiti di verifica e controllo dei trattamenti insieme alla nuova disciplina per i flussi transfrontalieri di dati. Infine, il 18 maggio 2018 il Comitato dei ministri del Consiglio d'Europa ha approvato il protocollo di aggiornamento della Convenzione n. 108 del 1981 (cosiddetto "108+") con cui si è provveduto ad integrare la Convenzione 108 con le nuove prescrizioni del GDPR, come riportato nell'Alert citato.

Firma e ratifica

Nei trattati si distingue tra firma e ratifica dello stesso. La **firma** è l'atto con cui uno Stato manifesta la propria intenzione di diventare parte del trattato. In generale, la firma precede la ratifica. La **ratifica** (detta anche "strumento di ratifica"), invece, documenta che uno Stato esprime il proprio assenso ad essere vincolato da un trattato, cioè si impegna formalmente a rispettare le prescrizioni del trattato. Lo strumento di ratifica viene emesso e firmato – a seconda delle procedure dei singoli Stati – dal capo dello Stato, dal capo del governo o dal ministro degli esteri.

Stati aderenti alla Convenzione 108

Attualmente sono 54 – inclusa l'Argentina – i Paesi che hanno firmato e ratificato la Convenzione 108; come si nota, un numero superiore rispetto a quello degli Stati membri del Consiglio d'Europa (47).

Stati firmatari della 108+

Attualmente sono 25 gli Stati firmatari della 108+, cioè quasi tutti gli Stati membri della UE – eccettuata l'Italia ma inclusa l'UK nonostante la "brexit" – oltre alla Federazione Russa e – tra i non membri del Consiglio d'Europa – l'Uruguay.
Di converso, nessuno di tali Stati ha finora provveduto alla ratifica.

Convenzione 108 ed Argentina

A partire dal 1 giugno 2019 la Convenzione 108 e la 181 entreranno in vigore relativamente all'Argentina, la quale si aggiungerà agli altri due Paesi del continente americano: Messico e Uruguay che vi hanno già provveduto in precedenza. Quindi, rispetto alla complessiva cornice data protection che ha la propria fonte nel Consiglio d'Europa, rimane fuori dalla ratifica dell'Argentina l'ultimo protocollo di aggiornamento della 108+.

Argentina nella white list dei paesi adeguati

Va ricordato, comunque, che l'Argentina attualmente fa parte della *white list* dei Paesi per i quali la Commissione UE ha emesso una propria decisione che ne attesta l'adeguatezza. Tramite il riconoscimento che i sistemi nazionali di protezione dei dati personali dei Paesi di tale elenco offrono garanzie equivalenti a quelle presenti nella UE, viene a trovare legittimazione il flusso estero di dati che parte dal territorio della UE ed ha come destinazione questi Paesi.

Correlazione tra white list UE e Convenzione 108

Come riportato nell'Alert citato, i lavori preparatori del GDPR e quelli per la modernizzazione della Convenzione 108 (108+) si sono svolti in parallelo con l'obiettivo di assicurare un approccio consistente in entrambi i sistemi normativi, tanto che il GDPR [Considerando (105)] riconosce che nel valutare l'adeguatezza del livello di protezione nei paesi terzi (ai fini della white list) «*si dovrebbe tenere in considerazione l'adesione dei paesi terzi alla convenzione del Consiglio d'Europa*» n.108 «*e relativo protocollo addizionale*».

10.
Valutazione prima della DPIA

Il GDPR chiede all'impresa di valutare. Il nuovo regime introdotto dal GDPR è basato sul rischio e questo approccio presuppone una costante capacità valutativa ad opera dell'azienda titolare del trattamento dei dati.
L'attenzione collettiva è stata attratta dall'istituzione della valutazione d'impatto (DPIA) ponendo in secondo piano la circostanza che quasi ogni regola del GDPR presuppone un processo valutativo del titolare, come dimostra la stessa determinazione del "rischio elevato", presupposto di obbligatorietà della DPIA.

Sintesi

Valutazione continua

In base alla riforma non è più sufficiente limitarsi a rispondere alle prescrizioni di legge ma occorre che l'azienda valuti preventivamente gli impatti che il proprio trattamento possa causare in termini di rischi per gli interessati.

Valutazione del rischio

L'obbligo gravante sui titolari del trattamento di realizzare la valutazione dei rischi data protection, costituisce:

- la declinazione del **principio di responsabilizzazione** del titolare del trattamento di dati personali, volto all'efficientamento dell'obbligo normativo e dei diritti degli interessati;
- una specificazione dell'**obbligo generale** di assicurare una **gestione adeguata dei rischi** connessi al trattamento di dati personali; la gestione dei rischi, costituisce l'insieme delle attività coordinate volte a indirizzare e controllare l'organizzazione in relazione ai rischi.

Rischio nel GDPR

Il "rischio" data protection può avere probabilità e gravità diverse, in relazione al contesto ed ambito applicativo, alla natura dei dati personali, alla finalità del trattamento.
Il rischio è la probabilità che il trattamento causi danni fisici, materiali o immateriali, alle persone cui si riferiscono i dati; ciò include la profilazione o il trattamento che potrebbe portare a discriminazione, furto d'identità, danno alla reputazione o inversione della pseudonimizzazione (cioè il passaggio da un'informazione codificata ad una resa nuovamente identificativa).

Bene soggetto a rischio GDPR

Il rischio per la protezione dei dati personali è in riferimento a "diritti e libertà" degli interessati, cioè riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione (come illustrato dalle Linee Guida wp248 rev.01).

Misure di contrasto ai rischi

Il Regolamento prevede che i titolari attuino **misure tecniche e organizzative** adeguate ed efficaci a garantire e ad essere in grado di dimostrare che il trattamento sia effettuato in conformità al GDPR.
L'**approccio** è applicato in via **scalare** in quanto la garanzia di adeguatezza ed efficacia delle misure di contrasto è commisurata alla probabilità e gravità del rischio e queste sono a loro volta «determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento» [Considerando (76)-(77) ed articoli 24 e 32].

Processo di valutazione dei rischi riferito ai trattamenti

La valutazione dei rischi sui diritti e le libertà degli interessati, conseguenti all'effettuazione di specifici trattamenti, si distingue in due principali tipologie:

1. La valutazione preliminare.
2. La **valutazione d'impatto** o DPIA.

Il processo di valutazione dei rischi relativi ai trattamenti si compone di distinte fasi che hanno l'obiettivo di identificare e minimizzare i rischi impattanti i diritti e le libertà fondamentali degli interessati, incoraggiando sistemi di protezione adeguati ed efficaci.

Valutazione prima della DPIA

Prima della DPIA occorre effettuare una precisa valutazione detta "preliminare". La valutazione viene detta "preliminare" per due motivi:

1. in quanto essa **precede la valutazione d'impatto**, la quale diventa obbligatoria solo se la valutazione precedente attesta la presenza di un rischio elevato nel trattamento considerato;
2. perché tale valutazione deve essere effettuata **prima che il trattamento sia realizzato**, in quanto il legislatore persegue l'obiettivo di utilizzare i dati personali in contesti a rischio contenuto.

Pertanto, il binomio valutazione preliminare / DPIA consente di:

1. individuare i trattamenti a potenziale rischio elevato;
2. mitigare il rischio "elevato" sino a soglie contenute.

Oggetto di valutazione preliminare e di DPIA

Si è detto che la valutazione preliminare precede ed è condizione essenziale della DPIA; nel senso che la DPIA può ritenersi obbligatoria solo se, in precedenza, il rischio connesso ad un determinato trattamento sia stato valutato (o si sarebbe dovuto valutare) di **livello elevato** per i diritti e le libertà degli interessati.

Insieme alla distinzione temporale, le due valutazioni si differenziano anche per il loro oggetto:

- La valutazione preliminare deve essere effettuata su tutti i trattamenti posti in essere dall'azienda-titolare (al fine di riscontrarne eventualmente il livello elevato del connesso rischio).
- La DPIA riguarda solo quei trattamenti già considerati a **probabile rischio elevato** (riscontrati mediante la valutazione preliminare); nei casi dubbi, tuttavia, le linee guida wp248 rev.01 raccomandano «*di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati*».

Metodologia delle due valutazioni

Sotto il profilo metodologico, è importante che la valutazione preliminare sia impostata in modo agevole in quanto essa deve essere in grado:

- di scansionare tutti i trattamenti, quindi essa deve poter intervenire anche su ampia scala;
- di completarsi in tempi ragionevolmente rapidi.

Il primo aspetto è di particolare importanza nella fase di messa a norma delle attività aziendali, il secondo assume rilevanza specie nell'attuazione del principio della protezione dei dati fin dalla progettazione ("**by design**").

Di converso, la DPIA deve seguire un metodo ed avere un contenuto minimo, entrambi specificati dalla norma, di maggiore complessità [art. 35(7)].

Prima fase della valutazione preliminare

L'attività di valutazione preliminare dei rischi presuppone una previa attività di raccolta delle informazioni rilevanti in relazione a ciascun trattamento, attività da svolgersi prima che inizino nuovi trattamenti e, per quanto riguarda i trattamenti in essere, da effettuarsi preliminarmente in caso di cambiamenti dei parametri inseriti.

È pertanto necessario verificare che i dati utilizzati per effettuare la valutazione preliminare siano aggiornati e coerenti rispetto alle informazioni censite all'interno del registro dei trattamenti.

Aggiornamento della valutazione

«*(I) titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*» (wp248 rev.01).

Una nuova valutazione del rischio, per i trattamenti già analizzati e risultati a rischio non elevato, va effettuata ogniqualvolta risultino circostanze idonee ad incidere sui criteri di rilevazione di cui alle Linee Guida wp248 rev.01; a titolo esemplificativo, come nel caso di mutamento del rischio conseguentemente all'adozione di nuove tecnologie oppure in caso di utilizzo dei dati personali per finalità differenti da quelle originarie.

"Elevato rischio"

Considerato che la constatazione della probabilità di un elevato rischio fa scattare l'obbligo di effettuare la DPIA, sorge il problema di stabilire **quando un rischio debba considerarsi "elevato"**.
In proposito vengono in aiuto sia il GDPR sia il WPArt29 con un proprio documento di linee guida, il wp248 rev.01 del 4 aprile 2017, come modificato e adottato da ultimo il 4 ottobre 2017.
Il GDPR interviene secondo due direttrici:

- fornendo una **lista di esempi** di trattamenti da considerarsi ad elevato rischio (art. 35.3);
- prevedendo che siano le autorità di controllo a rilasciare ***white list*** e ***black list***, cioè elenchi di trattamenti tipo che comportano rischi elevati ed elenchi di trattamenti per i quali si può escludere la presenza di rischi specifici.

In proposito si veda anche l'Editoriale del 19 ottobre 2017.

Esempi di "elevato rischio"

Tre sono gli esempi di trattamenti con elevato rischio citati nel GDPR:

1. una **valutazione sistematica e globale di aspetti personali** relativi a persone fisiche, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o analoghi su dette persone fisiche;
2. il trattamento, su larga scala, di dati sensibili o giudiziari; o
3. la **sorveglianza sistematica su larga scala** di una **zona accessibile al pubblico**.

Lista del Garante o "black list"

Il GDPR stabilisce che le ASN pubblichino liste di trattamenti tipici per i quali si ritiene probabile un "elevato rischio" ("**black list**") insieme ad elenchi di trattamenti riguardo ai quali si ritiene di poter escludere questa circostanza ("**white list**").
A fronte del parere espresso dall'EDPB sul progetto di elenco del Garante italiano (parere 12/2018 del 25/9/2018) quest'ultimo ne ha accolto i rilievi ed ha emesso il provvedimento n. 467 del 18/10/2018 [doc. web n. 9058979] con allegata la lista definitiva delle tipologie di trattamento a presumibile rischio elevato.
In proposito si veda anche l'Editoriale del 22 novembre 2018.

Criteri di determinazione dell'elevato rischio

In parallelo alla pubblicazione delle liste dei trattamenti a rischio elevato, le linee guida wp248 rev.01 indicano i criteri atti ad accertare la sussistenza di un rischio elevato. Si tratta di criteri di valutazione che vanno essi stessi giudicati con ponderazione, evitando applicazioni acritiche. In proposito si veda anche l'Editoriale del 22 febbraio 2018.
Nel tentativo di fornire dei principi orientativi, il gruppo di lavoro evidenzia che la concomitante presenza di due o più di tali criteri è sintomo di rischio elevato sebbene non possa escludersi che in determinate circostanze la presenza anche di uno solo di tali criteri possa rendere obbligatoria la DPIA.
Questa osservazione lascia ad intendere nuovamente che l'esercizio valutativo è comunque un compito proprio del titolare del trattamento.

11.
EDPB: l'ottava plenaria e prima panoramica dell'implementazione del GDPR

Il 12/13 marzo si è tenuta l'ottava sessione plenaria del Comitato europeo (EDPB). Gli argomenti trattati hanno riguardato l'ePrivacy sia in relazione all'interazione tra Direttiva ePrivacy e GDPR sia riguardo al futuro regolamento ePrivacy, nonchè in merito all'uso dei dati personali nel corso di campagne elettorali. In aggiunta, lo stesso EDPB ha rilasciato una panoramica sulla prima fase di attuazione del GDPR, con speciale riferimento alla cooperazione tra le autorità di supervisione nazionali ed il funzionamento del meccanismo di coerenza (art. 63, GDPR).

Interazione tra direttiva ePrivacy e GDPR

Nel proprio parere n. 5/2019 l'EDPB sottolinea che «*le autorità per la protezione dei dati sono competenti per controllare le operazioni di trattamento dei dati disciplinate dalle norme nazionali sulla ePrivacy solo se la legislazione nazionale conferisce tale competenza a tali autorità e tale controllo deve avvenire nell'ambito dei poteri di vigilanza assegnati all'autorità dalla legislazione nazionale che recepisce la direttiva ePrivacy*». D'altro canto, l'eventuale attrazione di un trattamento di dati personali nell'ambito di applicazione della direttiva ePrivacy, «*non limita la competenza delle autorità di protezione dei dati ai sensi del GDPR*».

Autorità competente in materia ePrivacy

Detto diversamente, se la questione rientra nell'ambito esclusivo della disciplina ePrivacy, le ASN sono competenti solo se tale competenza è prevista dalla normativa nazionale di recepimento della direttiva 2002/58/CE. Di converso, se un'operazione di trattamento di dati personali rientra anche nell'ambito ePrivacy, le ASN «*rimangono competenti per quanto riguarda le operazioni di trattamento effettuate su dati personali che non sono soggetti a una o più regole specifiche contenute nella direttiva e-privacy*», mentre «*le autorità designate come competenti ai sensi della direttiva ePrivacy dagli Stati membri sono le sole responsabili dell'applicazione delle disposizioni nazionali di recepimento della direttiva ePrivacy applicabili a quella specifica operazione di trattamento*».

Garante in materia ePrivacy

A tal riguardo occorre ricordare che, secondo la normativa italiana, le autorità competenti in materia ePrivacy sono il Garante e, per specifici ambiti, l'Autorità per le garanzie nelle comunicazioni (Parte II, Titolo X del codice privacy). Il Garante per la protezione dei dati ha la competenza di applicare direttamente le regole nazionali di ePrivacy in aggiunta al GDPR. Le norme ePrivacy contenute nel codice privacy sono soggette alle sanzioni amministrative (20 milioni o 4% del fatturato globale totale annuo) dettate dall'articolo 166, comma 2, del codice; il Garante è l'autorità competente all'irrogazione delle stesse (art. 166.3 del codice). Il futuro regolamento ePrivacy – ancora in corso di negoziazione – dovrebbe avvalorare questa impostazione della normativa italiana.

Dichiarazione sul futuro regolamento ePrivacy

La dichiarazione dell'EDPB invita i legislatori dell'UE (cioè Consiglio e Parlamento) di «*intensificare gli sforzi verso l'adozione del regolamento ePrivacy, che è essenziale per completare il quadro dell'UE per la protezione dei dati e la riservatezza delle comunicazioni elettroniche*»; considerate le discussioni in corso all'interno del Consiglio per l'adozione della posizione comune, l'EDPB invita a non «*abbassare il livello di protezione offerto dall'attuale direttiva ePrivacy*» in quanto il futuro regolamento «*dovrebbe integrare il GDPR fornendo ulteriori forti garanzie per tutti i tipi di comunicazioni elettroniche*».

Il regolamento ePrivacy si rende necessario sia per adeguare le prescrizioni normative allo sviluppo della tecnologia sia per includere nell'ambito applicativo della disciplina i servizi di comunicazione basati su IP (cosiddetti "Over-the-Top") che non sono attualmente coperti dalla direttiva 2002/58/CE; «*al fine di garantire che la riservatezza delle comunicazioni degli utenti finali sia protetta durante l'utilizzo di questi nuovi servizi e di creare condizioni di parità per i fornitori di servizi di comunicazione elettronica e servizi funzionalmente equivalenti*».

Segretezza delle comunicazioni

L'EDPB sottolinea che il diritto alla segretezza delle comunicazioni – riconosciuto dall'articolo 7 della Carta dei Diritti Fondamentali dell'Unione Europea (Charter) – «*deve essere applicato a tutte le comunicazioni elettroniche, indipendentemente dal modo in cui sono inviate, a riposo e in transito, dal mittente al destinatario e deve inoltre proteggere l'integrità delle apparecchiature terminali di ciascun utente*».

L'accumulazione e combinazione di contenuti o metadati delle comunicazioni elettroniche, «*può consentire di trarre conclusioni molto precise sulla vita privata delle persone che implicano rischi elevati per i loro diritti e le loro libertà*» da cui il supporto all'attuale approccio caratterizzato da «*ampi divieti, ristrette eccezioni*».

Consenso ePrivacy

L'EDPB ricorda che, già secondo la disciplina vigente, l'uso di dati di traffico – al di là di quanto necessario per la fornitura di un servizio di comunicazione elettronica – è soggetto all'obbligo di raccogliere il preventivo consenso dell'utente. Il "consenso ePrivacy" ha lo stesso significato del "consenso GDPR". In particolare, è necessario che il consenso sia libero e specifico. La libertà del consenso implica l'illegittimità di qualsiasi condizionamento. Allo stesso modo, il requisito della specificità del consenso ne presuppone l'obbligatorietà, indipendentemente dal fatto che l'utente abbia effettuato l'accesso.

Analogamente, il Comitato ritiene che l'eventuale necessità del trattamento di dati di traffico per l'esecuzione di un contratto non possa costituire un'ipotesi di esclusione del consenso, fatta salva la sola eccezione di esigenze di fatturazione.

Cookies wall

Il requisito della libertà del consenso fa ritenere vietato l'uso dei "**cookies wall**", vale a dire di quelle tecniche che impediscono agli utenti che non consentono, di accedere a un sito Web o a un servizio. Sulla illegittimità dei *cookies wall* è intervenuta in questi giorni l'ASN olandese con un proprio provvedimento.

Cookie e modalità di raccolta del consenso

Come noto, l'attuale disciplina sui cookie prescrive che il loro utilizzo richieda il preventivo consenso informato dell'utente, quando non si tratti di cookie necessari per il funzionamento del sito web (cosiddetti "cookie tecnici", v. art. 122, codice privacy).

L'articolo 10 della proposta di regolamento prevede che gli utenti abbiano il controllo sull'uso delle capacità di memorizzazione delle loro apparecchiature terminali. Il Parlamento UE – in base la principio della privacy per impostazione predefinita (by default) – ha introdotto specifiche condizioni in relazione alle impostazioni del software e per fornire una soluzione tecnica per i siti Web volta ad ottenere un valido consenso.

L'EDPB ritiene che tali prescrizioni dovrebbero «*applicarsi esplicitamente ai sistemi operativi di smartphone, tablet o qualsiasi altro "user agent", al fine di garantire che le applicazioni di comunicazione possano tenere conto delle scelte dei loro utenti, non importa quali sono i mezzi tecnici coinvolti. Le impostazioni sulla privacy dovrebbero facilitare l'espressione e la revoca del consenso in modo facile, vincolante e applicabile nei riguardi di tutte le parti e agli utenti dovrebbe essere offerta una scelta chiara al momento dell'installazione, consentendo loro di dare il proprio consenso se lo desiderano.*».

Uso di dati personali per campagne elettorali

Anche in considerazione dell'approssimarsi delle votazioni europee, l'EDPB ha rilasciato la dichiarazione 2/2019 in cui evidenzia una serie di punti chiave che devono essere presi in considerazione quando partiti politici e candidati elaborano i dati personali nel corso delle campagne elettorali.

Nel documento del Comitato si ribadisce in sintesi:

- I dati personali che rivelano opinioni politiche sono una **categoria speciale di dati** ai sensi del GDPR.
- I **dati personali** che sono stati **resi pubblici** o altrimenti condivisi dai singoli elettori, come ad esempio quelli presenti sui social media, sono comunque protetti dal GDPR.
- Gli elettori devono ricevere **adeguata informativa** circa l'uso dei propri dati.
- La **profilazione** connessa alla messaggistica di campagne mirate, in linea di principio, è lecita solo **con il consenso esplicito** dell'interessato.
- In caso di **campagna mirata**, gli elettori devono avere informazioni sul **perché** ricevono un messaggio particolare, chi ne è **responsabile** (cioè, il titolare) e come possono esercitare i loro **diritti** in quanto soggetti interessati.

Cooperazione tra le ASN

Contrariamente al passato, il GDPR ha creato un obbligo per le ASN di cooperare, al fine di fornire un'applicazione coerente del GDPR. Secondo l'EDPB (Rapporto EDPB LIBE sull'applicazione del GDPR) in questi nove mesi dalla piena applicazione del GDPR l'attività di cooperazione tra le ASN si è dimostrata molto positiva sebbene ciò abbia comportato un ulteriore carico lavorativo ed una maggiore incidenza sulle disponibilità finanziarie delle autorità.

Strumenti di cooperazione fra ASN

La cooperazione si attua nei casi che implicano una componente transfrontaliera avvalendosi dei seguenti strumenti:

- l'**assistenza reciproca (art. 61)**, la cui procedura consente a ciascuna ASN di chiedere informazioni ad altre ASN, ma anche di richiedere altre misure per una cooperazione efficace (quali autorizzazioni preventive, indagini, ecc.);
- le **operazioni congiunte (art. 62)**, tramite le quali le ASN di diversi Stati membri possono condurre indagini congiunte e misure congiunte di esecuzione;
- il **meccanismo di cooperazione dello "sportello unico" ("One-Stop-Shop", art. 56)**, che introduce l'intervento obbligatorio di un'autorità capofila per i casi transfrontalieri (cioè quando il titolare del trattamento o il responsabile del trattamento ha uno stabilimento in più di uno Stato membro o nei casi in cui l'attività di trattamento

dei dati impatta in modo sostanziale individui in più di uno Stato membro). Prima di avviare una procedura One-Stop-Shop per i casi transfrontalieri, è necessario identificare l'autorità che guiderà la cooperazione (ASN capofila) e le altre autorità di vigilanza interessate (ASN interessate). I criteri per l'individuazione dell'autorità capofila sono stati oggetto degli Editoriale del 6 luglio 2017 e del 20 luglio 2017, cui si rinvia.

Meccanismo di coerenza

Come ricordato nel documento citato, «*uno dei compiti principali dell'EDPB è garantire l'applicazione coerente del GDPR*»:

- fornendo «*orientamenti generali sull'interpretazione del GDPR, che contribuiranno a una comprensione e applicazione comuni delle disposizioni da parte delle parti interessate, delle autorità di vigilanza e del pubblico in generale*». In proposito, il Comitato ricorda che «*dal 25 maggio 2018, l'EDPB ha approvato 16 linee guida preparate dal Gruppo di lavoro articolo 29 (predecessore del Comitato) e ha adottato 5 linee guida aggiuntive*»;
- mediante l'adozione di opinioni (art. 64) e decisioni (art. 65) di coerenza. «*Queste decisioni riguardano principalmente le autorità nazionali di vigilanza e garantiscono una coerente applicazione e vincolatività del GDPR*».

12.
CGUE: l’avvocato generale su consenso e consenso cookie

Sono state pubblicate le conclusioni dell'avvocato generale Maciej Szpunar relative alla causa C-673/17 Planet49 GmbH c. Bundesverband con importanti passaggi sui requisiti di validità del consenso, ante e post GDPR, nonchè sulle caratteristiche del consenso per i cookie, sia in relazione all'attuale disciplina ePrivacy sia riguardo al GDPR. L'Editoriale odierno se ne occupa, considerato che i punti affrontati nel documento fanno chiarezza su alcuni snodi della disciplina sulla protezione dei dati personali che appaiono di non immediata lettura e che le conclusioni dell'avvocato generale sono normalmente fatte proprie dalla Corte di Giustizia della UE nella propria decisione finale.
In aggiunta, il documento contribuisce a precisare il quadro delle interazioni fra le due discipline del GDPR e dell'ePrivacy oggetto della recente dichiarazione dell'EDPB, di cui si è detto nello scorso Alert del 21 marzo 2019.

Sintesi

Dall'analisi delle conclusioni dell'avvocato generale nella causa C-673/17 Planet49 GmbH c. Bundesverband possono trarsi le seguenti indicazioni di sintesi:

- La **disciplina** cosiddetta **ePrivacy**, diversamente dal GDPR, **riguarda qualsiasi informazione** oggetto di comunicazioni elettroniche anche se **non** sono qualificabili come "dati personali".
- L'**informativa sui cookie**, oltre a soddisfare i requisiti di chiarezza, comprensibilità ed esaustività deve indicare la durata funzionale di ciascun cookie ed indicare il nominativo di terzi che possano eventualmente accedere alle informazioni in essi contenute.
- Il **consenso al trattamento** dei dati personali deve consistere in una **manifestazione attiva ed inequivocabile**, potendosi registrare una sostanziale continuità tra i due regimi della direttiva 95/46/CE e del successivo GDPR.
- **Identici requisiti** di validità riguardano il **consenso per il trattamento dei dati delle comunicazioni elettroniche**, anche se non necessariamente di natura "personale".
- Pertanto, la disciplina del **consenso in entrambi i contesti GDPR e ePrivacy risulta omogenea**.
- Il **consenso** dovendo essere libero **non può essere soggetto a condizioni**.
- Riguardo all'esecuzione di un contratto o alla prestazione di un servizio il **consenso non può essere richiesto come condizione per l'esecuzione o la fruizione**, salvo che esso risulti «*necessario all'esecuzione di tale contratto*».
- I **dati personali possono formare oggetto di una controprestazione** ("vendita"), in tal caso il consenso al loro utilizzo risulta "necessario" all'esecuzione del contratto e, quindi, sarà valido nonostante l'apparente "condizionamento".
- Allo stesso modo il **consenso per l'impianto dei cookie** può essere agganciato alla fruizione di un servizio web nel caso in cui i dati acquisiti tramite i cookie sono necessari per il servizio in questione (come nel caso in cui il servizio ha lo specifico scopo di acquisire dati "consensati").
- La disciplina **ePrivacy** prescrive il **consenso dell'utente o contraente prima che sia impiantato un cookie** nel dispositivo di quest'ultimo (o si acceda alle informazioni in esso registrate).

- Una **casella di spunta preselezionata** adoperata per la manifestazione di assenso **inibisce la libertà del consenso** rendendolo invalido in base ad entrambe le discipline del GDPR e ePrivacy.
- Il **consenso per i cookie richiesto contemporaneamente ad altre finalità** (ad esempio per la comunicazione dei dati a terzi a fini pubblicitari), **viola il requisito della specificità**, inibisce la libera e consapevole determinazione dell'interessato, per cui risulta altrettanto invalido.

Causa C-673/17

La causa C-673/17 è venuta alla fase delle conclusioni dell'avvocato generale. Essa riguarda una pronuncia pregiudiziale chiesta alla CGUE e proposta dalla Corte federale di giustizia della Germania (Bundesgerichtshof) per conoscere l'esatta interpretazione del diritto europeo in merito ai seguenti quesiti:

1. «*Quali informazioni debbano essere comunicate dal fornitore di servizi all'utente, affinché quest'ultimo sia informato, in termini chiari e completi*» in base alla disciplina ePrivacy. «*Se in tali informazioni rientrino altresì la durata della funzione dei cookie e il fatto che terzi abbiano accesso ai cookie stessi*».
2. Se il consenso può essere considerato valido in base alla disciplina ePrivacy se viene raccolto «*tramite una casella preselezionata che l'utente deve (de)selezionare per negare il suo consenso*».
3. Se ai fini del requisito del consenso, avuto riguardo al combinato tra disciplina ePrivacy e direttiva 95/46/CE «*la situazione differisca nel caso in cui le informazioni archiviate (mediante cookie, nda) o consultate consistano in dati personali*».
4. Se in presenza delle medesime circostanze, il consenso sia valido secondo il GDPR.

Fatti di causa

La vicenda ha riguardato la pratica messa in atto dalla società tedesca Planet49 la quale per raccogliere dati personali da poter "rivendere" a terzi a fini pubblicitari, invogliava gli utenti registrati a partecipare ad un gioco a premi a condizione che gli stessi utenti avessero acconsentito all'uso dei cookie di profilazione. A tale scopo, l'utente doveva immettere il proprio nome e l'indirizzo in un modulo riportato in una pagina del sito, in cui si trovavano due didascalie accompagnate da caselle di spunta.

Con la prima casella, l'utente autorizzava alla comunicazione dei propri dati personali a terzi a fini pubblicitari, mediante modalità di contatto tradizionali (es. posta) e automatizzate (es. email ed sms). «*La partecipazione al gioco a premi era possibile solo selezionando quantomeno la prima casella*».

Con la seconda casella, corredata di un segno di spunta preinserito, l'utente autorizzava all'impianto nel proprio dispositivo di cookie di profilazione sempre a fini pubblicitari. Di conseguenza, l'utente avrebbe dovuto deselezionare la casella per negare il proprio consenso; in aggiunta, questo consenso per i cookie non era prestato separatamente, bensì contemporaneamente alla conferma della partecipazione a un gioco a premi.

Tutela ePrivacy

La vicenda pone in evidenza le interazioni esistenti tra le due discipline

- della protezione dei dati personali – la quale trova la propria fonte giuridica, nella direttiva 95/46/CE e, successivamente, nel GDPR che l'ha sostituita;

- della privacy nelle comunicazioni elettroniche o ePrivacy, disciplinata dalle direttive 2002/58/CE e 2009/136/CE, recepite nel nostro ordinamento tramite il titolo X di Parte II del codice privacy (in attesa del prossimo regolamento UE, si vedano in tema gli Editoriali del 19 gennaio 2017, 2 febbraio 2017, 16 febbraio 2017 e 2 novembre 2017, nonchè gli Alert del 15 marzo 2018, 21 giugno 2018 e 21 marzo 2019).

Cookie

Come riportato nel documento in commento, «*(u)n cookie è un mezzo per raccogliere informazioni generate da un sito web e salvate da un browser di un utente Internet. Si tratta di un piccolo elemento di dati o file di testo, solitamente di dimensioni inferiori a un Kbyte, che un sito web chiede al browser di un utente Internet di memorizzare nel disco rigido locale del computer o del dispositivo mobile dell'utente*».
Si veda anche il tema "Cookie" nella sezione Argomenti del DPtel®.

Informativa propedeutica al consenso

Secondo la disciplina ePrivacy, il fornitore di servizi deve informare l'utente in modo chiaro e completo in merito al trattamento dei dati tramite i cookie, in particolare sulle ragioni del tracciamento dei suoi dati, ossia sugli scopi del trattamento.
«*L'obbligo di informare è legato al consenso, da intendersi nel senso che, perché possa esservi il consenso, deve esservi sempre prima l'informazione*».

Informativa per i cookie

L'avvocato generale evidenzia nella sue conclusioni come l'obbligo di informativa in relazione all'uso dei cookie vada interpretato in senso ampio, in quanto «*non ci si può attendere che l'utente medio di Internet possegga un elevato livello di conoscenza della funzione dei cookie*», «*a causa della complessità tecnica dei cookie, dell'asimmetria informativa tra fornitore e utente e, più in generale, della relativa mancanza di conoscenza da parte di qualsiasi utente medio di Internet*». Tramite l'informativa, «*l'utente dev'essere in grado di valutare gli effetti delle proprie azioni. Le informazioni fornite devono essere chiaramente comprensibili e non soggette ad ambiguità o interpretazione e devono essere sufficientemente dettagliate, in modo da consentire all'utente di comprendere il funzionamento dei cookie effettivamente impiegati*».

Indicazione della durata dei cookie

«*(L)a durata della funzione dei cookie costituisce un elemento del requisito del consenso informato (...) in materia di qualità e accessibilità delle informazioni agli utenti (...) (a)nche se il cookie* è essenziale. (...) Tali informazioni sono fondamentali per consentire agli interessati di adottare decisioni informate prima del trattamento». Come sostenuto anche dal governo italiano che ha presentato proprie osservazioni scritte, «*poiché i dati raccolti dai cookie devono essere eliminati quando essi non sono più necessari per conseguire lo scopo originario, ne deriva che il periodo di memorizzazione dei dati raccolti dev'essere chiaramente comunicato all'utente*».

Individuazione di terzi con accesso ai cookie

«*(A)ffinché l'informazione sia chiara e completa, un utente dev'essere esplicitamente informato quanto al fatto se i terzi abbiano accesso o meno all'installazione dei cookie. Qualora i terzi abbiano accesso, la loro identità dev'essere rivelata.*».

Consenso: requisiti di validità

Per la validità giuridica del consenso al trattamento di dati personali e di quello al trattamento di dati nelle comunicazioni elettroniche occorre che vengano rispettati determinati requisiti. Si veda anche la scheda di sintesi sul consenso in DPtel®.

Per la disciplina sui dati personali

Le regole in tema di consenso non sono sostanzialmente mutate dal passaggio di regime dalla direttiva 95/46/CE al GDPR. Anche l'avvocato generale fa rilevare che pur nella vigenza della direttiva il consenso doveva «*essere manifestato in maniera attiva*», in quanto la norma «*fa riferimento a una* ***manifestazione*** *della volontà della persona interessata, con cui evidentemente si indica un comportamento attivo*» [art.2, lett.h) della direttiva; nello stesso senso il WPArt29 nei pareri 2/2010, wp171 e 15/2011, wp187); in aggiunta, in tema di «*principi relativi alla legittimazione del trattamento dei dati (personali), (la stessa direttiva) stabilisce che la persona interessata ha manifestato il proprio consenso in maniera* ***inequivocabile***» [art. 7, lett.a) della direttiva]. L'inequivocabilità della manifestazione conduce inevitabilmente a supporre un comportamento attivo di assenso.

Altra condizione di validità è che il consenso sia "**specifico**" per una determinata finalità, cioè risulti separato da altre manifestazioni di assenso eventualmente richieste.

Il GDPR ribadisce e irrobustisce questi concetti stabilendo che «*il consenso dell'interessato (è) qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato*» (art. 4, p.11 GDPR) e pertanto «*richiede una manifestazione inequivocabile della volontà dell'interessato e un'azione positiva inequivocabile con cui si manifesta il proprio assenso*». Si veda anche il Considerando (32) che esclude che possa «*configurare consenso il silenzio, l'inattività o la preselezione di caselle*». Come rilevato anche dall'avvocato generale «*(i)l consenso attivo è ora, pertanto, espressamente previsto dal*» GDPR.

Per la disciplina sulle comunicazioni elettroniche

La direttiva 2009/136/CE che ha modificato la direttiva 2002/58/CE, ha imposto che «l'abbonato o l'utente in questione [dev'aver espresso] preliminarmente il proprio consenso», sostituendo, in tal modo, il sistema di opt-out [rifiuto] informato, previsto dalla direttiva 2002/58/CE e «*più facile da rispettare, con un sistema di opt-in [consenso] informato*».

«*(I) requisiti per il consenso non differiscono notevolmente per quanto riguarda i cookie e, più in generale il trattamento dei dati personali*» come sottolineato anche dal WPArt29 nei citati pareri 2/2010 sulla pubblicità comportamentale online, wp171 e 15/2011 sulla definizione di consenso, wp187.

Consenso cookie e consenso GDPR sono diversi?

La disciplina generale sulla protezione dei dati personali e quella sulla privacy nelle comunicazioni elettroniche sono distinte ma si integrano: quando ci si riferisce ai cookie o ad altre forme di tracciamento online, trova applicazione il regime ePrivacy che, in ogni caso, va interpretato secondo i principi del GDPR. Entrambi i regimi prevedono il consenso dell'interessato (GDPR) o dell'utente / contraente (ePrivacy) come requisito di legittimità del trattamento dei dati (personali o di traffico) e tale consenso presuppone i medesimi requisiti di validità giuridica nei due contesti.

Il consenso può essere soggetto a condizioni?

Il requisito della libertà del consenso (l'interessato manifesta l'intenzione "libera") non ammette che esso sia soggetto a condizionamenti tanto da limitarne la capacità di auto-determinazione.

Il consenso per l'uso di dati personali può essere condizionato all'esecuzione di un contratto?

Il Considerando (43) del GDPR specificamente riporta che il consenso si presume che non sia stato liberamente espresso «*qualora l'esecuzione di un contratto, compresa la prestazione di un servizio, sia subordinata al consenso sebbene esso non sia necessario per tale esecuzione*», in parallelo, nella parte normativa del regolamento, si legge che «*(n)el valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*» [art. 7(4) GDPR].

Riprendendo l'istituto giuridico del diritto tedesco sul consumo, l'avvocato generale fa rilevare come questa disposizione del GDPR introduca il «**divieto di pratiche di vendita aggregata**», che si verifica nell'ipotesi in cui la stipula di un contratto (nel caso, la partecipazione al gioco a premi), indebitamente incorpora in automatico la conclusione di altro contratto, distinto e funzionalmente non necessario (la prestazione del consenso all'utilizzo dei dati personali a fini pubblicitari). Sotto questo profilo, il divieto contenuto nel GDPR non appare assoluto, come risulta dall'espressione «*si tiene nella massima considerazione*» e dalla condizione che il consenso non sia «*necessario all'esecuzione del contratto*». L'espressione «*si tiene nella massima considerazione*» evidenzia che le eventuali casistiche di "vendita aggregata" vanno valutate con attenzione al fine di verificarne la legittimità; la condizione della "non necessità del consenso all'esecuzione del contratto" indica che l'ipotesi opposta di un consenso necessario per l'esecuzione del contratto rappresenta un'eccezione al "divieto di vendita aggregata". Sulla base di questa impostazione giuridica, l'avvocato generale sottolinea come a suo giudizio nel caso di specie lo scopo del gioco a premi è chiaramente quello dell'acquisizione di dati personali per finalità pubblicitarie, per cui il consenso dell'utente a tale utilizzo risulta "necessario" per la partecipazione al gioco. Di conseguenza, in questo caso vale l'eccezione e la subordinazione della partecipazione al gioco alla prestazione del consenso dell'utente all'utilizzo dei propri dati personali a fini pubblicitari non dovrebbe considerarsi una "vendita aggregata" illegittima («*In una tale situazione il trattamento di questi dati personali è, a miio avviso, necessario per la partecipazione al gioco a premi*»).

Il consenso può formare oggetto di una vendita di dati personali?

Argomentando ulteriormente sulla scia della tesi della eccezione del divieto di vendita aggregata nel caso di "subordinazione del consenso necessitata" dall'esecuzione del contratto, trova legittimazione l'ipotesi di fornitura di dati personali (quindi, del consenso al loro utilizzo per determinate finalità) come "merce di scambio". Ovviamente, anche in tale circostanza occorrerà prestare particolare attenzione all'adeguatezza dell'informativa, tale da permettere all'interessato di adottare decisioni informate prima del trattamento.

La fruizione di un servizio web può essere subordinato al consenso cookie?

Le conclusioni cui si è giunti sulla libertà del consenso per l'uso di dati personali e della legittima subordinazione del consenso all'esecuzione di un contratto o fornitura di un servizio solo a patto che il consenso risulti "necessario" per l'esecuzione del contratto stesso, valgono anche nel dominio ePrivacy e, in particolare, in relazione ai cookie.

Cioè la situazione non differisce nel caso in cui le informazioni memorizzate o consultate consistano in dati personali o meno. Già la Commissione aveva sottolineato, che la disciplina ePrivacy ha lo scopo di proteggere l'utente da qualsiasi interferenza con la sua sfera privata, indipendentemente dal fatto che si tratti di dati personali o di altro tipo [art. 5(3), direttiva 2002/58]. Sul punto si vedano anche i pareri del WPArt29 2/2010 sulla pubblicità comportamentale, wp171, 2/2013 sulle applicazioni per dispositivi intelligenti, wp202 nonchè i considerando (24) e (25) della direttiva 2002/58/CE, secondo cui

«*(l)'accesso al contenuto di un sito Internet specifico può tuttavia continuare ad essere subordinato all'accettazione in conoscenza di causa di un marcatore o di un dispositivo analogo, se utilizzato per scopi legittimi*».

Quando occorre il consenso per i cookie?

Per la disciplina ePrivacy l'impianto di un cookie nel dispositivo dell'utente oppure l'accesso alle informazioni già archiviate nel browser dell'utente sono legittimi solo mediante un preventivo consenso **informato** dell'utente o contraente.

Fa eccezione a questa regola generale:

1. il caso in cui la memorizzazione o l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un utente sono realizzati al solo fine di effettuare la trasmissione di una comunicazione su una rete di comunicazione elettronica;
2. qualora la memorizzazione o l'accesso siano strettamente necessari per fornire all'utente un servizio della società dell'informazione esplicitamente richiesto da parte sua [art. 5(3), seconda frase, direttiva 2002/58].

Distinzione tra consenso, rifiuto e opposizione

Fermo restando che il consenso costituisce il requisito di legittimità dell'impianto di un cookie nel dispositivo dell'utente oppure per l'accesso alle informazioni già archiviate nel browser dell'utente, la direttiva 2002/58/CE prescrive anche che al contraente e all'utente debitamente informati debba essere «*offerta la possibilità di rifiutare tale trattamento da parte del titolare del trattamento*» [art.5(3), direttiva 2002/58/CE). Quindi, il diritto al rifiuto è aggiuntivo al consenso preventivo e non si sostituisce ad esso; analogamente, il diritto di opposizione consiste nel diritto dell'utente di revocare il consenso già prestato oppure di opporsi all'uso di un cookie che in origine non necessitava di consenso.

Operativamente – ad esempio – questo scenario si traduce (secondo il provvedimento generale del Garante del 2014, doc. web n. 3118884) in quanto segue:

- l'**obbligo di informativa** si scompone;
  - (a) in una prima informativa semplificata contenuta in un banner pubblicato sulla pagina di atterraggio del sito;
  - (b) una seconda informativa estesa contenuta nella cookie policy raggiungibile da qualsiasi pagina del sito tramite un collegamento ipertesto.

- il **consenso** viene raccolto inizialmente in maniera semplificata tramite un elemento di discontinuità, dopo la comparsa del banner, rappresentato dalla continuazione della navigazione nel sito o da qualsiasi altra azione dell'utente diversa dall'abbandonare il sito stesso;
- il **diritto al rifiuto** consiste appunto nell'abbandonare il sito oppure nel configurare le impostazioni del proprio browser in modo da non consentire l'impianto di tutti o di alcuni tipi di cookie sebbene, come sottolineato dall'avvocato generale, «*talune prove empiriche dimostrano in modo inconfutabile che le persone modificano raramente le impostazioni predefinite, dando vita a un fenomeno definito "default inertia"*»;
- il **diritto di opposizione** si soddisfa consentendo all'utente di accedere ad una specifica area del sito web dove poter modificare le proprie scelte in questo ambito, in modo articolato.

Una casella di spunta preselezionata è valida per il consenso?

A. Secondo la direttiva 95/46/CE?

Anche se non menzionata in modo esplicito nel testo della direttiva 95/46/CE, la modalità di raccolta del consenso tramite una casella di spunta preselezionata è stata generalmente considerata illegittima in quanto in contrasto col requisito del "consenso libero e informato". Come evidenziato dall'avvocato generale e riportato sopra, «*non è sufficiente, a tal proposito, che la dichiarazione del consenso dell'utente sia pre-formulata e che l'utente debba opporsi attivamente qualora non acconsentisse al trattamento dei dati. Infatti, in quest'ultima situazione, non è noto se tale testo pre-formulato sia stato letto e compreso. La situazione non* è *inequivocabile. Un utente può aver letto o meno il testo; può non averlo fatto per pura negligenza. In una simile circostanza, non è possibile stabilire se il consenso sia stato espresso liberamente.*».

B. Secondo il GDPR?

Come riportato in precedenza, il GDPR ha tolto ogni dubbio (in realtà, esigui) sui requisiti di validità del consenso affermando che «*il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano. (...) Non dovrebbe pertanto configurare consenso il silenzio, l'inattività o* ***la preselezione di caselle***» [Considerando (32), GDPR, enfasi aggiunta].

C. Secondo la disciplina ePrivacy?

Come indicato sopra, le conclusioni cui si perviene su questo fronte riguardo alla disciplina sulla protezione dei dati personali sono estensibili anche all'ambito ePrivacy in quanto «*i requisiti per il consenso non differiscono notevolmente per quanto riguarda i cookie e, più in generale il trattamento dei dati personali*».

Il consenso cookie richiesto contemporaneamente ad altre finalità, è valido?

Infine, il requisito della specificità del consenso – che accomuna entrambe le discipline sulla protezione dei dati personali ed ePrivacy, richiede che il consenso, se dovuto, si riferisca a ciascuna finalità del trattamento, in modo separato; si tratta di una diretta conseguenza del requisito della libertà del consenso in quanto l'autodeterminazione dell'interessato può estrinsecarsi nella sua pienezza, solo a patto che questi possa decidere in modo differenziato. Ne consegue che il consenso per l'impianto di cookie o per l'accesso alle informazioni archiviate nel dispositivo

dell'utente non può essere "accorpato" al consenso per altre finalità, ad esempio formando parte dello stesso atto oppure utilizzando il medesimo pulsante o casella di spunta per manifestare entrambi i consensi.

13.
Passi avanti per la certificazione GDPR

La certificazione GDPR costituisce un importante strumento volontario (*soft law*) per dimostrare il livello di responsabilizzazione (*accountability*) di un titolare o di un responsabile del trattamento. Di recente, alcuni passaggi hanno evidenziato come il complesso processo che porta alla certificazione GDPR abbia compiuto significativi passi avanti. Queste notizie fanno ben sperare che, in tempi prevedibilmente ragionevoli, l'armamentario della compliance GDPR possa arricchirsi di un nuovo importante strumento di ausilio: la certificazione ai sensi dell'articolo 42 del regolamento.
In questo contesto, andrebbe distinto tra:

- certificazioni "in tema GDPR" e;
- certificazioni "ai sensi del GDPR".

Certificazioni "in tema GDPR"

Negli ultimi tempi il mercato ha proposto molte offerte "in tema di GDPR", più o meno attendibili. Si tratta di iniziative per lo più legittime che hanno lo scopo di applicare esistenti schemi di certificazione a specifici aspetti o prescrizioni del regolamento al fine di poter verificare (e certificare) il relativo livello di maturità raggiunto, nell'ambito di riferimento, dall'azienda che assume il ruolo di titolare o responsabile del trattamento. Si tratta di un attestato di maturità riferito ad un processo individuato piuttosto che una verifica di conformità normativa.
Con queste certificazioni "in tema GDPR" questo livello di maturità riscontrato nell'azienda certificata viene pur sempre attestato da un ente di certificazione accreditato dall'Organismo unico di accreditamento (Accredia, per l'Italia); il processo considerato – com'è tipico della metodologia di certificazione – svolge la funzione di una valutazione operata da una terza parte indipendente (ente di certificazione) secondo criteri standard ed oggettivi (schema di certificazione). In questo ambito riferito al GDPR "per relazione", tuttavia, non vi è nessuna certezza giuridica che i criteri adottati ed il processo di accertamento e valutazione possano risultare pienamente conformi ed esaustivi, rispetto al dettato normativo.
Le **certificazioni "in tema GDPR"** sono fuori dall'ambito applicativo degli articoli 42 e 43 GDPR che disciplinano la **certificazione "ai sensi del GDPR";** le prime possono attestare competenze o attendibilità su determinati profili oggetto della certificazione, i quali risultano di ausilio alla conformità GDPR; di converso, gli stessi attestati non possono invece certificare la conformità "ai sensi del GDPR" (cioè dei menzionati articoli 42 e 43).
In queste circostanze, a loro volta, gli enti di certificazione ufficialmente accreditati da Accredia per il rilascio di certificazioni in base a determinati schemi applicabili in via generale (cioè, non specificamente al GDPR) provvedono a verificare e certificare se determinati ambiti operativi posti in essere da aziende rispondenti ai dettami del GDPR, o ruoli soggettivi, soddisfano i requisiti dei citati schemi.

Esempi delle certificazioni per DPO

Un esempio di certificazione "in tema GDPR" sono quelle attualmente proposte riguardo ai nuovi profili professionali data protection, spesso basate sulla norma UNI 11697:2017 "Attività professionali non regolamentate – Profili professionali relativi al trattamento e alla protezione dei dati personali", la quale sebbene indirizzi anche la figura del DPO, non trova tuttavia base giuridica nel GDPR, né tanto meno nei citati articoli 42 e 43 sulla certificazione "ai sensi del GDPR" che, invece, si basa sulla norma UNI CEI EN ISO/IEC 17065:2012.

Certificazioni "ai sensi del GDPR"

Le certificazioni "ai sensi del GDPR", diversamente dalle altre sopra citate, sono finalizzate a «*dimostrare la conformità al presente regolamento dei trattamenti effettuati dai*» titolari e responsabili del trattamento e sono solo quelle conformi agli articoli 42 e 43 del regolamento.
Queste due disposizioni stabiliscono principalmente:

- La competenza di entrambi Accredia e Garante, per le attività di accreditamento degli enti di certificazione in base alla norma UNI CEI EN ISO/IEC 17065:2012.
- La competenza del Garante o dell'EDPB per l'approvazione
  - dei **requisiti di accreditamento** [art. 43(3)] e;
  - dei **criteri per la certificazione** [art. 42(5)].

Competenza, requisiti e criteri

Quanto alla **competenza** per l'accreditamento degli enti di certificazione e l'approvazione degli schemi "ai sensi del GDPR", l'articolo 2-septiesdecies del codice privacy riconosce una primazia di Accredia e l'intervento surrogatorio del Garante, solo in caso di grave inadempimento dei compiti da parte di Accredia stessa.
Riguardo alle condizioni per le certificazioni, il GDPR richiede il rispetto di

- **requisiti di accreditamento specifici ed aggiuntivi** a quelli determinati dal regolamento UE 765/2008, i quali devono essere approvati (anzichè individuati) dall'ASN o dall'EDPB [**art. 43(3), GDPR**];
- **criteri di certificazione specifici ed aggiuntivi** a quelli della norma UNI CEI EN ISO/IEC 17065:2012, i quali devono essere approvati (anzichè individuati) dall'ASN o dall'EDPB [**art. 42(5), GDPR**].

Allegato 2 a Linee guida 1/2018 di EDPB

In merito alla valutazione per l'approvazione dei criteri di certificazione, l'EDPB ha emesso le linee guida 1/2018 ed il relativo Allegato 2, sottoposto a consultazione pubblica, di cui sono appena scaduti i termini. L'allegato identifica gli argomenti che un'ASN e l'EDPB prenderanno in considerazione e applicheranno ai fini dell'approvazione dei requisiti di un meccanismo di certificazione. Gli aspetti considerati nell'allegato andrebbero tenuti in considerazione dagli organismi di certificazione e dai proprietari di schemi che desiderano redigere e presentare tali requisiti aggiuntivi per l'approvazione, motivandone adeguatamente l'eventuale mancata copertura.

Convenzione Garante – Accredia

Garante ed Accredia hanno stipulato una convenzione di cooperazione il 20 marzo 2019 mediante la quale «*Accredia comunicherà all'Autorità gli accreditamenti rilasciati, i ricorsi degli Organismi accreditati e le decisioni assunte, le scadenze dei certificati, i provvedimenti sanzionatori, l'elenco delle certificazioni e le relative revoche e sospensioni rilasciate dagli Organismi. Il Garante comunicherà ad Accredia gli aggiornamenti della normativa, le novità sugli schemi di certificazione approvati a livello nazionale ed europeo, nonché le informazioni su problematiche che potrebbero emergere da reclami pervenuti all'Autorità. La Convenzione ha la durata di un anno con tacito rinnovo per un ulteriore anno.*»

Pubblicazione sui "Meccanismi di certificazione data protection"

Su commissione del Direttorato generale per la Giustizia e i Consumatori della Commissione UE, è stato pubblicato nel marzo 2019, il rapporto finale su "Meccanismi di certificazione Data Protection – Studio sugli articoli 42 e 43 del Regolamento (UE) 2016/679".

Il Rapporto evidenzia come, «*nonostante la novità dei meccanismi di protezione dei dati del GDPR, si possono trarre insegnamenti preziosi dall'analisi delle certificazioni esistenti: metodologie di valutazione, accordi contrattuali e auditor*». Per questo, la pubblicazione evidenzia che «*le autorità di vigilanza dovranno utilizzare tutta la guida e la conoscenza di altri campi e, in particolare, gli standard tecnici per valutare i criteri di certificazione nel campo del data protection*» e che «*si dovrebbe guardare alle certificazioni esistenti per identificare le migliori pratiche*».

In aggiunta, il rapporto avverte che «*interrogativi derivano dall'eventuale adozione di diversi modelli di accreditamento negli Stati membri relativi al riconoscimento delle certificazioni negli Stati membri, all'armonizzazione delle tecniche di controllo, alla valutazione fra enti omogenei, allo slittamento di funzioni*». «*Esiste una mancanza strutturale di conoscenza nel mercato per quanto riguarda la disponibilità di norme tecniche pertinenti nel contesto della protezione dei dati*» e «*le parti interessate rilevanti (associazioni industriali, PMI e grandi imprese) sembrano favorire gli standard europei e internazionali rispetto a quelli nazionali*».

14.
Sanzione dell'ICO per e-mail marketing

La Gran Bretagna della brexit non è destinata ad allontanarsi dalla UE sotto il profilo della disciplina data protection, nemmeno quando il paese uscirà dall'Unione. Un recente provvedimento sanzionatorio inflitto dall'autorità di supervisione inglese (ICO - Information Commissioner's Office) ci consente di ritornare sulla disciplina ePrivacy e, nello specifico, sulla corretta gestione delle comunicazioni commerciali per posta elettronica, su cui si continua a registrare molta confusione sul mercato.

Sintesi

La sanzione di 40.000 sterline ha riguardato una società inglese che si è rivolta ad una terza parte fornitrice di servizi di generazione di contatti di potenziali clienti (lead generation) per inviare circa 2 milioni di e-mail di natura promozionale nell'arco di un anno. L'azienda committente aveva lanciato questa campagna nella convinzione che gli indirizzi e-mail utilizzati fossero consensati a fini marketing e che il consenso rilasciato coprisse anche il suo trattamento, ma l'ICO è stato di diverso avviso ed ha inflitto la sanzione menzionata.

La vicenda costituisce un importante precedente riguardo ai limiti della legittimità dei dati ottenuti da list broker per l'uso a fini commerciali e, con non poca sorpresa, evidenzia un'interpretazione giuridica dell'autorità inglese, che sembrerebbe più restrittiva di quella adottata in proposito dal Garante italiano.

Disciplina dell'e-mail marketing

Sulle regole in materia di marketing elettronico si veda quanto riportato nel DPtel® alla voce Direct Marketing.

La disciplina dell'uso degli indirizzi e-mail per l'invio di comunicazioni commerciali non ha subìto variazioni con l'avvento del GDPR in quanto le fonti normative continuano ad essere le direttive ePrivacy 2002/58/CE e 2009/136/CE. In futuro, tali direttive saranno sostituite dal regolamento ePrivacy che attualmente è ancora in discussione presso il Consiglio europeo, come già indicato in precedenti commenti.

L'utilizzo di posta elettronica per finalità di marketing richiede il consenso preventivo dei destinatari (che in ottica privacy rivestono il ruolo di interessati) (artt. 6 GDPR e 130, comma 2, del codice).

Ipotesi del "soft opt-in"

Eccezione al consenso preventivo degli interessati per l'e-mail marketing è rappresentata dalla condizione del cosiddetto "soft opt-in" – previsto dal comma 4, dello stesso articolo 130 (v. anche Provv. gen. 29 maggio 2003 sullo spamming confermato da "Linee guida in materia di attività promozionale e contrasto allo spam – 4 luglio 2013" (doc. web n. 2542348) par. 6.1). Per potersi avvalere di tale deroga occorre che siano soddisfatte alcune condizioni:

1. l'utente deve essere un cliente del titolare del trattamento (anziché un mero consumatore);
2. il cliente deve aver rilasciato il proprio indirizzo e-mail nel corso di una transazione commerciale;
3. all'atto del rilascio dell'indirizzo e-mail il cliente deve essere stato adeguatamente informato sulla possibilità d'uso dell'e-mail per promuovere prodotti o servizi analoghi e del diritto di opporsi in qualsiasi momento;

4. ad ogni successiva comunicazione elettronica si deve ricordare al cliente il diritto di opporsi (il cosiddetto "unsubscribe", in ambito elettronico) e consentirgli agevolmente di farlo.

Trattandosi di una previsione che trova anch'essa la propria fonte normativa nella direttiva ePrivacy, essa è presente nelle leggi nazionali di attuazione dei singoli Stati membri dell'Unione, tra cui anche la Gran Bretagna.

Fatto

Una società inglese ("Grove"), interessata a promuovere nuova clientela, si rivolge ad un fornitore di indirizzi e-mail da poter utilizzare, anche da parte di terzi, per finalità di marketing. Per rendere legittima la propria attività di list broker, infatti, il fornitore ha raccolto il consenso degli interessati (tramite propri siti web) anche per l'uso degli stessi indirizzi, sempre a fini marketing, da parte di terze parti ai quali il fornitore intende fornire le liste dietro corrispettivo. Nell'informativa rilasciata agli interessati, il fornitore specifica questa circostanza e rinvia l'interessato ad ulteriori liste identificative delle categorie merceologiche di appartenenza delle terze parti, potenziali cessionarie delle liste. L'identificazione avviene, quindi, a livello categoriale e non nominativo, in quanto Grove non viene mai citata come possibile acquirente delle liste. Confidando nella legittimità dell'uso a fini marketing di tali indirizzari, anche avvalorata da un paio di consulenze richieste in proposito, Grove effettua tramite intermediari circa due milioni di trasmissioni commerciali via email nel corso di un intero anno.

Condizioni per la validità del consenso "indiretto"

Come già riportato nelle proprie linee guida sul Direct Marketing, l'ICO ha ritenuto che quando un soggetto comunica ad un'organizzazione di acconsentire a ricevere promozioni commerciali da parte di terzi (il cosiddetto "consenso indiretto") e tali comunicazioni avvengono con canali automatizzati o elettronici (cioè, via sms, e-mail, chiamate senza operatore e simili) occorre che tali terzi siano individuati in via specifica e non solo per categoria merceologica; «*ciò perchè le regole sul marketing elettronico sono più stringenti, per rispondere alla natura maggiormente invasiva dei messaggi elettronici*».

Verifica della validità del consenso

Quando si acquistano liste di indirizzari per finalità di marketing da fornitori esterni, spesso l'azienda acquirente si limita a (o si accontenta di) richiedere a quest'ultimo un'attestazione confermativa che le citate liste siano validamente consensate per le finalità cui sono destinate. Come giustamente fatto rilevare dall'ICO, spetta in ogni caso al titolare del trattamento (quindi, all'azienda cliente) assicurarsi che la propria attività sia conforme alla disciplina sulla protezione dei dati e sull'ePrivacy e, pertanto, che sia stato effettivamente acquisito un valido consenso per l'invio di tali messaggi commerciali. In sostanza, si tratta di una "due diligence" preliminare che il titolare non può avocare a terzi, siano essi lo stesso fornitore, intermediari o eventualmente consulenti incaricati ad hoc; come di fatto è successo nel caso in esame, avendo Grove richiesto a due consulenti, preliminarmente al lancio della propria campagna, di verificare la legittimità del consenso acquisito dal list broker.

Inapplicabilità del "soft opt-in"

Nel caso in cui il consenso acquisito dal list broker risultasse non estendibile alla comunicazione commerciale del terzo, quest'ultimo non potrebbe nemmeno avvalersi dell'eccezione del "soft opt-in", in quanto il terzo acquirente delle liste di indirizzari normalmente non ha una relazione pregressa con gli utenti che ricevono il messaggio promozionale per i suoi prodotti. Come anticipato, infatti, l'eccezione del "soft opt-in" «*può essere invocata solo dall'organizzazione che ha raccolto i dettagli del contatto*» (sussistendone le ulteriori condizioni).

Condizioni del consenso "informato"

Dopo aver ribadito le consuete indicazioni affinchè il consenso possa ritenersi valido, in quanto informato (informazione concisa, trasparente, intelligibile e facilmente accessibile: v. art. 12(1) GDPR), l'authority inglese evidenzia che «*(i)l problema chiave è ciò che viene detto all'utente al momento del consenso*» per cui «*il consenso indiretto può essere valido ma solo se è sufficientemente chiaro e specifico, il riferimento alle "terze parti in genere" non sarà sufficiente per dimostrare un valido consenso.*».

Individuazione dei terzi

Di conseguenza, nelle situazioni come quella qui rappresentata «*(i)l consenso non sarà valido se agli individui viene chiesto di accettare di ricevere marketing da "organizzazioni simili", "partner", "terze parti selezionate" o altra analoga descrizione generica*». Nel caso specifico, l'authority rileva che «*le politiche sulla privacy elencano una vasta gamma di settori dai quali gli utenti possono ricevere marketing, e inoltre non riescono a fornire agli stessi la possibilità di specificare i tipi di promozioni che vorrebbero ricevere*», con ciò facendo intuire che il vizio non riguarderebbe solo il profilo informativo volto ad ottenere un assenso informato, ma anche in relazione ad un difetto di discernimento a danno di un consenso consapevole.
Quindi, occorre che i terzi vengano individuati in modo specifico, per nome «*o identificati in modo tale da suggerire che potrebbero legittimamente istigare il marketing diretto ai contraenti/utenti*».

Posizione del Garante italiano

Su questo specifico profilo della modalità di individuazione dei terzi promotori, al fine di poter considerare l'originario consenso validamente estendibile ai terzi sino a coprire la legittimità delle loro comunicazioni commerciali, sembra di cogliere qualche differenza di approccio rispetto all'impostazione seguita dal Garante italiano.
Nel provvedimento generale "Consenso al trattamento dei dati personali per finalità di "marketing diretto" attraverso strumenti tradizionali e automatizzati di contatto" del 15 maggio 2013 (doc. web n. 2543820) ed ancor più nel documento "Linee guida in materia di attività promozionale e contrasto allo spam" del luglio 2013 (doc. web n. 2542348), par. 2.6.3, il nostro Garante già allora evidenziava che «*i titolari del trattamento, mediante moduli contrattuali cartacei o appositi form on-line, raccolgono un generico consenso al trattamento per le finalità promozionali proprie e di soggetti terzi ai quali comunicano (e/o talvolta cedono) i dati personali raccolti, senza individuare tali soggetti né nell'informativa né nella formula di acquisizione del consenso e senza indicarne la categoria economica o merceologica di riferimento*».
Questo fenomeno riveste importanza anche all'interno di un medesimo gruppo aziendale cioè nella «*particolare ipotesi in cui il soggetto terzo – a cui viene fatta la comunicazione dei dati raccolti per finalità di marketing – sia una società controllata, controllante, o comunque a vario titolo collegata con il soggetto che ha raccolto i dati personali degli interessati*».

Riferimento alle categorie economiche o merceologiche

In quella occasione, dopo aver confermato l'illegittimità della «*acquisizione di un unico e generico consenso da parte degli interessati per siffatta finalità*», l'autorità italiana ribadiva la necessità di «*rilasciare ai medesimi (utenti) un´idonea informativa, (...), che individui, oltre agli altri elementi indicati nella norma, anche ciascuno dei terzi o,* ***in alternativa, indichi le categorie (economiche o merceologiche) di appartenenza degli stessi (ad esempio: "finanza", editoria", "abbigliamento"*** *(...)*» (enfasi aggiunta). «*Peraltro,* ***nel caso in cui i terzi siano stati individuati singolarmente*** *e siano stati forniti all´interessato anche gli altri elementi (...) relativi al trattamento che verrà da questi svolto, non sarà necessario che i predetti soggetti rilascino agli interessati un´*ulteriore informativa in quanto (...) l´informativa "può non comprendere gli elementi già noti alla persona che fornisce i dati"» [come oggi richiamato dagli articoli 13(4) e 14(5)(a) del GDPR].

«***Laddove invece la richiesta di consenso non sia accompagnata da un´informativa con tali requisiti****, i terzi (...) potranno inviare ai medesimi interessati le comunicazioni promozionali in questione solo dopo il rilascio di una propria informativa*» (enfasi aggiunte). Quest'ultima frase faceva intendere che qualora l'informativa avesse fatto riferimento ai terzi, indicandoli solo in base alle categorie economiche o merceologiche di appartenenza, la mancata indicazione nominativa degli stessi non avrebbe inficiato il consenso, rendendo necessaria la sola riproposizione dell'informativa da parte del medesimo terzo.

Conclusioni sull'interpretazione dell'ICO

Risulta evidente che se l'interpretazione dell'ICO qui commentata dovesse essere condivisa anche dalle altre ASN, il business delle liste di contatti a fini promozionali subirebbe un notevole impatto, soprattutto per le attività di marketing automatizzato (cioè, comunicazioni commerciali via telefono senza operatore, sms, mms, e-mail e simili). Difatti, risulterà particolarmente difficile per il list broker, all'atto della raccolta dei dati di contatto, riuscire ad individuare adeguatamente i terzi ai quali questi stessi potrebbero essere comunicati o ceduti per le medesime finalità, dandone contezza nell'informativa all'utente. Seguendo questa impostazione, è prevedibile che l'ambito di commercializzazione dei dati raccolti venga a restringersi significativamente, limitandosi ai già clienti ed a qualche potenziale.

Rosario Imperiali @Ros_Imperiali

15.
Nona sessione plenaria dell'EDPB

La nona sessione plenaria dell' EDPB si è tenuta il 9 e 10 aprile 2019 affrontando alcuni temi di rilievo come il rilascio definitivo delle linee guida n.1/2018 sulla certificazione nonché le linee guida riguardo alla portata e all'applicazione della base giuridica dell'esecuzione di obblighi contrattuali [articolo 6(1)(b), GDPR] nel contesto dei servizi della società dell'informazione.

Linee guida sulla base giuridica dell'esecuzione di obblighi contrattuali

Secondo il comunicato stampa rilasciato dal Comitato (il documento, infatti, all'atto della redazione di questo Alert non è ancora disponibile, in attesa dei preliminari «*controlli legali, linguistici e di formattazione*»), queste linee guida contengono «*osservazioni generali riguardanti i principi di protezione dei dati e l'interazione dell'articolo 6 (1) (b) con altre basi legali. Inoltre, le linee guida contengono indicazioni sull'applicabilità dell'articolo 6 (1) (b) in caso di raggruppamento di servizi separati e di risoluzione del contratto*».

Si ricorda che l'articolo 6(1)(b) indica una delle basi giuridiche che rendono legittimo il trattamento di dati personali (nè sensibili nè giudiziari) quando: «*b) il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso*».

Queste linee guida formeranno oggetto di un nostro approfondimento non appena il documento sarà reso disponibile.

Linee guida 1/2018 sulla certificazione

Nel corso della nona riunione plenaria, l'EDPB ha approvato le linee guida 1/2018 sulla certificazione, in versione definitiva. Per un'analisi generale sul tema, si rinvia a quanto già indicato nei precedenti Editoriali del 14 giugno 2018 e del 28 giugno 2018; le considerazioni contenute negli Editoriali citati rimangono tuttora attuali. In questa sede seguiremo un approccio di sintesi per una migliore comprensione di questo tema complesso e ad alto contenuto tecnico. In questo senso, affronteremo i seguenti profili:

- Forme d'uso delle linee guida 1/2018.
- Chi accredita e chi certifica.
- Tempi di durata.
- Possibili ruoli dell'ASN nel rilascio delle certificazioni GDPR.
- Ruolo dell'ASN riguardo ai meccanismi di certificazione GDPR.
- Influenza dei meccanismi di certificazione.
- Distinzioni tra requisiti e criteri.
- Oggetto della certificazione GDPR.

Antefatti

Le linee guida 1/2018 prendono spunto dal documento wp261 elaborato dal WPArt29 prima della costituzione dell'EDPB e mai venuto alla luce in versione finale. Dal suo canto, in una delle sue prime uscite ufficiali, il 25 maggio 2018 l'EDPB ha adottato una prima versione delle linee guida 1/2018 che integravano il precedente wp261. All'esito dei risultati avuti a seguito della procedura di consultazione pubblica tenutasi tra maggio e luglio 2018, l'EDPB ha infine adottato una versione finale il 23 gennaio 2019, con una correzione intervenuta il 9 aprile 2019; il testo finale rappresenta il documento qui in esame.

Struttura delle linee guida 1/2018

Analogamente alla versione originaria, il documento passa in rassegna le finalità ed i concetti chiave relativi al tema della certificazione – come prevista dagli articoli 42 e 43 del GDPR – precisando il ruolo delle autorità di supervisione nazionali e degli organismi di certificazione, con un focus specifico sul processo di approvazione dei criteri di certificazione spettante all'ASN o all'EDPB.

Forme d'uso delle linee guida 1/2018

Come indicato nello stesso documento, le linee guida possono essere utilizzate da diversi attori per svariate finalità, come sintetizzato nella tabella che segue:

Utilizzatore	Finalità	Fonte normativa
Allegato A.1 - Attività giornalistica	Delibera n. 491	n. 3 del 4/1/2019
ASN ed EDPB	ai fini dell'**approvazione dei criteri di certificazione**	[art. 42(5), 58(3)(f), 70(1)(o)]
Organismi di certificazione	per la **stesura e revisione dei criteri di certificazione** prima della presentazione all'ASN competente per l'approvazione	art. 42(5)
ASN	al fine della **stesura dei propri criteri di certificazione**	art. 42(5)
EDPB	ai fini dell'**approvazione di un sigillo europeo** di protezione dei dati	[artt. 42(5) e 70(1)(o)]
EDPB	quando fornisce alla Commissione europea un **parere sugli obblighi di certificazione**	art. 70(1)(q) e 43(8)
Commissione europea	al fine di **specificare i requisiti** da prendere in considerazione per i meccanismi di certificazione, se e quando **adotta atti delegati**	art. 43(8)
organismi nazionali di accreditamento (es. Accredia)	per tener conto dei criteri di certificazione **in vista dell'accreditamento** degli organismi di certificazione conformemente alla norma EN-ISO / IEC 17065/2012 e dei requisiti supplementari	art. 43
titolari e responsabili del trattamento	quando definiscono la propria **strategia di conformità al GDPR** e considerano la certificazione come mezzo per dimostrare la conformità	

Forme d'uso delle linee guida 1/2018.

Chi accredita e chi certifica

Le due tabelle che seguono indicano, sotto il duplice profilo del GDPR e della normativa nazionale di attuazione,

1. i soggetti legittimati all'accreditamento degli organismi di certificazione;
2. i soggetti autorizzati a rilasciare certificazioni ai sensi del GDPR.

	GDPR	Codice privacy
Soggetti ⇒	• ASN e/o • Organismo Nazio nale di Accreditamento	Accredia o, in subordine, Garante privacy
Articoli ⇒	43(1)	2-septiesdecies

Soggetti legittimati all'accreditamento per le certificazioni GDPR.

	GDPR	Codice privacy
Soggetti ⇒	• Organismi di certificazione • ASN • EDPB (*in via alternativa*)	n/a
Articoli ⇒	42(5)	n/a

Soggetti legittimati al rilascio di certificazioni GDPR.

Tempi di durata

La tabella in basso indica i tempi di durata di accreditamento e certificazione GDPR.

	Accreditamento	Certificazione
Durata ⇒	max 5 anni, rinnovabili	3 anni, rinnovabili
Articoli ⇒	43(4)	42(7)

Tempi di durata di accreditamenti e certificazioni GDPR.

Possibili ruoli dell'ASN nel rilascio delle certificazioni GDPR

La tabella che segue evidenzia i possibili ruoli che l'ASN può assumere in relazione alla certificazione GDPR, secondo quanto è astrattamente previsto nel GDPR come ammissibile e quanto invece sia presumibile avvenga in Italia riguardo al Garante.

	ASN secondo GDPR	Garante in Italia
Modelli ipotizzabili ⇒ *(ipotesi cumulabili)*	emette essa stessa la certificazione, in relazione al proprio schema di certificazione;	improbabile
	emette essa stessa la certificazione, nel rispetto del proprio schema di certificazione, ma delega in tutto o in parte il processo di valutazione a terzi;	improbabile
	crea il proprio schema di certificazione e affida agli organismi di certificazione la procedura di certificazione che rilascia la certificazione	improbabile
	incoraggia il mercato a sviluppare meccanismi di certificazione	Sì

Possibili ruoli dell'ASN riguardo al rilascio di certificazioni GDPR.

Ruolo dell'ASN riguardo ai meccanismi di certificazione GDPR
La tabella sotto indica compiti e poteri di ciascuna ASN in relazione ai meccanismi di certificazione GDPR.

Tema	Compiti	Articolo GDPR
Criteri ⇒	**valutare i criteri** di uno schema di certificazione e presentare un progetto di decisione;	42(5)
	comunicare all'EDPB il progetto di decisione quando l'ASN intende approvare i criteri di certificazione e prendere in considerazione il parere dell'EDPB;	64(1)(c),(7), 70(1)(t)
	approvare i criteri per la certificazione prima che l'accreditamento e la certificazione possano aver luogo;	58(3)(f), 42(5), 43(2)(b)
	pubblicare i criteri di certificazione;	43(6)
Certificazione ⇒	fungere da **autorità competente** per i sistemi di certificazione **a livello UE**, che possono comportare l'approvazione da parte dell'EDPB di **sigilli europei** di protezione dei dati;	42(5), 70(1)(o)
	ordinare a un ente di certificazione (a) di **non rilasciare la certificazione** o (b) di **ritirare la certificazione** se i requisiti per la certificazione (procedure o criteri di certificazione) non sono o non sono più soddisfatti.	58(2)(h)

Compiti e poteri delle ASN in relazione ai meccanismi di certificazione GDPR.

Influenza dei meccanismi di certificazione

La tabella seguente sintetizza i profili del GDPR sui quali i meccanismi di certificazione esercitano una specifica influenza.

Profilo di incidenza	Articolo GDPR
Dimostrazione di conformità al GDPR	42(1)
Appropriatezza delle garanzie nei rapporti **responsabile/titolare** e **sub-responsabile/ responsabile**	28(5)
Adeguatezza delle misure tecnico-organizzative	24(1)(3), 25 e 32(1)(3)
Legittimità dei flussi esteri di dati personali	46(2)(f)
Determinazione delle sanzioni amministrative	83(2)(j)

Profili di influenza dei meccanismi di certificazione GDPR.

Distinzioni tra requisiti e criteri

La tabella che segue indica le principali distinzioni tra i requisiti ed i criteri nei meccanismi di certificazione GDPR.

	Requisiti	Criteri
Riferimento ⇒	Accreditamento	Certificazione
Chi li stabilisce ⇒	• Garante [artt. 55/56, 57(1)(n)] oppure • EDPB [art. 64(1)(c), 43(1)]	• Organismo di certificazione [art. 43(2)(c)
Chi li approva ⇒	n/a	• Garante [art. 58(3)(f), 42(5), 43(2)(b) oppure • EDPB [art. 70(1)(o), 42(5)]

Distinzioni tra requisiti e criteri nei meccanismi di certificazione GDPR.

Oggetto della certificazione GDPR

La tabella sotto indica il possibile oggetto della certificazione GDPR ossia quello che comunemente viene indicato come bersaglio della valutazione ("target of evaluation, "ToE").

		Articolo GDPR
Chi si certifica ⇒	Titolare o responsabile del trattamento	42(2),(7)
Cosa si certifica ⇒ **(ToE)**	Operazione o set di operazioni di trattamento Eventualmente risultante in un prodotto, servizio o processo	42(1)

Target of Evaluation dei meccanismi di certificazione GDPR.

16.
Necessità contrattuale come base giuridica, in consultazione pubblica

Il 9 aprile 2019, il Comitato europeo per la protezione dei dati ("EDPB") ha adottato – e sottoposto a consultazione pubblica sino al 25 maggio – nuove linee guida sull'ipotesi in cui il trattamento dei dati è «*necessario per l'esecuzione di un contratto a cui l'interessato è parte o al fine di adottare provvedimenti su richiesta dell'interessato prima di stipulare un contratto*». È questo il caso della motivazione ("base giuridica") che giustifica il trattamento dei dati personali, prevista dall'articolo 6, paragrafo 1, lettera b), del GDPR.

Sintesi

Le linee guida EDPB 2/2019 considerano il significato della base giuridica della **"necessità contrattuale"** e, in particolare, se essa possa essere utilizzata per giustificare il trattamento dei dati da parte dei **servizi online** per scopi come il miglioramento del servizio, la prevenzione delle frodi, la pubblicità mirata (tutte ipotesi risolte in modo negativo) e la personalizzazione dei servizi (opzione considerata come ammissibile qualora la personalizzazione sia una componente essenziale ed attesa del servizio).

Le linee guida considerano il concetto di "**necessità**" come si applica all'espressione "necessario per l'esecuzione di un contratto", in particolare al trattamento di dati personali nel contesto di contratti per servizi online, indipendentemente dal modo in cui i servizi sono finanziati (a pagamento o mediante la raccolta dei dati personali dell'utente).

Necessità contrattuale e servizi online

Sebbene l'ipotesi della "necessità contrattuale" rappresenti una motivazione che permette il trattamento di dati personali in via generale e molte delle considerazioni contenute nelle linee guida valgano in senso lato, l'EDPB ha inteso concentrare le proprie riflessioni soprattutto riguardo ai **servizi online**, cioè quelli «*normalmente fornit(i) dietro retribuzione, a distanza, per via elettronica e su richiesta individuale di un destinatario di servizi*»; tra questi sono inclusi anche quei **servizi apparentemente gratuiti** ma finanziati tramite la pubblicità.

La ragione di questa attenzione particolare risiede in una molteplicità di aspetti:

- i servizi online tipicamente non sono negoziati su base individuale;
- la tecnologia odierna consente ai titolari del trattamento di raccogliere ed elaborare una gran quantità di dati personali;
- le condizioni generali di contratto possono eventualmente massimizzare raccolta e utilizzo di dati con formulazioni generiche;
- gli utenti hanno scarsa (o nessuna) consapevolezza e controllo dell'uso dei propri dati personali.

Possibili violazioni

Le prassi in atto relative ai servizi online e che, talvolta, si registrano anche in altri contesti dove la base giuridica del trattamento è la "necessità contrattuale", spesso contraddicono i principi della **specificità di scopo** e di **minimizzazione dei dati** di cui all'articolo 5 del GDPR.

Il riferimento a scopi generici come l'uso di espressioni vaghe del tipo "**migliorare l'esperienza degli utenti**", "**scopi di marketing**", "**scopi di sicurezza IT**" o "**future ricerche**", oltre a non soddisfare il requisito della "specificità", ledono la **ragionevole aspettativa**

dell'interessato e provocano inattese sorprese all'interessato, pregiudicando l'ulteriore principio di correttezza [art. 5(1)(a)].

Base giuridica

In attuazione dell'articolo 8 della Carta dei diritti fondamentali dell'UE – che stabilisce che il trattamento di dati personali deve essere effettuato per una **motivazione legittima determinata per legge** – il GDPR elenca sei condizioni che identificano le basi giuridiche dei trattamenti, fra queste vi è quella della "necessità contrattuale".

La corretta individuazione della base giuridica – che va comunicata all'interessato tramite l'informativa ed il riscontro all'accesso – consente di stabilire quale sia il quadro giuridico di riferimento per quello specifico trattamento, con i conseguenti obblighi del titolare e diritti degli interessati; ad esempio, se la base giuridica è la "necessità contrattuale", l'interessato potrebbe vantare il diritto alla portabilità (art. 20) ma non il diritto di opposizione [art. 21(1)]; di converso, se il trattamento trovasse la sua giustificazione nel consenso dell'interessato, quest'ultimo potrebbe revocarlo ed anche esercitare il diritto di opposizione.

In aggiunta, il criterio della "necessità contrattuale" ammette il trattamento, subordinatamente a garanzie e misure adeguate, «*in situazioni in cui (...) è opportuno e necessario trattare i dati in un determinato contesto al fine di perseguire un interesse legittimo specifico*» mentre il trattamento basato sul consenso dell'interessato trova la sua giustificazione nel mero potere del soggetto di autorizzare il trattamento (wp217 §III.1.1). Pertanto, una circostanza di confusione nella determinazione della base giuridica – ad esempio, assumendo erroneamente che la firma di un contratto corrisponda al consenso al trattamento dei dati personali – non consentirebbe all'interessato di effettuare le proprie valutazioni in merito alla fornitura dei dati personali e, pertanto, verrebbe a violare entrambi i principi di trasparenza e correttezza.

Individuazione della base giuridica

L'individuazione della base giuridica da parte dei titolari del trattamento è un'operazione delicata che si fonda sulla legge; essa va fatta prima dell'inizio del trattamento, dopo aver correttamente identificato le relative finalità ed aver tenuto conto della delimitazione delle operazioni attese entro i confini degli scopi specificati.

Difatti, finalità e basi giuridiche sono in stretta correlazione ed una vaga identificazione delle finalità può provocare l'individuazione di molteplici basi giuridiche; evidenziare all'interessato più basi giuridiche per lo stesso trattamento non solo è in contrasto col GDPR ma confonde l'interessato riguardo alle motivazioni, ai suoi diritti ed in merito alle conseguenze che il trattamento possa causare nei suoi confronti.

In ogni caso, la preliminare individuazione effettuata dal titolare può essere contestata da chi vi abbia interesse (interessati, autorità, terzi) e, alla fine, giudicata dai tribunali.

Operazione non discrezionale

L'individuazione della base giuridica che legittima il trattamento non è operazione rimessa alla scelta discrezionale del titolare del trattamento. Essa si fonda su una valutazione oggettiva che trae fonte dalla legge; se un trattamento si rende necessario per:

- **adottare misure precontrattuali su richiesta dell'interessato** (ad esempio, il trattamento da parte di un'impresa assicuratrice della marca e dell'età dell'autoveicolo per effettuare un preventivo richiesto dall'interessato);
- **dare esecuzione ad un contratto** (come il trattamento dell'indirizzo dell'interessato affinché possa essere effettuata la consegna delle merci acquistate online o il trattamento degli estremi della carta di credito per l'esecuzione del pagamento) la relativa base giuridica "dovrà" essere la "necessità contrattuale" anzichè, ad esempio, il consenso dell'interessato.

Di converso, come si ribadirà in seguito, se il trattamento non risultasse necessario per l'esecuzione del contratto, lo stesso potrebbe essere effettuato legittimamente solo facendo affidamento su una diversa base giuridica.

Requisiti per la "necessità contrattuale"

Affinchè il titolare del trattamento possa fondare la legittimità del trattamento sulla base giuridica della "necessità contrattuale" occorre che egli sia in grado di **dimostrare** che:

1. esiste un contratto;
2. **il contratto sia valido** secondo la legge locale sui contratti, applicabile al caso;
3. **il trattamento è oggettivamente necessario** per l'esecuzione del contratto.

Analogamente per l'altra ipotesi rientrante nel criterio della "necessità contrattuale", vale a dire quando il trattamento è necessario al fine di adottare misure precontrattuali su richiesta dell'interessato, occorre che il titolare sia in grado di **dimostrare** che:

1. le misure sono state effettivamente richieste dall'interessato;
2. **le misure sono oggettivamente necessarie** per stipulare un determinato contratto;
3. **il tipo di contratto da stipulare è giuridicamente valido** secondo la legge applicabile.

Concetto di "necessità"

Il criterio di "necessità" – presente nella base giuridica della "necessità contrattuale" – è comune a tutte le basi giuridiche dell'articolo 6, ad eccezione di quella del consenso dell'interessato (cioè, "l'esecuzione di un contratto", "l'adempimento di un obbligo legale", la "salvaguardia di interessi vitali" e "il perseguimento dell'interesse legittimo").

Il criterio di "necessità" va interpretato in modo rigoroso ed oggettivo:

- **nel primo senso (rigore)**, in quanto il vincolo di necessità non discende dal fatto che alcuni trattamenti di dati siano coperti da un contratto per poterne dedurre in automatico la loro necessità alla sua esecuzione;
- **sotto il secondo profilo (oggettività)** i trattamenti devono risultare essenziali per l'esecuzione del contratto anzichè discendere dalla volontà unilaterale del titolare (come sarebbe il caso in cui dati, finalità ed operazioni fossero decisi in condizioni generali di contratto, unilateralmente stabilite dal fornitore).

Nel **documento wp217** sulla base giuridica dell'interesse legittimo del WPArt29, ad esempio, si faceva notare che nel caso di servizi on line, la motivazione della "necessità contrattuale" «*non è un fondamento giuridico adeguato per creare un profilo dei gusti e delle scelte di stile di vita dell'utente sulla base della sequenza di clic che ha effettuato su un sito web e degli articoli che ha acquistato (...). Anche se tali attività di trattamento sono espressamente menzionate in caratteri minuscoli nel contratto (...)*».

In conclusione, **il criterio di necessità** – cioè la valutazione se il trattamento dei dati è necessario all'esecuzione contrattuale – **si ricava dalla funzione o finalità tipica del contratto (**la cosiddetta ***ratio***) da quanto è permesso o è scritto nelle condizioni contrattuali: giocoforza ne rimane escluso il «*trattamento utile ma non oggettivamente necessario per l'esecuzione del servizio contrattuale o per l'adozione di misure precontrattuali pertinenti su richiesta dell'interessato, anche se necessario per altri fini commerciali del titolare del trattamento*» (EDPB 2/2019 §25).

Ulteriori basi giuridiche di riferimento

Quando i dati personali che si intende raccogliere non sono giustificati dallo stretto collegamento funzionale con la genesi o l'esecuzione contrattuale, il titolare dovrà far ricorso ad ulteriori motivazioni giuridiche come, il più delle volte, il **libero ed informato consenso** dell'interessato [art. 6(1)(a)] oppure il **legittimo interesse** del medesimo interessato o di terzi [art. 6(1)(f)], sussistendone i presupposti di validità.

Sarà questa la situazione in cui ci si troverà sistematicamente in presenza di **speciali categorie di dati**, in quanto l'articolo 9 del GDPR – che prevede le condizioni per il trattamento legittimo dei cosiddetti "dati sensibili" – non considera la "necessità contrattuale" tra le motivazioni ammesse. Se i dati personali che occorre utilizzare per dare esecuzione ad un contratto rientrano nella speciale categoria (cioè sono "dati sensibili" secondo l'elencazione dell'art. 9(1) del GDPR) occorrerà verificare che sussista una delle deroghe al generale divieto di cui all'articolo 9, tra cui il consenso esplicito dell'interessato.

Situazioni specifiche

Miglioramen to del servizio

I servizi online raccolgono spesso informazioni dettagliate su come gli utenti interagiscono con il loro servizio (come la raccolta di parametri organizzativi relativi a un servizio, o dettagli sul coinvolgimento dell'utente) che **non possono essere considerati necessari** per la fornitura del servizio, in quanto il servizio potrebbe essere fornito in assenza del trattamento di tali dati personali.

Trattamenti per finalità anti-frode

Il trattamento a fini di prevenzione delle frodi – che può comportare il monitoraggio e la profilazione dei clienti – secondo l'EDPB **non può ritenersi oggettivamente necessario** per l'esecuzione di un contratto con un interessato. La base giuridica di riferimento, secondo i contesti, potrà essere "obbligo legale" o "legittimo interesse".

Pubblicità comportamentale

Sebbene molti servizi online "gratuiti" si finanzino tramite la pubblicità comportamentale indirizzata ai propri utenti – per cui si potrebbe ritenere che tale attività ed il relativo trattamento dati siano intrinsecamente connessi all'erogazione del servizio – la pubblicità comportamentale non è elemento essenziale dei servizi online. Il nesso di interdipendenza è di natura economica piuttosto che obiettivamente giuridico. Per questo, il trattamento di dati personali per pubblicità comportamentale **non può avvalersi della base giuridica della "necessità contrattuale"** quando si erogano servizi online.

Trattamenti per la personalizzazione dei contenuti

Per determinare se il trattamento per la personalizzazione dei contenuti può essere considerato come un aspetto intrinseco di un servizio online, occorrerà valutare

- la **natura del servizio** fornito,
- le **aspettative dell'interessato medio** alla luce non solo dei termini del servizio ma anche del modo in cui il servizio viene promosso agli utenti
- **se** il servizio può essere **fornito senza personalizzazione**.

17.
Ruolo privacy dell'OdV

Alla fine di marzo 2019 l'AODV231 (Associazione dei Componenti degli Organismi di Vigilanza ex D.Lgs.231/2001) ha rilasciato un interessante documento di studio sulla qualificazione soggettiva dell'OdV riguardo alla vigente disciplina sulla protezione dei dati personali. In questa sede ne riportiamo i tratti salienti, rinviando ad un eventuale intervento dell'Editoriale per una sua analisi critica.

Conclusioni dello studio

Terza via

Intervenendo nel dibattito incentratosi sulla qualificazione alternativa dell'OdV come titolare del trattamento – autonomo rispetto all'azienda di cui è parte – oppure di responsabile del trattamento, lo studio avanza una possibile "terza via".

L'OdV, secondo lo studio – nella sua tipica conformazione standard e salve specifiche particolarità dovute ad eventuali incarichi aggiuntivi – «*in quanto "parte dell'impresa", non (è) qualificabile né come Titolare né come Responsabile del trattamento (...) (mentre) ai fini dell'osservanza delle norme relative alla protezione dei dati l'inquadramento soggettivo dell'Organismo di Vigilanza (collegiale o monocratico) (è) assorbito da quello della Ente/società vigilata della quale, appunto, l'OdV è "parte"*».

OdV "parte" dell'azienda oggetto di vigilanza

Sempre secondo lo studio, quindi, l'OdV sarebbe "parte" dell'azienda oggetto della sua vigilanza senza possedere una qualificazione soggettiva distinta, in relazione alla disciplina della protezione dei dati personali. Si ritiene ammissibile l'esistenza – interpretando il GDPR – di un "ventre molle" dell'azienda titolare del trattamento, dove non sarebbe necessario avere una specifica qualificazione soggettiva privacy, essendo sufficiente esserne "parte".

Soggetti designati al trattamento

L'individuazione dell'OdV a fini data protection come mera "parte" dell'azienda, secondo lo studio, si giustificherebbe con l'ulteriore esclusione, in via residuale, dell'inquadrabilità dell'OdV anche come "soggetto designato" al trattamento. Tale esclusione sarebbe motivata dalle seguenti considerazioni:

- in quanto la norma dell'articolo 29 del GDPR «*fa esclusivo riferimento soggettivo "a persone fisiche", mentre l'OdV normalmente è un organismo collegiale da considerare come tale anche ai fini della qualificazione privacy*»;
- perchè – operando una combinazione con l'articolo 2-quaterdecies dell'attuale codice privacy – «*tale norma* ***consente, non impone****, la designazione e, comunque, quest'ultima implica un'essenziale soggezione dei soggetti designati, o autorizzati, alla illimitata "autorità diretta" del Titolare (o Responsabile), "in base alle istruzioni [da questi] impartite … senza apprezzabili margini di autonomia", condizione questa* ***davvero troppo restrittiva per risultare compatibile con l'istituzionale autonomia di iniziativa e controllo di cui deve essere dotato l'OdV ex art. 6, co. 1, lett. b), del d.lgs. 231/2001***» (enfasi aggiunta).

Conclusioni sulla "terza via"

In sostanza, quindi, lo studio sembrerebbe introdurre una nuova tesi secondo cui, l'attuale disciplina di GDPR e codice privacy ammetterebbe che:

- i dati personali possano essere utilizzati da soggetti facenti parte dell'organizzazione dell'azienda titolare (come i membri dell'OdV) senza necessità che essi abbiano un inquadramento soggettivo;
- all'interno dell'organizzazione aziendale possano esservi soggetti (come i membri dell'OdV) che trattano dati personali senza che essi ricevano istruzioni da parte dell'azienda titolare.

Tesi dell'OdV autonomo titolare

Passaggio preliminare all'opzione della "terza via" è stata l'analisi critica operata dallo studio, alle due tesi alternative circa l'individuazione dell'OdV come titolare autonomo o responsabile del trattamento dei dati personali che tale organismo utilizza nello svolgimento del proprio ufficio.
La tesi che riconosce nell'OdV una distinta titolarità del trattamento rispetto all'azienda oggetto di vigilanza si fonda essenzialmente sul potere di autonomia che la legge riconosce all'organismo: se l'OdV gode di autonomi poteri di iniziativa e controllo, secondo questa tesi, parimenti autonomo deve conseguentemente risultare il potere decisionale nell'uso strumentale dei dati personali per l'esercizio della propria funzione. Tale autonomo potere decisionale esercitato su finalità e mezzi del trattamento dei dati sarebbe l'elemento indicativo dell'autonoma titolarità.

Critica della tesi della titolarità distinta

A. **OdV nel suo complesso** - Lo studio sottolinea in via preliminare che «*la corretta qualificazione ai fini della normativa sulla privacy (...) deve riferirsi all'OdV nel suo complesso, come organismo collegiale, e non a ciascun suo membro, singolarmente considerato. Anche perché se così non fosse, nel caso (di gran lunga più frequente) di composizione mista dell'OdV, si potrebbe determinare un'irrazionale disparità di regime privacy tra membri «interni» e membri «esterni» dello stesso OdV, (ritenendo soltanto i primi già «coperti» dall'inquadramento privacy predeterminato dal rapporto di lavoro subordinato con l'ente vigilato).*».
B. **Autonomia di funzioni ed attività conseguenti** - Il primo rilievo mosso alla tesi dell'autonoma titolarità è stata quella di essere fondata sull'equazione "autonomia di poteri di iniziativa e di controllo" e "autonoma determinazione di finalità e mezzi del trattamento", con ciò confondendo ed indebitamente estendendo l'autonomia delle funzioni alle attività necessarie per il loro assolvimento (cioè, «*l'autonomia nell'esercizio del "compito di vigilare" non può essere confusa con l'autonomia nella determinazione delle finalità della vigilanza e quindi dei trattamenti strumentali ad essa*»); infatti, secondo lo studio, le finalità del trattamento dei dati di interesse dell'OdV non sarebbero determinate dall'OdV stesso ma sono predeterminate dalla legge, sono declinate dal modello di gestione adottato dall'organo dirigente ed in qualche modo dipendono dalle regole di funzionamento dell'OdV disciplinate dall'organo dirigente.
C. **Dati oggetto del trattamento dell'OdV sono quelli dell'ente vigilato** - Ulteriore profilo critico della tesi dell'autonoma titolarità sarebbe rappresentato, stando allo studio, dalla constatazione che «*i dati oggetto dei loro (dell'Odv) trattamenti sono sempre e soltanto quelli che l'ente vigilato ha diritto e legittimazione a trattare. In altre parole, la base giuridica del trattamento dei dati da parte dell'OdV fa capo esclusivamente all'ente vigilato.*».
D. **Determinazione da parte della legge** - Da ultimo, l'individuazione della titolarità in capo all'OdV non potrebbe nemmeno trovare la propria fonte in una eventuale

determinazione di legge [articolo 4, punto 7), secondo periodo del GDPR] in quanto nel caso di specie la legge non imporrebbe all'Odv di porre in essere trattamenti di dati per finalità e con mezzi direttamente definiti dalla legge stessa nè la norma disciplinerebbe «*anche le modalità e i criteri specifici da adottare per la sua (dell'OdV) nomina*». In tal modo lo studio sembrerebbe adottare una lettura discutibile del passaggio normativo citato.

Critica della tesi dell'OdV responsabile del trattamento

Sull'altro fronte della tesi alternativa della qualificazione dell'OdV come responsabile del trattamento, la principale critica sollevata ha riguardato il difetto del presupposto dell'autonoma soggettività dell'OdV. Infatti, criterio essenziale per il ruolo di Responsabile è «*"essere una persona giuridica distinta dal [Titolare]", come autorevolmente precisato dalla pluricitata Opinion 1/2010 del Art. 29 Data Protection Working Party. Il che non è concepibile per l'OdV, dato il suo istituzionale carattere «interno» rispetto all'ente vigilato ex art. 6, co. 1, lett. b), d.lgs. 231/2001, ovvero dato "il requisito dell'appartenenza all'ente"*».

18.
Ruolo privacy dell'OdV

Lo scorso Alert ci ha dato notizia di uno studio predisposto dall'AODV231 (Associazione dei Componenti degli Organismi di Vigilanza ex D.Lgs.231/2001) in merito al ruolo che si ritiene debba assumere l'Organismo di Vigilanza riguardo all'utilizzo di dati personali nello svolgimento del proprio mandato tipico. Lo studio affronta diversi profili ed offre interessanti spunti che, a nostro giudizio, meritano qualche riflessione che affidiamo a questa puntata.

Sintesi

Sulla base della considerazione che l'organismo di vigilanza 231 è "parte" dell'azienda su cui vigila, uno studio dell'AODV231 sul tema dell'inquadramento soggettivo dello stesso OdV in materia data protection giunge alla conclusione che ad esso non possa imputarsi un ruolo distinto da quello dell'ente/società di pertinenza. A questa conclusione lo studio giunge a seguito di un'analisi critica delle tre possibili alternative (a) OdV quale titolare di un autonomo trattamento (b) OdV responsabile del trattamento per conto dell'ente/azienda e (c) individuazione dei singoli membri dell'OdV (collegiale) come soggetti autorizzati al trattamento (art. 29, GDPR).

Il commento di questa puntata si sofferma criticamente sulla tesi che ammetterebbe l'esistenza di componenti dell'assetto organizzativo aziendale che, in quanto "parte" dell'azienda stessa, potrebbero utilizzare dati personali di pertinenza, senza essere sottoposti al potere direttivo ed al controllo dell'azienda-titolare. Si fa rilevare come un tale assunto sarebbe in contrasto con gli articoli 24, 29 e 32(4) e con la definizione di "terzi" di cui all'articolo 4(f). Anche secondo precedenti del WPArt29, coloro che in azienda eventualmente utilizzassero dati personali senza o oltre le istruzioni del titolare del trattamento, verrebbero automaticamente a qualificarsi come titolari di autonomi trattamenti, in quanto determinerebbero in autonomia relative finalità e modalità. Pertanto, anche alla luce di questo percorso di analisi si perviene alla medesima conclusione che individua l'OdV come autonomo titolare a seguito della sua tradizionale autonomia decisionale anche in merito ai trattamenti dei dati personali necessari per lo svolgimento delle proprie tipiche funzioni di vigilanza.

L'OdV è parte dell'azienda

Come riportato dall'Alert, l'OdV, secondo lo studio – nella sua tipica conformazione standard e salve specifiche particolarità dovute ad eventuali incarichi aggiuntivi – «*in quanto "parte dell'impresa", non (è) qualificabile né come Titolare né come Responsabile del trattamento (...) (mentre) ai fini dell'osservanza delle norme relative alla protezione dei dati l'inquadramento soggettivo dell'Organismo di Vigilanza (collegiale o monocratico) (è) assorbito da quello della Ente/società vigilata della quale, appunto, l'OdV è "parte"*».

Da questa tesi conseguirebbe che per l'OdV non si riscontri una qualificazione soggettiva distinta – a fini data protection – da quella dell'azienda di cui "è parte".

Assetto organizzativo e impresa

La nota circolare 285 di Banca d'Italia dal titolo "Disposizioni di vigilanza per le banche" sottolinea che «*(e)fficaci assetti organizzativi (…) costituiscono per tutte le imprese condizione essenziale per il perseguimento degli obiettivi aziendali*» (Circ. 285, Tit.IV, Cap 1).

Parafrasando questo condivisibile assunto può sostenersi con correttezza che qualsiasi obiettivo aziendale – quindi anche quello di conformità alle leggi – presuppone un efficace assetto organizzativo per poter essere conseguito. Pertanto, dato un obiettivo, non può essere messo in discussione se un assetto organizzativo (peraltro "efficace") occorra o meno, piuttosto, oggetto di dibattito può essere

lo stabilire "quale" assetto organizzativo possa ritenersi efficace in un determinato contesto.
Non c'è imprenditore – quindi, impresa – senza l'organizzazione dei fattori produttivi e di scambio, come insegna la definizione dell'articolo 2082 del codice civile.

Autonomia organizzativa dell'imprenditore

All'imprenditore spetta la scelta organizzativa della propria impresa, cioè quale sia il disegno dell'assetto organizzativo interno per il perseguimento di tutti gli obiettivi aziendali. L'articolo 41 della nostra Costituzione, infatti, statuisce che «*(l)'iniziativa economica privata è libera*» ed incontra limiti solo in ipotesi di contrasto all'utilità sociale, «*alla sicurezza, alla liberta', alla dignita' umana*».

Modello organizzativo DP nel GDPR

Il **principio dell'autonomia organizzativa** dell'imprenditore-titolare del trattamento di dati personali è fatto proprio – implicitamente – dal GDPR e – esplicitamente – dal codice privacy novellato.
Il GDPR si limita a tracciare le linee di confine del profilo organizzativo del titolare del trattamento:

- **le misure organizzative**, insieme a quelle tecniche, costituiscono la linfa vitale della protezione da garantire in via adeguata ai dati personali che si utilizzano; le misure organizzative sono strumento essenziale di garanzia dell'effettiva protezione e quest'ultima assurge a principio di liceità del trattamento [art.5(1)(f), GDPR];
- **l'adeguata protezione** dei dati personali, perseguita anche mediante misure organizzative, è tra i sintomi più significativi del livello di responsabilizzazione del titolare del trattamento, cioè l'*accountability* con funzione di collante delle ulteriori prescrizioni normative (art. 24, GDPR);
- **l'accesso ai dati personali** da parte di chi agisce sotto la diretta autorità dell'imprenditore-titolare, è soggetto a specifiche istruzioni impartite dal titolare in merito al loro utilizzo; proprio quest'ultima disposizione, come vedremo in seguito, rappresenta il punto di raccordo tra il profilo meramente organizzativo (art. 29) e quello tecnico di sicurezza [art. 32(4), GDPR].

Modello organizzativo DP nel codice privacy

A mero scopo esplicativo, il codice privacy novellato ricorda l'autonomia dell'imprenditore – sia esso titolare o responsabile del trattamento – riguardo al disegno del proprio assetto organizzativo interno ai fini della protezione dei dati personali.
L'articolo 2-quaterdecies distingue, nei due commi in cui si struttura, le ipotesi di:

1. **attribuzione di «*specifici compiti e funzioni*** *connessi al trattamento di dati personali (...) a persone fisiche espressamente designate*» che facciano parte dell'assetto organizzativo del titolare o del responsabile, i quali comunque rimangono responsabili (comma 1, enfasi aggiunta);
2. **autorizzazione al trattamento** dei dati personali a «*persone che operano sotto la propria autorità diretta*» (comma 2).

Quindi, il primo comma prevede l'ipotesi di attribuzione mediante deleghe, di «*specifici compiti e funzioni*» di pertinenza del titolare o del responsabile, a propri dipendenti appositamente

individuati e designati. Questa previsione indirizza il tema delle scelte in merito all'assetto organizzativo data protection operate dall'imprenditore: sono questi i casi delle figure che nella prassi assumono la denominazione, ad esempio, di "**coordinatore privacy**" (punto di contatto per tutte le questioni sul tema, o anche esecutore materiale dell'operatività data protection), "**data manager**" (responsabile di funzione con compiti di presidio degli aspetti data protection di pertinenza), "**referente privacy**" (operatore data protection dell'area funzionale per conto del data manager), "**comitato privacy**" (organo di coordinamento strategico e di guida nell'implementazione data protection aziendale).

Designati al trattamento o "incaricati"

Il comma 2 dell'articolo 2-quaterdecies del codice privacy indirizza il profilo della modalità (anch'essa di libera scelta) con cui l'imprenditore – titolare o responsabile – autorizza i propri dipendenti (i cosiddetti "incaricati") all'accesso ai dati, impartendo le istruzioni specifiche prescritte dagli articoli 29 e 32(4) del GDPR.

Compatibilità del ruolo degli "incaricati" col GDPR

Su questo fronte, le prescrizioni già in atto relativamente agli incaricati del trattamento (secondo il codice privacy previgente) risultano compatibili col GDPR.

Posizione del Garante sulla compatibilità del ruolo degli "incaricati"

Recita testualmente la Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali pubblicata dal Garante: «*Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento, in particolare alla luce del principio di "responsabilizzazione" di titolari e responsabili del trattamento che prevede l'adozione di misure atte a garantire proattivamente l'osservanza del regolamento nella sua interezza. In questo senso, e anche alla luce degli artt. 28, paragrafo 3, lettera b), 29, e 32, paragrafo 4, in tema di misure tecniche e organizzative di sicurezza, si ritiene che titolari e responsabili del trattamento possano mantenere in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi negli anni anche attraverso gli interventi del Garante (si veda art. 30 del Codice e, fra molti,* ***doc. web n. 1507921****, ovvero* ***doc. web n. 1508059*** *per quanto riguarda la pubblica amministrazione, ovvero* ***doc. web n. 1813953*** *in materia di tracciamento delle attività bancarie) in quanto misure atte a garantire e dimostrare "che il trattamento è effettuato conformemente" al regolamento (si veda art. 24, paragrafo 1, del regolamento).*».

Compatibilità in base all'evoluzione normativa

Per esigenze di agevole comprensione continueremo a chiamare "incaricati", i soggetti autorizzati al trattamento.

Come anticipato, il GDPR affronta il tema degli incaricati agli articoli 29 e 32(4).

La prescrizione dell'articolo 29 non è di nuovo conio in quanto essa è la riproposizione – con poche modifiche di ordine formale – dell'articolo 16 della direttiva 95/46/CE, rubricato "Riservatezza dei trattamenti". L'articolo 16 della direttiva era poi confluito nell'articolo 30 del codice privacy previgente; da questa combinazione normativa deriva il condivisibile assunto del Garante, sopra riportato, secondo cui «*Le disposizioni del Codice in materia di incaricati del trattamento sono pienamente compatibili con la struttura e la filosofia del regolamento*». Detto diversamente, se l'articolo

29 del GDPR è la riproposizione sostanziale dell'articolo 16 della direttiva e l'articolo 30 del codice previgente è la traslazione dell'articolo 16 della direttiva, logica vorrebbe che quanto disposto in base all'articolo 30 del codice previgente risulti attualmente conforme all'articolo 29 del GDPR.

Articolo 29 del GDPR

L'articolo 29 del GDPR, già articolo 16 della direttiva 95/46/CE, introduce un obbligo di confidenzialità da parte di chi agisce sotto l'autorità di titolare e responsabile – nonchè del responsabile stesso – i quali non possono trattare i dati personali di pertinenza del titolare se non sono istruiti in tal senso dal titolare medesimo. A conferma di ciò, la rubrica dell'analogo articolo 16 della direttiva recitava "Riservatezza dei trattamenti". Quindi, tutti coloro che agiscono sotto l'autorità del titolare o del responsabile (cioè ne fanno "parte"), così come lo stesso responsabile, hanno un obbligo di riservatezza sia nei riguardi del titolare sia nei confronti della legge. La logica della prescrizione normativa è che nessuno facente parte dell'assetto organizzativo dell'imprenditore-titolare possa utilizzare i dati personali di sua pertinenza sottraendosi al potere decisionale (ed al conseguente obbligo di controllo) del titolare medesimo, esercitato impartendo specifiche istruzioni. Rimane da chiedersi quali siano le conseguenze di una violazione di tale obbligo: quesito che affronteremo più avanti.

Critica alla tesi di "parte" che agisce senza istruzioni

Dalla ricostruzione giuridica sopra accennata emerge chiaramente che non vi possa essere "parte" dell'organizzazione aziendale che utilizzi dati personali se non appositamente autorizzata dal titolare del trattamento. Per queste ragioni, solleva perplessità l'affermazione contenuta nello studio citato per cui, da un lato, l'OdV sarebbe "parte" dell'azienda oggetto della sua vigilanza senza possedere una qualificazione soggettiva distinta, in relazione alla disciplina della protezione dei dati personali; dall'altro lato, l'inquadramento soggettivo dell'OdV (collegiale o monocratico) «*ai fini dell'osservanza delle norme relative alla protezione dei dati (...) sia assorbito da quello della Ente/società vigilata della quale, appunto, l'OdV è "parte"*». Stando alla tesi qui criticata si verrebbe ad ammettere che una "parte" dell'organizzazione aziendale (cioè l'OdV) possa legittimamente utilizzare dati personali in autonomia, senza rispettare nè necessitare di istruzioni specifiche da parte del titolare e senza una propria qualificazione soggettiva: opzione, come visto, in contrasto con la legge.

Comparazione tra art. 29 ed art. 32(4) GDPR

Se, come visto, l'articolo 29 del GDPR non rappresenta una novità rispetto alla direttiva abrogata, la formulazione dell'articolo 32(4), invece, è di nuovo conio.

Da una lettura sommaria i testi delle due prescrizioni, considerata la loro accentuata somiglianza, apparirebbero quasi una duplicazione, frutto di una distrazione redazionale del legislatore. Per agevolarne la comparazione li riproduciamo di seguito:

Art. 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento	Articolo 32 - Sicurezza del trattamento
Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.	4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.

Articolo 32(4)

Dalla comparazione dei due testi normativi dell'articolo 29 e del paragrafo 4 dell'articolo 32 salta in evidenza che, nonostante l'accentuata somiglianza dei testi, essi contengono due distinti obblighi:

- l'articolo 29 impone ai soggetti che agiscono sotto l'autorità di titolare o responsabile (ed allo stesso responsabile) di utilizzare i dati personali di pertinenza del titolare solo dietro sue specifiche istruzioni (quindi, gli incaricati non possono utilizzare i dati personali senza o oltre tali istruzioni);
- il paragrafo 4 dell'articolo 32, invece, impone al titolare ed al responsabile di fare in modo che chiunque agisca sotto la loro autorità ed abbia accesso ai dati personali, vi provveda secondo le istruzioni ricevute dal titolare.

In conclusione,

- la prescrizione dell'articolo 29 è un obbligo di riservatezza indirizzato verso coloro che agiscono sotto l'autorità diretta di titolare o responsabile e che hanno accesso ai dati, imponendo loro di attenersi alle istruzioni impartite dal titolare;
- quella dell'articolo 32(4) è una misura organizzativa di sicurezza (tant'è che è inscritta nell'articolo 32, rubricato "Sicurezza del trattamento") che titolare e responsabile sono tenuti ad adottare.

Ruoli DP

In conclusione, i ruoli soggettivi in materia di protezione dei dati personali possono suddividersi nelle due categorie di:

- ruoli legali o statutari, cioè previsti specificamente dal GDPR (es. titolare, responsabile);
- ruoli discrezionali, cioè frutto dell'autonomia privata dell'imprenditore – sia esso titolare o responsabile del trattamento – nel disegno del proprio assetto organizzativo di presidio operativo di tale disciplina (ad es. comitato privacy, coordinatore privacy, data manager, ecc.).

La distribuzione degli ambiti di responsabilità per i ruoli legali è determinata dalla legge, mentre per i ruoli discrezionali la responsabilità rimane in capo al titolare ed al responsabile del trattamento; cioè i cosiddetti "ruoli discrezionali" non sono soggetti di imputazione giuridica, in quanto il loro operato sarà sempre riconducibile al titolare o al responsabile di pertinenza. Di conseguenza, l'eventuale trasgressione compiuta dal soggetto delegato potrà incidere sulla relazione contrattuale di lavoro che lega il delegato al proprio datore di lavoro (titolare o responsabile del trattamento) ma – in linea generale – non esonera da responsabilità il medesimo titolare o responsabile, di fronte alla legge ed agli eventuali danneggiati (v. art. 2049, c.c.).

Operazioni di trattamento svolte oltre le istruzioni del Titolare

Si è chiarito che chi fa parte dell'organizzazione aziendale del titolare o del responsabile del trattamento ed ha accesso ai dati personali può legittimamente farlo solo dietro specifiche istruzioni del titolare e, conseguentemente, si è criticata la tesi secondo cui l'OdV sarebbe parte dell'organizzazione dell'azienda vigilata che, in quanto tale, potrebbe accedere ai dati personali di sua pertinenza ma senza specifiche istruzioni. Rimane da chiarire quali siano le conseguenze giuridiche dell'accesso ai dati personali dell'azienda-titolare in assenza di istruzioni in tal senso.
Il combinato disposto degli articoli 29 e 32(4) del GDPR inducono a considerare le seguenti possibili conseguenze:

1. il soggetto che utilizza i dati personali senza istruzioni del titolare, lo fa per perseguire finalità e modalità del trattamento determinate in autonomia, assumendo quindi il ruolo di titolare autonomo, distinto dall'azienda-titolare di cui è parte;
2. l'azienda-titolare può essere ritenuta responsabile per violazione di sicurezza, non avendo fatto quanto necessario per adempiere all'obbligo ad essa rivolto dall'articolo 32(4).

In relazione alla prima conseguenza, l'OdV risulterebbe titolare del trattamento, contraddicendo le critiche sollevate nello studio, e dovrebbe rispondere a tutte le prescrizioni che il GDPR indirizza nei riguardo del titolare, trovandosi inevitabilmente in difetto per le precedenti omissioni.
Riguardo alla seconda conseguenza, anche l'azienda vigilata dall'OdV sarebbe in difetto perchè avrebbe consentito ad una "parte" della propria organizzazione di trattare dati personali di propria pertinenza senza che venissero impartite specifiche istruzioni, in violazione dell'articolo 32(4).

La "parte" priva di istruzioni è titolare autonoma

La conclusione cui si è giunti è che la "parte" dell'organizzazione aziendale del titolare del trattamento (quindi anche l'OdV) che utilizza dati personali di pertinenza dell'azienda, senza aver ricevuto specifiche istruzioni dal titolare, automaticamente si inquadra come titolare di un autonomo trattamento di cui determina finalità e modalità.
Questa conclusione è avvalorata, in via speculare, anche dalla definizione di "terzo" contenuta nel GDPR: «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento **e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile**» (enfasi aggiunta, art. 4, punto 10, GDPR). Quindi, gli "incaricati" sono gli unici che, insieme al responsabile del trattamento, sono "parte" del titolare e non rientrano nel campo d'applicazione delle particolari disposizioni relative ai terzi; per cui se non si è "incaricati" (cioè non si agisce in base alle specifiche istruzioni impartite dal titolare) si è, inevitabilmente, terzi (e non più "parte") con tutte le conseguenze che ne derivano secondo la disciplina data protection.
Ulteriore conferma a quanto qui sostenuto ci sembra venga da un esempio, che riportiamo di seguito, contenuto nel parere 1/2010 del Gruppo di lavoro dell'articolo 29 sui concetti di titolare e responsabile del trattamento, wp169, tuttora sostanzialmente valido.

Esempio n.4 del wp169

«*Esempio n. 4: Controllo segreto dei dipendenti*
Un membro del consiglio d'amministrazione di una società decide di controllare segretamente i dipendenti

dell'impresa, anche se tale decisione non è ufficialmente approvata dal consiglio d'amministrazione. La società deve essere considerata come il titolare del trattamento e deve far fronte agli eventuali ricorsi dei dipendenti i cui dati siano stati oggetto di utilizzo abusivo, nonché rispondere di ciò.
La responsabilità della società deriva in particolare dal fatto che, in quanto titolare del trattamento, è tenuta a garantire l'osservanza delle disposizioni in materia di sicurezza e riservatezza. Un utilizzo abusivo dei dati da parte di un dirigente dell'impresa o di un dipendente potrebbe essere considerato come la conseguenza di misure di sicurezza inadeguate. Tutto questo indipendentemente dal fatto che, in una fase ulteriore, anche il membro del consiglio d'amministrazione o altre persone fisiche all'interno della società possano essere considerate responsabili, sia civilmente – anche nei confronti dell'impresa –, sia penalmente. Ciò potrebbe accadere ad esempio se il membro del consiglio d'amministrazione usasse i dati raccolti per ottenere favori personali dai dipendenti: dovrebbe allora essere considerato come "titolare del trattamento" e rispondere di questo specifico utilizzo dei dati.».

Precedenti analoghi di soggetti "parte" che sono "titolari"

La conclusione che una "parte" dell'organizzazione dell'azienda titolare del trattamento – come nel caso dell'OdV – possa essere considerata come autonomo titolare non deve meravigliare. Vi sono altri esempi che militano in tal senso.

Medico competente

Il medico competente che svolge una specifica funzione all'interno della disciplina sulla sicurezza sul lavoro, anche se è legato all'azienda di riferimento tramite un rapporto di lavoro subordinato (cioè è un dipendente della stessa) assume il ruolo privacy di titolare autonomo per quanto attiene il trattamento di dati personali del personale aziendale ai fini della sorveglianza sanitaria e per la gestione della cartella sanitaria (v. Relazione annuale 2018 par. 13.1 e Provv. 13/12/2018, allegato 1 (doc. web n. 9068972) par. 1.1, lett. g)).

Possibili ruoli aggiuntivi dell'OdV

In definitiva, il ruolo "privacy" dell'OdV appare inquadrabile come quello di titolare autonomo riguardo alle attività tipiche di tale organismo effettuate mediante il trattamento di dati personali, in quanto in tale ambito l'OdV opera decidendo autonomamente su finalità (nel solco di quanto previsto dal d.lgs 231/2001) e modalità del trattamento di dati personali che utilizza nello svolgimento del proprio mandato.
Nulla esclude che il medesimo OdV, tuttavia, in relazione ad eventuali attività aggiuntive ed accessorie che lo vedessero coinvolto, potrà rivestire ruoli "privacy" diversificati, da valutare in base alle reali circostanze di fatto del caso specifico.

19.
Facebook condannata dall'antitrust tedesca per la politica sui dati

Con una propria decisione datata 6 febbraio 2019, l'autorità antitrust tedesca (Bundeskartellamt) ha imposto a Facebook stringenti restrizioni nella raccolta ed utilizzo dei dati degli utenti ritenendo che le attuali pratiche dell'azienda violino le regole della concorrenza.
La decisione, che non è definitiva in quanto è suscettibile di ricorso in appello presso l'Alta Corte Regionale di Dusseldorf, costituisce un ulteriore esempio delle forti interazioni tra i distinti domini della concorrenza, della tutela dei consumatori e del data protection.

Oggetto della decisione

Nella decisione del 6 febbraio 2019 (qui riportata in sintesi) il profilo in contestazione non ha riguardato le modalità d'uso delle informazioni raccolte dagli utenti del social network dopo che gli utenti si sono registrati; sotto questo profilo, l'autorità della concorrenza ha tenuto conto del fatto che una rete sociale finanziata pubblicamente ha bisogno di elaborare una grande quantità di dati personali.
Di converso, il Bundeskartellamt ha ritenuto che gli interessi degli utenti prevalgono sul modello di business basato sulla pubblicità personalizzata quando si tratta di accumulare dati da fonti esterne al social network, in particolare quando gli utenti hanno un controllo insufficiente sul trattamento dei loro dati e sulla loro correlazione ai loro account Facebook.
A questo proposito è interessante notare come su questo aspetto venga descritta dal Bundeskartellamt la linea di contatto tra il dominio antitrust e quello data protection: «*Per quanto riguarda questa parte del trattamento dei dati, è stato necessario intervenire dal punto di vista del diritto della concorrenza perché i limiti di protezione dei dati stabiliti nel GDPR sono stati chiaramente superati, anche in considerazione della posizione dominante di Facebook.*».

Modello di business di Facebook

L'uso privato di Facebook.com è subordinato alla registrazione dell'utente, con la creazione di un proprio profilo. Usando il loro vero nome, gli utenti possono inserire informazioni su se stessi e sulla loro situazione personale e impostare un'immagine del profilo. Sulla base di queste informazioni, viene creato un sito personalizzato per ciascun utente. Facebook finanzia il suo social network attraverso la pubblicità online offerta agli editori e ad altre aziende. Gli annunci corrispondono al profilo individuale dell'utente del social network. L'obiettivo è di presentare agli utenti annunci potenzialmente interessanti per loro in base al loro comportamento commerciale personale, ai loro interessi, al potere d'acquisto e alle condizioni di vita ("targeting" o "pubblicità mirata").

Fonti terze rispetto a Facebook.com

In aggiunta ai dati degli utenti che si registrano sulla piattaforma del social network, Facebook accumula altri dati dei medesimi utenti provenienti da fonti ulteriori come:

- **altri servizi di proprietà di Facebook** come Instagram o WhatsApp;
- **siti di terze parti** che includono interfacce come i pulsanti "Mi piace" ("Like") o "Condividi" ("Share"). Laddove tali interfacce visibili sono incorporate in siti Web e app, il flusso di dati su Facebook inizierà già quando questi vengono richiamati o installati. Non è nemmeno necessario, ad es., scorrere o fare clic su un pulsante "Mi piace": basterà richiamare un sito Web con un pulsante "Mi piace" incorporato per avviare in automatico il flusso di dati verso Facebook. Spesso non occorre che il simbolo di Facebook

sia visibile agli utenti di un sito Web, in quanto i dati degli utenti potranno ugualmente essere trasmessi da molti siti Web a Facebook, come nel caso in cui il sito Web utilizzi il servizio "Facebook Analytics" in background per eseguire analisi degli utenti.

Posizione dominante di Facebook

Il Bundeskartellamt ha rilevato che a fine 2018 Facebook aveva una posizione dominante sia sul mercato globale sia su quello tedesco, dove la propria quota di mercato risultava superiore al 95% (utenti attivi giornalieri) e ad oltre l'80% (utenti attivi mensili).

Fondamento giuridico della decisione

Nella valutazione dell'autorità, la condotta di Facebook rappresenta un abuso di sfruttamento della propria posizione dominante. Questa valutazione si pone nel solco della giurisprudenza della Corte federale di giustizia, secondo cui non solo i prezzi eccessivi, ma anche i termini e le condizioni contrattuali inadeguati costituiscono un abuso di sfruttamento di posizione dominante (i cosiddetti termini commerciali di sfruttamento). Quindi, le aziende dominanti non possono usare pratiche di sfruttamento a discapito della controparte del mercato, cioè in questo caso i consumatori che usano Facebook, specie se la pratica dello sfruttamento rappresenta un ostacolo per i concorrenti che non sono in grado di accumulare un analogo così vasto tesoro di dati.

Conclusioni della decisione

A conclusione del procedimento iniziato nel marzo 2016, il Bundeskartellamt ha proibito a Facebook Inc., USA, Facebook Ireland Ltd., Irlanda e Facebook Germany GmbH, di utilizzare il social network Facebook (Facebook.com) riguardo a utenti privati residenti in Germania, che utilizzano anche i servizi aziendali WhatsApp, Oculus, Masquerade e Instagram, subordinando tale utilizzo – senza il consenso degli utenti – alla raccolta da parte di queste società di dati, relativi all'utente ed ai dispositivi, e combinando tali informazioni con gli account utente di Facebook.com. Il Bundeskartellamt evidenzia come non esista un consenso effettivo alla raccolta delle informazioni degli utenti «*se il loro consenso è un prerequisito per l'utilizzo del servizio Facebook.com*». Considerato il superiore potere di mercato di Facebook, «*un segno di spunta obbligatorio sulla casella per accettare i termini di utilizzo della società non è una base adeguata per un trattamento così intenso dei dati. L'unica scelta che l'utente ha è di accettare la combinazione completa di dati o di astenersi dall'utilizzare il social network. In una situazione così difficile, la scelta dell'utente non può essere definita consenso volontario*». In conclusione, l'addebito del Bundeskartellamt muove dalla considerazione che (1) la posizione dominante di Facebook.com (2) in aggiunta alla prassi della raccolta e utilizzo "forzosi" dei dati personali dei suoi utenti (3) ed all'aggregazione di tali dati con quelli desunti dagli altri servizi aziendali di WhatsApp, Oculus, Masquerade e Instagram, rappresenta uno sfruttamento abusivo di posizione dominante a danno dei consumatori e dei concorrenti.

Antitrust italiana contro Facebook per raccolta di dati degli utenti

Come indicato nell'Alert del 13 dicembre 2018, cui si rinvia, anche l'Autorità Garante della Concorrenza e del Mercato (l'italiana "Agcm") aveva comminato due sanzioni per complessivi 10 milioni di euro nei confronti di Facebook Ireland Ltd. e della sua controllante Facebook Inc. per presunte violazioni del codice del consumo (articoli 21 e 22).

L'addebito mosso a Facebook consisteva nell'aver **indotto ingannevolmente** gli utenti consumatori a ritenere che la fornitura del servizio di social network fosse gratuito; di converso, la registrazione alla piattaforma Facebook, in fase di attivazione dell'account, determinava un'attività di raccolta, con intento commerciale, dei dati forniti dall'utente, senza che questi fosse informato adeguatamente ed immediatamente.
In aggiunta, l'Agcm aveva contestato a Facebook l'attuazione di una **pratica aggressiva** (in violazione degli articoli 24 e 25 del cod. consumo) in quanto l'azienda esercitava «*un indebito condizionamento nei confronti dei consumatori registrati, i quali subiscono, senza espresso e preventivo consenso – quindi in modo inconsapevole e automatico – la trasmissione dei propri dati da Facebook a siti web/app di terzi, e viceversa, per finalità commerciali. L'indebito condizionamento deriva dall'applicazione di un meccanismo di preselezione del più ampio consenso alla condivisione di dati.*» (Comunicato stampa Agcm).

Uso dei dati tra disciplina concorrenziale e tutela dei consumatori

Come si nota dalle due vicende sopra riportate, la medesima prassi commerciale (la raccolta di dati personali da più fonti, senza un'adeguata informativa ed un libero consenso degli interessati) provoca violazioni nei tre distinti ma correlati domini della disciplina della concorrenza, della tutela dei consumatori e della tutela dei dati personali.
Come dichiarato dal presidente del Bundeskartellamt, Andreas Mundt, «*I dati oggi sono un fattore decisivo nella competizione. Nel caso di Facebook sono il fattore essenziale per stabilire la posizione dominante dell'azienda. (...) Pertanto, proprio nel settore della raccolta dei dati e dell'uso dei dati, Facebook, in quanto società dominante, deve rispettare le norme e le leggi applicabili in Germania e in Europa.*».

20.
Finalità del trattamento tra principi di liceità e basi giuridiche – Prima parte

Il dominio della protezione dei dati personali è una sorta di margherita che si suole esaminare, in prevalenza, prendendo in considerazione i vari petali che la compongono, lasciando sullo sfondo il cuore della corolla che è alla base dell'intera struttura.
Istituti come l'informativa ed il consenso, la valutazione dei rischi e quella di impatto, la mappatura dei trattamenti e la gestione del data breach, sono senza dubbio rilevanti ma occorrerebbe tener presente che essi sono l'espressione funzionale di principi e regole generali che costituiscono il cuore della struttura regolatoria.
Così come un petalo non può essere esaminato correttamente prescindendo dalla struttura di cui fa parte, allo stesso modo, l'analisi di istituti, ruoli soggettivi e prescrizioni di dettaglio della disciplina sulla protezione dei dati personali non può prescindere da una corretta comprensione della piattaforma strutturale di riferimento su cui questi stessi traggono fondamento.
La puntata odierna vuole essere la prima di una serie volta ad identificare gli elementi della piattaforma di base della disciplina di riferimento.

Sintesi

I principi di liceità (art. 5) e le basi giuridiche (art. 6) trovano applicazione per qualsiasi trattamento di dati personali, salvo limitate deroghe. Ogni trattamento deve rispettare questi principi e deve poter trovare giustificazione in un determinato fondamento giuridico, tra quelli elencati all'articolo 6. Successivamente, "il perchè" i dati vengono utilizzati (la cosiddetta "finalità") indirizza la disciplina applicabile al caso specifico, la quale in seconda battuta subisce correttivi ed adeguamenti in relazione alla natura dei dati ed alla tipologia di interessati oggetto di trattamento.

Elementi della piattaforma regolatoria

Uno sguardo generale della complessa disciplina sulla protezione dei dati personali pone in evidenza come essa sia strutturata su più livelli: talune "regole" – essenzialmente posizionate nella parte iniziale del GDPR – hanno valore generale e si applicano pressoché indistintamente a qualunque tipologia di trattamento e di contesto: queste "regole" di primo livello sono, ad esempio, i principi di liceità (art. 5) e le basi giuridiche (art. 6). Le ulteriori "regole", invece, appaiono di un livello subordinato al precedente, ne sono l'implementazione attuativa e variano in base alle specifiche caratteristiche del trattamento e del contesto (ad esempio, informativa, consenso, valutazioni varie, misure tecnico-organizzative, ecc.).

Principi, basi giuridiche e finalità

Guardando all'intera disciplina sui dati personali tramite una visione d'insieme, viene in evidenza che gli elementi di quella che sopra si è chiamata "piattaforma strutturale", sono i principi di liceità (art. 5) e le basi giuridiche (art 6). Di converso, la finalità del trattamento è il criterio guida che indirizza l'applicazione concreta di "principi" e "basi giuridiche" nei rispettivi contesti – cioè l'applicazione delle regole di secondo livello.
Alcuni esempi possono meglio chiarire il concetto: l'informativa (artt. 13 e 14, GDPR) è lo strumento giuridico (di secondo livello) che dà attuazione pratica al principio di trasparenza (di primo livello); l'informativa subisce variazioni anche significative, in dipendenza delle finalità e modalità del trattamento. Analogamente, le prescrizioni che fanno riferimento ad obblighi

di valutazione (es. la valutazione d'impatto) sono espressione del principio di accountability, anch'esse sono strettamente correlate alle finalità e modalità del trattamento, tanto che queste ultime ne possono persino determinare l'obbligatorietà o meno.

Centralità della finalità nella disciplina data protection

Se, da un lato, principi e basi giuridiche sono le regole di primo livello essenzialmente applicabili a qualsiasi trattamento, la finalità dello stesso (cioè a quale fine si utilizzano i dati: come nel caso di esigenze di gestione del personale o per promozione commerciale o per l'esecuzione di un contratto) rappresenta il principale parametro di contesto per l'adeguamento di tali regole; cioè la finalità del trattamento consente di adattare le regole attuative dei principi e delle basi giuridiche, in rapporto all'impatto che tale utilizzo di dati possa provocare in relazione ai diritti ed alle libertà degli interessati.

Nozione di finalità

La finalità è lo scopo del trattamento, la sua "ragion d'essere", essa risponde alla domanda sul "perchè" determinate categorie di dati personali riferite ad altrettanti interessati siano utilizzate dal soggetto che ne dispone. Finalità e modalità del trattamento identificano il titolare, cioè il soggetto cui sono primariamente indirizzate le prescrizioni del GDPR come primo soggetto responsabile del corretto utilizzo dei dati personali a tutela dei diritti e delle libertà degli interessati.

Finalità in relazione alla titolarità

È titolare chi ha il potere di adottare le decisioni in merito alle motivazioni di fondo, allo scopo ultimo dell'utilizzo dei dati personali.
Invero, la definizione di titolare collega tale posizione anche al potere di determinare le modalità del trattamento; recita la definizione dell'articolo 4, è titolare chi «*singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*».

Riferimento ai "mezzi"

Il parere 1/2010 (wp169) del Gruppo di lavoro dell'articolo 29, tuttora valido anche dopo la piena applicazione del GDPR, evidenzia che «*(l)a determinazione degli "strumenti"* (il precedente termine della direttiva sostituito dal GDPR con quello di "mezzi", nda) *ingloba quindi questioni sia tecniche che organizzative la cui decisione può anche essere delegata ai responsabili del trattamento (ad es. "quale hardware o software utilizzare?"), nonché elementi essenziali tradizionalmente e intrinsecamente riservati al titolare del trattamento, come "quali dati trattare?", "per quanto tempo trattarli?", "chi vi ha accesso?", e così via. In questo contesto, mentre la determinazione della finalità del trattamento farebbe scattare in ogni caso la qualifica di titolare del trattamento, la determinazione dei mezzi implicherebbe una titolarità solo qualora riguardi gli aspetti fondamentali dei mezzi. In tale ottica, è del tutto possibile che i mezzi tecnici ed organizzativi siano determinati esclusivamente dal responsabile del trattamento.*».

Finalità come elemento individualizzante la titolarità

Il criterio identificativo della titolarità, di conseguenza, si desume dal potere di determinare la finalità del trattamento, come emerge dal medesimo documento wp169 del WPArt29 in cui si legge che «*quando le finalità sono chiaramente definite, ma vi sono pochi orientamenti, se non nessuno, quanto*

ai mezzi tecnici ed organizzativi – gli strumenti dovrebbero rappresentare una ragionevole via per realizzare la o le finalità perseguite e il titolare del trattamento dei dati dovrebbe essere pienamente informato in merito. Se un contraente influisce sulla finalità del trattamento e lo effettua (anche) a proprio beneficio – usando ad esempio, i dati personali ricevuti per generare servizi a valore aggiunto –, si renderebbe allora titolare (o eventualmente co-titolare) del trattamento per un'altra attività di trattamento, e sarebbe quindi soggetto a tutti gli obblighi della normativa applicabile in materia di protezione dei dati.».

Finalità come elemento qualificante il trattamento

Sebbene la definizione del termine "trattamento" contenuta nel GDPR (come in origine nella direttiva 95/46/CE) fa solo riferimento a «*qualsiasi operazione o insieme di operazioni (...) applicate a dati personali*», in realtà, le differenti tipologie di trattamento si distinguono tra loro soprattutto in virtù della pertinente finalità perseguita. In particolare, è la finalità l'elemento che maggiormente qualifica la tipologia di trattamento, anche rispetto ad ulteriori elementi rilevanti come la natura dei dati personali (ad es. se comuni o sensibili o giudiziari o comunque particolarmente delicati in relazione agli interessati) o la categoria di soggetti interessati coinvolti (ad es. se soggetti vulnerabili o meno). I seguenti profili sono testimonianza della centralità della finalità in relazione al trattamento.

L'esplicitazione della finalità contribuisce alla trasparenza (la finalità deve essere esplicita), la sua specificità contribuisce alla certezza del diritto e alla prevedibilità (essa deve essere specifica) e, infine, la sua liceità contribuisce alla liceità del trattamento. D'altro canto, il divieto di perseguire finalità incompatibili con quella originaria della raccolta dei dati mira a proteggere l'interessato impostando dei limiti su come i titolari possano legittimamente utilizzare i suoi dati e a rafforzare la correttezza del trattamento. La limitazione della finalità evita che i dati possano essere utilizzati in modo «*inaspettato, inappropriato o altrimenti discutibile*».

Principio di limitazione della finalità

La finalità è in stretta correlazione con il trattamento; il nesso "trattamento-finalità" è tanto rilevante da sostanziare il principio "di limitazione della finalità". In base a tale principio ogni trattamento deve riferirsi ad una finalità specifica, in quanto i limiti sulle modalità d'uso dei dati personali da parte dei titolari rappresentano una garanzia per i soggetti interessati. Come rilevato nel parere 3/2013 del WPArt29 (wp203) «*(i)l principio di limitazione delle finalità ha due componenti principali: i dati personali devono essere raccolti per scopi "specificati, espliciti e legittimi" (specifica degli obiettivi) e non essere "ulteriormente trattati in modo incompatibile" con tali scopi (uso compatibile).*». Quindi, è vietato per il titolare perseguire col trattamento una finalità diversa ed incompatibile con quella specificata al momento della raccolta perchè tale alterazione vanificherebbe le determinazioni dell'interessato in merito al trattamento ed il potere di controllo sull'uso dei propri dati.

Finalità come parametro per la disciplina applicabile

La finalità consente di inquadrare il trattamento nella cornice della disciplina pertinente – come avviene distinguendo un trattamento per finalità di marketing rispetto ad uno analogo per finalità amministrativo-contabili; d'altro canto, i riferimenti alla natura dei dati ed alla categoria di interessati coinvolti, forniscono importanti informazioni di dettaglio di quel medesimo trattamento che possono incidere anche pesantemente sulla disciplina applicabile, senza tuttavia

ribaltarla: un trattamento per finalità di marketing sarà sempre tale e come tale sarà valutato, pur se dovesse riguardare speciali categorie di dati (come per i dati sanitari) eventualmente riferiti a categorie vulnerabili di soggetti (come nel caso di pazienti). Categorie di dati e di interessati potranno incidere sulle regole attuative dei principi (ad esempio imponendo interpretazioni restrittive dei principi di necessità e pertinenza o di minimizzazione) o sulle condizioni richieste per il trattamento (come quelle dettate dagli articoli 8-10 del GDPR) ma non modificheranno la tipologia del trattamento come determinata dalla corrispondente finalità.

Finalità e principi

In conclusione, la finalità non è un mero elemento descrittivo del trattamento ma vincola lo stesso ad una determinata disciplina, a tutela degli interessati.

Come precisato dal citato documento wp263, «*la specifica della finalità è un prerequisito per l'applicazione di altri requisiti di qualità dei dati, tra cui l'adeguatezza, la pertinenza, la proporzionalità e l'accuratezza dei dati raccolti e i requisiti relativi al periodo di conservazione dei dati.*». I soggetti di solito hanno un'aspettativa su come i dati saranno utilizzati in relazione agli scopi specificati e realmente perseguiti, per cui è giusto onorare queste aspettative e «*preservare la fiducia e la certezza del diritto, motivo per cui la limitazione delle finalità è una salvaguardia così importante, una pietra angolare della protezione dei dati*».

21.
Clausole contrattuali tipo: deciderà la GGUE

Il 31 maggio 2019 la Corte Suprema dell'Irlanda ha respinto l'appello avanzato da Facebook contro la decisione dell'Alta Corte irlandese di rinviare alla Corte di Giustizia dell'UE la decisione sulla validità giuridica delle attuali clausole contrattuali tipo ("SCC"), approvate dalla Commissione UE come adeguato strumento di garanzia nei flussi di dati personali verso paesi esteri privi di una protezione adeguata.

SCC

Le cosiddette "clausole contrattuali standard" (o "SCC") sono le clausole tipo di protezione dei dati personali adottate dalla Commissione che hanno lo scopo di vincolare contrattualmente il soggetto importatore dei dati all'adozione di tutele adeguate sui dati trasmessi; esse, pertanto, si sostituiscono alle prescrizioni del GDPR che non sono applicabili nel paese di destinazione. La sottoscrizione delle SCC rappresenta una garanzia adeguata sulla cui base il trasferimento di dati personali, anche verso paesi privi di sistemi di protezione legale comparabili a quello dell'Unione, risulta comunque valido giuridicamente [art. 25(6) dir. 95/46/CE e 46(2)(c) GDPR] .
Attualmente, sono classificati come SCC tre distinti modelli di clausole veicolati mediante altrettante decisioni della Commissione:

- **2001/497/EC** del 15 giugno 2001 (per i **trasferimenti tra titolari** del trattamento);
- **2004/915/EC** che modifica la decisione 2001/497 riguardo all'introduzione di un set alternativo di clausole contrattuali per il trasferimento di dati personali verso paesi terzi (**trasferimenti tra titolari**);
- **2010/87/EU** del 5 febbraio 2010 relativamente a clausole contrattuali tipo per il trasferimento di dati personali a responsabili del trattamento stabiliti in paesi terzi (**trasferimenti titolare-responsabile**).

SCC 2010/87/EU

Sebbene tutte e tre le decisioni della Commissione hanno formato oggetto delle contestazioni dinanzi all'Alta Corte irlandese, questo giudice ha rilevato che il casi specifico riguardava la sola decisione del 2010 in quanto Facebook aveva dichiarato in giudizio che il trasferimento dei dati personali del Sig. Schrems dall'Irlanda (cioè da Facebook Ireland Ltd) agli Stati Uniti (Facebook Inc.) avveniva sulla base di quest'unico strumento di garanzia.
Di conseguenza, il rinvio dei quesiti alla CGUE riguarderà solo lo strumento delle clausole tipo 2010/87/EU (cioè quello dei trasferimenti tra titolari stabiliti sul territorio UE e responsabili del trattamento stabiliti fuori dalla UE), anche se non è difficile immaginare che le decisioni adottate dalla Corte avranno immediate ripercussioni anche sugli altri due modelli tipo.

Iter giudiziario

La decisione della Corte Suprema irlandese ha riguardato l'appellabilità della decisione dell'Alta Corte di rinviare l'analisi di undici quesiti alla CGUE.
In precedenza, infatti, il Sig. Schrems – cittadino austriaco – aveva avanzato un reclamo dinanzi l'autorità di supervisione irlandese per la protezione dei dati personali ("ASN"), lamentando che gli strumenti delle SCC non fossero validi giuridicamente in quanto non avrebbero assicurato un'adeguata protezione (si veda in seguito). La contestazione si fondava sul fatto che il Sig. Schrems, essendo utente del social di Facebook, vedeva i propri dati personali pertinenti,

trasferiti dalla UE (in particolare da Facebook Ireland Ltd., società di gestione del social per l'area europea) verso gli Stati Uniti (cioè a Facebook Inc., casa-madre americana) sulla base della garanzia dello strumento delle clausole contrattuali tipo 2010/87/EU. Le contestazioni del Sig. Schrems sono state successivamente condivise dall'ASN, quindi, la decisione dell'autorità è stata vagliata dall'Alta Corte la quale, ritenendo la materia di competenza unionale, ha disposto il rinvio alla CGUE.
Contro tale decisione di rinvio, Facebook ha proposto appello alla Corte Suprema che ha emesso la decisione qui esaminata.

Schrems I

La vertenza sulla validità delle SCC prende le mosse dalla vicenda che ha portato all'invalidazione dell'analogo strumento chiamato "Safe Harbour" a seguito della sentenza della CGUE nella causa Schrems / Commissione per la protezione dei dati (causa C-362/14) ("Schrems I").

Contestazione sul Safe Harbour

Anche in quella circostanza il Sig. Schrems contestava la validità del cosiddetto accordo "Safe Harbor" stipulato tra l'Unione europea e gli Stati Uniti d'America. In breve, nella sua decisione del 26 luglio 2000 (2000/520/CE) ("Decisione sull'Approdo Sicuro"), la Commissione europea aveva stabilito, in conformità dell'articolo 25, paragrafo 6, della direttiva 95/46/CE, che si sarebbe ottenuto un livello adeguato di protezione in relazione ai dati trasferiti dall'UE a un'organizzazione stabilita negli Stati Uniti, qualora tale organizzazione si fosse conformata ai principi stabiliti nella Decisione sull'approdo sicuro ed avesse auto-dichiarato di essere conforme a tali principi.
In quel precedente, il Sig. Schrems si era lamentato del fatto che, alla luce delle rivelazioni riguardanti la sorveglianza da parte delle agenzie di sicurezza statunitensi (in particolare l'Agenzia per la sicurezza nazionale ("NSA")) di dati trasferiti dall'UE a organizzazioni con sede negli Stati Uniti, non vi era alcuna protezione significativa negli Stati Uniti, di diritto o nella pratica, relativi ai dati così trasferiti.

Decisione dell'autorità irlandese

Interessante rilevare che nel precedente Schrems I, la ASN irlandese aveva inizialmente ritenuto la denuncia "frivola e vessatoria". Di conseguenza, evidenziando di non avere giurisdizione per valutare la validità degli accordi Safe Harbor, si avvalse dei poteri discrezionali conferitile dal Data Protection Act del 1988, e decise di non procedere a un'indagine formale completa della denuncia, in quanto essa stessa vincolata dalla Decisione sull'Approdo Sicuro.
Contro la decisione dell'ASN, il sig. Schrems ricorse all'Alta Corte e quest'ultima fece rinvio alla CGUE.

Invalidazione del Safe Harbour

In particolare, la CGUE ritenne che la Decisione sull'Approdo Sicuro non fosse valida, sancendo il principio per cui quando «*l'autorità nazionale di supervisione ritiene che le obiezioni avanzate dalla persona che ha presentato un reclamo relativo alla protezione dei suoi diritti e delle sue libertà in relazione al trattamento dei suoi dati personali siano fondate, tale autorità deve (...) avere la possibilità di avviare un procedimento giudiziario.*

Spetta al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di supervisione interessata di presentare le obiezioni che essa ritiene siano ben fondate di fronte ai giudici nazionali, in modo che questi ultimi, se condividono i suoi dubbi sulla validità della decisione della Commissione» possano rinviare la questione al giudizio della CGUE.

Privacy Shield

A seguito della decisione di invalidazione del Safe Harbour ed al fine di sostituire lo strumento di garanzia con altro giuridicamente valido, la Commissione – con decisione di esecuzione (UE) 2016/1250 del 12 luglio 2016 – riconosce l'adeguatezza della protezione fornita dallo Scudo Privacy tra UE-U.S. (di seguito "Decisione sullo Scudo Privacy").

Secondo il Considerando 14 di tale decisione «*(l)o scudo UE-USA per la privacy si fonda su un sistema di autocertificazione in base al quale l'organizzazione statunitense s'impegna a rispettare un insieme di principi in materia di privacy, ossia i principi del regime dello scudo UE-USA per la privacy, comprensivi dei principi supplementari (collettivamente denominati qui di seguito «principi»), emanati dal Dipartimento del Commercio degli USA e riportati nell'allegato II della presente decisione. Lo scudo si applica sia ai titolari sia ai responsabili del trattamento (procuratori), con la specificità che un contratto deve vincolare il responsabile del trattamento ad agire esclusivamente secondo le istruzioni del titolare del trattamento dell'UE e a prestargli assistenza per rispondere alle persone che esercitano i loro diritti nell'ambito dei principi*».

Schrems II: oggetto della contestazione

Le contestazioni avanzate da Max Schrems ed avallate dall'ASN irlandese nella vicenda Schrem II sono sostanzialmente riferite ai seguenti aspetti:

1. **Trattamento indiscriminato e su larga scala di dati personali** - Le agenzie statunitensi sono coinvolte in "trattamenti indiscriminati su larga scala" di dati consistenti nella ricerca su larga scala di comunicazioni. Secondo Schrems, la totalità dei dati personali che passano attraverso la rete di comunicazione negli Stati Uniti è resa disponibile direttamente alle agenzie governative degli Stati Uniti, sia per consultazione, ricerca o altro.
2. **Sorveglianza legale se non vietata** - La sorveglianza da parte del governo degli Stati Uniti dei dati di cittadini non statunitensi è "legale se non espressamente vietata". Questa considerazione sarebbe basata sulla valutazione dell'Alta Corte secondo cui «*(g)li esperti hanno identificato il Quarto Emendamento della Costituzione come la protezione più importante contro la sorveglianza illegale del governo. Il Quarto Emendamento si applica alle perquisizioni e ai sequestri che avvengono negli Stati Uniti (come i dati trasferiti negli Stati Uniti). L'ipotesi prevalente è che, allo stato attuale della legge, i cittadini non UE privi di una sostanziale connessione volontaria con gli Stati Uniti (come la maggior parte dei cittadini dell'UE) non possono presentare un caso basato sul Quarto Emendamento.*». Cioè la maggiore tutela giuridica contro abusi governativi in tema di sorveglianza non sarebbe disponibile alla maggior parte dei cittadini UE.
3. **Limitazione non proporzionata al diritto di difesa** - Vi sono preoccupazioni fondate sul fatto che le limitazioni all'esercizio del diritto a un ricorso effettivo da parte degli interessati dell'UE negli Stati Uniti non siano proporzionate e/o non siano strettamente necessarie ai sensi dell'articolo 52, paragrafo 1, della Carta.

Inferenza tra Privacy Shield e SCC

Tra i quesiti posti all'esame della CGUE vi è quello della possibile inferenza del Privacy Shield sulle clausole tipo; ci si chiede se sulla base della procedura di attestazione dell'adeguatezza da parte della Commissione, la decisione sullo Scudo per la privacy costituisca una constatazione di applicazione generale, vincolante per le autorità di protezione dei dati e i tribunali degli Stati membri, secondo cui gli Stati Uniti garantirebbero un livello adeguato di protezione ai sensi dell'articolo 25, paragrafo 2, della direttiva, in ragione della legislazione nazionale statunitense o degli impegni internazionali assunti dagli USA.

Il quesito è stato portato all'attenzione della CGUE in quanto sebbene la Decisione relativa allo Scudo per la privacy non contenga un'attestazione generale dell'adeguatezza della legge statunitense, il giudice irlandese di prima istanza ha concluso che la rilevanza della Decisione dello scudo per la privacy nei confronti delle SCC non è chiara.

Va sottolineato, in ogni caso, che Facebook non ha fatto affidamento sulla Decisione dello scudo per la privacy per trasferire i dati a Facebook Inc. negli Stati Uniti, in quanto i trasferimenti di dati sono stati effettuati in base alle decisioni SCC. In virtù di ciò, l'ASN irlandese ha evidenziato che la Decisione sullo Scudo per la privacy non ha alcuna applicazione alla vicenda in oggetto.

L'interrogativo sulla possibile inferenza del Privacy Shield sulle SCC – riguardando misure del diritto dell'UE – è in ogni caso di stretta competenza della CGUE.

Legge applicabile: Direttiva 95/46/CE

Per entrambi i casi Schrems I e Schrems II la legge applicabile di riferimento è la Direttiva 95/46/CE in quanto i quesiti pertinenti si riferiscono al periodo antecedente alla data di piena applicazione del GDPR.

Dubbi di legittimità data protection da parte del giudice

Come detto in precedenza, la decisione della GGUE sul caso Schrem I, ha chiarito che «s*petta al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di supervisione interessata di presentare le obiezioni che essa ritiene siano ben fondate di fronte ai giudici nazionali, in modo che questi ultimi, se condividono i suoi dubbi sulla validità della decisione della Commissione*» possano rinviare la questione al giudizio della CGUE».

Di conseguenza, spetta al giudice di prima istanza, e solo ad esso, decidere se fare un rinvio e, in effetti, se ritirare o emendare lo stesso.

Come evidenziato dalla Corte Suprema irlandese, «*(l)a ragione della necessità di tale procedura era, naturalmente, che nessun tribunale nazionale ha la competenza per invalidare una misura del diritto dell'Unione, perchè quel potere è riservato alla CGUE. Ne è conseguito che era necessario un meccanismo in base al quale i casi di dubbio potessero essere rinviati all'unico tribunale (che è la CGUE) che aveva la giurisdizione di invalidare la misura del diritto dell'Unione, qualora convinto che la misura in questione risultasse illegale.*».

Giurisdizione esclusiva della CGUE

Poichè la CGUE gode di competenza esclusiva a decidere su questioni di pertinenza del diritto dell'Unione, alla fine spetterà alla CGUE determinare il modo in cui affrontare le questioni sollevate dall'Alta Corte irlandese (la Corte Suprema ha infatti sollevato il dubbio sull'effettiva necessità di tutte le 11 domande inoltrate), nonchè determinare se le Decisioni SCC in generale

o, in particolare, la Decisione del 2010 sono valide, «*poiché la CGUE è l'unico tribunale competente a prendere una tale decisione*».

Tipi di rinvio alla CGUE

Nell'affrontare l'ammissibilità dell'appello sulla decisione di rinvio alla CGUE, la Corte Suprema irlandese ha sottolineato come si possano distinguere due tipi di rinvio:

- quello in cui il profilo di diritto comunitario influenza la decisione di merito sottoposta al giudizio della corte nazionale di merito;
- quello in cui il quesito sottoposto alla CGUE esaurisce la materia del contendere.

Rinvio strumentale all'azione

Il motivo per cui potrebbe essere richiesto un rinvio alla CGUE potrebbe consistere nella circostanza che la questione portata all'attenzione dei giudizi di merito dello Stato membro, possa essere concessa o rifiutata (o, ove concessa, essere riconosciuta in modo appropriato) dipendendo almeno in parte da una questione contestata del diritto dell'Unione, la cui risoluzione sia necessaria per la determinazione definitiva del procedimento. Come rilevato dalla Corte Suprema irlandese, «*in tali casi, il rinvio è semplicemente un mezzo per consentire al giudice nazionale di esercitare la propria giurisdizione per rilasciare una decisione appropriata nei procedimenti di cui è intestatario*.»
Spetta al giudice nazionale di riferimento determinare i fatti e giungere a una conclusione in merito alla questione se condivida le preoccupazioni dell'ASN. Una tale determinazione dei fatti (o della legge nazionale, se pertinente) formulata da un giudice nazionale è una "decisione" che può essere oggetto di appello. «*La CGUE non emette alcun ordine che vincoli le parti del procedimento ma piuttosto, fornisce orientamenti vincolanti al giudice nazionale sulla corretta interpretazione di qualsiasi misura pertinente del diritto dell'Unione in modo da consentire a tale giudice nazionale di determinare correttamente il procedimento conformemente al diritto dell'Unione e al medesimo giudice nazionale di rendere qualsiasi ordine vincolante per le parti derivante da tale determinazione.*
In tali casi, la questione tornerà sempre al giudice nazionale per la pronuncia della decisione appropriato.».

Rinvio che combacia con l'azione

In una differente categoria rientrano i casi in cui la questione di merito si esaurisce – come nella vicenda Schrems – nel giudizio di validità di una misura dell'Unione.
In tali evenienze, la posizione assunta dalla CGUE consisterà nel giudicare queste misure valide o invalide, tant'è che i giudici nazionali non avranno alcun ruolo ulteriore dovendo limitarsi a recepire le conclusioni della Corte di giustizia sul punto.
Si pensi al caso in cui non vi sia controversia tra le parti sui fatti e sui principi pertinenti del diritto nazionale, laddove l'unica "decisione" formulata dal giudice nazionale sia quella di rinvio alla CGUE insieme alla determinazione della forma delle domande da porre alla Corte.

Appello delle decisioni di rinvio

Nel caso in cui la decisione del giudice nazionale non riguardi la valutazione dei fatti, ma la mera decisione di rinvio alla CGUE, questa non sarebbe appellabile in quanto, altrimenti, si arriverebbe ad ammettere l'appello sul rinvio. In Schrem I l'unica funzione del giudice nazionale era quella di determinare se esso condivideva i dubbi di validità prospettati dall'ASN relativamente al Safe

Harbour; in caso affermativo, il giudice locale era tenuto a rinviare la questione alla CGUE.
Di converso, l'eventuale decisione del giudice nazionale di non rinviare alla CGUE sarebbe comunque suscettibile di appello della parte interessata.

Conclusioni

Con questo ultimo passo della Corte Suprema irlandese ora tocca alla CGUE esprimersi in merito alla validità delle attuali SCC. È presumibile che la decisione – stando anche al precedente Schrems 1 – avrà esito negativo finendo coll'invalidare gli attuali modelli tipo. In tale evenienza si prospetterebbe un grave vuoto giuridico che occorrerebbe colmare il più rapidamente possibile da parte della Commissione; le SCC attualmente rappresentano una delle più agevoli misure di salvaguardia per la legittimazione dei flussi transfrontalieri di dati personali verso paesi non inclusi nella lista bianca di quelli a protezione "adeguata".

22.
Cybersecurity Act

Il 7 giugno 2019 la Gazzetta Ufficiale della UE ha pubblicato il regolamento comunemente denominato Cybersecurity Act o "Regolamento sulla cybersicurezza" (Regolamento (UE) 2019/881 del 17 aprile 2019).
Questo intervento, a livello di quadro generale sulla sicurezza di internet in ambito unionale, completa precedenti azioni della UE in questo ambito, come la direttiva NIS (direttiva (UE) 2016/1148) ed il GDPR (regolamento (UE) 2016/679).

Sintesi

L'Unione europea ha approvato il cosiddetto Cybersecurity Act che introduce un complessivo quadro normativo per armonizzare la politica di resilienza da attacchi cibernetici in tutto il territorio europeo. A questo fine, il regolamento interviene su due versanti principali:

- **il primo**, rinnovando il ruolo ed il mandato conferito all'agenzia europea **ENISA** che, d'ora in poi, sarà un centro di competenza permanente sul tema e fornirà supporto agli Stati membri nell'implementazione delle relative politiche di sicurezza;
- **il secondo**, mediante la istituzione di un **processo di certificazione europeo sulla sicurezza cibernetica**, riconosciuto da tutti gli Stati membri.

Il Cybersecurity Act, quindi, è un ulteriore passo verso una maggiore sicurezza del mondo digitale europeo che aveva già registrato precedenti importanti sia col GDPR sia con la direttiva NIS.

Razionale

L'ambiente informatico è divenuto strategico per la gestione e lo sviluppo delle nostre società; reti, sistemi informativi e servizi di comunicazione elettronica (tecnologie dell'informazione e comunicazione, cosiddette "TIC") «*svolgono un ruolo essenziale nella società e sono diventati i pilastri della crescita economica (...) in settori essenziali quali la sanità, l'energia, la finanza e i trasporti e, in particolare, contribuiscono al funzionamento del mercato interno*».
L'incremento della digitalizzazione e della connettività – anche grazie all'avvento dell'Internet degli oggetti ("Internet of things" o IoT) – «*comporta maggiori rischi connessi alla cibersicurezza*» mentre di converso, «*la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza (...) la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tali rischi, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'Unione*» [Considerando (1-3)].

Precedenti

La politica di supporto alla sicurezza cibernetica in ambito UE è stata perseguita con una pluralità di interventi tra cui i principali sono il GDPR e la direttiva NIS, pur con le dovute differenze connesse ai diversi contesti di riferimento.

GDPR

Sebbene l'ambito applicativo del GDPR sia confinato al dominio dei dati personali, il tema della sicurezza è affrontato dal regolamento in modo strategico sotto il profilo quantitativo e qualitativo.
Dal punto di vista quantitativo, la definizione molto ampia di "dato personale" fa rientrare nel dominio applicativo del GDPR la quasi totalità del patrimonio informativo di cui necessita un'organizzazione, qualsiasi sia il settore di appartenenza. **Sotto il profilo qualitativo**, la

sicurezza delle informazioni è un principio di liceità del trattamento dei dati personali, nel senso che l'uso degli stessi non può ritenersi lecito se sprovvisto di un adeguato sistema di misure tecnico-organizzative di salvaguardia. Per il GDPR, pertanto, un utilizzo non sicuro di dati personali è illecito e suscettibile di sanzioni e di provvedimenti inibitori, con gravi ripercussioni sul business aziendale. La declinazione di dettaglio di questo principio si ritrova nella prescrizione dell'articolo 32 che impone al titolare del trattamento di adottare misure tecnico-organizzative adeguate al rischio nonchè nella regolamentazione del processo di violazione dei dati personali ("data breach"), la più completa disciplina sul tema in ambito unionale (artt. 33 e 34).

Direttiva NIS

La direttiva 2016/1148 che costituisce il primo atto giuridico della UE sulla sicurezza cibernetica (detta "direttiva NIS") – oggetto dell'Alert del 5 luglio 2018, cui si rinvia – affronta il tema della sicurezza nelle infrastrutture critiche e della disciplina di eventuali data breach in tali ambiti, istituendo «*i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri*». La direttiva NIS, come indica il termine, è basata sullo strumento giuridico della "direttiva" unionale anzichè su quello del "regolamento" per cui, diversamente da quest'ultimo, si indirizza agli Stati membri e deve essere recepita da questi tramite atti normativi nazionali. Per l'Italia, la direttiva NIS è stata recepita tramite il decreto legislativo n. 65/2018.
Differentemente dal GDPR, la direttiva NIS:

- non si riferisce a qualsiasi tipologia di organizzazione ma unicamente ai gestori di infrastrutture critiche (cioè quelli dell'energia e dei trasporti, quello bancario, infrastrutture dei mercati finanziari, settore sanitario, fornitura e distribuzione di acqua potabile, infrastrutture digitali) ed ai fornitori di servizi digitali (precisamente, mercato online, motori di ricerca online, servizi di cloud computing);
- impone agli operatori dei servizi essenziali e ai fornitori dei servizi digitali di notificare solo gli incidenti che abbiano un impatto rilevante sui servizi forniti (in tal caso, si tiene conto del numero degli utenti interessati, della durata dello stesso e della diffusione geografica, relativamente all'area interessata dall'incidente), sebbene anche nel contesto NIS, vi sia l'obbligo di adottare le misure per prevenire e minimizzare gli impatti degli incidenti nonchè di individuare le misure tecniche e organizzative relative alla gestione dei rischi.

Obiettivi

Lo strumento giuridico del regolamento è stato prescelto sulla base della considerazione che «*le competenze in materia di cibersicurezza e autorità incaricate dell'applicazione della legge e le relative risposte politiche sono prevalentemente nazionali*» mentre gli attacchi informatici avvengono spesso attraverso le frontiere tanto da richiedere un intervento normativo uniforme.
Gli obiettivi del Cybersecurity Act sono quelli di:

- **creare un quadro normativo di riferimento** – omogeneo a livello UE – a supporto della resilienza agli attacchi informatici;
- **creare un mercato unico della sicurezza** cibernetica per prodotti, servizi e processi;
- **accrescere la fiducia dei consumatori** nelle tecnologie digitali.

Iter

Come anticipato, il Cybersecurity Act è stato pubblicato nel GUCE il 7 giugno 2019 ed entra in vigore il 27 giugno 2019, cioè venti giorni dopo la sua pubblicazione, salvo limitate eccezioni (applicabili il 28 giugno 2021) (art. 69). In precedenza, l'atto era stato proposto dalla Commissione nel settembre 2017, l'accordo politico tra le istituzioni europee era stato raggiunto il 10 dicembre 2018 nel corso del quinto incontro del trilogo e, successivamente, il testo comune del regolamento era stato approvato dal Parlamento, il 12 marzo 2019, e dal Consiglio il 9 aprile 2019.
Il Cibersecurity Act sostituirà il precedente regolamento (UE) 526/2013 con il quale si era dato l'ultimo rinnovo al mandato dell'ENISA, sino al 2020.

Contenuti

Il regolamento sulla cybersicurezza si compone essenzialmente di due parti:

1. quella in cui vengono specificati il ruolo ed il mandato della rinnovata agenzia europea sulla sicurezza cibernetica ("ENISA") (artt. 1-45);
2. quella in cui si istituisce un sistema europeo per la certificazione della sicurezza informatica di dispositivi, prodotti e servizi digitali (artt. 46-65).

ENISA

L'Agenzia europea per la sicurezza delle reti e dell'informazione ("ENISA") era stata istituita nel 2004, con mandato limitato sia sotto il profilo della competenza (prevalentemente consultiva, per contribuire all'obiettivo generale di garantire un livello elevato di sicurezza delle reti e dei sistemi informativi nella UE) sia sotto quello temporale (in quanto, nonostante i ripetuti rinnovi, il mandato all'agenzia sarebbe infine scaduto nel 2020).
Il Cybersecurity Act trasforma l'ENISA in un'agenzia permanente – un vero centro di competenza europeo sulla cybersecurity – ampliandone le competenze che includono:

- l'**attività di supporto alla gestione operativa degli incidenti informatici** da parte degli Stati membri nonchè nello sviluppo e nell'attuazione delle politiche comunitarie;
- un ruolo di primo piano nella **gestione del sistema di certificazione introdotto dal regolamento**, mediante la predisposizione di schemi europei per la certificazione sulla sicurezza cibernetica che saranno poi adottati dalla Commissione mediante atti di esecuzione.

Certificazioni

L'ulteriore principale intervento del Cybersecurity Act consiste nell'aver introdotto un quadro normativo per la certificazione sulla sicurezza in internet di valenza unionale per assicurare un approccio comune sul mercato interno dell'Unione e, da ultimo, per migliorare la sicurezza cibernetica dei prodotti digitali incrementando la fiducia riposta dai consumatori nel mercato digitale. «*Le automobili connesse e automatizzate, i dispositivi medici elettronici, i sistemi di controllo per l'automazione industriale e le reti elettriche intelligenti sono solo alcuni esempi di settori in cui la certificazione è già ampiamente utilizzata o*» nei quali si svilupperà, come anche dovrebbe avvenire nell'ambito delle infrastrutture strategiche affrontate dalla direttiva NIS [v. considerando (65)].

Anche in questo caso, la certificazione introdotta dal Cybersecurity Act lascia impregiudicata «*l'istituzione di meccanismi di certificazione nonchè di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità*» al GDPR «*dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento*» anche nel caso che le operazioni di trattamento siano integrate nelle TIC [v. Considerando (74)].

Processo di certificazione

La certificazione sulla sicurezza cibernetica disciplinata dal Cybersecurity Act parte da schemi di certificazione che – come detto – sulla base di un quadro complessivo di regole comunitarie, vengono realizzati dall'ENISA, sono approvati dalla Commissione con atti di esecuzione, e conseguentemente vengono riconosciuti in tutti gli Stati membri; in questo modo si viene a modificare la situazione precedente che annoverava schemi di certificazione specifici per prodotti e sistemi TIC, esistenti presso singoli paesi ma non riconosciuti a livello transnazionale: si veda, ad esempio, il caso dei contatori intelligenti (o "smart meters") i cui produttori sono sottoposti a distinti processi di certificazione in Francia, Gran Bretagna e Germania. Quindi, il Cybersecurity Act non istituisce schemi di certificazione direttamente operativi ma definisce un quadro regolatorio per la loro creazione.

Una volta adottato uno schema di certificazione europeo, le aziende volontariamente potranno presentare domanda di certificazione dei propri prodotti, servizi o processi agli organismi di certificazione nazionali (in Italia, l'OCSI, Organismo di Certificazione della Sicurezza Informatica); salvo che la certificazione di sicurezza non venga espressamente richiesta come obbligatoria per specifici prodotti o servizi da eventuali norme di settore.

Obiettivi dei sistemi di certificazione europea sulla sicurezza

Gli obiettivi di maggiore interesse per la certificazione della sicurezza sono:

- appurare che i sistemi, servizi o processi siano in grado di **proteggere i dati dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati** durante l'intero ciclo di vita;
- verificare che siano in grado di **proteggere i dati dalla distruzione, dalla perdita o dall'alterazione accidentali o non autorizzate**, oppure dalla mancanza di disponibilità;
- che **l'accesso** di persone, programmi o macchine sia limitato esclusivamente ai dati, ai servizi o alle funzioni per i quali questi **dispongono dei diritti di accesso**;
- che siano state **individuate e documentate le dipendenze e vulnerabilità note**, che sia possibile registrare a quali dati, servizi o funzioni è stato effettuato l'accesso, in quale momento e da chi;
- che sia possibile **ripristinare tempestivamente la disponibilità e l'accesso ai dati**, ai servizi e alle funzioni in caso di incidente fisico o tecnico;
- che siano utilizzati criteri di **"security by design"** per la progettazione di prodotti e servizi, e **"by default"**, in modo che tali prodotti implementino le impostazioni più sicure, ed infine che il software e l'hardware dei prodotti TIC siano costantemente aggiornati per mezzo di meccanismi protetti.

Livelli di affidabilità dei sistemi europei di certificazione cibernetica

Tenendo conto che non tutti i sistemi, processi e servizi hanno lo stesso profilo di rischio, il Cybersecurity Act prevede tre livelli di certificazione differenti (art. 52 commi 5, 6 e 7):

- Un **livello di affidabilità "di base"** per il quale il produttore/fornitore può ricorrere all'autocertificazione, ove prevista; in questa ipotesi può bastare un riesame della documentazione tecnica, o attività di valutazione sostitutive di effetto equivalente intese a **ridurre al minimo i rischi di base noti di incidenti e attacchi informatici**.
- Un **livello di affidabilità "sostanziale"** per il quale la valutazione di sicurezza è effettuata a un livello inteso a **ridurre al minimo i rischi noti alla cibersicurezza ed i rischi di incidenti ed attacchi informatici commessi da soggetti che dispongono di abilità e risorse limitate**. Le attività di valutazione comprendono almeno un riesame per verificare l'assenza di vulnerabilità pubblicamente note e un test per dimostrare che i prodotti o servizi attuino correttamente le necessarie funzionalità di sicurezza.
- Un **livello di affidabilità "elevato"**, per il quale la valutazione di sicurezza è effettuata a un livello inteso a **ridurre al minimo il rischio di attacchi informatici avanzati, commessi da attori che dispongono di abilità e risorse significative**. Le attività di valutazione comprendono: un riesame per dimostrare l'assenza di vulnerabilità pubblicamente note, un test per dimostrare che i prodotti TIC attuano correttamente le necessarie funzionalità di sicurezza allo stato tecnologico più avanzato, e una valutazione della loro resistenza agli attacchi commessi da soggetti qualificati mediante test di penetrazione.

Valore dei certificati sulla sicurezza informatica

I certificati europei sulla sicurezza informatica non attestano o garantiscono che un prodotto o servizio certificato in base ad un determinato schema accreditato sia sicuro bensì che lo stesso risponda agli specifici requisiti definiti nello schema. I certificati così rilasciati saranno riconosciuti in tutti gli Stati membri dell'Unione, facilitando sia gli affari degli operatori che agiscono a livello transnazionale sia la fiducia e consapevolezza degli acquirenti circa il livello di sicurezza certificato.

Sicurezza by design e by default

Obiettivo del legislatore tramite la certificazione europea sulla sicurezza è quello di promuovere la sicurezza informatica sin dalla fase iniziale di progettazione e sviluppo dei prodotti TIC e di quelli di consumo che costituiscono gli IoT ("security by design"). Questo consentirà agli utenti di conoscere il livello di sicurezza dei prodotti/servizi scelti assicurando che le misure di sicurezza siano verificate in modo indipendente.

Le organizzazioni dovrebbero configurare i TIC da loro progettati «*in modo da garantire un livello di sicurezza superiore che dovrebbe consentire al primo utente di ricevere una configurazione predefinita con le impostazioni più sicure possibili («sicurezza predefinita»), riducendo al contempo l'onere in capo agli utenti di*» doverlo essi stessi configurare in modo adeguato. La sicurezza predefinita dovrebbe essere possibile senza necessità di «*conoscenze tecniche specifiche o di un comportamento non intuitivo da parte dell'utente, e dovrebbe funzionare in modo semplice e affidabile quando attuata*».

23.
Linee guida su codici di condotta ed allegati su certificazione e accreditamento

L'undicesima riunione plenaria del Comitato europeo (EDPB) ha adottato i seguenti documenti:

- linee guida sui codici di condotta;
- allegato alle linee guida sull'accreditamento;
- allegato 2 sulle linee guida sulla certificazione.

Linee guida sui codici di condotta

«*Le linee guida intendono contribuire a chiarire le procedure e le regole coinvolte nella presentazione, approvazione e pubblicazione di codici di condotta a livello sia nazionale che europeo*».

Sulla natura dei codici di condotta di cui agli articoli 40 e 41 del GDPR e sul contenuto delle relative linee guida emesse dall'EDPB ci siamo già soffermati in occasione dell'Editoriale del 28 febbraio 2019, cui si rinvia. In quell'occasione descrivemmo il testo delle linee guida sottoposte a consultazione pubblica; nell'undicesima riunione plenaria del giugno 2019, l'EDPB ha adottato il testo definitivo delle stesse, a seguito della conclusione della citata consultazione: Linee guida 1/2019 sui codici di condotta e gli organismi di monitoraggio secondo il regolamento 2016/679, versione 2.0, 4 giugno 2019.

Novità del testo definitivo: codici di condotta anche intersettoriali

Un'importante novità del testo definitivo riguarda la precisazione che «*i codici non devono necessariamente essere confinati o limitati a un settore specifico. Ad esempio, un codice potrebbe essere applicato a settori separati che hanno un'attività di trattamento comune la quale condivide le stesse caratteristiche e esigenze di trattamento*». Quando un codice è intersettoriale può essere nominato più di un organismo di controllo ai sensi dell'articolo 41. In tal caso, il codice deve specificare i settori per i quali ciascun organismo di monitoraggio svolgerà le sue funzioni e i meccanismi di controllo disponibili ad ognuno.

Allegato alle linee guida sull'accreditamento

L'obiettivo delle linee guida è fornire indicazioni su come interpretare e attuare le disposizioni dell'articolo 43 del GDPR per l'accreditamento degli organismi di certificazione che rilasciano la certificazione conformemente al GDPR.

In materia di accreditamento ci siamo già soffermati in occasione delle seguenti puntate dell'Editoriale cui si rinvia:

- 18 aprile 2019;
- 14 giugno 2018;
- 25 gennaio 2018.

L'allegato che è stato approvato definitivamente, a conclusione della procedura di consultazione pubblica, «*fornisce una guida sui requisiti aggiuntivi per l'accreditamento degli organismi di certificazione che devono essere stabiliti dalle autorità di supervisione. Tali requisiti aggiuntivi, prima di essere adottati dalle autorità di supervisione, devono essere sottoposti all'approvazione del comitato europeo per la protezione dei dati a norma dell'articolo 64, paragrafo 1, lettera c)*».

Linee guida 4/2018 e criteri di accreditamento

La relazione tra le linee guida 4/2018, che contengono l'allegato ora adottato in via definitiva, ed i criteri di accreditamento aggiuntivi allo standard ISO/IEC 17065/2012, stabiliti dalle ASN,

può sintetizzarsi come segue:

1. le linee guida sull'accreditamento forniscono indirizzi rivolti alle ASN per la determinazione dei requisiti aggiuntivi per l'accreditamento degli organismi di certificazione che rilasciano i certificati ai sensi del GDPR;
2. i requisiti aggiuntivi sono stabiliti dalle ASN sulla base delle citate linee guida;
3. prima di essere adottati, i medesimi requisiti devono essere approvati dall'EDPB.

Viene reso noto che, per facilitare coerenza e tempestività dei progetti di decisione delle ASN, l'EDPB sta preparando una procedura in materia di certificazione ed accreditamento e per approvare i sigilli europei di protezione dei dati.

Il documento definitivo ed integrale, comprensivo di linee guida ed allegato, reca ora il titolo "Linee guida 4/2018 relative all'accreditamento degli organismi di certificazione ai sensi dell'articolo 43 del regolamento generale sulla protezione dei dati (2016/679) – versione 3.0 del 4 giugno 2019".

Cronologia degli aggiornamenti

Il documento delle linee guida fu originariamente approvato come "versione 1.0" dal WPArt29 il 6 febbraio 2018 (wp261) e successivamente fatto proprio dall'EDPB il 25 maggio 2018.

Successivamente, il 4 dicembre 2018, al termine della procedura di consultazione pubblica, l'EDPB ha adottato:

- il testo finale delle linee guida, in versione 2.0 ;
- l'allegato 1, in versione 1.0, da sottoporre a consultazione pubblica.

Infine, il 4 giugno 2019 è stato approvato ed aggiunto alle linee guida, l'allegato 1, in versione 2.0, a conclusione della consultazione pubblica.

Allegato 2 alle linee guida sulla certificazione

L'EDPB ha adottato la versione finale dell'allegato 2 delle linee guida sulla certificazione, a seguito della consultazione pubblica.

«*L'allegato 2 identifica gli argomenti che le autorità di supervisione sulla protezione dei dati e l'EDPB prenderanno in considerazione e applicheranno per l'approvazione dei criteri per un meccanismo di certificazione*» ai sensi dell'articolo 42, paragrafo 5, del GDPR.

L'allegato 2 rappresenta, quindi, una guida per gli organismi di certificazione ed i proprietari di schemi che desiderano redigere e presentare i criteri per l'approvazione. La guida elenca una serie di profili che dovrebbero essere presi in considerazione al momento di redigere i criteri.

Linee guida 1/2018

Lo scopo principale delle linee guida 1/2018 – di cui l'allegato citato fa parte – «è quello di identificare i criteri generali che possono essere rilevanti per tutti i tipi di meccanismi di certificazione emessi ai sensi dell'art. 42 e art. 43 GDPR».

Il documento integrale – cioè comprensivo delle linee guida e dei relativi allegati – è stato rilasciato con la dicitura "Linee guida 1/2018 sulla certificazione e sull'individuazione dei criteri di certificazione ai sensi degli articoli 42 e 43 del regolamento – versione 3.0 del 4 giugno 2019".

In materia di certificazione ci siamo già soffermati in occasione delle seguenti puntate cui si rinvia:

- 18 aprile 2019;
- 4 aprile 2019;
- 28 giugno 2018;
- 14 giugno 2018;
- 25 gennaio 2018.

Cronologia degli aggiornamenti

Il testo originario delle linee guida 1/2018 fu uno dei primi documenti adottati dall'EDPB, il 25 maggio 2018 e sottoposto a consultazione pubblica.
Il 23 gennaio 2019, al termine della procedura di consultazione pubblica, l'EDPB ha adottato il testo definitivo (versione 2.0) delle linee guida 1/2018 e contestualmente ha adottato l'allegato 2 (versione 1.0), sottoponendolo a consultazione pubblica.
Infine, il 4 giugno 2019 si è proceduto all'inclusione del testo definitivo dell'allegato 2 (versione 2.0) alle linee guida.

Novità del testo definitivo

Rispetto al testo originario dell'allegato, alcuni aspetti sono stati aggiunti ad alcune sezioni, ad esempio,

- se i criteri riguardano l'obbligo del titolare del trattamento / responsabile del trattamento di nominare un DPO: nel senso che viene chiesto se i criteri verificano che l'organizzazione abbia valutato se un DPO debba essere nominato come richiesto dall'articolo 37 e se il DPO soddisfi i requisiti di cui agli articoli da 37 a 39;
- l'obbligo di tenere un registro delle attività di trattamento: nel senso che si accerta se i criteri verificano che il registro dei trattamenti sia obbligatorio ai sensi dell'articolo 30, paragrafo 5 e soddisfi in modo adeguato i requisiti dell'articolo 30.

24.
Approvato il codice di condotta sulle informazioni commerciali

Con deliberazione del 12 giugno 2019, il Garante ha approvato il "Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali", quasi in contemporanea con l'adozione da parte dell'EDPB delle linee guida sui codici di condotta, oggetto dello scorso Alert. Si tratta del primo esempio della categoria di "codici di condotta" di nuovo conio istituita dal GDPR, all'articolo 40.

Sintesi

I codici di condotta sono uno degli strumenti di regolamentazione volontaria o "dal basso", previsti dal GDPR (art. 40), insieme ai meccanismi di certificazione ed ai marchi e sigilli sulla protezione dei dati personali (art. 42). Tali strumenti servono per integrare e meglio attuare principi e regole del GDPR in specifici contesti, incrementando il senso di fiducia da parte del mercato e degli interessati.

Nel contesto nazionale italiano, i codici di condotta del GDPR si sostituiscono ai "codici di deontologia e di buona condotta" disciplinati dal codice privacy previgente (art. 12). La norma di adeguamento nazionale (dlgs 101/2018) ha operato una distinzione all'interno dei precedenti codici deontologici, suddividendoli tra

- quelli che potranno rientrare nella categoria dei "codici di condotta" dell'art. 40, come il codice SIC e quello sulle informazioni commerciali;
- quelli che, invece, possono considerarsi come regole speciali relative a specifici settori – chiamate "regole deontologiche" – che si avvalgono dei margini di flessibilità ed autonomia che il GDPR riconosce agli Stati membri (come quelli per l'attività giornalistica, per scopi storici, per scopi statistici SISTAN e ricerca scientifica, per scopi statistici e scientifici, per investigazioni difensive e azioni in giudizio).

In questo scenario, il Garante privacy ha recentemente approvato il "Codice di condotta per il trattamento dei dati personali in materia di informazioni commerciali", valido in ambito nazionale, ai sensi dell'articolo 40 del GDPR. La piena applicazione delle regole di questo codice è legata al futuro accreditamento dell'Organismo di monitoraggio che dovrà vigilare sul rispetto delle sue norme da parte degli aderenti.

Codici deontologici, regole deontologiche e codici di condotta

L'applicazione del Regolamento ha creato un definitivo assestamento nella materia dei codici volontari in ambito di protezione dei dati personali; in questo contesto sono state utilizzate, in fasi diverse, le espressioni "codice deontologico", "regole deontologiche" e "codici di condotta".

Codici deontologici

L'espressione "**codice deontologico**" – o per esteso "codice di deontologia e di buona condotta" – è stata utilizzata dal codice privacy previgente (art. 12) per indicare una particolare tipologia di normazione di natura volontaria, promossa dal Garante e sottoscritta dalle categorie interessate, previa verifica di conformità alla disciplina legale da parte dell'autorità. Sulla base della speciale procedura di formazione, dettata dall'articolo 12, la norma allora riconosceva alla conformità a tali regole provenienti "dal basso", valore «*di condizione essenziale per la liceità e correttezza del trattamento*» di titolari pubblici e privati (art. 12.3).

Regole deontologiche

A seguito dell'applicazione del GDPR – come evidenziato nell'Editoriale dell'11/10/2018 – la citata disciplina è stata sostituita da quella prevista dal regolamento per i codici di condotta (artt. 40 e 41, GDPR) per cui, come riportato nell'Alert del 10/1/2019, le disposizioni dei precedenti codici deontologici ritenute conformi al GDPR – e rientrante in ambiti rimessi alla flessibilità degli Stati membri – sono state ridenominate "**regole deontologiche**" e – secondo quanto dispone l'articolo 20 del dlgs 101/2018 – sono state pubblicate dal Garante e successivamente allegate al codice privacy riformato (v. Alert del 24/1/2019). Anche per le "regole deontologiche", così come avveniva per le disposizioni dei codici deontologici del codice previgente, il rispetto delle stesse «*costituisce condizione essenziale per la liceità e la correttezza del trattamento dei dati personali*» (art. 2-quater, comma 4, codice privacy). Pertanto, la violazione delle disposizioni in esse contenute comporta l'illiceità del trattamento svolto.

Codici di condotta

Come ribadito nel citato Editoriale dell'11/10/2018, i "codici di condotta" propriamente detti trovano la propria fonte normativa nell'articolo 40 del GDPR e vanno realizzati secondo le disposizioni del regolamento. Diversamente dai "codici deontologici" del previgente codice privacy (e dalle attuali "regole deontologiche") il rispetto dei codici di condotta (di cui all'art. 40 GDPR) è elemento utile a dimostrare l'osservanza del GDPR ma non è condizione di liceità del trattamento.

Nella preventiva verifica di compatibilità dei precedenti codici deontologici privacy rispetto al GDPR, il Garante ha ritenuto che il codice sui Sistemi di Informazione Creditizia ("SIC") ed il codice sulle informazioni commerciali (già Allegato A.7 del previgente codice) potevano essere inquadrati nella categoria dei codici di condotta disciplinati dal regolamento.

Procedura per i codici di condotta

I codici di condotta dell'articolo 40 sono elaborati dalle associazioni e dagli altri organismi rappresentanti le categorie di titolari e responsabili del trattamento e sono sottoposti all'autorità di controllo competente, la quale esprime un parere sulla conformità del progetto di codice al GDPR e, in caso favorevole, lo approva (art. 40.5, GDPR). Quindi, la procedura prevede

- una prima valutazione di ammissibilità;
- un successivo giudizio di conformità e, in caso positivo;
- una finale approvazione da parte dell'autorità.

Linee guida EDPB 1/2019

Il Comitato europeo, in data 4 giugno 2019, ha adottato in via definitiva le linee guida 1/2019 che hanno lo scopo di «*stabilire i criteri minimi richiesti da un'autorità di supervisione competente ("CompSA") prima di accettare di effettuare una revisione approfondita e la valutazione di un codice*» nonchè i fattori «*da prendere in considerazione nel valutare se un determinato codice fornisce e contribuisce alla corretta ed efficace applicazione del GDPR*» (v. Alert del 20/6/2019).

Codice di condotta sulle informazioni commerciali

A conclusione di un articolato iter di confronto per l'aggiornamento del precedente codice (già Allegato A.7 del previgente codice) e per la verifica di conformità al GDPR, sulla scia delle citate linee guida EDPB 1/2019, l'autorità italiana ha approvato il "Codice di condotta predisposto dall'Associazione Nazionale tra le Imprese di Informazioni Commerciali e di Gestione del Credito (Ancic)" (di seguito "Codice sulle informazioni commerciali") la cui efficacia è subordinata, come previsto dal GDPR:

- al completamento dei lavori in seno all'EDPB per la definizione di criteri uniformi per l'accreditamento degli Organismi di monitoraggio;
- al completamento della fase di accreditamento dell'Organismo di monitoraggio, menzionato nel codice di condotta di nuovo conio.

Il vecchio Codice deontologico sulle informazioni commerciali rimarrà comunque in vigore fino al 19 settembre 2019, cioè sino all'intero periodo della definizione della procedura di approvazione (6 mesi + 6 mesi) prevista dall'art. 20 del dlgs 101/2018, decorrente dalla data di entrata in vigore del citato dlgs 101/2018 (19 settembre 2018).

Organismo di monitoraggio e relativo accreditamento

Il GDPR stabilisce che il controllo obbligatorio del rispetto dei codici di condotta da parte degli aderenti che si impegnano ad applicarlo, possa essere effettuato (oltre che dall'autorità di supervisione) da un organismo di monitoraggio competente e che il codice stesso ne debba prevedere i meccanismi operativi (artt. 40.4 e 41, GDPR). Il codice di condotta presentato da Ancic prevede tale organismo di monitoraggio – esterno ad Ancic – che dovrà essere accreditato da parte del Garante ai sensi dell'art. 41 del Regolamento; l'accreditamento è condizione per l'approvazione del progetto di codice per cui il Garante, nella propria deliberazione, ne ha subordinato l'efficacia alla conclusione della fase di accreditamento. Questa, infatti, per poter giungere a completamento, richiede la definizione di criteri uniformi per l'accreditamento da parte dell'EDPB.

Ambito di applicazione

Il Codice sulle informazioni commerciali riguarda il «*trattamento di dati personali provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque o pubblicamente accessibili (c.d. fonti pubbliche), nonché (i)l trattamento di dati personali forniti direttamente dagli interessati*», effettuato da titolari per la prestazione a terzi di servizi di informazione commerciale. Vanno ricompresi nell'ambito anche i trattamenti «*che presuppongono l'elaborazione di informazioni commerciali, da parte dei fornitori, mediante processi statistici o modelli automatizzati, oppure tramite analisi e valutazioni effettuate da esperti, anche sulla base di classificazioni predefinite, allo scopo di formulare un giudizio sulla solidità, solvibilità ed affidabilità del soggetto censito, eventualmente espresso in termini predittivi, probabilistici o in forma di indicatori alfanumerici, codici o simboli*», fatta eccezione per l'ambito dei sistemi informativi creditizi ("SIC") oggetto di norme specifiche. Quindi il Codice sulle informazioni commerciali si applica a servizi informativi o anche valutativi «*a committenti per verifiche sulla situazione economica, finanziaria e patrimoniale degli interessati, nonché sulla loro solidità, solvibilità ed affidabilità*».

Il trattamento oggetto del codice è limitato al territorio dello Stato italiano ed è applicabile solo a livello nazionale.

Soggetti "committenti"

I soggetti "committenti" che, insieme ai fornitori, possono aderire al codice – cioè coloro che richiedono al fornitore un servizio di informazione commerciale – possono essere soggetti privati o pubblici. In merito a questi ultimi ed all'applicabilità ad essi della base giuridica del legittimo interesse, sorge qualche perplessità come indicato più in basso al paragrafo "Base giuridica: legittimo interesse".

Dati sensibili e giudiziari

Il trattamento dei dati personali effettuati nello svolgimento di informazioni commerciali non può riguardare dati sensibili o giudiziari, eccetto per i dati giudiziari provenienti da fonti pubbliche nel rispetto di quanto stabilito nel decreto del Ministero della giustizia di cui all'articolo 2-octies del codice privacy (in attesa di emanazione) e senza che il fornitore possa utilizzarli a fini dell'elaborazione di informazioni valutative (art. 4.5, codice di condotta).

Informativa agli interessati

Considerato il rilevante numero di interessati, tale da comportare un impiego di mezzi da ritenersi manifestamente sproporzionato rispetto al diritto tutelato, il fornitore rende l'informativa all'interessato, in forma non individuale, attraverso l'informativa pubblicata sul portale Internet www.informativaprivacyancic.it da Ancic, in rappresentanza dei fornitori di informazioni commerciali.

Base giuridica: legittimo interesse

Base giuridica del trattamento pertinente è il legittimo interesse perseguito dal titolare (fornitori che prestano i servizi e committenti che li richiedono) «*quale può essere il monitoraggio e la prevenzione di frodi, la garanzia della sicurezza e dell'affidabilità dei servizi forniti dai committenti, la solidità della gestione e la corretta esecuzione di rapporti commerciali ed attività economiche e finanziarie tra questi ultimi ed il soggetto censito*».

In proposito, suscita qualche perplessità l'inclusione nell'ambito applicativo del codice anche dei "committenti" soggetti pubblici riguardo la previsione del legittimo interesse come base giuridica e la preclusione per i soggetti pubblici di avvalersene, contenuta nel GDPR (art. 6.1, secondo capoverso). Il codice, come già indicato, prevede che il presupposto di liceità del relativo trattamento sia il nesso di necessità in relazione «*al perseguimento dei legittimi interessi dei fornitori che prestano i servizi di informazioni commerciali (...)* ***nonché dei committenti*** *che li richiedono per legittime verifiche (...)*» (enfasi aggiunta, art. 6.1).

D'altro canto, secondo la disposizione del GDPR citata (art. 6.1, secondo cpv.), la base giuridica del perseguimento del legittimo interesse del titolare o di terzi «*non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esercizio di loro compiti*». Rimane da capire, pertanto, se il riferimento ai soggetti pubblici debba intendersi limitato ai soli casi in cui essi agiscono al di fuori dell'«*esercizio di loro compiti*», cioè, in sostanza, all'interno della disciplina data protection di stampo privatistico.

Infine, secondo il codice, ogni decisione valutativa basata sulle informazioni commerciali oggetto del servizio «è rimessa esclusivamente ai committenti ed è basata sull'insieme dei dati personali ed informazioni in loro possesso».

Data breach

Per le violazioni di dati personali ed in relazione ai conseguenti adempimenti, «*i fornitori si impegnano ad osservare le linee guida, le raccomandazioni e le best practices adottate dall'EDPB o da altre autorità di settore competenti, ferma restando la possibilità di adottare propri standard e procedure*». Il richiamo così operato dal codice conferisce valore giuridico vincolante (ancorchè di natura pattizia) a «*le linee guida, le raccomandazioni e le best practices adottate dall'EDPB o da altre autorità di settore competenti*».

25. Eurobarometro 2019: livello di consapevolezza GDPR nella UE

Propedeutica all'accountability è la consapevolezza del dovere.
Da pochi giorni l'Eurobarometro ha pubblicato il sondaggio speciale 487 che gli è stato commissionato dalla Direzione generale per la Giustizia e i Consumatori della Commissione europea per esplorare in particolare il livello di consapevolezza del GDPR nei 28 Stati membri.
Come spesso accade nei sondaggi, vi sono almeno due chiavi di lettura, una ottimistica o "da bicchiere mezzo pieno" ed una meno, "da bicchiere mezzo vuoto".
In entrambi i casi, le rilevazioni offrono più di uno spunto di interesse.

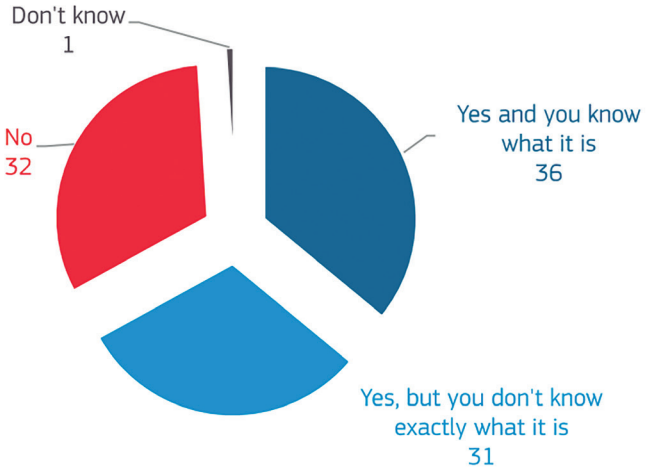
Riscontri di interesse

L'iniziativa (suddivisa in un sommario e nel rapporto completo) suscita interesse sia per i contenuti in sé, segmentabili per paese di riferimento e commisurabili con la media europea, sia anche per la possibilità, in taluni casi, di verificare lo scostamento rispetto alla precedente rilevazione del 2015.

La consapevolezza del GDPR: dipende dall'angolo di visuale

Nelle organizzazioni si è soliti dire che "i numeri parlano una voce sola": nel senso che il riferimento numerico è quanto di più oggettivo possa esserci e, di conseguenza, dovrebbe essere al riparo da interpretazioni discordanti. Il condizionale è doveroso in quanto la dialettica interpretativa può attecchire anche in contesti caratterizzati da mere evidenze numeriche, come il sondaggio dell'Eurobarometro.
Ad esempio, a livello aggregato, il sondaggio indica che due/terzi dei rispondenti (il 67%) ha sentito parlare del GDPR: questa indicazione potrebbe risultare confortante, tant'è che la Commissione UE, nell'infografica realizzata per celebrare il primo anniversario del GDPR, la pone in evidenza come risultato positivo acquisito; se si osserva più in dettaglio la composizione di questo cluster, tuttavia, si nota che poco più di un terzo (il 36%) ne ha sentito parlare e sa di cosa si tratta, mentre poco meno di un terzo (il 31%) ne ha sentito parlare ma non sa di cosa si tratta.

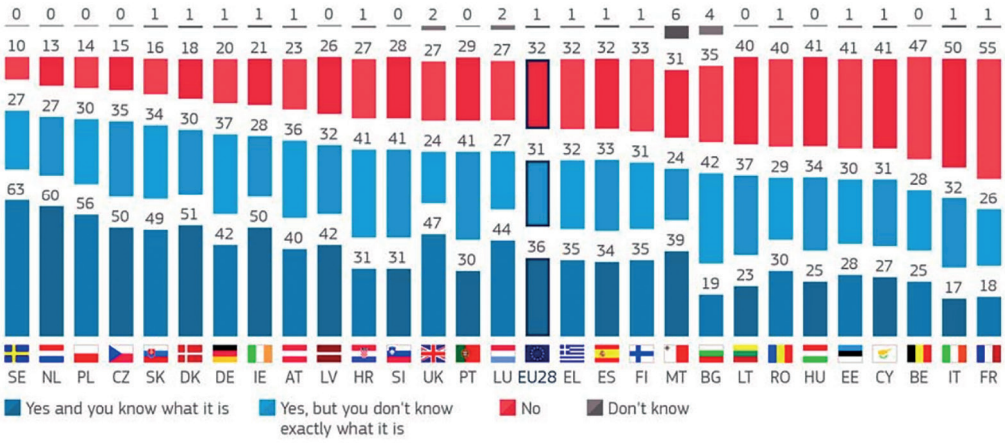
QB17 Have you heard of the General Data Protection Regulation (GDPR), wich came into force in 2018? **(% - EU)**



Base: all respondents (N=27,524)

L'Italia è al penultimo posto in questa graduatoria e fa meglio solo rispetto alla Francia. Nel nostro paese solo il 17% ha sentito parlare e sa cos'è il GDPR mentre circa un terzo (il 32%) ne ha sentito parlare ma non sa cosa sia e ben la metà (50%) risulta essere totalmente all'oscuro. Di conseguenza, una significativa percentuale (82%) non sa cosa sia il regolamento generale sulla protezione dei dati personali.

QB17 Have you heard of the General Data Protection Regulation (GDPR), wich came into force in 2018? **(%)**

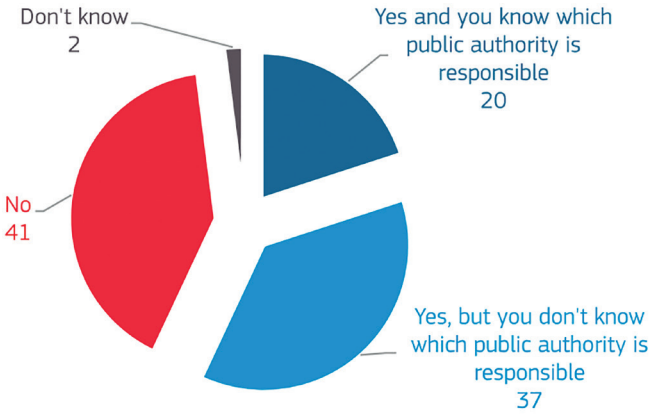


Base: all respondents (N=27,524)

Consapevolezza dell'authority nazionale di supervisione

Se l'autorità nazionale di supervisione è un importante presidio per la tutela dei propri diritti in questo contesto, il livello di consapevolezza riguardo alla sua esistenza e la sua corretta individuazione incidono direttamente sull'effettività delle tutele. Il 57% è a conoscenza dell'esistenza di un'autorità competente nel proprio paese (in Italia è il 55%) con un incremento di ben 20 punti percentuali rispetto alla corrispondente rilevazione del 2015.

QB16 Have you heard about the existence of a public authority in (OUR COUNTRY) responsible for protecting your rights regarding your personal data? **(% - EU)**

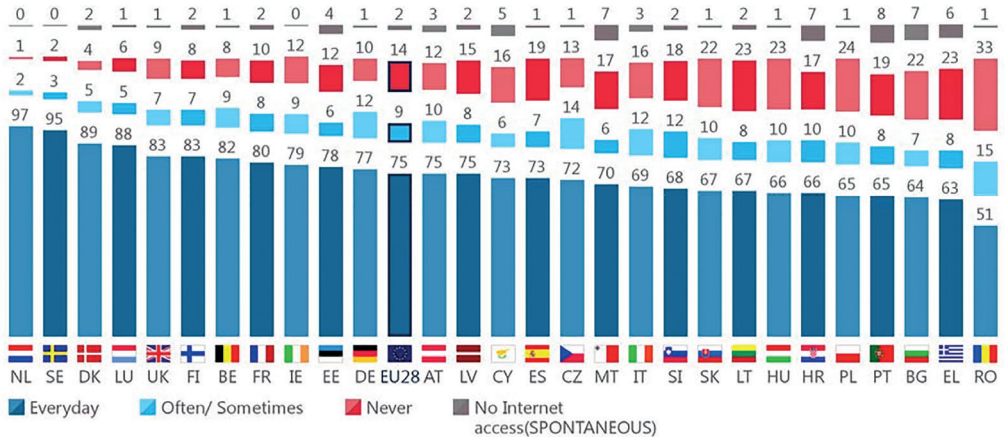


Total 'Yes'	No	Don't Know
57% (+20)	41% (-20)	2% (=)

(March 2019 – February/March 2015)

La lettura "in negativo" dello stesso dato, tuttavia, evidenzia come ben il 37% non sarebbe in grado di individuare quale sia l'autorità pubblica competente (stessi valori per l'Italia) mentre il 41% risultano non saperne nulla (in Italia il 43%).

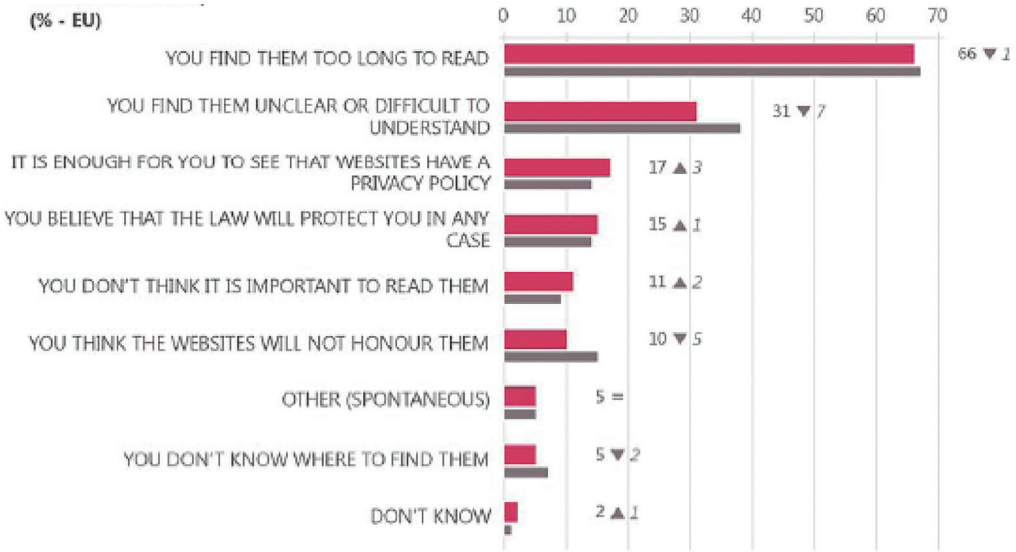
D62R Use of the Internet **(%)**



La lettura delle policy privacy sul web

Da tempo si sa che la trasparenza come sino ad oggi è veicolata su internet non soddisfa lo scopo: i documenti sono scritti in modo eccessivamente tecnico ed i testi risultano troppo lunghi tanto da scoraggiarne la lettura. Recentemente Google è stata sanzionata dal CNIL (l'autorità di supervisione francese) anche per la farraginosità delle proprie politiche privacy pubblicate sul web che, in alcuni casi, richiedevano all'utente anche sino a cinque rimbalzi (collegamenti ipertesto) per trovare le informazioni di interesse (v. l'Editoriale del 31 gennaio 2019).

QB15 What are the reasons why you do not usually read privacy statements, or only read them partially? (MULTIPLE ANSWERS POSSIBLE) **(% - EU)**



Base: respondents who do not read privacy statement or only partially (N=19,516)

Il Gruppo di lavoro dell'articolo 29 (WPArt29) ha indirizzato il problema in più di un'occasione ed ha suggerito di utilizzare modalità redazionali a più livelli, collassabili, in modo da consentire all'utente di individuare celermente il tema di interesse e poterlo approfondire secondo il proprio gradimento. Il GDPR ha dedicato l'intero articolo 12 alle modalità trasparenti di informazioni e comunicazioni da fornire all'interessato; eppure anconra molta strada deve essere compiuta su questo versante. Non sorprende, quindi, che solo il 13% dei rispondenti che utilizzano Internet dichiara di leggere la policy nella sua interezza mentre preoccupa che la comparazione con le analoghe rilevazioni del 2015 denota un peggioramento di 7 punti percentuali tra coloro chei dichiarano di non leggere le policy, in tutto o in parte. Le ragioni vengono indicate nella lunghezza dei documenti (66%) nella difficoltà di comprensione dei relativi contenuti (31%) mentre per il 17% è sufficiente constatare l'esistenza del link a fondo pagina.

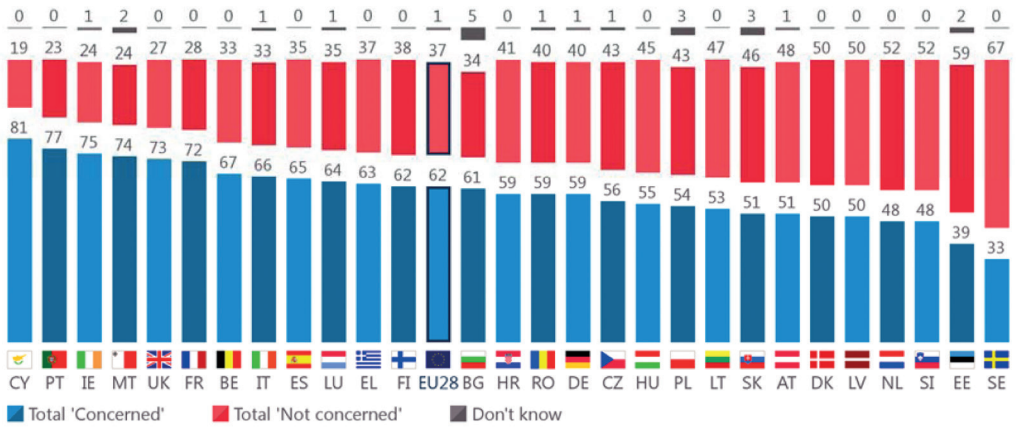
Ottenimento dell'informativa in caso di fornitura di dati

A completamento dell'analisi sulla trasparenza data protection sul web, è stato chiesto al campione del sondaggio se essi ricevono l'informativa privacy quando forniscono i propri dati personali su Internet ed uno su cinque (22%) dichiara di essere sempre informato al riguardo, mentre la percentuale sale al 57% se si includono nel *cluster* anche coloro che dichiarano di ricevere l'informativa solo in alcune occasioni.

Preoccupazione della perdita di controllo riguardo ai dati personali forniti in rete

Il risultato registrato riguardo alla lettura delle privacy policy sul web va interpretato anche alla luce degli esiti del quesito sul livello di preoccupazione degli utenti in merito alla perdita di controllo dei propri dati personali forniti on line.

QB10 How concerned are you about having complete control over the information you provide online? Would you say you are? **(%)**



Base: respondents who feel to have only partial or no control over the information provided online (N=15,915)

La scarsa propensione alla lettura delle policy privacy non va interpretata come generale disinteresse per la materia, in quanto il livello di sensibilità dell'utenza appare elevato (62% complessivo tra preoccupati 46% e molto preoccupati 16%), sebbene diminuito di 5 punti percentuali rispetto alla medesima rilevazione del 2015. In Italia le rilevazioni denotano una fetta complessiva dei preoccupati pari al 67%.

26.
Big data: indagine conoscitiva congiunta di Garante, AGCM e AGCOM

Con un comunicato congiunto, l'Autorità Garante della Concorrenza e del Mercato ("AGCM"), l'Autorità per le Garanzie nelle Comunicazioni ("AGCOM") e il Garante per la protezione dei dati personali hanno reso noto la prossima pubblicazione del documento finale riguardo agli esiti dell'indagine conoscitiva svolta in materia di Big data. Nel frattempo, sono state anticipate «*le principali linee guida di cooperazione sul tema, nonché le raccomandazioni di policy condivise dalle tre autorità*» con la pubblicazione del documento "Big data – Indagine conoscitiva congiunta – Linee guida e raccomandazioni di policy".

Sintesi

L'uso massivo delle informazioni nell'ambito della società "data driven" – in particolare, dei dati personali – è un fenomeno vasto e globale, che non è limitato a specifici settori ma investe l'economia nel suo complesso. In questo scenario, i cosiddetti "big data" sollevano interrogativi che sono a cavallo tra concorrenza, privacy e pluralismo, così da richiedere uno stretto coordinamento ed un costante confronto tra le tre autorità di garanzia. In questa prospettiva, nel maggio 2017, il Garante, l'AGCM e l'AGCOM hanno avviato congiuntamente un'indagine conoscitiva sulle implicazioni dello sviluppo dell'economia digitale e, in particolare, del fenomeno dei Big Data per i tre domini supervisionati da tali autorità. Il documento conclusivo di tale indagine è prossimo alla pubblicazione ma, nel frattempo, è stato anticipato un documento di "Linee guida e raccomandazioni di policy" che contiene interessanti considerazioni sull'intreccio di concorrenza, privacy e pluralismo in tema di dati personali.

Antitrust, privacy e pluralismo: il caso Fb

L'esigenza di un coordinamento tra le tre autorità ha indotto il Supervisore Europeo per la protezione dei dati personali ("EDPS") ad istituire la Digital Clearing House per valutare le implicazioni dei Big Data sotto il profilo della tutela del consumatore, della concorrenza e della protezione dei dati personali ed ai cui lavori prendono parte sia l'AGCM sia l'AGCOM.
I Big Data sono espressione di una raccolta massiva di dati, «*acquisiti spesso non per esigenze attuali ma in vista di future, eventuali necessità e riutilizzati per fini ulteriori non sempre compatibili con quelli originari*» (Big Data e Libertà nella dimensione digitale).
Evidenza emblematica della confluenza dei tre domini dell'antitrust, della privacy e del pluralismo sull'identico tema dei dati personali è fornito dalle vicende che da ultimo hanno interessato Facebook.

AGCM contro Fb per violazione del codice del consumo

Nell'Alert del 13 dicembre 2018, cui si rinvia, l'antitrust italiana ha sanzionato in solido Facebook Inc. e Facebook Ireland Ltd. al pagamento di una somma pecuniaria complessiva di 10 milioni di euro per due distinte pratiche commerciali scorrette a danno dei consumatori:

- per aver **ingannato gli utenti** facendogli ritenere che l'iscrizione al social fosse gratuita, anzichè precisare in fase di attivazione dell'account che essa, in effetti, realizza una **transazione di natura commerciale** il cui corrispettivo è rappresentato dallo **sfruttamento commerciale dei dati personali degli utenti-iscritti**; e

- mediante la **trasmissione e l'uso dei medesimi dati** da parte di Fb e di terzi, per finalità commerciali, **senza espresso e preventivo consenso dei consumatori registrati**, peraltro **condizionando indebitamente** la libertà di scelta di questi ultimi, tramite la pre-selezione dell'opzione di consenso alla trasmissione e la **prospettazione di rilevanti limitazioni** del social network e dei siti web/app di terzi nell'eventualità di deselezione.

Antitrust tedesca contro Fb per abuso di posizione dominante

Il Bundeskartellamt, autorità antitrust tedesca, ha condannato Facebook per abuso di posizione dominante, come riportato nell'Alert del 23 maggio 2019, avendo quest'ultima combinato i dati degli account utenti del social network Facebook (Facebook.com), cioè di privati residenti in Germania, con le informazioni dei medesimi utenti di servizi aziendali WhatsApp, Oculus, Masquerade e Instagram, subordinando tale utilizzo – senza il consenso degli interessati – alla fornitura dei dati.

Garante privacy contro Fb per illecito trattamento di dati personali (Cambridge Analytica)

Sempre Facebook, questa volta sul versante italiano e sotto il profilo della protezione dei dati personali, ha subito una sanzione di 1 milione di euro a causa della comunicazione da parte di FB dei dati di utenti italiani alla app Thisisyourdigitallife, «*senza che questi l'avessero scaricata, fossero stati informati della cessione dei loro dati e avessero espresso il proprio consenso a questa cessione*». Il provvedimento di ordinanza ingiunzione è stato adottato dal Garante italiano sulla base delle disposizioni del precedente codice privacy; la sanzione è stata comunque ingente, in quanto «*le violazioni su informativa e consenso erano state commesse in riferimento ad una banca dati di particolare rilevanza e dimensioni – fattispecie questa per la quale non è ammesso il pagamento in misura ridotta*» e l'ammontare della sanzione «*tiene conto, oltre che della imponenza del database, anche delle condizioni economiche di Facebook e del numero di utenti mondiali e italiani della società*».

CNIL contro Google per analoghe violazioni data protection

L'Editoriale del 31 gennaio 2019 ha commentato il caso della sanzione inferta a Google dall'autorità privacy francese (CNIL) per la somma di 50 milioni di euro per aver effettuato trattamenti di dati personali degli utenti dei propri servizi – in particolare per pubblicità comportamentale – quando essi configurano il sistema operativo del proprio cellulare Android e creano un account Google

- rilasciando **informative poco chiare e non agevolmente accessibili** dagli utenti;
- in **assenza di una specifica base giuridica** per il trattamento dei dati e la profilazione.

Profilazione algoritmica, sfruttamento economico del dato e concentrazione di potere

Le linee guida delle tre autorità evidenziano come insieme «*agli indubbi vantaggi in termini di riduzione dei costi di transazione per imprese e cittadini consumatori,* (il fenomeno dei Big data trascina con sè) *nuovi rischi sotto il profilo concorrenziale, della protezione del dato personale e del pluralismo informativo*». La concentrazione di un enorme quantitativo di dati di vario tipo «i*n capo ai grandi operatori digitali, attivi*

su scala globale, (...) ha dato luogo a inedite forme di sfruttamento economico del dato e della sua valorizzazione ai fini della profilazione algoritmica legata a diversi scopi commerciali, generando nuove concentrazioni di potere, inteso non solo come 'potere di mercato', ma più in generale come potere economico e potere tout court, interessando i diritti fondamentali, i profili concorrenziali, il pluralismo e la stessa tenuta dei sistemi democratici.».

Dimensione globale del fenomeno

Il sistema dell'economia dei dati ha assunto una dimensione globale a seguito della crescente interdipendenza dei mercati e dei sistemi economici. Per questo le autorità antitrust istituite in ogni Stato membro e riunite nella Rete Europea della Concorrenza (European Competition Network – ECN), si confrontano riguardo all'applicazione delle regole di concorrenza relative ad operatori digitali all'interno del gruppo di lavoro, denominato "ECN Digital Markets". Il GDPR, nell'ambito della disciplina di protezione dei dati personali, ha previsto il modello di cooperazione rafforzata tra autorità nazionali di protezione dei dati personali (artt. 60 ss). Sotto il profilo del pluralismo informativo, l'Autorità per le Garanzie nelle Comunicazioni partecipa, in ambito BEREC, all'analisi riguardo all'impatto dell'economia dei dati (Data Economy) sui mercati delle comunicazioni elettroniche.

Economia dei dati e come merce di scambio

Con riferimento alla cosiddetta "economia dei dati" viene in evidenza il fenomeno dello scambio implicito di servizi a fronte del rilascio di permessi circa l'uso del dato personale, inteso come merce di scambio. A tal riguardo l'AGCOM ha «*evidenziato come molte app mostrino una relazione inversa tra prezzo di acquisto dell'app e permessi richiesti all'utente, talvolta anche per la medesima app. Appare indispensabile che l'utente, nelle decisioni di acquisto del servizio e di cessione del dato abbia piena consapevolezza della relazione tra permessi necessari al funzionamento dell'app e permessi ulteriori richiesti a seguito di cessione del dato. Sia l'applicazione della normativa sulla protezione dei dati personali che la strumentazione propria della tutela del consumatore possono offrire un contributo importante per la riduzione di tale asimmetria informativa, garantendo che gli utenti ricevano un'adeguata, puntuale e immediata informazione circa le finalità della raccolta e dell'utilizzo dei loro dati e siano posti nella condizione di esercitare consapevolmente ed effettivamente le proprie scelte di consumo. In questa prospettiva, appaiono opportune misure volte a rendere maggiormente consapevoli i consumatori nel momento in cui forniscono il consenso al trattamento dei loro dati personali.*». Il nuovo codice europeo delle comunicazioni elettroniche di cui alla Direttiva UE 2018/1972 dell'11 dicembre 2018, evidenzia che «*i servizi di comunicazione elettronica sono spesso forniti all'utente finale non solo in cambio di denaro, ma in misura sempre maggiore e in particolare in cambio della comunicazione di dati personali o di altri dati*» concludendo che il concetto di remunerazione dovrebbe pertanto ricomprendere anche «*le situazioni in cui l'utente finale è esposto a messaggi pubblicitari come condizione per l'accesso al servizio o le situazioni in cui il fornitore del servizio monetizza i dati personali raccolti in conformità del regolamento (UE) 2016/679*» (par. 16).

Asimmetria informativa tra grandi piattaforme ed altri operatori

Asimmetrie informative analoghe a quelle rilevate tra operatori ed utenti si registrano tra le grandi piattaforme digitali e gli altri operatori che si avvalgono di tali piattaforme; al riguardo, si rende necessario incrementare «*la trasparenza dei criteri con i quali i dati vengono analizzati ed elaborati (ad esempio, nella definizione del ranking relativo al posizionamento e alla visibilità sulla piattaforma) e favorendo*

l'ingresso di nuovi intermediari dei dati che, su mandato degli utenti e nel rispetto della normativa a tutela della privacy, possano interfacciarsi con le grandi piattaforme globali con un accresciuto potere negoziale in merito alla contrattazione sul valore del dato e sul suo impiego commerciale».

Promozione del pluralismo online

Ai fini della garanzia del pluralismo e della correttezza dell'informazione sulle piattaforme digitali, in aggiunta alle iniziative di autoregolazione, vengono caldeggiate «*iniziative legislative volte ad assicurare alle autorità indipendenti preposte alla tutela del pluralismo, poteri di audit e ispettivi circa la profilazione algoritmica ai fini della selezione delle informazioni e dei contenuti, nonché in relazione agli esiti dell'applicazione delle policy e delle regole che le piattaforme digitali globali si sono date in tema di rimozione di informazioni false o*» di espressioni d'odio (*hatespeech*).

Opt-in crocevia per privacy, antitrust e tutela del pluralismo

Con riferimento alle piattaforme digitali globali, i meccanismi di opt-in in merito al grado di profilazione prescelto, è una misura che soddisfa non solo le prescrizioni sulla protezione dei dati personali ma, insieme ad un'adeguata informativa, «*anche ai fini della tutela del pluralismo on-line, in relazione alla selezione dei contenuti operante attraverso la profilazione del consumatore*».

Portabilità del dato in favore della concorrenza ed a tutela del consumatore-utente

La portabilità del dato personale, sancita tramite il riconoscimento del diritto privacy alla portabilità dall'articolo 20 del GDPR, «*costituisce un obiettivo con una forte valenza pro-concorrenziale* (... la cui tutela) *potrebbe richiedere obblighi di mobilità e portabilità dei dati personali ulteriori rispetto a quelli previsti in generale dal*» GDPR, per «*lo sviluppo della competizione nei vari ambiti di valorizzazione economica del dato e, di conseguenza, una più efficace tutela del consumatore-utente*».

27.
Valzer di sanzioni “privacy”, 12a plenaria EDPB ed altre news

Molte le notizie interessanti da registrare sotto il cielo del data protection in queste ultime due settimane:

- **sanzioni "privacy" che fanno "rumore"**, non solo irrogate sul versante del vecchio continente ma anche oltre-atlantico;
- relazione annuale ENISA sugli **incidenti di sicurezza nei servizi fiduciari**;
- modifica della **legge tedesca sui requisiti minimi per l'obbligatorietà della nomina del DPO**;
- provvedimenti adottati nella dodicesima seduta plenaria dell'EDPB tenutasi il 9 e 10 luglio 2019 su **videosorveglianza**, **white list per DPIA**, **clausole contrattuali tipo tra titolari e responsabili**, **criteri di accreditamento degli organismi di monitoraggio dei codici di condotta**, **competenza dell'autorità di supervisione in caso di trasferimento dello stabilimento unico o principale**, implicazioni derivanti dal **Clouds Act** statunitense (Clarifying Lawful Overseas Use of Data Act).

Panorama delle sanzioni "privacy"

Stiamo assistendo ad un crescendo di sanzioni amministrative irrogate per violazioni inerenti la disciplina della protezione dei dati personali, da autorità di controllo non solo della UE; le somme in questione hanno registrato un'*escalation* che, in breve, è passata dall'ordine delle centinaia di migliaia di euro, ai milioni, sino ad atterrare da ultimo su valori di miliardi.
L'autorità di supervisione inglese, l'ICO, ha predisposto un interessante strumento di raccolta e descrizione delle sanzioni irrogate nel frattempo dalle diverse autorità di supervisione degli Stati membri dell'Unione in base al GDPR, reperibile all'indirizzo http://www.enforcementtracker.com/. Di seguito offriamo alcuni esempi di questa vertiginosa ascesa.

Garante privacy contro Wind Tre

Nel novembre 2018 [doc. web n. 9079005], applicando la disciplina del previgente codice privacy, il Garante italiano aveva multato Wind Tre per **600 mila euro** per violazioni data protection nel corso di attività di marketing telefonico, anche tramite SMS. Gli addebiti consistevano nell'aver usato senza consenso i dati dei clienti a fini promozionali e, sempre senza consenso, nell'averli comunicati alla rete dei propri partner commerciali.

Garante privacy per violazioni in tema di telemarketing e teleselling

Con ordinanza ingiunzione dell'11 aprile 2019 [doc. web n. 9116053] il Garante sanziona per oltre **2 milioni di euro** un'azienda che svolge attività di telemarketing e teleselling tramite "call center" per conto di più committenti, per non aver fornito l'informativa ed acquisito il consenso dagli interessati per il trattamento dei propri dati a fini di marketing. Anche in questo caso la sanzione viene irrogata applicando la disciplina del previgente codice privacy, per ciascuna delle violazioni riscontrate.

CNIL contro Google

Avevamo commentato, nella puntata dell'Editoriale del 31 gennaio 2019, la sanzione inferta a Google dall'autorità privacy francese (CNIL) per la somma di **50 milioni di euro** per aver

effettuato trattamenti di dati personali degli utenti dei propri servizi – in particolare per pubblicità comportamentale – quando essi configurano il sistema operativo del proprio cellulare Android e creano un account Google, a seguito di informative inadeguate e per l'assenza di una specifica base giuridica. In questa circostanza, il CNIL ha applicato le prescrizioni del GDPR.

Garante privacy contro Facebook per Cambridge Analytica

Nel medesimo Editoriale del 31/1/2019 si è data notizia del provvedimento di ordinanza ingiunzione con cui il Garante italiano condannava Facebook al pagamento della somma di **un milione di euro** – sulla base delle disposizioni del precedente codice privacy – per violazioni compiute dall'azienda di Zuckerberg in materia di informativa e consenso «*in riferimento ad una banca dati di particolare rilevanza e dimensioni*» avuto riguardo allo scandalo di Cambridge Analytica.

L'autorità di supervisione inglese (ICO) sanziona per data breach

L'8 ed il 9 luglio 2019 l'autorità di supervisione UK (ICO) ha comunicato l'intenzione di sanzionare British Airways e Marriott International, rispettivamente per **183 milioni** e **99 milioni di sterline**, entrambi per importanti casi di data breach, applicando le regole del GDPR.

Caso British Airways

Il caso British Airways ha riguardato un incidente informatico notificato all'ICO nel settembre 2018, quindi dopo la piena applicazione del regolamento europeo (25 maggio 2018). L'incidente, che ha visto coinvolto circa 500.000 clienti, era in parte consistito nel dirottamento su un sito fraudolento, del traffico degli utenti diretto sul sito web di BA. L'indagine dell'autorità inglese ha rilevato che le informazioni (inclusi il login, la carta di pagamento e i dettagli della prenotazione del viaggio oltre a informazioni su nome e indirizzo) sono state compromesse a causa delle pessime disposizioni sulla sicurezza dell'azienda. L'ICO ha indagato su questo caso come autorità di supervisione capofila per conto di – ed in collaborazione con – altre autorità di protezione dei dati degli Stati membri dell'UE. British Airways avrà ora l'opportunità di presentare osservazioni all'ICO in merito ai risultati delle indagini e alle sanzioni proposte, prima che l'autorità adotti la propria decisione finale.

Caso Marriott International

Anche nel caso Marriott l'ICO ha notificato all'azienda – al termine di una complessa fase investigativa – la propria intenzione di sanzionarla per una somma pari a 99 milioni di sterline per violazioni del GDPR a seguito di un incidente informatico notificato all'autorità nel novembre 2018.

Il breach ha riguardato una serie di dati personali relativi a ospiti della catena alberghiera Starwood, acquisita nel 2016 da Marriott, residenti in 31 paesi dello Spazio Economico Europeo (SEE). L'indagine ha accertato che i sistemi del gruppo Starwood sono stati compromessi nel 2014, ma l'incidente è stato scoperto solo nel 2018. L'ICO ha ritenuto Marriott responsabile per non aver effettuato un'adeguata due diligence quando ha comprato Starwood e per non aver fatto quanto necessario per proteggere i suoi sistemi.

FTC sanziona Fb per 5 miliardi di dollari per Cambridge Analytica

Nel marzo 2018 la Federal Trade Commission – l'agenzia governativa statunitense cui compete la tutela dei consumatori e del mercato interno – all'indomani della notizia dello scandalo Cambridge Analytica aveva intrapreso le proprie indagini accertando l'accesso abusivo ai dati personali di 87 milioni di utenti Facebook. «*La Ftc è fermamente e completamente impegnata ad usare tutti i mezzi a sua disposizione per proteggere la privacy dei consumatori*», aveva fatto sapere il direttore ad interim dell'agenzia Tom Pahl. Giorni orsono i media hanno dato la notizia dell'approvazione da parte di FTC di una bozza di accordo con Facebook (cosiddetto "*consent decree*"), in base al quale l'azienda di Zuckerberg si impegnerebbe a pagare circa 5 miliardi di dollari per porre fine all'indagine della FTC volta a verificare se FB abbia violato un precedente "consent decree" con cui FTC imponeva alla società di proteggere meglio la privacy degli utenti.
L'accordo dovrà essere formalizzato dal Dipartimento di Giustizia il quale, storicamente, non interviene sui contenuti dell'intesa.

Fumo negli occhi?

Il voto della FTC è stato 3-2, con i tre repubblicani della FTC che hanno votato a favore dell'accordo mentre i due democratici hanno votato contro (ritenendo le misure richieste a Fb non sufficientemente restrittive). La contrarietà dei democratici induce ad una diversa chiave interpretativa di quella che altrimenti parrebbe essere la sanzione del secolo: cinque miliardi di dollari di sanzione è una misura realmente deterrente per Fb? Un editoriale di Mila Fiordalisi apparso il 13 luglio su CorCom titola "La multa da 5 miliardi a Facebook? Un regalo senza precedenti". L'articolo evidenzia che sebbene sia la più alta sanzione mai comminata, «*il titolo è balzato in Borsa ai massimi da luglio dello scorso anno. E non a caso. Misure stringenti in tema di privacy sarebbero state ben più onerose*». Cinque miliardi sarebbero il guadagno di appena un mese per Fb. «*La Ftc avrebbe potuto optare, oltre alla multa, per una decisione nel merito delle azioni presenti e future in tema di privacy, inasprendo le policy e i controlli a carico di Facebook*».
Queste considerazioni forniscono la cifra dei problemi in gioco: gli Over the Top (OTT) hanno acquisito un potere economico globale che sembrerebbe scalfire i tradizionali strumenti coercitivi del potere politico degli stati sovrani. Per questo le iniziative di raccordo, come l'indagine conoscitiva congiunta delle tre authority italiane sui Big Data (v. l'Editoriale dell'11 luglio 2019) o quella di cooperazione tra i regolatori francesi, appaiono come i primi passi compiuti dal potere politico per affilare le armi contro i nuovi signori del pianeta.

Relazione annuale ENISA sugli incidenti di sicurezza nei servizi fiduciari

L'agenzia europea sulla cybersicurezza (European Union Agency for Cybersecurity – ENISA) ha pubblicato la relazione annuale sugli incidenti di sicurezza nei servizi fiduciari per l'anno 2018, da cui si possono trarre interessanti spunti a livello generale nel contesto della sicurezza cibernetica. I **servizi fiduciari elettronici** sono una gamma di servizi relativi a firme elettroniche, certificati digitali, sigilli elettronici, validazione temporale elettronica, ecc. che vengono utilizzati nelle transazioni elettroniche per renderle sicure. Trattandosi, quindi, di strumenti atti a garantire la sicurezza delle transazioni ed a incrementare la fiducia degli utenti nell'intero settore digitale, si comprende bene come il monitoraggio degli incidenti di sicurezza relativi a tale contesto sia di particolare rilevanza. Il tema dei servizi fiduciari elettronici prestati al

pubblico è stato disciplinato dal noto regolamento n. 910/2014 (noto come regolamento eIDAS, v. Editoriale del 5 aprile 2018) attualmente in vigore (1 luglio 2016). Il regolamento eIDAS prescrive che gli incidenti che causino un significativo impatto ai servizi fiduciari devono essere notificati all'autorità competente: la relazione, pertanto, esamina l'andamento di tali notifiche e le caratteristiche degli incidenti che ne formano oggetto. In sintesi, «*azioni dolose e guasti del sistema sono le cause principali degli incidenti segnalati: in caso di guasto del sistema, la percentuale corrispondente (39% del totale) è coerente con l'anno precedente (36% del totale nel 2017). Le azioni dolose sono aumentate rapidamente dallo scorso anno (7% del totale nel 2017) e rappresentano quasi i due quinti degli incidenti segnalati (39% del totale); (...) all'incirca la metà degli incidenti segnalati ha influito sulla creazione qualificata di certificati qualificati per le firme elettroniche.*».

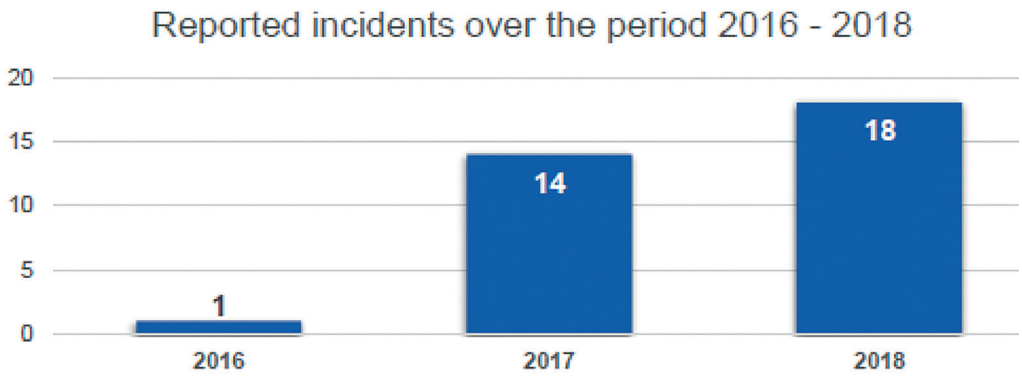


Fig. 1 - Andamento delle notifiche data breach in ottica eIDAS.

La Germania modifica le condizioni per l'obbligatorietà del DPO

Il 28 giugno 2019, il parlamento tedesco (Bundestag) ha approvato una nuova legge imponendo diverse modifiche all'attuale legge federale tedesca sulla protezione dei dati, tra cui la soglia di sbarramento che fa scattare l'obbligatorietà della designazione del DPO, sinora prevista nell'assegnazione di operazioni di trattamento automatizzato di dati personali ad un numero di dipendenti superiore a 9 unità: quindi, il numero di 9 non riguarda la totalità dei dipendenti dell'azienda di riferimento ma solo di quei lavoratori che utilizzano dati personali in via automatizzata (anche se la differenza tra i due concetti, allo stato delle condizioni lavorative correnti, diviene sempre più labile). La nuova legge – che prima di entrare in vigore deve essere approvata dal Consiglio federale tedesco (Bundesrat) – aumenta il numero minimo della citata soglia di dipendenti da 10 a 20, in tal modo eliminando l'obbligo del DPO per un significativo numero di imprese, visto che l'80% delle imprese tedesche registrano meno di 20 dipendenti.

La Germania è uno di quei pochi paesi europei che aveva previsto normativamente la figura del DPO già durante la vigenza della direttiva 95/46/CE, avvalendosi della facoltà prevista all'articolo 18 della medesima direttiva, come possibile alternativa all'obbligo di notifica dei trattamenti all'autorità.

Dodicesima sessione plenaria dell'EDPB

Il 9 e 10 luglio 2019, in occasione della dodicesima sessione plenaria, il Comitato europeo ha adottato una serie di importanti iniziative:

- il rilascio di **linee guida 3/2019 sulla videosorveglianza** sottoposte a consultazione pubblica;
- il parere congiunto EDPB-EDPS 1/2019 alla Commissione LIBE sulle implicazioni del **Cloud Act statunitense**: Il CLOUD Act consente alle autorità di contrasto statunitensi di richiedere la fornitura di dati da parte dei fornitori di servizi cloud negli Stati Uniti, indipendentemente da dove sono memorizzati i dati. L'EDPB e l'EDPS sottolineano che un accordo globale UE-USA sia lo strumento più appropriato per garantire il necessario livello di protezione degli interessati dell'UE e certezza del diritto per le imprese;
- il parere 14/2019 sulle **clausole contrattuali tipo per responsabili,** emesse dall'autorità danese, oggetto di una nostra prossima analisi;
- il parere 9/2019 sui **criteri di accreditamento degli organismi di monitoraggio dei Codici di condotta**, emessi dall'autorità austriaca;
- il parere 8/2019 sulla **competenza dell'autorità di supervisione in caso di trasferimento dello stabilimento unico o principale,** ciò può verificarsi quando lo stabilimento principale è trasferito all'interno del SEE, uno stabilimento principale è trasferito nel SEE da un paese terzo o quando non vi è più un singolo stabilimento principale nel SEE. Se, in tali circostanze, il ruolo di autorità capofila passa ad un'altra autorità di supervisione, la nuova autorità capofila coopererà con la precedente e con le altre autorità interessate per raggiungere un consenso, secondo la procedura di cooperazione dell'articolo 60;
- il parere sulle "liste bianche", ai sensi dell'articolo 35.5, cioè dei **trattamenti per i quali non si ritiene necessaria la DPIA**, emesse dalle autorità francese (parere 13/2019), spagnola (parere 12/2019) e ceca (parere 11/2019).

Bozza di linee guida 3/2019 su videosorveglianza

Il Comitato europeo ha adottato il testo preliminare delle linee guida 3/2019 sulla videosorveglianza. Il documento è sottoposto a consultazione pubblica che terminerà il 6 settembre 2019.

I titolari che hanno intenzione di installare impianti di videosorveglianza dovranno tener conto, pertanto, del combinato disposto delle linee guida 3/2019 dell'EDPB (nella versione che sarà quella finale) e del provvedimento generale del Garante del 2010 [doc. web. n. 1712680].

Contenuti delle linee guida 3/2019

Il testo preliminare delle linee guida 3/2019, su cui ci soffermeremo in altra tornata, è strutturato come segue:

- **Ambito di applicazione**: in cui viene precisato cosa è disciplinato dal regolamento e cosa rimane fuori dall'applicazione del GDPR.
- **Liceità del trattamento**: in cui viene ribadita la necessità di documentare per iscritto la finalità perseguita tramite ciascuna telecamera.

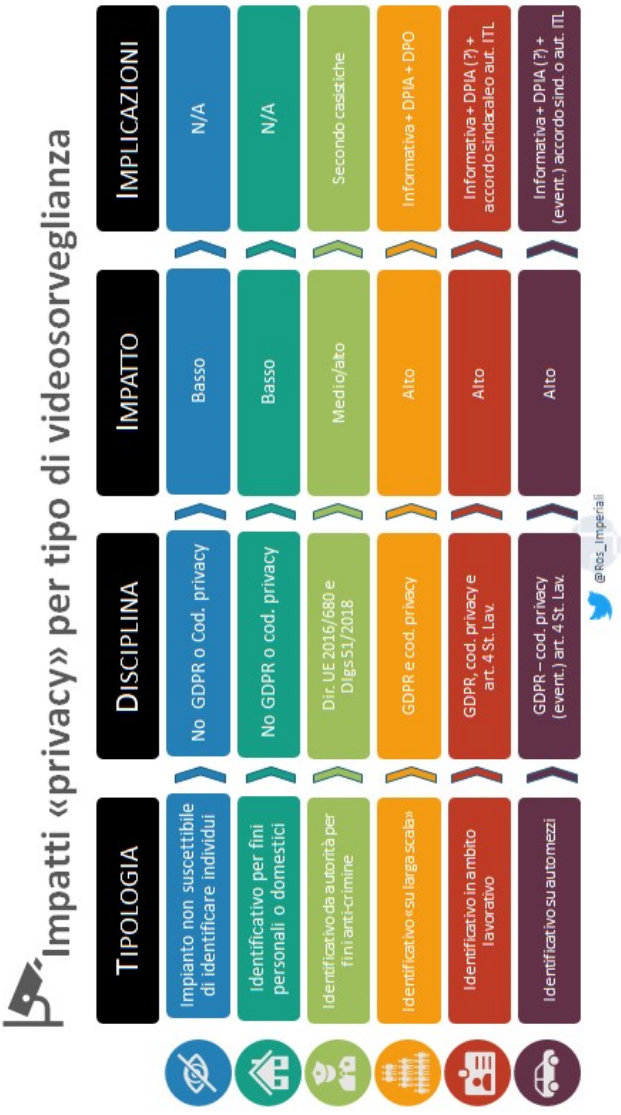
- **Basi giuridiche**: dove si sottolinea come la condizione di liceità cui si farà ricorso più frequentemente sarà il legittimo interesse del titolare, seguita dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.
- **Consenso**: si evidenzia, inoltre, che il ricorso al consenso degli interessati appare come ipotesi del tutto residuale, su base di eccezione.
- **Speciali categorie di dati personali**: nel caso di raccolta di speciali categorie di dati personali – come nella videosorveglianza collegata a sistemi di riconoscimento facciale – occorre rispettare le prescrizioni relative all'uso di tali dati (art. 9) e al trattamento di dati biometrici, prima fra tutte, la raccolta del consenso "esplicito" degli interessati.
- **Informativa**: considerate le particolari modalità del trattamento di videosorveglianza, l'informativa viene rilasciata su due livelli, il primo con cartellonistica che riporta le informazioni principali ed un secondo livello che contiene per esteso quanto prescritto dall'articolo 13
- **Comunicazione a terzi**: la divulgazione delle immagini a terzi costituisce un trattamento ulteriore rispetto alla raccolta e conservazione, per cui deve trovare giustificazione in una specifica base giuridica.
- **Diritti**: tutti i diritti degli interessati devono poter essere esercitati anche riguardo ai trattamenti con videosorveglianza; le particolari caratteristiche dello stesso possono determinare alcune specificità come per l'esercizio del diritto di accesso.
- **Conservazione dei dati**: le immagini vanno conservate per un tempo limitato, funzionale alla finalità perseguita (su questo aspetto il provvedimento generale del Garante del 2010 contiene disposizioni di dettaglio che sono tuttora valide).
- **Misure tecnico organizzative**: le linee guida suggeriscono l'adozione di misure sia di natura fisica sia riguardo ai sistemi ed ai dati.
- **DPIA**: per ogni impianto di videosorveglianza si dovrà valutare la sussistenza di un presumibile rischio elevato per i diritti e le libertà degli interessati, tale da rendere obbligatoria una specifica DPIA; già il GDPR prescrive la DPIA per le due ipotesi di (a) monitoraggio sistematico di un'area accessibile al pubblico, su larga scala e (b) trattamento di speciali categorie di dati personali, su larga scala.

In una prossima tornata approfondiremo in dettaglio il contenuto delle linee guida 3/2019.

28.
EDPB: bozza linee guida 3/2019 su videosorveglianza - Prima puntata

L'Alert del 18 luglio 2019 ha dato notizia del rilascio della versione preliminare delle linee guida 3/2019 sulla videosorveglianza da parte dell'EDPB. Il documento è sottoposto a consultazione pubblica che terminerà il 6 settembre 2019. La materia è di interesse visto il diffuso utilizzo di telecamere di videosorveglianza da parte di enti ed imprese per finalità di sicurezza pubblica, organizzative, produttive, di sicurezza sul lavoro o di tutela del patrimonio aziendale. In aggiunta, lo sviluppo della tecnologia ci evidenzia importanti evoluzioni in questo ambito soprattutto collegate ad applicazioni biometriche, come quella del riconoscimento facciale, con gravi impatti riguardo ai diritti ed alle libertà degli interessati.

Sintesi



Il Comitato europeo (EDPB) ha rilasciato la versione preliminare delle linee guida 3/2019 sulla videosorveglianza, sottoponendola alla procedura di consultazione pubblica. Imprenditori pubblici e privati dovranno attenersi a tali indicazioni insieme al rispetto delle prescrizioni imposte dal provvedimento generale del Garante del 2010 sulla videosorveglianza, avendo particolare cura alla corretta disposizione della cartellonistica ed ai suoi contenuti, ai ruoli assegnati a coloro che hanno accesso alle immagini ed alle misure di sicurezza a tutela delle stesse. In aggiunta, quando l'attività di videosorveglianza viene svolta in ambito lavorativo, essa si trova ad un crocevia normativo caratterizzato dallo Statuto dei Lavoratori (l. n. 300/1070), da GDPR e codice privacy (dlgs n. 196/2003) e da talune norme speciali. Eventuali violazioni alle disposizioni dell'articolo 4 dello Statuto, non solo determinano un'ipotesi di contravvenzione penale (che sarà il giudice penale a verificare) ma comportano anche l'illiceità del trattamento dei relativi dati personali (cioè le immagini raccolte) per violazione dell'articolo 5(1)(a) del GDPR. Il rispetto della procedura multilivello prevista dallo Statuto è quindi un presupposto di liceità fondamentale.

Videosorveglianza e dati personali

Le immagini e tracce audio registrate dagli impianti di videosorveglianza sono qualificabili come "dati personali", in quanto consentono di identificare, anche indirettamente, singoli individui (Provv. 8 aprile 2010, doc. web n. 1712680; v. anche, del Gruppo di lavoro dei Garanti europei, parere n. 8/2001 wp 48 e parere 4/2007 sulla nozione di "dato personale", wp 136). Quindi, le operazioni di raccolta e registrazione di immagini e suoni, effettuate con queste apparecchiature, costituiscono un trattamento di dati personali, che deve essere conforme alle disposizioni in materia (cioè GDPR e codice privacy).

Videosorveglianza nei diversi ambiti

Il fenomeno della videosorveglianza ha un ambito di applicazione molto ampio e, secondo contesti e finalità, mutano le condizioni della disciplina.

Di interesse è la precisazione contenuta nelle linee guida 3/2019 secondo cui la **finalità** perseguita deve essere **documentata per iscritto riguardo a ogni telecamera in uso** (potendo queste essere raggruppate per scopi comuni) (articolo 5, paragrafo 2, GDPR). Si consideri, ad esempio, un unico sistema di videosorveglianza in cui alcune telecamere soddisfino esigenze di controllo accessi per motivi di sicurezza privata, altre di tutela del patrimonio ed altre ancora di tutela dei luoghi di lavoro.

In aree pubbliche

La **videosorveglianza su aree pubbliche** può determinare un monitoraggio di individui su larga scala con importanti implicazioni sui diritti e libertà di costoro. Questo rischio è riflesso nel GDPR allorquando:

- la **sorveglianza sistematica su larga scala di una zona accessibile al pubblico** è considerata situazione che rende obbligatoria la valutazione di impatto (DPIA, art. 35(3)(c) GDPR);
- il **monitoraggio regolare e sistematico degli interessati su larga scala**, fa scattare l'obbligo di designazione del DPO, se esso rappresenta l'attività principale di titolare o responsabile del trattamento (art. 37(1)(b) GDPR).

Ambito lavorativo

Gli **impianti di telecamere in ambito lavorativo** soddisfano prevalentemente finalità di protezione e incolumità del personale e di eventuali visitatori, di protezione del patrimonio aziendale e di acquisizione di prove (cd. controlli difensivi).
L'installazione di un impianto di videosorveglianza in azienda vede l'applicazione sia delle norme sulla protezione dei dati personali sia di quelle statutarie sui controlli "a distanza" che si applicano indistintamente ai soggetti sia pubblici che privati; mentre, ad oggi, manca in Italia una regolamentazione normativa specifica sulla videosorveglianza. Resta vietata l'installazione di impianti di videosorveglianza aventi lo scopo di controllare l'attività dei lavoratori mentre è ammessa la videosorveglianza per finalità organizzative, produttive, di sicurezza sul lavoro o di tutela del patrimonio aziendale, purchè nel rispetto della procedura multilivello dell'accordo sindacale o, in mancanza, dell'autorizzazione ITL (art. 4, l. n. 300/1970).

Videosorveglianza fuori dall'ambito GDPR

In talune circostanze, l'impianto di videosorveglianza non è soggetto all'applicazione del GDPR. In alcuni casi, ad esso si applicano disposizioni diverse, sempre nel dominio della tutela dei dati personali, in altre ipotesi, invece, le telecamere possono essere installate senza che sia prevista alcuna specifica disciplina.

Finalità anti-crimine

La videosorveglianza spesso persegue finalità di sicurezza pubblica o costituisce una forma di difesa passiva e di deterrenza di fenomeni criminosi e vandalici. In particolare il trattamento dei dati personali **da parte delle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati** o esecuzione di sanzioni penali, compresa la tutela e la prevenzione di minacce alla sicurezza pubblica, esula dall'ambito applicativo del GDPR e rientra nella direttiva UE 2016/680, attuata in Italia col decreto legislativo 51/2018.

Finalità personali o domestiche

Analogamente, l'installazione di **telecamere in luoghi privati per finalità personali o domestiche**, esula dall'ambito di applicazione dell'intera disciplina sulla protezione dei dati personali, a condizione che le riprese non riguardino aree pubbliche oppure che le immagini registrate non siano poi pubblicate su Internet.

Immagini non identificative

Altra ipotesi di esclusione dell'applicazione della norma è il caso di impianti di videosorveglianza che **non siano suscettibili di identificare individui**, nemmeno indirettamente, come, ad esempio, le telecamere a bassa risoluzione poste sulle vie di comunicazione stradali al fine di verificare il flusso dei veicoli, inidonee a catturare dettagli come il numero delle targhe o l'identità dei passeggeri.

Provvedimento generale del Garante del 2010

Il tema della videosorveglianza è stato affrontato in precedenza dal Garante italiano con due provvedimenti generali del 2004 e del 2010 [doc. web. n. 1712680], quest'ultimo sostitutivo del

precedente. Il provvedimento del 2010 può ritenersi compatibile con le disposizioni del GDPR e, quindi, produce i suoi effetti anche dopo la piena applicazione del regolamento europeo (25 maggio 2018).

Contenuti delle linee guida 3/2019

Il testo preliminare delle linee guida 3/2019 è strutturato come segue:

- **Ambito di applicazione**: in cui viene precisato cosa è disciplinato dal regolamento e cosa rimane fuori dall'applicazione del GDPR.
- **Liceità del trattamento**: in cui viene ribadita la necessità di documentare per iscritto la finalità perseguita tramite ciascuna telecamera.
- **Basi giuridiche**: dove si sottolinea che la base giuridica applicabile con maggior frequenza sarà il legittimo interesse del titolare, seguita dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri.
- **Consenso**: si, evidenzia inoltre, che il ricorso al consenso degli interessati appare come ipotesi del tutto residuale, su base di eccezione.
- **Speciali categorie di dati personali**: nel caso di raccolta di speciali categorie di dati personali – come nella videosorveglianza collegata a sistemi di riconoscimento facciale – occorre rispettare le prescrizioni relative al trattamento di dati biometrici, prima fra tutte, la raccolta del consenso "esplicito" degli interessati e consentire una soluzione alternativa, meno invasiva.
- **Informativa**: considerate le particolari modalità del trattamento di videosorveglianza, l'informativa viene rilasciata su due livelli, il primo con cartellonistica che riporta le informazioni principali ed un secondo livello che contiene per esteso quanto prescritto dall'articolo 13.
- **Comunicazione a terzi**: la divulgazione delle immagini a terzi costituisce un trattamento ulteriore rispetto alla raccolta e conservazione, per cui deve trovare giustificazione di una specifica base giuridica.
- **Diritti**: tutti i diritti degli interessati devono poter essere esercitati anche riguardo ai trattamenti con videosorveglianza; le particolari caratteristiche dello stesso possono determinare alcune specificità come nel caso dell'esercizio del diritto di accesso.
- **Conservazione dei dati**: le immagini vanno conservate per un tempo limitato, funzionale alla finalità perseguita (su questo aspetto il provvedimento generale del Garante del 2010 contiene disposizioni di dettaglio che sono tuttora valide).
- **Misure tecnico organizzative**: le linee guida suggeriscono l'adozione di misure sia di natura fisica sia riguardo ai sistemi ed ai dati.
- **DPIA**: per ogni impianto di videosorveglianza si dovrà valutare la sussistenza di un presumibile rischio elevato per i diritti e le libertà degli interessati, tale da rendere obbligatoria una specifica DPIA; già il GDPR prescrive la DPIA per le due ipotesi di (a) monitoraggio sistematico di un'area accessibile al pubblico, su larga scala e (b) trattamento di speciali categorie di dati personali, su larga scala.

Ambito di applicazione: identificazione di individui

L'impianto di videosorveglianza rientra nell'ambito della disciplina sulla protezione dei dati nei limiti in cui le immagini degli individui ripresi consentano il loro riconoscimento, in via diretta

o indiretta (V. Parere 4/2007 del Gruppo dei Garanti europei dell'art. 29, wp 136, par. 1.). L'affermazione va chiarita nel senso che per l'applicabilità della disciplina sulla protezione dei dati non è necessario che la riconoscibilità sia effettiva ma basta che essa risulti materialmente possibile. Diverso, invece, è il caso in cui il sistema sia strutturato in modo tale che le riprese abbiano un livello di risoluzione tale da non consentire comunque l'identificazione oppure il sistema stesso sia configurato in modo da alterare le sagome riprese in modo da non consentirne l'identificazione: ad esempio perché scopo dell'impianto di videosorveglianza sia la registrazione dei soli movimenti umani e non anche il riconoscimento delle persone riprese. In conclusione, se l'impianto è strutturato in modo tale che non sia possibile in alcun modo identificare gli individui ripresi, ad esso non si applicherà nè il GDPR nè il codice privacy. Va ricordato, tuttavia, che nell'ambito lavorativo sia il divieto del controllo dell'attività lavorativa sia l'obbligo della procedura in presenza di finalità legittime «*non è escluso né dalla circostanza che* ***tali apparecchiature siano state solo installate ma non ancora funzionanti****, né dall'eventuale preavviso dato ai lavoratori, i quali quindi siano avvertiti del controllo suddetto, né infine dal fatto che tale controllo sia destinato ad essere discontinuo perché esercitato in locali dove i lavoratori possono trovarsi solo saltuariamente*» (Cass. 6.3.1986, n. 1490).

Liceità del trattamento

L'installazione delle telecamere deve soddisfare tutte le prescrizioni di legge (ad es. Statuto, GDPR e codice privacy). In base al principio del rispetto del divieto di controllo "a distanza" dell'attività dei lavoratori, ad esempio, il citato provvedimento del Garante del 2010 esclude l'utilizzo delle telecamere «*per verificare l'osservanza (…) dell'orario di lavoro e la correttezza nell'esecuzione della prestazione lavorativa (ad es. orientando la telecamera sul badge)*».

Legge concretezza

Rispetto alla posizione assunta dal Garante nel citato provvedimento del 2010 va sottolineato che la cosiddetta "legge concretezza" è intervenuta con un'apposita disposizione di contrasto ai cosiddetti "furbetti del cartellino" nella pubblica amministrazione. In base all'articolo 2 della legge n. 56/2019, a fini di prevenzione dell'assenteismo, si è stabilito che «*ai fini della verifica dell'osservanza dell'orario di lavoro, le amministrazioni pubbliche (... con talune eccezioni), introducono, (...) sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi, in sostituzione dei diversi sistemi di rilevazione automatica, attualmente in uso, nel rispetto dei principi di proporzionalità, non eccedenza e gradualità sanciti dall'articolo 5, paragrafo 1, lettera c), del (GDPR), e del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea.*». Il termine "gradualità" riportato nella legge non è in sintonia con la terminologia del GDPR che si riferisce, piuttosto, al principio di minimizzazione, vale a dire che i dati raccolti siano limitati a quanto necessario rispetto alle finalità del trattamento.

L'individuazione delle modalità attuative per l'introduzione di tali nuovi sistemi è demandata ad un decreto del Presidente del Consiglio dei ministri, avente natura regolamentare, previo parere del Garante sulle modalità' di trattamento dei dati biometrici, nel rispetto delle prescrizioni previste dal GDPR per il trattamento dei dati sensibili (art. 9), e delle misure di garanzia definite dal Garante stesso (ai sensi dell'articolo 2-septies del codice privacy).

Basi giuridiche

In prospettiva di protezione dei dati, deve preliminarmente stabilirsi il presupposto giuridico che legittima il trattamento delle immagini registrate dall'impianto (ad esempio, se l'installazione sia necessaria per eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, oppure, in quanto essa rientri nell'adempimento di un obbligo di legge oppure perché sia necessaria per soddisfare un interesse legittimo del titolare del trattamento.
Sebbene, in teoria, ognuna delle basi giuridiche elencate all'articolo 6 del GDPR può costituire il fondamento che legittima l'installazione, quelle che risulteranno di fatto prevalenti riguardo alla videosorveglianza sono:

- il legittimo interesse del titolare del trattamento;
- il compito di interesse pubblico o connesso all'esercizio di pubblici poteri (per gli enti pubblici);
- in circoscritte ipotesi, il consenso degli interessati.

Legittimo interesse

L'interesse del titolare del trattamento o di un terzo, che può rappresentare la giustificazione giuridica della legittimità dell'installazione e del relativo trattamento di dati [ai sensi dell'art. 6(1) (f) GDPR], può avere natura giuridica, economica o immateriale; in ogni caso, occorre che tale interesse sia effettivo ed attuale anzichè vago o teorico. In caso di opposizione alla videosorveglianza da parte dell'interessato, il titolare può proseguire in tale attività solo nel caso in cui il proprio interesse risulti "cogente", tale da prevalere sugli interessi, diritti e libertà dell'interessato oppure sia necessario per l'accertamento, l'esercizio o la difesa di un diritto in giudizio. Pertanto, in un reale contesto di documentato pericolo, un impianto di videosorveglianza a difesa della proprietà e contro atti di vandalismo, può fondarsi sul legittimo interesse del titolare. La valutazione del bilanciamento degli interessi in gioco, quelli del titolare e degli interessati (specie riguardo agli effetti negativi che possono essere prodotti nei loro confronti), va effettuato caso per caso, giudicando se non sussistano soluzioni meno intrusive per soddisfare le medesime necessità. L'intensità dell'impatto sui diritti e le libertà degli interessati, la tipologia di immagini raccolte, l'ampiezza geografica del monitoraggio, il numero di interessati coinvolti, la ragionevole aspettativa degli interessati, sono tutti importanti criteri del giudizio di bilanciamento dei contrapposti interessi.

Consenso

Su base di eccezione, in casi residuali, il fondamento giuridico che legittima l'installazione di un impianto di videosorveglianza può riscontrarsi anche nel consenso degli interessati.
In linea generale, l'ipotesi può sussistere in quelle circostanze in cui, di regola, la videosorveglianza è posta nell'interesse o a corredo di specifiche attività svolte dagli interessati; questi ultimi devono poter essere liberi di scegliere se acconsentire o meno alle riprese senza che un eventuale rifiuto ne condizioni l'operato o si renda tecnicamente ingestibile.
Le linee guida 3/2019 propongono al riguardo l'esempio di atleti che richiedono il monitoraggio durante gli esercizi individuali al fine di analizzare le loro tecniche e prestazioni. In tal caso il preventivo consenso, in quanto libero, costituirebbe il fondamento giuridico per le riprese, mentre un eventuale diniego potrebbe essere gestito escludendo dalle riprese l'allenamento degli interessati che si sono rifiutati.

Diversamente, laddove una società sportiva prendesse l'iniziativa di monitorare un'intera squadra per lo stesso scopo, il consenso potrebbe non essere valido, poiché i singoli atleti potrebbero sentirsi spinti a dare il consenso (cioè potrebbero sentirsi condizionati) per evitare che l'eventuale rifiuto possa influire negativamente sui compagni di squadra.

29.
Carte fedeltà e marketing

Con la newsletter n. 456 del 22 luglio, il Garante ha reso nota la pubblicazione del provvedimento relativo alle interrelazioni tra eventuali programmi di fedeltà – con emissione delle relative fidelity card – e l'utilizzo dei dati personali così raccolti per l'ulteriore finalità di marketing. Il provvedimento, sebbene riguardi trattamenti soggetti all'applicazione del previgente codice privacy (cioè prima del GDPR), presenta numerosi spunti – ancorchè di contenuto non innovativo – che consentono di riassumere le maggiori avvertenze che la funzione marketing di un'azienda dovrebbe avere ben presente e riuscire a tenere sotto controllo.
Con questa puntata, il Servizio di Informazione Giuridica del DPtel® è sospeso per la pausa feriale estiva e riprende con la puntata dell'Editoriale del 5 settembre; la redazione augura buone vacanze a tutti i suoi lettori.

Finalità di fidelizzazione e di marketing

I programmi fedeltà – detti anche "loyalty program" basati sulle carte fedeltà – sono programmi per clienti abituali, progettati per ricompensare la fedeltà al fornitore e per incoraggiarli a restare tali tramite sconti, premi o altre facilitazioni esclusive. In realtà, l'iscrizione al programma da parte del cliente determina la conclusione di un contratto con l'azienda, tramite il quale il cliente può avvalersi di determinati benefici rispettando specifiche condizioni indicate dal fornitore. Ne consegue, che la raccolta e l'uso dei dati personali necessari per l'esecuzione del programma fedeltà risponde a questa specifica finalità la cui base giuridica consiste nella **necessità di dare esecuzione al contratto** di cui è parte il cliente interessato (art. 6.1, b), GDPR).
L'eventuale uso dei medesimi dati personali per soddisfare esigenze promozionali risponde, invece, alla distinta finalità di marketing, per la quale occorre individuare una specifica base giuridica, rintracciabile nel **preliminare consenso specifico** dell'interessato.
L'insegnamento che al riguardo può trarsi da questa vicenda è che costituisce grave errore confondere la fidelizzazione con la promozione commerciale, di conseguenza utilizzando indiscriminatamente i dati personali raccolti per la prima anche per soddisfare la seconda.

E-mail marketing

Dopo aver precisato che la finalità di fidelizzazione è autonoma e distinta da quella di promozione commerciale, occorre che l'azienda faccia molta attenzione alla base giuridica della finalità di marketing in combinazione col canale comunicativo prescelto. Infatti, se la promozione si attua con una modalità automatizzata (es. email, telefono senza operatore, sms, mms, fax) troverà applicazione, oltre al GDPR, anche la disciplina sul marketing elettronico, attualmente contenuta nel titolo X, capo I del codice privacy (sostanzialmente, l'art. 130). Secondo tale disciplina, le comunicazioni commerciali tramite e-mail presuppongono il consenso esplicito preventivo dell'utente (salvo l'ipotesi del cosiddetto soft-spam, indirizzato al comma 4 dell'articolo 130).
Non aver ricevuto un consenso valido e preliminare alla trasmissione della email commerciale – oppure non essere in grado di dimostrarne l'effettività – rende la stessa illecita e sanzionabile.

Consenso specifico e libero

Il GDPR – non innovando peraltro rispetto alla precedente disciplina – ha sancito che il consenso è una manifestazione di volontà "specifica" e "libera", cioè deve risultare in associazione ad una finalità determinata e deve permettere una scelta scevra da condizionamenti. Sopra si è ribadito che le finalità di fidelizzazione e di marketing sono distinte ed autonome e che ciascuna

deve riscontrare una specifica base giuridica: quella di **fidelizzazione** trova riscontro nella **necessità di eseguire il relativo contratto**, mentre quella di **marketing** si fonda sul **libero e specifico consenso** dell'interessato.
La vicenda in esame mostra, invece, che il consenso veniva richiesto per finalità di marketing insieme ad altre finalità contrattuali e paracontrattuali (quindi esso non era specifico) e che per poter accedere al programma fedeltà occorreva necessariamente rilasciare il consenso all'utilizzo dei propri dati personali per finalità di promozione commerciale (cioè il consenso risultava condizionato e, quindi, non libero).

Opposizione: modalità operative

L'articolo 12 del regolamento prescrive al titolare del trattamento di adottare misure tecnico-organizzative per agevolare l'esercizio dei diritti dell'interessato. Questo obbligo di agevolazione deve mirare a facilitare:

1. l'inoltro della richiesta da parte dell'interessato;
2. la gestione dell'istanza da parte del titolare (nelle fasi di ricezione, gestione e riscontro);
3. il riscontro finale (cioè la soddisfazione) della richiesta, in modo che esso si completi nei tempi stabiliti.

1. Fase di inoltro della richiesta

Il caso in esame ha rilevato, invece, che l'interessato aveva utilizzato invano tre distinti canali per inoltrare la propria richiesta di opposizione al trattamento per finalità di marketing (cioè, per evitare la ricezione di email promozionali):

- contattando il servizio clienti;
- utilizzando la procedura automatica di cancellazione dalla mailing list indicata nelle comunicazioni in questione (cosiddetto "*unsubscribe*");
- accedendo al sito web della Società.

Questa vicenda insegna che non è sufficiente prevedere distinti canali di comunicazione per consentire all'interessato di esercitare i propri diritti, in quanto occorre anche che gli stessi canali vengano adeguatamente presidiati gestiti.

2. Fase di gestione della richiesta

Nonostante le ripetute richieste dell'interessato di bloccare (opposizione) l'invio di email promozionali al proprio indirizzo di posta elettronica, la società ricevente non è riuscita a darvi esecuzione.
Questo precedente evidenzia come da un'istanza inoltrata da un interessato nell'ambito dell'esercizio dei propri diritti, deve necessariamente scaturire un vero piano d'azione interno volto a:

- **effettuare le necessarie ricerche** per rispondere esaurientemente alla richiesta;
- **processare il riscontro coerentemente alla tipologia di richiesta** (ad esempio, in caso di accesso, provvedere alla stampa dei dati personali dell'interessato, in ipotesi di opposizione al marketing, invece, effettuare la cancellazione dei dati personali utilizzati per tale finalità);

- **rimuovere gli ostacoli che si frappongono all'esecuzione della richiesta** (ad esempio, nel caso in esame le richieste dell'interessato erano state gestite con l'emissione di appositi "ticket" – cioè richieste di intervento tecnico – che tuttavia erano rimasti inevasi a seguito di complicazioni causate dall'operazione di migrazione dei dati stessi su una diversa piattaforma, come precisato in seguito).

3. Fase di riscontro della richiesta

A causa di difficoltà tecniche dovute alla migrazione dei dati acquisiti su una nuova piattaforma informatica, la società destinataria delle richieste non era riuscita a soddisfare le stesse, cioè non era stata in grado di bloccare l'invio delle email promozionali nonostante le ripetute opposizioni dell'interessato.
Questa circostanza insegna che gli impatti data protection derivanti da modifiche tecnologiche vanno valutate a priori, secondo il principio "by design" sancito dal GDPR (art. 25, v. infra); in tal modo l'azienda avrebbe avuto modo di decidere il blocco delle trasmissioni email durante la fase di migrazione e/o di adottare eventuali ulteriori rimedi per il periodo di transizione. In mancanza, il titolare ha dimostrato negligenza e mancanza di accountability.

Opposizione: omesso riscontro

In aggiunta al trattamento svolto per finalità di marketing nonostante l'omissione di un consenso valido a tal proposito, la società oggetto del provvedimento non è riuscita a dare soddisfazione alle richieste di opposizione degli interessati, volte a non ricevere più email promozionali. Si ricorda che in tali circostanze il **diritto di opposizione** è del tutto **discrezionale** e determina un obbligo di cancellazione dei dati personali utilizzati a fini di marketing da parte del titolare.
L'insegnamento che se ne trae è che qualsiasi campagna pubblicitaria deve preventivamente assicurarsi che eventuali opposizioni da parte degli individui che compongono il target possano essere effettivamente ed efficacemente soddisfatte, pervenendo alla reale cancellazione (cioè blocco dell'uso ulteriore) dei pertinenti dati personali.

Riscontro: difficoltà tecniche

Nella vicenda in esame sembra che il mancato riscontro fosse addebitabile a difficoltà tecniche derivanti dalla migrazione dei dati personali coinvolti su una diversa piattaforma informatica. Questo ci induce ad alcune riflessioni:

- **variazioni tecnologiche significative** presuppongono una preliminare **valutazione di impatto** dei rischi conseguenti; questa valutazione deve consentire di prevedere i possibili rischi conseguenti a tali operazioni e prevenire eventuali violazioni e danni;
- anche in mancanza della citata valutazione, la **normale diligenza** avrebbe richiesto di sospendere le operazioni di trasmissione delle email di marketing, durante e sino al completamento del processo di migrazione;
- particolare attenzione si sarebbe dovuta prestare ai **prevedibili errori** scaturenti tradizionalmente da qualsiasi processo di migrazione, al fine di mitigarne gli effetti pregiudizievoli.

Riscontro: tracciamento

Come si fa a dimostrare di aver **messo in atto misure adeguate** per riscontrare correttamente le **istanze degli interessati**?

Innanzitutto dimostrando di avere adottato soluzioni tecniche volte ad assicurare, ad esempio in ambito marketing, l'effettiva esecuzione della revoca del consenso precedentemente rilasciato oppure dell'opposizione al trattamento. Altra avvertenza è quella di verificare che la **casella postale** eventualmente creata e pubblicata come punto di contatto **per l'esercizio dei diritti**, sia sempre **attiva e presidiata**, in modo da poter reagire prontamente alle richieste.

Documentazione probatoria

La raccolta dei consensi a fini marketing va **opportunamente documentata** e – nel rispetto del principio di accountability – l'azienda titolare deve essere in grado di provarne l'**effettività e validità**, tracciando per ciascun interessato gli «*adempimenti imposti dalla normativa, e in particolare la* ***corretta, efficiente, tempestiva e costante gestione della relativa documentazione****, con particolare riferimento ai seguenti punti:*

- *elementi circostanziati riguardo all'****origine dei dati****, quali in particolare:*
  - ***modalità e data dell'acquisizione****;*
- ***modalità e testo*** *con cui venga fornita l'****informativa*** *ai sensi dell'art.13 del Regolamento UE;*
- ***opzioni di consenso (o dissenso)****, formulate in sede di raccolta dei dati, rispetto alle distinte finalità di trattamento dichiarate dalla Società (e in particolare, finalità promozionali e di profilazione), ai sensi degli artt. 6-7 e 22, par. 2, lett. c), del Regolamento UE, nonché 130 del Codice, incluse le* ***eventuali successive variazioni della volontà degli interessati****, con specifica indicazione di elementi circostanziati, quali*
  - *la* ***data****, la* ***modalità*** *e* ***formula di (ri)acquisizione del consenso***».

Mancato riscontro, segnalazioni, ispezioni e conseguenti provvedimenti

La vicenda qui commentata testimonia l'articolazione del processo di innesco degli **"inconvenienti" data protection**:

- esso trae origine da una **violazione** alla norma (in questo caso l'omesso riscontro alle reiterate richieste di esercizio dei diritti);
- prosegue con le **segnalazioni** inoltrate dall'interessato all'autorità di supervisione (o, in altri casi, con l'immediato ricorso all'autorità giudiziaria);
- le segnalazioni innescano **approfondimenti dell'autorità** oppure ispezioni;
- le violazioni accertate provocano **provvedimenti** di vario tipo a carico dell'azienda, adottati anche in via cumulativa, come;
  - **ammonimenti e ingiunzioni**, la cui violazione è sanzionata in sede amministrativa con un massimale pari a 20 milioni o al 4% del giro d'affari globale annuo;
  - **divieti**, la cui trasgressione è punita penalmente con la reclusione da tre mesi a due anni, insieme alla sanzione amministrativa indicata al punto precedente;
  - **obbligo di comunicare al Garante**, entro un termine perentorio, l'attuazione delle azioni prescritte, la cui violazione è punita con la sanzione amministrativa di cui al primo punto (art. 166.2 cod. privacy) ;
  - **eventuali sanzioni** specifiche.

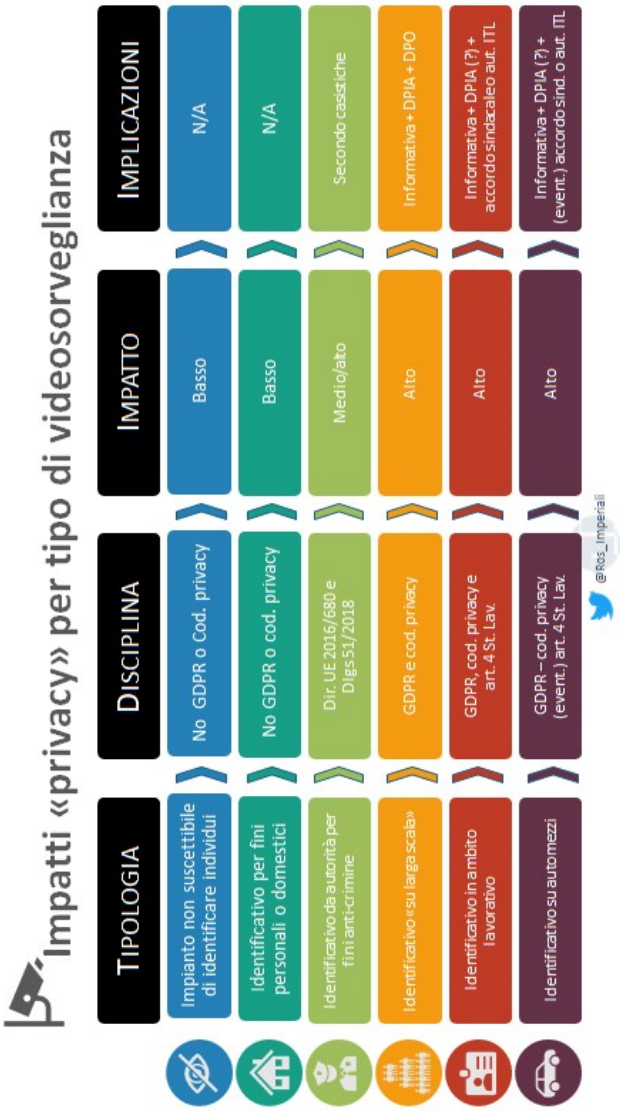
L'insegnamento complessivo che può desumersi da questa vicenda è l'esigenza di preparare l'azienda ad essere in grado di riuscire ad interrompere la concatenazione di eventi sopra rappresentata e rimediare tempestivamente alle carenze evidenziate, anche qualora la prescrizione normativa fosse già stata violata.

30.
EDPB: bozza linee guida 3/2019 su videosorveglianza - Seconda parte

Non mi è possibile riprendere i commenti dell'Editoriale senza rivolgere un breve pensiero a Giovanni Buttarelli, prematuramente scomparso lo scorso mese, pietra miliare del tema della protezione dei dati personali. La dialettica tra noi, talvolta aspra, non ha mai scalfito il senso di amicizia che ci legava anche se, avendo entrambi un carattere non facile, preferivamo la reciproca canzonatura. Ciao Giovanni, mi sembra ancora una delle tue prese in giro...

Questo commento continua la serie di valutazioni sul tema della videosorveglianza, cogliendo spunto dalla pubblicazione della versione preliminare delle linee guida 3/2019 sulla videosorveglianza da parte dell'EDPB. Il documento è sottoposto a consultazione pubblica che terminerà il 6 settembre 2019.

Sintesi



Il Comitato europeo (EDPB) ha rilasciato la versione preliminare delle linee guida 3/2019 sulla videosorveglianza, sottoponendola alla procedura di consultazione pubblica. Imprenditori pubblici e privati dovranno attenersi a tali indicazioni insieme al rispetto delle prescrizioni imposte dal provvedimento generale del Garante del 2010 sulla videosorveglianza, avendo particolare cura alla corretta disposizione della cartellonistica ed ai suoi contenuti, ai ruoli assegnati a coloro che hanno accesso alle immagini ed alle misure di sicurezza a tutela delle stesse. In aggiunta, quando l'attività di videosorveglianza viene svolta in ambito lavorativo, essa si trova ad un crocevia normativo caratterizzato dallo Statuto dei Lavoratori (l. n. 300/1070), da GDPR e codice privacy (dlgs n. 196/2003) e da talune norme speciali. Eventuali violazioni alle disposizioni dell'articolo 4 dello Statuto, non solo determinano un'ipotesi di contravvenzione penale (che sarà il giudice penale a verificare) ma comportano anche l'illiceità del trattamento dei relativi dati personali (cioè le immagini raccolte) per violazione dell'articolo 5(1)(a) del GDPR. Il rispetto della procedura multilivello prevista dallo Statuto è quindi un presupposto di liceità fondamentale.

Videosorveglianza e dati personali

L'Alert del 18 luglio 2019 ha dato notizia del rilascio della versione delle linee guida 3/2019 sottoposte a consultazione pubblica. L'Editoriale del 25 luglio 2019 ha fornito un primo commento su taluni aspetti della videosorveglianza, sia di carattere generale – per offrire un quadro complessivo su questo delicato tema – sia desunti dal documento dell'EDPB.

Ci si è soffermati sulla interrelazione tra videosorveglianza e dati personali, si è fatta una carrellata dei principali contesti applicativi tra cui le installazioni in aree pubbliche e quelle in ambito lavorativo, sottolineando le casistiche che esulano dalla portata applicativa del GDPR (cioè quelle per finalità anti-crimine, quelle a fini meramente personali e quelle che catturano immagini non suscettibili di identificare individui, nemmeno indirettamente).

Provvedimento 2010 del Garante e linee guida 3/2019 dell'EDPB

Come accennato in occasione dei precedenti commenti, il tema della videosorveglianza dovrà tenere conto di un set di norme (GDPR, codice privacy e statuto dei lavoratori, quando applicabile, oltre ad eventuali ulteriori norme di settore) e di due fonti non normative, il provvedimento generale del Garante, del 2010, e le linee guida 3/2019 dell'EDPB (in inglese), in versione definitiva (cioè quando saranno pubblicate al termine della procedura di consultazione pubblica).

Speciali categorie di dati personali

Vi possono essere situazioni in cui le immagini raccolte col sistema di videosorveglianza catturino informazioni qualificabili come dati "sensibili" o "speciali categorie di dati personali" regolate dall'articolo 9 del GDPR. L'esempio tipico è quello di un impianto installato in reparti di un ospedale per controllare lo stato di salute dei pazienti.

In queste circostanze, il titolare deve:

- individuare una **deroga al divieto di trattamento dei dati sensibili** (art. 9, GDPR);
- individuare la **base giuridica** a fondamento del trattamento (art. 6, GDPR).

Considerata l'ampia portata definitoria di queste speciali categorie di dati personali, il contesto della videosorveglianza che include dati sensibili necessita di una precisazione contenuta nelle

linee guida 3/2019: l'impianto di videosorveglianza si ritiene che includa dati sensibili **solo allorquando** il relativo trattamento di dati sia **finalizzato a ricavare informazioni di questa natura**. Ne consegue che non sarà considerato tale il caso di immagini da cui si possa desumere indirettamente un'informazione qualificabile come "sensibile", come ad esempio quelle che riprendono soggetti con gli occhiali da vista oppure che utilizzano sedie a rotelle o altre di analogo tenore.

Videosorveglianza con dati biometrici

Una valutazione aggiuntiva va operata in ipotesi d'uso di dati biometrici in concomitanza con la videosorveglianza – come nel caso del **riconoscimento facciale** – in quanto tale applicazione provoca gravi impatti su interessi, diritti e libertà degli interessati. Gli impatti discendono

- dall'**elevato livello di intrusività** di queste soluzioni tecniche, le quali possono condizionare molteplici libertà dell'individuo e;
- dalle **gravi conseguenze** che potrebbero derivare in ipotesi di errori o malfunzionamenti tecnici dell'applicazione (secondo le linee guida, «*I ricercatori riferiscono che il software utilizzato per l'identificazione, il riconoscimento o l'analisi del viso si comporta diversamente in base all'età, al sesso e all'etnia della persona che sta identificando. Gli algoritmi si comporterebbero in base a dati demografici diversi, pertanto la distorsione nel riconoscimento facciale minaccia di rafforzare i pregiudizi della società.*»).

Criteri per individuare la natura biometrica della videosorveglianza

La videosorveglianza biometrica si individua tramite la compresenza di tre criteri:

- **natura dei dati** – i dati catturati devono riguardare caratteristiche fisiche, fisiologiche o comportamentali dell'individuo;
- **mezzi e modalità del trattamento** – i dati devono desumersi tramite specifiche operazioni tecniche di trattamento;
- **finalità del trattamento** – i dati devono essere utilizzati allo scopo di identificare in modo univoco il soggetto; se, invece, l'impianto serve solo per distinguere una categoria di persone da un'altra, senza individuazione univoca, non si ha videosorveglianza biometrica in quanto questo criterio sarebbe assente.

Il Considerando (51) del GDPR risulta in linea con questa chiave interpretativa, laddove esclude che la **fotografia ordinaria** possa essere considerata un dato biometrico; essa lo diventerebbe solo quando fosse trattata «*attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica*».

Consenso per la videosorveglianza biometrica

La videosorveglianza biometrica fonda la propria base giuridica sul **consenso esplicito** dell'interessato cui vanno aggiunte le condizioni prescritte dal provvedimento del Garante del 12 novembre 2014 (doc. web n. 3556992) sul trattamento dei dati biometrici.

Consenso esplicito

La videosorveglianza con associato il riconoscimento facciale presuppone il consenso esplicito dell'interessato, così come negli altri casi in cui le telecamere sono finalizzate a catturare dati sensibili degli individui, nel significato sopra specificato. È comprensibile che l'innalzamento della soglia

di validità del consenso – dalla dimensione **"inequivocabile"** alla manifestazione **"esplicita"** – implichi talune maggiori difficoltà operative nella raccolta del consenso preliminare, connesse alle caratteristiche tecniche dell'impianto. I titolari che intendano installare simili impianti è bene che ne tengano conto sin dalle prime fasi di ideazione del progetto. I sistemi biometrici che si ha intenzione di installare in ambienti non controllati, inevitabilmente catturano le impronte del viso (ma il ragionamento vale anche per altre tipologie di dati sensibili) di tutti coloro che transitano nel raggio d'azione delle telecamere. Per questo motivo può rendersi particolarmente problematico assicurarsi che tutti coloro che sono effettivamente ripresi abbiano rilasciato un preventivo consenso esplicito ed informato; così come problematico potrebbe risultare il disporre di soluzioni tecniche che permettano di escludere dalle riprese coloro che hanno manifestato il diniego. In aggiunta, affinchè il consenso possa considerarsi "libero", sarà necessario che in aggiunta al riconoscimento biometrico sia resa disponibile una soluzione alternativa e meno intrusiva, utilizzabile da coloro che hanno negato il consenso ovvero da adottarsi anche per l'eventualità di indisponibilità o malfunzionamento della soluzione biometrica principale.

Informativa

Il principio di trasparenza impone che gli interessati siano informati preventivamente che un sistema di videosorveglianza è in funzione col dettaglio dei luoghi monitorati. Nel caso della videosorveglianza si applica l'articolo 13 che concerne l'informativa da rilasciare quando i dati personali sono raccolti direttamente presso l'interessato, in quanto – come osservato nelle linee guida wp260 rev.01 – questo ambito include i dati personali che sono raccolti «*da una persona interessata mediante monitoraggio (ad esempio utilizzando dispositivi di acquisizione dati automatizzati o software di acquisizione dati come telecamere)*» (v. par. 26, wp260 rev.01).

Multilivello

Considerato il contesto tecnico-operativo delle telecamere ed il volume di informazioni che vanno obbligatoriamente rilasciate nell'informativa, i titolari del trattamento possono utilizzare un approccio a più livelli (come suggerito nei documenti del WPArt29 wp260 rev.01, par. 35 e wp89, p. 22) dove le informazioni più importanti dovrebbero essere visualizzate sul cartello di avviso (primo livello) mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello) di agevole reperimento per l'interessato.

Cartellonistica

Come già riportato nel citato provvedimento del Garante del 2010, «*le informazioni visualizzate possono essere fornite in combinazione con un'icona al fine di fornire, in modo facilmente visibile, comprensibile e chiaramente leggibile, una panoramica significativa dell'elaborazione prevista (articolo 12, paragrafo 7, GDPR). Il formato delle informazioni deve essere adattato alla singola ubicazione (wp89 p. 22)*».

Posizionamento

Il cartello va collocato «*in modo tale che l'interessato possa facilmente riconoscere le circostanze della sorveglianza prima di entrare nell'area monitorata (approssimativamente a livello degli occhi) (...) L'interessato deve essere in grado di stimare quale area è acquisita da una telecamera in modo da poter evitare la sorveglianza o adattare il suo comportamento, se necessario*».

Contenuto del cartello

Il cartello dovrebbe contenere le informazioni più importanti. Si coglie immediatamente un salto di qualità nella individuazione di queste informazioni essenziali di primo livello rispetto sia alla prassi odierna sia anche alle precedenti indicazioni contenute nel citato provvedimento del Garante del 2010. Secondo le linee guida 3/2019, queste dovrebbero riguardare:

- i dettagli delle finalità del trattamento;
- l'identità del titolare del trattamento;
- l'esistenza dei diritti dell'interessato;
- informazioni sui maggiori impatti del trattamento che potrebbero cogliere di sorpresa l'interessato;
- i dati di contatto del DPO (se applicabile);
- il riferimento al secondo livello più dettagliato di informazioni e dove e come trovarlo.

Di seguito riportiamo una comparazione tra gli esempi di cartellonistica indicati nel provvedimento 2010 del Garante e nelle linee guida 3/2019 da cui emerge con immediatezza la diversità e l'incremento di elementi informativi richiesti per il primo livello del cartello.

Fig. 1 - Cartello indicato a titolo esemplificativo nel provvedimento 2010 del Garante.

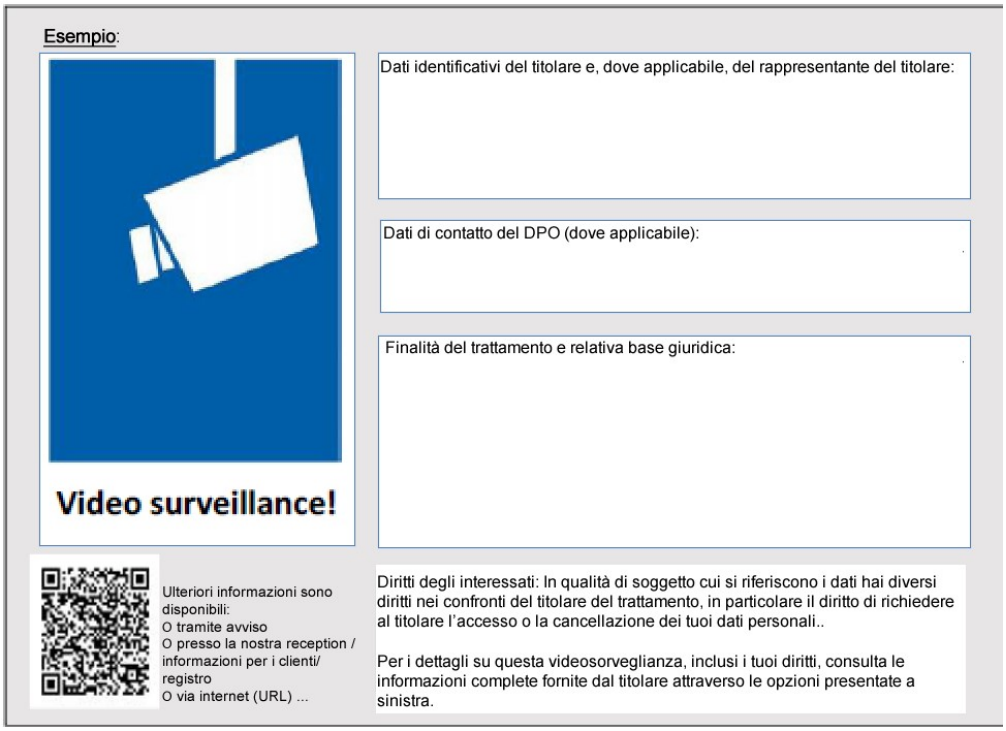


Fig. 2 - Cartello indicato a titolo di esempio nelle linee guida 3/2019 dell'EDPB.

31.
Prescrizioni per dati sensibili e data breach

L'ASN italiana, il Garante privacy, al termine della procedura di consultazione pubblica, ha rilasciato le prescrizioni per il trattamento di categorie particolari di dati nonchè un modello per la notifica di violazioni di dati personali ("data breach") insieme ad una scheda informativa su questo tema.

Provvedimento sul trattamento di dati sensibili

L'Alert del 10 gennaio 2019 aveva dato notizia dell'iter di adeguamento al GDPR delle precedenti autorizzazioni generali in merito al trattamento dei dati sensibili (ora denominati "categorie particolari di dati personali"), alla luce delle disposizioni introdotte dalla legge di adeguamento che ha aggiornato il codice privacy previgente (d.lgs. 10 agosto 2018, n. 101).

Il provvedimento dell'Authority che ora si esamina (provv. n. 146 del 5/6/2019, doc. web n. 9124510) porta a conclusione l'iter allora iniziato, con l'emissione delle prescrizioni da seguire in caso di trattamento di speciali categorie di dati personali.

Fonte giuridica

Il provvedimento in parola trova la propria fonte giuridica nell'articolo 21 del decreto di adeguamento (d.lgs. n. 101/2018) che ha demandato al Garante il compito di individuare, con proprio provvedimento di carattere generale. le prescrizioni contenute nelle autorizzazioni generali già adottate, che risultano compatibili col GDPR.

Ambito di intervento

L'ambito di intervento, in base al citato articolo 21, riguarda i trattamenti:

- necessari per adempiere un obbligo legale [art. 6(1)(c), GDPR];
- necessari per l'esecuzione di un compito di interesse pubblico [art. 6(1)(e), GDPR];
- necessari per assolvere obblighi o esercitare diritti del titolare in materia di lavoro [art. 9(2)(b)];

- relativi a dati genetici, biometrici o dati relativi alla salute [art. 9(4);
- relativi a libertà di espressione e di informazione (art. 85);
- relativi all'accesso del pubblico ai documenti ufficiali (art. 86);
- relativi al numero di identificazione nazionale (art. 87);
- relativi all'ambito del rapporto di lavoro (art. 88);
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici (art. 89);
- che interferiscono con attività professionali soggette a obblighi di segretezza (art. 90);
- presso chiese o associazioni religiose (art. 91).

Durata degli effetti delle prescrizioni

Le prescrizioni del provvedimento n. 146 produrranno effetti fino all'emanazione delle regole deontologiche e all'adozione delle misure di garanzia previste rispettivamente agli articoli 2-quater e 2-septies del codice.

Non esaustività delle prescrizioni

In aggiunta alle prescrizioni ora introdotte, restano in ogni caso fermi gli obblighi previsti da norme di legge o di regolamento o dalla normativa eurounitaria che stabiliscono divieti o limiti più restrittivi in materia di trattamento di dati personali.

Struttura del provvedimento n. 146

Il provvedimento n. 146 si compone di una parte dispositiva e di un allegato che racchiude in cinque distinti paragrafi, le prescrizioni relative al trattamento di categorie particolari di dati nei seguenti contesti:

1. nei **rapporti di lavoro** (aut. gen. n. 1/2016);
2. da parte degli **organismi di tipo associativo**, delle **fondazioni**, delle **chiese** e **associazioni o comunità religiose** (aut. gen. n. 3/2016);
3. da parte degli **investigatori privati** (aut. gen. n. 6/2016);
4. relativo a **dati genetici** (aut. gen. n. 8/2016);
5. per scopi di **ricerca scientifica** (aut. gen. n. 9/2016).

In un successivo Alert forniremo una descrizione sintetica del contenuto di queste prescrizioni.

Disciplina per i dati giudiziari

Per quanto riguarda i dati giudiziari (oggi denominati "dati personali relativi a condanne penali e reati") la precedente autorizzazione n. 7/2016 è stata ritenuta non compatibile con la nuova disciplina introdotta dal GDPR (art. 10) e successivamente completata dal decreto di adeguamento (d.lgs. n. 101/2018, art. 2-octies). Allo stato, si attende ancora la pubblicazione del decreto del Ministro della giustizia che indica i trattamenti consentiti e le appropriate garanzie per i diritti e le libertà degli interessati.

Violazioni di dati personali (data breach)

Il Garante ha emesso il provvedimento n. 157 sulla notifica delle violazioni di dati personali (data breach) del 30 luglio 2019 [doc. web n. 9126951].

Obblighi di notificazione derivanti da provvedimenti del Garante

Durante la disciplina previgente al Regolamento, l'Autorità aveva prescritto con propri provvedimenti, termini temporali, contenuto e modalità della comunicazione delle violazioni di dati personali in relazione a determinate tipologie di trattamento o categorie di titolari del trattamento; in particolare

- nel provvedimento sulle misure di sicurezza e modalità di **scambio dei dati personali tra amministrazioni pubbliche** del 2 luglio 2015 (doc. web n. 4129029, v. punto 1);
- nelle linee guida in materia di **Dossier sanitario** del 4 giugno 2015 (doc. web n. 4084632, v. punto 2);
- nel provvedimento generale prescrittivo **in tema di biometria** del 12 novembre 2014 (doc. web n. 3556992, v. punto 2);
- nel provvedimento in materia di attuazione della disciplina sulla **comunicazione delle violazioni di dati personali** del 4 aprile 2013 (doc. web n. 2388260);
- nel provvedimento recante prescrizioni in materia di circolazione delle informazioni in **ambito bancario** e di tracciamento delle operazioni bancarie del 12 maggio 2011 (doc. web n. 1813953, v. punto 5.2).

A seguito di quanto stabilito dall'articolo 33 del regolamento, i termini e contenuti indicati nei citati provvedimenti devono intendersi sostituiti:

- dai contenuti indicati nel provvedimento generale n. 157;
- riguardo ai termini, la notificazione deve avvenire senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui il titolare è venuto a conoscenza della violazione dei dati personali.

Modello di notificazione

Nel provvedimento n. 157, «*in un'ottica di semplificazione del corretto adempimento degli obblighi amministrativi posti in capo al titolare del trattamento*», il Garante ha indicato le informazioni da fornire, individuate in un apposito modello. L'uso del modello non è obbligatorio ma agevola il corretto soddisfacimento dell'adempimento della notificazione all'Autorità, quando la violazione determini un rischio per i diritti e le libertà degli interessati. Il modello in formato pdf va caricato sul proprio dispositivo per poi procedere alla sua compilazione.
Di converso, devono ritenersi obbligatorie le informazioni da comunicare, in esso individuate.

Informazioni da comunicare nella notifica al Garante

- La notifica può riguardare entrambi gli analoghi adempimenti previsti dal GDPR e dal d.lgs. 51/2018 sui trattamenti per finalità anticrimine e di polizia: occorre pertanto specificare a quale adempimento essa si riferisca.
- Va precisata la tipologia di notifica: cioè se "preliminare" (cioè in attesa di ulteriori informazioni aggiuntive), "completa" oppure "integrativa" (cioè a completamento di una precedente notifica preliminare).
- Vanno poi indicati i dati identificativi della persona che materialmente la effettua e la inoltra nonché quelli del titolare del trattamento.
- Successivamente, vanno riportati i dati di contatto per ottenere maggiori informazioni (nel caso si indicasse il DPO, occorre riportare il numero di protocollo assegnato alla

originaria comunicazione del titolare al Garante, dei dati di contatto del DPO).
- L'evidenza di eventuali ulteriori soggetti coinvolti nel trattamento oggetto di violazione come contitolare, responsabile del trattamento, rappresentante del titolare non stabilito nell'Ue.
- Informazioni di sintesi sulla violazione, come
  - l'indicazione di quando è avvenuta la violazione;
  - il momento in cui il titolare ne è venuto a conoscenza;
  - le modalità dell'avvenuta conoscenza;
  - i motivi dell'eventuale notifica oltre le 72 ore;
  - breve descrizione della violazione (natura, causa, categorie di dati oggetto di data breach, volume dei dati, categorie di interessati, numero approssimativo di interessati coinvolti).
- Informazioni di dettaglio della violazione (descrizione dell'incidente, descrizione delle categorie di dati, descrizione dei sistemi e infrastrutture IT coinvolti, misure T/O adottate su dati, sistemi e infrastrutture coinvolti).
- Possibili conseguenze e gravità della violazione (potenziali effetti negativi per gli interessati, stima della gravità della violazione su una scala a 4 livelli: trascurabile, basso, medio, alto, indicandone le motivazioni).
- Misure adottate a seguito della violazione.
- Eventuale comunicazione agli interessati.
- Altre informazioni (tra cui se è stata effettuata una segnalazione all'autorità giudiziaria o di polizia, se la violazione è stata notificata ad altri organismi di vigilanza o di controllo in virtù di ulteriori disposizioni normative, se la violazione è stata notificata ad altre autorità di controllo di altri Stati membri).

Come si effettua la notificazione al Garante

La notifica, sia essa predisposta o meno avvalendosi del modello messo a disposizione dall'Autorità,
- deve essere inviata al Garante tramite posta elettronica all'indirizzo protocollo@pec.gpdp.it;
- deve essere sottoscritta digitalmente (con firma elettronica qualificata/firma digitale);
  - in alternativa, va sottoscritta con firma autografa. In quest'ultimo caso la notifica deve essere presentata unitamente alla copia del documento d'identità del firmatario.
- L'oggetto del messaggio deve contenere obbligatoriamente la dicitura "NOTIFICA VIOLAZIONE DATI PERSONALI" e opzionalmente la denominazione del titolare del trattamento.

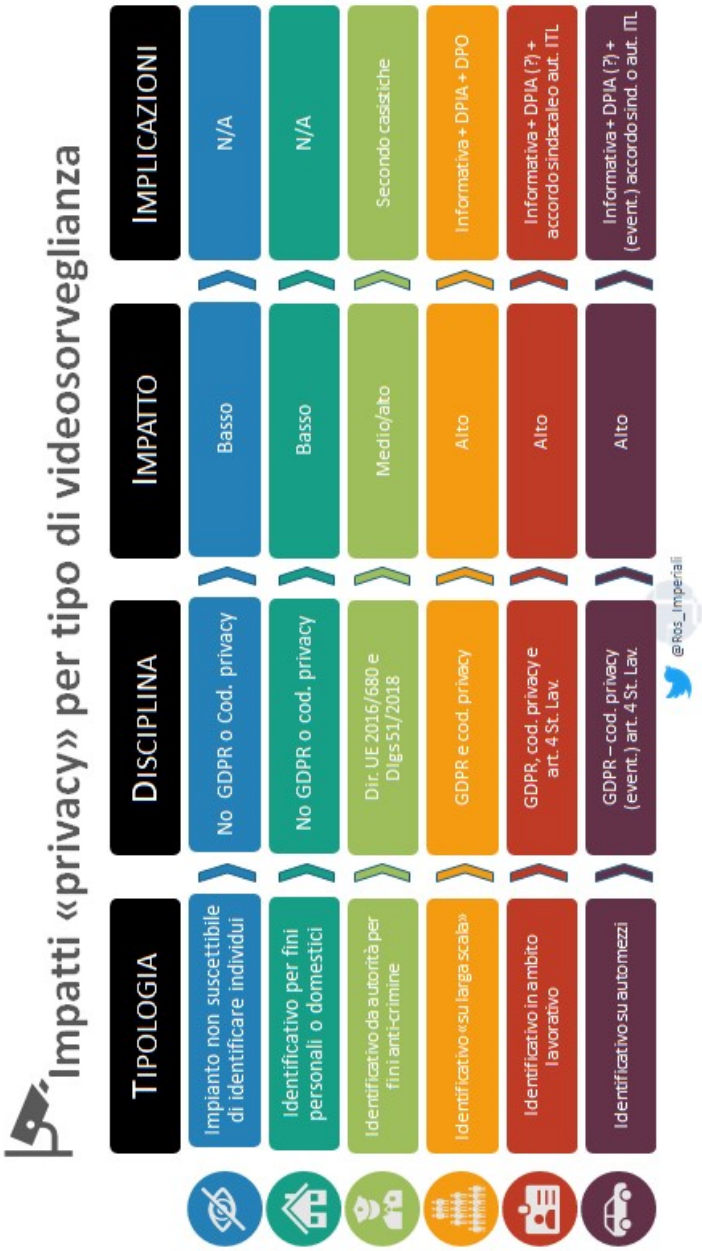
Scheda informativa sul data breach

L'Autorità ha reso disponibile sul proprio sito istituzionale un aggiornamento della scheda informativa, a carattere divulgativo, relativa alle violazioni di dati personali.

32.
EDPB: bozza linee guida 3/2019 su videosorveglianza - Terza parte

Questo commento completa la serie di valutazioni sul tema della videosorveglianza, cogliendo spunto dalla pubblicazione della versione preliminare delle pertinenti linee guida 3/2019 da parte dell'EDPB.
Il documento è sottoposto al procedimento di consultazione pubblica scaduto il 6 settembre 2019.

Sintesi



Il Comitato europeo (EDPB) ha rilasciato la versione preliminare delle linee guida 3/2019 sulla videosorveglianza, sottoponendola alla procedura di consultazione pubblica. Imprenditori pubblici e privati dovranno attenersi a tali indicazioni insieme al rispetto delle prescrizioni imposte dal provvedimento generale del Garante del 2010 sulla videosorveglianza, avendo particolare cura alla corretta disposizione della cartellonistica ed ai suoi contenuti, ai ruoli assegnati a coloro che hanno accesso alle immagini ed alle misure di sicurezza a tutela delle stesse. In aggiunta, quando l'attività di videosorveglianza viene svolta in ambito lavorativo, essa si trova ad un crocevia normativo caratterizzato dallo Statuto dei Lavoratori (l. n. 300/1070), da GDPR e codice privacy (dlgs n. 196/2003) e da talune norme speciali. Eventuali violazioni alle disposizioni dell'articolo 4 dello Statuto, non solo determinano un'ipotesi di contravvenzione penale (che sarà il giudice penale a verificare) ma comportano anche l'illiceità del trattamento dei relativi dati personali (cioè le immagini raccolte) per violazione dell'articolo 5(1)(a) del GDPR, con la conseguente inutilizzabilità delle immagini. Il rispetto della procedura multilivello prevista dallo Statuto è quindi un presupposto di liceità fondamentale.

Comunicazione a terzi

La comunicazione a terzi delle immagini tratte dal sistema di videosorveglianza rappresenta una **finalità ulteriore rispetto a quella della raccolta** e della conseguente visualizzazione e/o conservazione; pertanto, occorre individuare per essa una specifica base giuridica.

Comunicazione alle Forze dell'ordine

Nell'ipotesi di **comunicazione delle immagini alle Forze dell'ordine**, ad esempio, occorrerà distinguere tra due diverse situazioni:

1. il caso in cui la comunicazione è sollecitata dalle stesse FF.OO;
2. l'ipotesi che la comunicazione alle FF.OO. venga effettuata su iniziativa spontanea del titolare del trattamento.

Nel caso di cui al precedente punto 1., la base giuridica sarà individuata nella necessità di rispondere ad un obbligo legale [art. 6.1 c), GDPR] mentre l'uso delle immagini da parte delle stesse FF.OO. rientrerà nell'ambito della disciplina prevista dal dlgs. 51/2018, attuativo della direttiva 2016/680.

Nella circostanza di cui al precedente punto 2. (cioè quando la comunicazione alle FF.OO. avviene su iniziativa del titolare del trattamento), sarà il titolare a dover valutare preventivamente se sussistono i presupposti di necessità per soddisfare un legittimo interesse suo o di terzi, documentandone per iscritto le motivazioni [art. 6.1 f), GDPR].

Minimizzazione dei rischi – Videosorveglianza biometrica

Nel caso di videosorveglianza biometrica, i modelli biometrici non vanno trasferiti tra i sistemi biometrici; il luogo di conservazione dei dati biometrici deve risultare adeguato, i modelli vanno **conservati su dispositivi a disposizione esclusiva dell'utente** e se, per eccezione, sono conservati su data base centralizzati, vanno protetti con **crittografia** le cui chiavi vanno custodite da chi ha il compito di prevenire accessi abusivi.

I dati vanno compartimentalizzati, separando i dati biometrici dai restanti altri, sia in fase trasmissiva che di custodia/archivio. Va definita una politica di cifratura e di gestione delle

chiavi, l'integrazione di misure tecnico-organizzative per la rilevazione delle frodi, la proibizione dell'accesso in remoto ai data base.

Diritti

In merito all'attività di videosorveglianza possono essere esercitati tutti i diritti riconosciuti dal GDPR anche se alcuni di essi possono sollevare dubbi interpretativi o difficoltà attuative a causa delle particolarità tecniche delle attività di audio/video registrazione.
Il titolare del trattamento è tenuto a rispondere alle richieste dell'interessato senza indebito ritardo e al più tardi **entro un mese**.

Diritto di accesso

Il diritto di accesso si suddivide in via generale in due distinti diritti:

- quello di **avere conferma** da parte del titolare che i propri dati personali siano oggetto di trattamento;
- quello di **ricevere copia** di tali dati.

A. Esclusivo monitoraggio in tempo reale

Nel caso di videosorveglianza con esclusivo monitoraggio in tempo reale, si possono avere due distinte situazioni:

1. se all'atto della richiesta di accesso **la ripresa è terminata**, il titolare potrà solo dichiarare che allo stato nessun dato personale risulta essere oggetto di trattamento (mentre l'informativa è comunque sempre rilasciata sin dall'inizio);
2. qualora la **ripresa è ancora in atto**, il titolare probabilmente risponderà che al momento sono raccolti dati personali ma che questi (probabilmente) non riguardano l'interessato (in quanto si presume che l'interessato all'atto della richiesta non sia sotto il raggio di azione delle telecamere).

B. Ripresa continuativa con registrazione delle immagini

Se, invece, la ripresa è continuativa e prevede anche la registrazione delle immagini, l'interessato richiedente avrà diritto di

1. avere contezza se le immagini lo hanno ripreso;
2. avere copia delle immagini che lo riguardano.

Ciò comporta la necessità per il titolare di ricercare le immagini che riproducono le sembianze dell'interessato richiedente e questo comporta quanto segue:

- che il titolare disponga di una strumentazione tecnologica capace di ricercare ed estrapolare le immagini relative all'interessato dal set complessivo di quelle registrate;
- in mancanza, se il titolare non è in grado di identificare l'interessato dall'intero set di immagini, egli sarà legittimato a richiedere all'interessato di fornirgli la forchetta oraria in cui lo stesso ritiene di poter essere stato ripreso dalle telecamere, in modo da limitare la ricerca ad un sub-set più limitato di immagini.

Copia delle immagini

Una volta individuate le immagini che riprendono l'interessato, questi ha il diritto di riceverne

copia. Qualora le immagini estrapolate riprendono anche altri individui, il titolare dovrà provvedere alla loro anonimizzazione (ad esempio sfocando le immagini di terzi o parte di esse in modo da renderle insuscettibili di identificare i terzi) prima di consegnare le copie all'interessato richiedente.
Nel caso in cui la richiesta dell'interessato di ottenere copia delle immagini che lo ritraggono sia ricevuta dopo che le stesse siano eventualmente state cancellate per scadenza del periodo di conservazione, il titolare del trattamento si limiterà a fornire risposta che non vi sono dati personali riferiti all'interessato richiedente.

Richieste eccessive

Il regolamento prevede che in caso di richieste eccessive il titolare possa alternativamente

- addebitare all'interessato un **contributo spese** ragionevole [art. 12.5 a)];
- **rifiutarsi di dare riscontro** alla richiesta [art. 12.5 b)] dandone comunicazione all'interessato.

Sarà onere del titolare dimostrare il carattere eccessivo della richiesta.

Diritto di cancellazione

Se il sistema di videosorveglianza prevede anche la registrazione e conservazione delle immagini (cioè il titolare del trattamento continua a trattare i dati personali al di là del monitoraggio in tempo reale) l'interessato può richiedere la cancellazione dei dati personali se trova applicazione una delle circostanze elencate nell'articolo 17(1) GDPR [e, di converso, non si applica nessuna delle eccezioni elencate al paragrafo 17(3)]: come nel caso in cui le immagini (dati personali) non sono più necessarie per lo scopo per il quale sono state inizialmente memorizzate o quando il trattamento è illegale oppure quando è già scaduto il periodo di conservazione.
Per la videosorveglianza, l'operazione mediante la quale **si sfoca l'immagine** senza che da questa si possano recuperare i dati personali che vi erano contenuti, viene considerata come cancellazione in conformità con il GDPR.
Inoltre, in relazione alla **base giuridica del trattamento**, i dati personali devono essere cancellati:

- quando il fondamento è il **consenso**, ogni volta che il consenso viene revocato (e non esiste altra base giuridica per il trattamento);
- in ipotesi di **legittimo interesse**:
  - ogni volta che l'interessato esercita il diritto di opposizione e non vi sono motivi legittimi cogenti per il trattamento, oppure;
  - in caso di videosorveglianza a scopo di marketing diretto (compresa la profilazione) ogni volta che l'interessato si oppone discrezionalmente al trattamento.

Diritto di opposizione

Nel contesto della videosorveglianza, il diritto di opposizione può essere esercitato dall'interessato quando la base giuridica che la giustifica sia:

- l'**interesse legittimo** [articolo 6(1)(f), del GDPR] o
- la necessità di svolgere un **compito di interesse pubblico** [articolo 6(1)(e)].

Diversamente dalle ipotesi precedenti, quando si utilizza la videosorveglianza per scopi di **marketing diretto**, l'interessato ha il diritto di opporsi al trattamento in via assoluta e su base meramente discrezionale (articolo 21, paragrafi 2 e 3, del GDPR).
Pertanto, il titolare del trattamento che intenda installare un impianto di videosorveglianza dovrebbe essere in grado di interrompere immediatamente il trattamento dei dati personali dell'interessato da parte della telecamera (cioè far sì che la telecamera non continui a riprendere l'interessato), quando richiesto dall'interessato e quando tale richiesta risulti fondata.

Conservazione dei dati

La conservazione delle immagini (in alternativa al solo monitoraggio) è frutto di una specifica valutazione della sua **necessità** rispetto alle legittime finalità perseguite. In via generale, gli scopi della videosorveglianza sono la tutela del patrimonio e la necessità di premunirsi elementi di prova di eventuali illeciti, per cui la durata di conservazione dovrebbe essere commisurata al tempo (limitato) strettamente necessario per tali esigenze.
Argomentando dalla considerazione di fatto che nella prassi, eventuali danni sono accertati nel corso di uno/due giorni dall'evento, le linee guida concludono nel senso che il periodo di conservazione dovrebbe avere una durata di pochi giorni e che, maggiore sia questa forchetta temporale (specie se superiore alle 72 ore) maggiormente dettagliato dovrà essere l'argomentazione a fondamento della legittimità dello scopo e della necessità del tempo di conservazione. Pertanto, il periodo di conservazione deve essere chiaramente individuato per ogni specifica finalità (tutela del patrimonio, sicurezza pubblica o del lavoro, produzione, ecc.).
Lo statuto dei lavoratori, riconosce la liceità dell'installazione dell'impianto di videosorveglianza anche per finalità di produzione, organizzative e della sicurezza sul lavoro, sottoponendola alla procedura multi-livello del tentativo di accordo sindacale o, in mancanza, dell'autorizzazione dell'Ispettorato Territoriale del Lavoro (o della sua struttura centrale, l'INL).
In base alla riforma del GDPR ed al principio di accountability, spetta al titolare del trattamento stabilire quale sia il periodo di conservazione delle immagini in relazione ai principi di necessità e proporzionalità nonchè di dimostrare la correttezza della propria valutazione.
Campioni e riferimenti biometrici sono conservati per il tempo strettamente necessario per realizzare il sistema biometrico e, quindi, sono cancellati in modo sicuro.

Misure tecnico-organizzative

Le attività di videosorveglianza devono essere protette da misure tecnico-organizzative che siano proporzionali ai presumibili rischi per i diritti e le libertà degli interessati derivanti da distruzione accidentale o illecita, perdita, alterazione, oppure divulgazione o accesso non autorizzati ai dati di videosorveglianza.

By design

In questo ambito, riveste particolare importanza il rispetto del principio della protezione dei dati sin dalla fase di progettazione (by design) per cui i titolari dovrebbero impostare le proprie attività interne ed adottare politiche che garantiscano tale attuazione sia al momento della scelta dell'impianto sia al momento delle operazioni di trattamento. Ciò significa, ad esempio, che la scelta delle apparecchiature dovrà tenere in debita considerazione come – ed a che livello – queste

stesse siano in grado di soddisfare principi e requisiti per la protezione dei dati personali, come ad esempio la gestione dei diritti esercitati dagli interessati. Di conseguenza, sarà compito del titolare inserire i requisiti data protection tra le specifiche di acquisto dell'impianto commerciale di videosorveglianza.
In questa medesima prospettiva, devono essere disattivate funzioni dell'apparecchiatura che non risultano necessarie, ad esempio, quelle per il movimento illimitato di telecamere, la capacità di zoom, la trasmissione radio, registrazioni e analisi audio.

By default

In aggiunta, il connesso principio della protezione dei dati per impostazione predefinita (by default), presuppone che le apparecchiature prescelte possano vantare tecnologie integrate per il miglioramento della privacy ed impostazioni predefinite che riducano al minimo il trattamento dei dati personali e la loro più elevata protezione.
Esempi in tal senso sono i sistemi che consentono di mascherare aree non rilevanti per la sorveglianza o la cancellazione di immagini di terze persone, quando si forniscono riprese video su richiesta degli interessati.

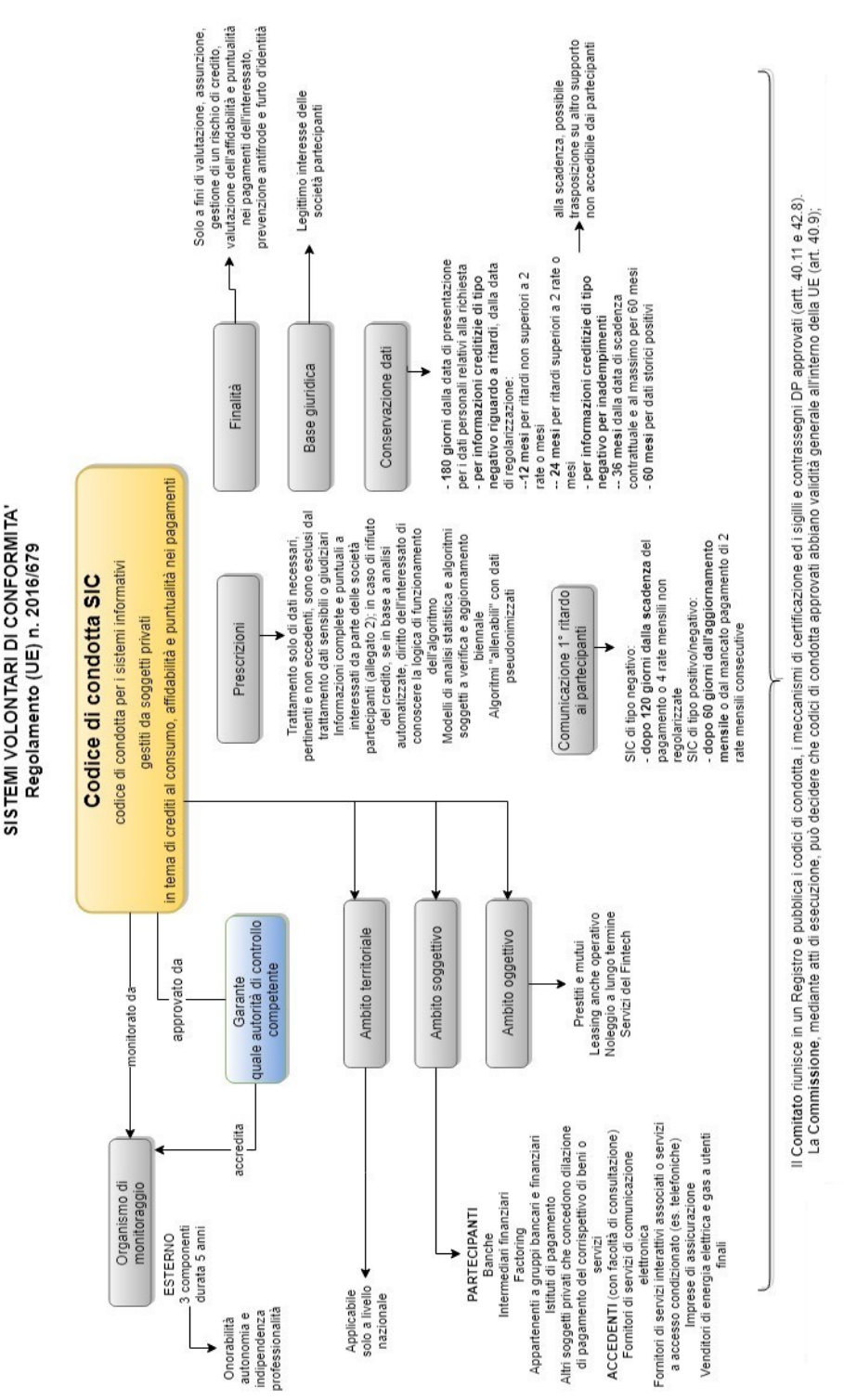
DPIA

Tra le misure di protezione di natura organizzativa è compresa l'esecuzione della valutazione di impatto quando questa risulti obbligatoria (art. 35). L'effettuazione della DPIA in merito ad un'attività di videosorveglianza costituisce una diretta manifestazione dell'accountability del titolare.
Le indicazioni del GDPR e quelle contenute nelle linee guida sulla DPIA, circa le casistiche che rendono obbligatoria tale valutazione, evidenziano alcune circostanze che sono direttamente riconducibili ad attività di videosorveglianza:

- se il trattamento costituisce un **monitoraggio sistematico di un'area accessibile al pubblico su larga scala** [art. 35(3)(c)];
- se il trattamento riguarda **categorie speciali di dati su larga scala** [art. 35(3)(b)];
- l'uso di un sistema di telecamere per **monitorare le autostrade** (v. linee guida su DPIA, wp248 rev.01).

Considerato che sia ragionevole presumere che molti casi di videosorveglianza richiederanno una DPIA, le linee guida suggeriscono di consultare anche le black list pubblicate dalle singole autorità di supervisione (cioè gli elenchi dei trattamenti considerati ad alto rischio tali da richiedere obbligatoriamente una DPIA).

33.
Approvato il codice di condotta SIC


SISTEMI VOLONTARI DI CONFORMITA'
Regolamento (UE) n. 2016/679
Codice di condotta SIC
codice di condotta per i sistemi informativi gestiti da soggetti privati
in tema di crediti al consumo, affidabilità e puntualità nei pagamenti
monitorato da
approvato da
Organismo di monitoraggio
ESTERNO
3 componenti
durata 5 anni
Onorabilità
autonomia e
indipendenza
professionalità
accredita
Garante
quale autorità di controllo competente
Ambito territoriale
Applicabile solo a livello nazionale
Ambito soggettivo
PARTECIPANTI
Banche
Intermediari finanziari
Factoring
Appartenenti a gruppi bancari e finanziari
Istituti di pagamento
Altri soggetti privati che concedono dilazione di pagamento del corrispettivo di beni o servizi
ACCEDENTI (con facoltà di consultazione)
Fornitori di servizi di comunicazione elettronica
Fornitori di servizi interattivi associati o servizi a accesso condizionato (es. telefoniche)
Imprese di assicurazione
Venditori di energia elettrica e gas a utenti finali
Ambito oggettivo
Prestiti e mutui
Leasing anche operativo
Noleggio a lungo termine
Servizi del Fintech
Prescrizioni
Trattamento solo di dati necessari, pertinenti e non eccedenti, sono esclusi dal trattamento dati sensibili o giudiziari
Informazioni complete e puntuali a interessati da parte delle società partecipanti (allegato 2); in caso di rifiuto del credito, se in base a analisi automatizzate, diritto dell'interessato di conoscere la logica di funzionamento dell'algoritmo
Modelli di analisi statistica e algoritmi soggetti a verifica e aggiornamento biennale
Algoritmi "allenabili" con dati pseudonimizzati
Comunicazione 1° ritardo ai partecipanti
SIC di tipo negativo:
- dopo 120 giorni dalla scadenza del pagamento o 4 rate mensili non regolarizzate
SIC di tipo positivo/negativo:
- dopo 60 giorni dall'aggiornamento mensile o dal mancato pagamento di 2 rate mensili consecutive
Finalità
Solo a fini di valutazione, assunzione, gestione di un rischio di credito, valutazione dell'affidabilità e puntualità nei pagamenti dell'interessato, prevenzione antifrode e furto d'identità
Base giuridica
Legittimo interesse delle società partecipanti
Conservazione dati
- 180 giorni dalla data di presentazione per i dati personali relativi alla richiesta
- per informazioni creditizie di tipo negativo riguardo a ritardi, dalla data di regolarizzazione:
--12 mesi per ritardi non superiori a 2 rate o mesi
-- 24 mesi per ritardi superiori a 2 rate o mesi
- per informazioni creditizie di tipo negativo per inadempimenti
-- 36 mesi dalla data di scadenza contrattuale e al massimo per 60 mesi
- 60 mesi per dati storici positivi
alla scadenza, possibile trasposizione su altro supporto non accedibile dai partecipanti
Il Comitato riunisce in un Registro e pubblica i codici di condotta, i meccanismi di certificazione ed i sigilli e contrassegni DP approvati (artt. 40.11 e 42.8).
La Commissione, mediante atti di esecuzione, può decidere che codici di condotta approvati abbiano validità generale all'interno della UE (art. 40.9);
Rosario Imperiali
@Ros_Imperiali

Il Garante ha pubblicato il provvedimento di approvazione del codice di condotta sui servizi di informazione creditizia comunemente chiamato "SIC" (codice di condotta per i sistemi informativi gestiti da soggetti privati in tema di crediti al consumo, affidabilità e puntualità nei pagamenti), a conclusione del procedimento previsto dall'articolo 20 del d.lgs. n. 101/2018 (norma di adeguamento del codice privacy al regolamento europeo) e nel rispetto delle prescrizioni del GDPR per questo tipo di strumenti di *soft law* (art. 40).
Questo codice di condotta si aggiunge al precedente sulle informazioni commerciali e, per la sua piena applicazione come l'altro citato, attende che si completi l'accreditamento dell'organismo di monitoraggio da parte del Garante, secondo i criteri che saranno indicati dall'EDPB.

Procedimento di approvazione

Il decreto di adeguamento del codice privacy al GDPR (dlgs. 101/2018) aveva previsto che il previgente codice SIC avrebbe continuato a produrre effetti a condizione che il procedimento per l'approvazione del nuovo codice sostituitivo si fosse esaurito entro 12 mesi a partire dal 19 settembre 2018, data di entrata in vigore del decreto, con l'approvazione da parte del Garante.
Il Garante, infatti, è l'autorità di supervisione territorialmente competente secondo quanto prescrive l'articolo 40 del GDPR, in quanto il SIC è un codice di condotta che trova applicazione solo nel nostro paese. Il termine dei dodici mesi è stato rispettato mediante il provvedimento del Garante del 12 settembre 2019 con cui si approva il testo del nuovo codice di condotta SIC. È già previsto che i gestori che sottoscrivono questo Codice di condotta proporranno al Garante un nuovo progetto entro un termine massimo di dodici mesi dall'entrata in vigore dello stesso.

Ambito territoriale

Il codice SIC ora approvato ha valenza solo all'interno del nostro paese e per questo motivo l'autorità di controllo competente per la sua approvazione è il Garante privacy.

Ambito oggettivo

Il SIC può essere di duplice natura:

1. **SIC negativo**: o centrale rischi a sistema "negativo" che detiene esclusivamente informazioni che riguardano rapporti di credito per i quali si sono verificati inadempimenti;
2. **SIC positivo/negativo**: poiché raccoglie tutte le informazioni sul rapporto di finanziamento, indipendentemente dal fatto che ci siano o meno degli inadempimenti.

In entrambi i casi le informazioni riguarderanno prestiti e mutui, rapporti di leasing anche operativo, noleggio a lungo termine, servizi del fintech (cioè la fornitura di servizi e prodotti finanziari erogati attraverso le più moderne tecnologie).
I dati personali oggetto di trattamento sono:

- **dati identificativi**, anagrafici e sociodemografici (quali, ad esempio: codice fiscale, partita Iva, dati di contatto);
- **dati relativi alla richiesta/rapporto** di credito;
- **dati di tipo contabile**, relativi, in particolare, agli utilizzi o ai pagamenti;
- **dati relativi al contenzioso** e ad attività di recupero del credito, alla cessione del credito o a eccezionali vicende che incidono sulla situazione soggettiva o patrimoniale degli interessati.

Non possono essere oggetto del SIC categorie particolari di dati personali o dati relativi a condanne penali e reati. I dati personali sono di tipo obiettivo, adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
Nel SIC sono registrati gli estremi identificativi del partecipante che ha comunicato i dati personali relativi alla richiesta/rapporto. Tali estremi sono accessibili al gestore o agli interessati e non anche agli altri partecipanti.

Ambito soggettivo

I sistemi di informazione creditizia sono caratterizzati da una triangolazione degli attori coinvolti:

- il **gestore del sistema** società di diritto privato il cui oggetto sociale consiste nel trattamento e nell'elaborazione di dati forniti da altri enti (c.d. partecipanti) nel sistema, in cui sono convogliate le informazioni creditizie di cui ci si avvale in regime di reciprocità;
- i **partecipanti**, cioè l'intera platea degli operatori finanziari (banche, altri intermediari finanziari, società di leasing, operatori economici che concedono dilazioni di pagamento, società di credito al consumo) che hanno diritto ad accedere ed utilizzare le informazioni contenute nel SIC per le finalità indicate e che, di converso, si impegnano ad alimentarlo mediante la trasmissione puntuale e tempestiva al SIG delle informazioni inerenti i rapporti di finanziamento con la propria clientela; ad essi si aggiungono gli **accedenti**, che sono persone giuridiche ulteriori cui il legislatore, in fasi successive, ha riconosciuto il diritto di consultare il SIG per le medesime finalità.
- il **soggetto interessato**, debitore o potenziale, cui si riferiscono i dati personali contenuti nel SIG.

Ne deriva che l'operatività e l'affidabilità dei SIC si basa essenzialmente su di una "triangolazione" di rapporti tra ente gestore ed enti partecipanti: questi ultimi, infatti, non si limitano ad un ruolo passivo di "interroganti", ma svolgono anche una funzione "attiva" di fornitori di informazioni, limitatamente ai rapporti di credito che li vedono coinvolti con i soggetti interessati al finanziamento, il tutto nel quadro di accordi contrattuali che li legano al SIC. Ciò comporta, dunque, che il gestore non ha rapporti né contrattuali né diretti con i soggetti oggetto di registrazione (cioè i debitori o richiedenti credito).

Ruoli soggettivi data protection

Il gestore del SIG è titolare del trattamento dei dati personali registrati nel SIC, di cui decide mezzi e modalità di funzionamento; mentre ciascun partecipante è «*titolare del trattamento dei dati personali raccolti in relazione a richieste/rapporti*» di credito.

Le distinte responsabilità dei titolari nel SIC

La fase di "raccolta" e contribuzione del dato nel SIC ricade sotto la responsabilità del partecipante e precede logicamente e cronologicamente quella di "registrazione" dei dati (che ricade sotto la responsabilità del gestore). La fase di raccolta delle informazioni da immettere nel SIC include ovviamente la correttezza e veridicità dei dati segnalati.
In altri termini,

- il "dato" segnalato discende dal rapporto negoziale instaurato tra partecipante e soggetto finanziato, al quale il gestore rimane estraneo (art. 1372 c.c.);

- è sempre il partecipante (intermediario bancario) a raccogliere e trasmettere al SIC i dati di segnalazione; al partecipante spetta l'adozione di idonee procedure di verifica per garantire la lecita utilizzabilità nel sistema, la correttezza, l'aggiornamento e l'esattezza dei dati comunicati al gestore;
- il gestore si limita a "registrare" il flusso informativo proveniente dall'ente partecipante, senza possibilità di effettuare verifiche di merito (veridicità/esattezza dei dati contribuiti).

Operazioni dovute dal gestore in caso di contestazione del debitore interessato

Il gestore del SIC, ove il soggetto censito contesti in tutto o in parte i dati iscritti a proprio nome, richiede agli intermediari segnalanti verifiche sull'esattezza dei dati registrati in archivio, invitandoli ad eseguire le necessarie rettifiche ovvero a comunicare la conferma dei dati segnalati e, nelle more, sospende la visibilità dei dati in contestazione ai partecipanti al proprio circuito informativo.

Prescrizioni

Preavviso di registrazione

Al verificarsi di ritardi nei pagamenti, il partecipante deve inviare all'interessato un preavviso circa l'imminente registrazione dei dati in uno o più SIC, le cui modalità di inoltro sono specificate nell'**allegato 1** del provvedimento. Tale preavviso ha lo scopo di alertare l'interessato in modo da consentirgli una rapida regolarizzazione evitando così la registrazione del proprio nominativo nel SIC, con tutti gli effetti che ne conseguono.

I dati relativi al primo ritardo possono essere resi accessibili ai partecipanti solo decorsi almeno quindici giorni dalla spedizione del preavviso all'interessato. Il partecipante deve dimostrare la ricezione di tale preavviso da parte dell'interessato.

Base giuridica

La base giuridica a fondamento della liceità del trattamento da parte di entrambi i titolari – il gestore ed i partecipanti – è stato individuato nel legittimo interesse degli stessi (nello specifico, la corretta misurazione del merito e del rischio creditizio, la corretta valutazione dell'affidabilità e della puntualità dei pagamenti dell'interessato, la prevenzione del rischio di frode, ivi inclusa la prevenzione del rischio del furto di identità), ai sensi dell'articolo 6(1)(f) del regolamento; pertanto, non è necessario acquisire il consenso dell'interessato.

Informativa

Al momento della raccolta dei dati personali relativi a richieste o rapporti, il partecipante fornisce all'interessato l'informativa privacy anche con riguardo al trattamento dei dati personali effettuato nell'ambito di un SIC. Il codice di condotta contiene un modello di informativa approvato, riportato in **allegato 3**. In caso di variazioni rispetto alle informazioni fornite originariamente, l'informativa aggiornata «è fornita attraverso comunicazioni periodiche, o attraverso uno o più siti internet e a richiesta degli interessati». In aggiunta all'informativa resa dal partecipante ad ogni singolo interessato, «*il gestore fornisce un'informativa più dettagliata attraverso il proprio sito internet e/o altre eventuali ulteriori modalità anche digitali*».

Decisioni automatizzate di scoring

I modelli o i fattori di analisi statistica, nonché gli algoritmi di calcolo sono verificati periodicamente con **cadenza almeno biennale** ed aggiornati in funzione delle risultanze di tali verifiche.

Diritti dell'interessato

Il codice prevede specifici diritti per l'interessato ad integrazione di quelli del regolamento.
Quando la richiesta non è accolta, l'interessato può richiedere al partecipante se, per istruire la richiesta di credito,

- ha consultato dati ottenuti mediante trattamenti o processi decisionali automatizzati di scoring, di fornirgli tali dati, nonché una spiegazione delle logiche di funzionamento;
- ha consultato anche dati personali di tipo negativo nelle banche di dati provenienti da fonti pubbliche «*ed ottenere dettagli circa la fonte da cui provengono i dati medesimi e gli estremi identificativi del gestore del SIC che ha fornito tali informazioni*».

Misure di sicurezza

Può accedere al SIC solo un **numero limitato di persone autorizzate per iscritto** al trattamento sotto l'autorità diretta del titolare o del responsabile, sotto vincolo di riservatezza ed istruite in tal senso. Partecipanti e gestore devono «*garantire un livello di sicurezza adeguato al rischio fin dalla fase della progettazione e per impostazione predefinita*», tali misure possono comprendere, se del caso, quelle indicate all'articolo 32 del GDPR.

Data breach

In caso di violazione di dati personali contenuti nei SIC il gestore comunica la violazione all'autorità di controllo compente e si impegna ad informare i partecipanti senza ingiustificato ritardo e, comunque, entro i termini fissati dal regolamento, unitamente alla descrizione dettagliata della violazione. Restano ferme le disposizioni pertinenti contenute nel GDPR.

Organismo di monitoraggio

Come prescritto dall'articolo 41 del regolamento, «*fatti salvi i compiti e i poteri dell'autorità di controllo competente*» il controllo di conformità alle regole di un codice di condotta è effettuato da un organismo di monitoraggio, «*in possesso del livello adeguato di competenze riguardo al contenuto del codice*».
L'organismo di monitoraggio del codice SIC sarà composto da 3 componenti con caratteristiche di onorabilità, autonomia e indipendenza nonchè professionalità, che dureranno in carica 5 anni.
L'organismo deve essere accreditato dal Garante sulla base dei criteri individuati dall'EDPB. Questo passaggio, non ancora completato in attesa dei citati criteri da parte del Comitato, pone il codice in uno stato di quiescenza.

34.
Consenso libero e “a pagamento”

Un'interessante vicenda per cui un operatore commerciale si propone come intermediario tra gli interessati e i titolari del trattamento per esercitare, per loro conto, il diritto alla portabilità ed acquisire dati personali delle carte fidelity registrate a nome degli stessi, al fine di crearne profili statistici da commercializzare sul mercato, offre lo spunto per fare qualche riflessione sul complesso tema della libertà del consenso e sulla legittimità del consenso come merce di scambio; ovvero, per meglio dire, sulla liceità della fornitura dei dati personali come elemento compensativo di beni o servizi.

Sintesi

- Sia Cassazione n. 17278/2018, la quale comunque ha deciso facendo anche ampio riferimento ai pertinenti passaggi del regolamento europeo, sia le linee guida wp258 rev.01 ammettono che i dati personali possano essere merce di scambio e considerano ammissibile, a determinate condizioni, che **il consenso "privacy"** per l'uso dei dati personali per ulteriori finalità, **possa essere vincolato ad un differente contratto per la fornitura di un prodotto/servizio**.
- In questi casi – comunque visti con particolare sfavore dal GDPR – occorre che il titolare dimostri che il consenso dell'interessato sia stato **realmente libero** e non condizionato, tanto da potersi considerare valido.
- La **prova** deve documentare che l'interessato, qualora avesse rifiutato il proprio consenso "privacy", avrebbe comunque potuto avvalersi di un **prodotto/servizio equivalente senza subire alcun pregiudizio**.
- Il **pregiudizio sussiste nell'ipotesi** in cui si vincoli la fruizione del prodotto/servizio al rilascio del consenso "privacy" senza che l'interessato abbia alternative equivalenti, ma anche nel caso in cui – almeno secondo le linee guida wp258 rev.01 – **l'alternativa "equivalente" risulti a pagamento**, contrariamente all'ipotesi gratuita originaria.
- Sembrerebbe **ammissibile che il consenso "privacy" sia collegato ad uno specifico incentivo** (ad es. uno sconto ad hoc, un gadget, una prestazione accessoria, la partecipazione ad una lotteria online), fruibile solo in caso di assenso dell'interessato al trattamento dei dati personali ma senza che questi venga escluso dalla fornitura principale, così da non produrre un pregiudizio per l'interessato in caso di diniego.

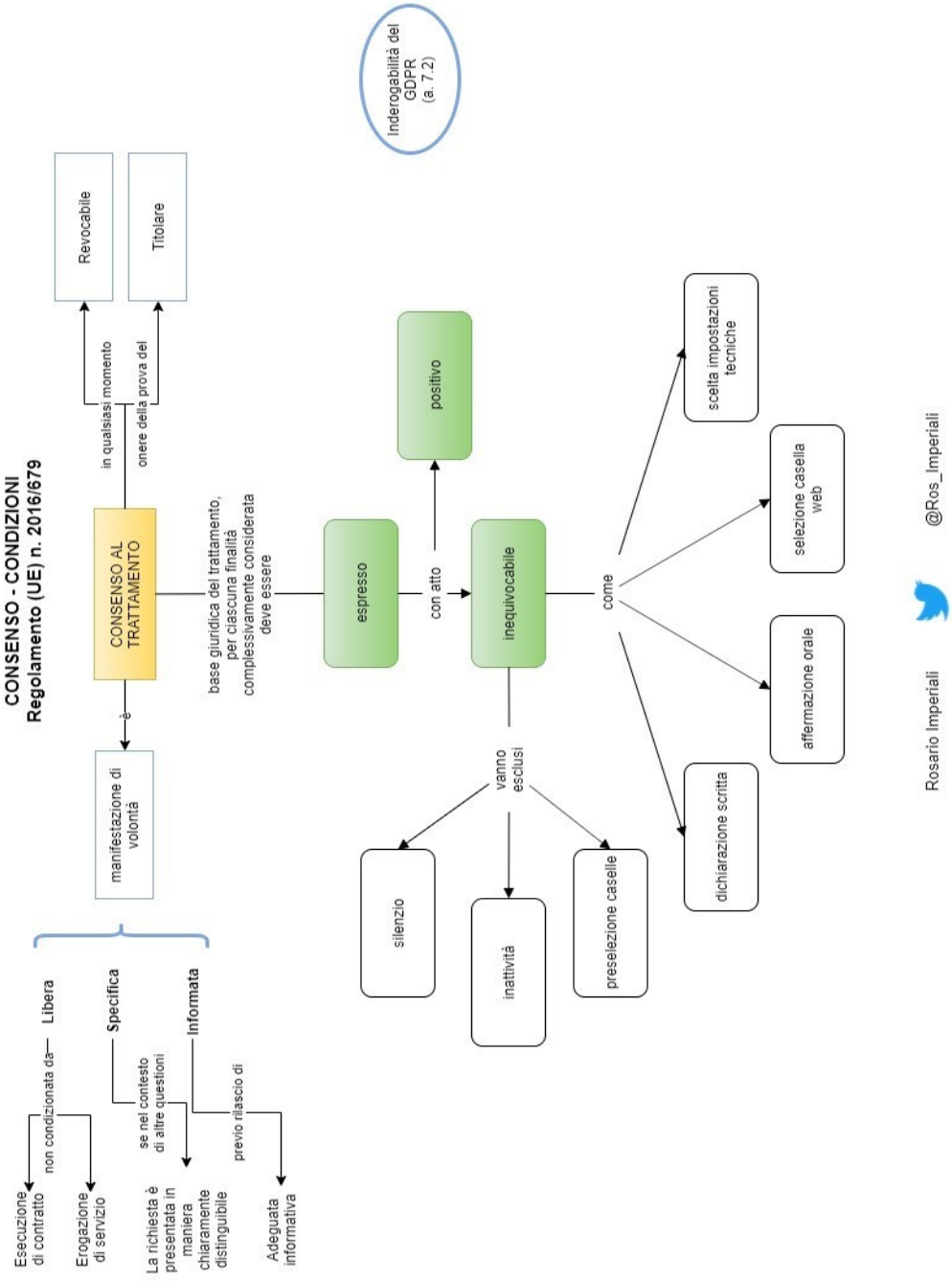


Fig. 1 - Le condizioni di un valido consenso.

Consenso nel GDPR

Una delle principali basi giuridiche del trattamento di dati personali – cioè delle condizioni che rendono legittimo un trattamento – è il consenso dell'interessato [art. 6.1, lett. a)], che è oggetto di un commento articolato nella sezione "Argomenti" del DPtel®.

Concetto

Il consenso è un'espressione attiva di volontà «*con la quale l'interessato manifesta il proprio assenso (…) che i dati personali che lo riguardano siano oggetto di trattamento*» [art. 4(11)].
Quindi il consenso deve riguardare il trattamento dei propri dati personali, autorizzandone l'uso, e deve essere rilasciato dal medesimo individuo al quale si riferiscono i dati personali in questione.

Requisiti del consenso valido

Il GDPR ribadisce e irrobustisce i requisiti del "valido consenso" stabilendo che «*il consenso dell'interessato (è) qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato*» (art. 4, p.11 GDPR).

Libertà del consenso

Il consenso deve essere libero cioè alla persona deve essere concessa **una vera scelta**, in caso contrario, esso perde la sua funzione di condizione di legittimità dell'uso dei dati personali [Considerando (42) e Art. 7.4].

Consenso legato ad un contratto

Il consenso per l'uso di dati personali può essere condizionato all'esecuzione di un contratto?
Il quesito riguarda l'eventuale legittimità di un contratto la cui esecuzione è condizionata al rilascio del consenso per il trattamento di dati personali per ulteriori finalità.
Il Considerando (43) del GDPR specificamente riporta che il consenso si presume che non sia stato liberamente espresso «*qualora l'esecuzione di un contratto, compresa la prestazione di un servizio, sia subordinata al consenso sebbene esso non sia necessario per tale esecuzione*», in parallelo, nella parte normativa del regolamento, si legge che «*(n)el valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto*» [art. 7(4) GDPR].
Riprendendo l'istituto giuridico del diritto tedesco sul consumo, nella causa C-673/17 dinanzi alla CGUE, l'avvocato generale [*Conclusioni dell'avvocato generale Maciej Szpunar relative alla causa C-673/17 Planet49 GmbH c. Bundesverband*] fa rilevare come questa disposizione del GDPR introduca il «*divieto di pratiche di vendita aggregata*», che si verifica nell'ipotesi in cui la stipula di un contratto (nel caso, la partecipazione al gioco a premi), indebitamente incorpora in automatico la conclusione di altro contratto, distinto e funzionalmente non necessario (la prestazione del consenso all'utilizzo dei dati personali a fini pubblicitari).

Divieto assoluto o relativo

Sotto questo profilo, il divieto contenuto nel GDPR delle "pratiche di vendita aggregata" non appare assoluto, come risulta dall'espressione «**si tiene nella massima considerazione**» e dalla condizione che il consenso non sia «**necessario all'esecuzione del contratto**»:

- l'espressione «**si tiene nella massima considerazione**» evidenzia che le eventuali casistiche di "vendita aggregata" vanno valutate caso per caso al fine di verificarne la legittimità;
- la condizione della "**non necessità del consenso all'esecuzione del contratto**" indica che l'ipotesi opposta di un consenso necessario per l'esecuzione del contratto rappresenta un'eccezione al "divieto di vendita aggregata".

Sulla base di questa impostazione giuridica, è stato ritenuto che lo scopo di un gioco a premi possa legittimamente essere quello dell'acquisizione di dati personali per finalità pubblicitarie, per cui il consenso dell'utente a tale utilizzo risulterebbe in tal caso "necessario" per la partecipazione al gioco (*conclusioni dell'avvocato generale nella causa C-673/17, cit.*). Di conseguenza, in questa ipotesi varrebbe l'eccezione della "necessarietà" e la subordinazione della partecipazione al gioco alla prestazione del consenso dell'utente all'utilizzo dei propri dati personali a fini pubblicitari non dovrebbe considerarsi una "vendita aggregata" illegittima («*In una tale situazione il trattamento di questi dati personali è, a mio avviso, necessario per la partecipazione al gioco a premi*») (v. al riguardo l'Editoriale del 28 marzo 2019).

Consenso "come condizione" rispetto al consenso "per l'esecuzione" del contratto

L'ipotesi del consenso al trattamento di dati personali per una determinata finalità richiesto **"come condizione per eseguire un contratto"** o per ottenere la fornitura di un servizio, va tenuta distinta dalla diversa circostanza in cui si evidenzia erroneamente il consenso dell'interessato **"come base giuridica per l'esecuzione di un contratto"**.

In questo secondo caso, il consenso dell'interessato per il trattamento dei suoi dati personali verrebbe richiesto dal titolare del trattamento al fine di poter dare esecuzione al contratto sull'erroneo presupposto che la base giuridica che legittimi l'uso dei dati personali **necessari** per dare esecuzione al contratto stesso risieda appunto nel consenso dell'interessato. In tale circostanza, l'errore insiste sul fatto che il trattamento di quei dati personali dell'interessato **che siano necessari** per dare esecuzione al contratto di cui l'interessato è parte (o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso) riscontra la propria base giuridica non tanto nel consenso piuttosto nella "necessità contrattuale", specificamente prevista per tale situazione all'articolo 6(1)(b) del GDPR.

La differente ipotesi del consenso richiesto (preteso) "come condizione per eseguire un contratto" si distingue dalla precedente casistica per due fattori:

- i dati personali in questione **non sono funzionalmente necessari** per l'esecuzione del contratto di riferimento;
- il rilascio del consenso al trattamento dei dati personali, ancorché questi non siano necessari, viene artificiosamente legato all'altro contratto come **condizione essenziale** per la sua esecuzione.

Dati necessari per l'esecuzione del contratto

Le linee guida wp259 rev.01 sottolineano che «*L'articolo 7, paragrafo 4, mira a garantire che la finalità del trattamento dei dati personali non sia mascherata né accorpata all'esecuzione di un contratto o alla prestazione di un servizio per il quale i dati personali non sono necessari*». Nel senso che «*le due basi giuridiche per la liceità del trattamento dei dati personali, ossia il consenso e l'esecuzione di un contratto, non possono essere riunite e rese indistinte*» per cui «*l'obbligo di acconsentire all'uso di dati personali aggiuntivi rispetto a quelli strettamente necessari, limita la scelta dell'interessato e ostacola l'espressione del libero consenso.*».

Detto diversamente:

- **Se i dati personali sono necessari** per dare esecuzione al contratto, non occorre il consenso dell'interessato per il relativo trattamento degli stessi per tale finalità, in quanto i dati personali necessari potranno essere utilizzati in virtù della base giuridica della "necessità contrattuale"
- **Se i dati personali non sono necessari** per l'esecuzione del contratto, allora occorre il consenso specifico dell'interessato per poterli utilizzare per la finalità dichiarata e, in tal caso, non si può condizionare la fornitura del contratto o servizio al rilascio del consenso al trattamento dei dati non necessari
- **Se ancora i dati personali non sono necessari per l'esecuzione** del contratto **ma risultano invece necessari per la finalità** del contratto (v. il caso della lotteria on line la cui partecipazione è finalizzata all'acquisizione e sfruttamento di dati personali a fini marketing) allora il consenso al trattamento (in quanto necessario per la legittima finalità perseguita) può essere validamente condizionato al contratto.

Rimane da valutare, quindi, entro quali limiti lo scopo della fornitura del contratto o servizio possa validamente vincolare al rilascio del consenso "privacy", per dati personali non necessari all'esecuzione della prima transazione.

Consenso e dati personali come merce di scambio

È oramai noto che la gratuità dei servizi on line si fonda su un modello di scambio non sempre trasparente o consapevole: da un lato, la fruizione del servizio privo di prezzo in danaro, dall'altro lato, l'uso a fini commerciali – da parte del fornitore – dei dati personali procurati "in chiaro" dall'utente e/o delle tracce da esso stesso lasciate mentre si avvale dell'opportunità offertagli.

Se, sotto il profilo economico, si evidenzia che questo scambio rende sostenibile (l'apparente) gratuità dei servizi menzionati in quanto, in mancanza, essi sarebbero disponibili solo a titolo oneroso, d'altro canto, ci si continua a interrogare in merito alla legittimità giuridica dell'uso dei dati personali come merce di scambio.

Pertanto, il tema della legittimità dei servizi del mercato digitale compensati con il valore dei dati personali conferiti dagli interessati, solleva due questioni principali:

- la **trasparenza verso l'interessato** della reale connotazione sinallagmatica del rapporto (servizio contro dati personali)
- la **commerciabilità dei dati personali**.

Trasparenza sui dati personali come controprestazione in natura

Far apparire all'utente che un servizio sia gratuito, solo perché non sia previsto il pagamento di un corrispettivo in danaro, mentre in realtà esso è compensato con prestazioni "in natura" come

l'acquisizione e l'uso di dati personali dell'utente stesso, è una pratica commerciale ingannevole che viola anche il principio di correttezza [Art. 5(1)(a), GDPR].
Nel novembre 2018 l'antitrust italiana ha sanzionato in solido Facebook Inc. e Facebook Ireland Ltd. al pagamento di una somma pecuniaria complessiva di 10 milioni di euro per due distinte pratiche commerciali scorrette a danno dei consumatori tra cui quella per aver **ingannato gli utenti** facendogli ritenere che l'iscrizione al social fosse gratuita, anzichè precisare in fase di attivazione dell'account che essa, in effetti, realizza una **transazione di natura commerciale** il cui corrispettivo è rappresentato dallo **sfruttamento commerciale dei dati personali degli utenti-iscritti** (v. Alert del 13 dicembre 2018).

Commerciabilità dei dati personali

Argomentando ulteriormente sulla scia della tesi che nel caso di subordinazione del consenso privacy "**necessitata**" dallo scopo intrinseco di un diverso contratto si avrebbe un'eccezione del divieto di vendita aggregata, si perviene all'affermazione che i dati personali possono formare oggetto di una controprestazione ("vendita"); in tal caso, il consenso al loro utilizzo risulta "necessario" all'esecuzione dell'altro contratto e, quindi, sarà valido nonostante l'apparente "condizionamento" (causa C-673/17, cit.).
Ovviamente, anche in tale circostanza occorrerà prestare particolare attenzione all'adeguatezza dell'informativa, tale da permettere all'interessato di adottare decisioni informate prima del trattamento.

Spunti regolatori

Non sembra dubbio che ai dati personali possa essere riconosciuto un valore economico, lo testimonia la prassi di mercato della remunerazione dei servizi mediante acquisizione di dati personali. Ne dà atto la **direttiva UE 2018/1972**, contenente il **nuovo codice europeo delle comunicazioni elettroniche**, in cui si legge che «*(n)ell'economia digitale i partecipanti al mercato sempre più spesso ritengono che le informazioni sugli utenti abbiano un valore monetario. I servizi di comunicazione elettronica sono spesso forniti all'utente finale non solo in cambio di denaro, ma in misura sempre maggiore e in particolare in cambio della comunicazione di dati personali o di altri dati. Il concetto di remunerazione dovrebbe pertanto ricomprendere le situazioni in cui il fornitore di un servizio chiede all'utente finale dati personali ai sensi del regolamento (UE) 2016/679 o altri dati, e questi glieli trasmette consapevolmente, per via diretta o indiretta*» [Considerando (16), direttiva (UE) 2018/1972].
Sotto il profilo giuridico, il diritto alla protezione dei dati personali «*non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità*»; si potrebbe fondatamente sostenere che esso vada contemperato con la tutela della libertà d'impresa riconosciuta dall'art. 16 della Carta di Nizza e dall'art. 41 della Costituzione italiana: rientrerebbe nella libertà d'impresa effettuare transazioni commerciali che prevedano il rilascio di dati personali a titolo compensativo di prodotti o servizi, altrimenti onerosi.

Linee guida EDPB

Le linee guida wp259 rev.01 sul consenso, fatte proprie dall'EDPB, sembrano anch'esse ammettere, in linea di principio, la legittima fungibilità dei dati personali come merce di scambio allorquando affermano che «*il regolamento generale sulla protezione dei dati non esclude tutti gli incentivi*».

Tuttavia, questa affermazione generale sembra trovare vaste limitazioni applicative che ne rendono la traduzione nella pratica di portata affatto residuale ed eccezionale.

Il caso Weople

Il consenso al trattamento di dati personali per determinate finalità non solo può levarsi a "corrispettivo in natura" a fronte della fornitura di un contratto o un servizio ma può anche rappresentare una "merce" che viene acquistata dietro pagamento di un prezzo.

Nel luglio 2019 l'Autorità Garante per la privacy ha posto all'attenzione del Comitato europeo per la protezione dei dati personali (EDPB) la questione relativa a "Weople", l'app che promette ai propri iscritti una remunerazione in cambio della cessione dei loro dati personali. L'aspetto centrale di questa operazione – che ha sollevato la richiesta del Garante verso una posizione comune in sede di EDPB – «*riguarda il delicato tema della "commerciabilità" dei dati, causata dall'attribuzione di un vero e proprio controvalore al dato personale*».

La Weople è un'app mediante la quale verrebbero condivisi con gli utenti i guadagni (a regime, il 90% degli utili) ottenuti tramite la vendita a terzi dei servizi di analisi e profilazione basati sui dati di consumo registrati nelle fidelity card rilasciate agli stessi utenti ed emesse da operatori commerciali. I dati di origine verrebbero acquisiti da Weople, in parte, tramite conferimento diretto da parte degli interessati ed in parte tramite l'esercizio su delega della portabilità da altri operatori economici.

In questo caso la remunerazione economica dei dati personali sarebbe manifesta, attribuendo un vero e proprio "controvalore" al dato personale.

La posizione dell'EDPB, sollecitata dal Garante italiano, dovrebbe definire con maggiore precisione il perimetro di validità del consenso e dei relativi dati personali come strumento compensativo della fornitura di prodotti e servizi ovvero come effettiva merce di scambio a titolo oneroso.

35.
Dalla decisione Planet49 sui cookie, poche ma importanti novità

Si è fatto un gran parlare in questi giorni della decisione della Corte di giustizia europea (CGUE) relativa alla causa Planet 49 ed ai profili innovativi che ne sarebbero conseguiti in merito al consenso dei cookie e a molto altro; in realtà poche sono le novità interpretative di rilievo, mentre la maggior parte dei contenuti della decisione ribadiscono letture oramai consolidate in questo ambito complesso e di natura altamente tecnica.
La puntata odierna dell'Alert intende fare un breve resoconto dei principali aspetti interpretativi di questa sentenza.

Sentenza della Corte nella causa C-673/17

Con sentenza del 1° ottobre 2017 la CGUE ha deciso in merito alla causa C-673/17 che essenzialmente verte su alcune importanti questioni relative alla protezione dei dati personali (regolata dal **GDPR**) ed all'interrelazione di questa materia con la tutela della vita privata nelle comunicazioni elettroniche (quel dominio che si è soliti indicare come **ePrivacy**).
In questo ambito, la Corte ha affrontato anche il tema del consenso dell'interessato e l'interrogativo se il **consenso richiesto per l'impianto dei cookie** debba considerarsi della stessa specie o diverso dal **consenso dell'interessato previsto dal GDPR** e inserito fra le basi giuridiche del trattamento [art. 6(1)(a)].
Come spesso accade, la Corte ha accolto le conclusioni dell'avvocato generale di cui abbiamo riferito in una precedente tornata (v. al riguardo l'Editoriale del 28 marzo 2019).

Disciplina ePrivacy

Le comunicazioni elettroniche insistono su alcune importanti libertà e diritti fondamentali dell'individuo come la **libertà di espressione**, la **segretezza della corrispondenza** e la **tutela della vita privata**.
La disciplina a tutela della vita privata nelle comunicazioni elettroniche è contenuta nelle **direttive 2002/58/CE e 2009/136/CE** ed è in attesa della riforma che tenga conto della mutata regolamentazione generale sulla protezione dei dati personali, introdotta col GDPR. È tuttora in discussione presso le istituzioni legislative europee la proposta di regolamento ePrivacy che dovrà sostituire le citate direttive ed allinearsi al GDPR.

Legge speciale

La disciplina ePrivacy, comunque, è in **rapporto di legge speciale rispetto al GDPR**: nel duplice senso che:

- il GDPR non impone obblighi ulteriori rispetto a quelli specifici dell'ePrivacy (v. art. 95, GDPR);
- nel caso in cui una questione sia regolata dall'ePrivacy, allora si applica quest'ultima e non il regolamento, seppure nel rispetto dei principi generali contenuti nel GDPR.

La natura di legge speciale della disciplina ePrivacy rispetto al GDPR trova diretta esplicazione riguardo a taluni profili specifici:

- la natura delle informazioni oggetto di tutela;
- la condizione di legittimità dell'uso delle tecnologie di tracciamento e dei cookie;
- la natura dei soggetti cui si riferiscono le citate informazioni.

Disciplina ePrivacy e interrelazione col GDPR

Entrambe le direttive 2002/58/CE e 2009/136/CE rinviano alla direttiva 95/46/CE per quanto riguarda i principi fondamentali della disciplina generale, come ad esempio il significato stesso di consenso e le sue condizioni di validità [v. Considerando (17) e art. 2(f), dir. 2002/58/CE]; infatti, **le direttive ePrivacy "precisano ed integrano" la disciplina generale** [v. art.1(2) dir. 2002/58/CE].

A sua volta, il GDPR nell'abrogare la direttiva 95/46/CE (a decorrere dal 25 maggio 2018), evidenzia che «*i riferimenti alla direttiva abrogata si intendono fatti al presente regolamento*» [art. 94(2), GDPR]. Pertanto, anche in ambito di comunicazioni elettroniche la piattaforma regolatoria rimane il GDPR, mentre le disposizioni previste nel contesto ePrivacy "precisano ed integrano" le prescrizioni del GDPR.

Natura delle informazioni oggetto di tutela

La disciplina ePrivacy, diversamente dal GDPR, tutela qualunque tipo di informazione e non semplicemente i "dati personali", sull'assunto che «*(l)e apparecchiature terminali degli utenti di reti di comunicazione elettronica e qualsiasi informazione archiviata in tali apparecchiature fanno parte della sfera privata dell'utente, che deve essere tutelata ai sensi della convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali[, firmata a Roma il 4 novembre 1950]*».

Su tale presupposto, è stato agevole per la CGUE confermare nella decisione dell caso Planet49 che nell'ePrivacy la «*tutela si applica a qualsiasi informazione archiviata in tale apparecchiatura terminale, indipendentemente dal fatto che si tratti o meno di dati personali*» per evitare il «*rischio che identificatori occulti o altri dispositivi analoghi si introducano nell'apparecchiatura terminale dell'utente a sua insaputa*» (par. 70 della sentenza).

Consenso GDPR e consenso ePrivacy

Altro aspetto della decisione sul caso Planet49 ha riguardato il requisito del consenso nei due contesti GDPR e ePrivacy:

- Nel GDPR il consenso è considerato una delle basi giuridiche del trattamento, insieme ad altre tassativamente elencate all'articolo 6: il consenso per essere valido, in base al medesimo regolamento, deve essere libero, specifico, informato e inequivocabile [v. art. 4(11)].
- Nell'ePrivacy, l'impianto di cookie nei dispositivi degli utenti o altre forme di tracciamento online, è legittimo **solo** previo consenso dell'utente.

Quindi, mentre per quanto attiene le condizioni di validità del consenso occorre sempre riferirsi al GDPR anche quando si è in ambito ePrivacy [v. Considerando (17) e art. 2(f), dir. 2002/58/CE], per quanto riguarda – invece – le condizioni di legittimità dell'uso di cookie o di altre tecnologie analoghe (cioè relativamente al contesto specifico delle comunicazioni elettroniche), occorre rifarsi alle disposizioni ePrivacy che le considerano legittime, lo si ripete, **solo previo consenso dell'utente**.

Natura dei soggetti cui si riferiscono le informazioni

In relazione al consenso dell'utente o del contraente, come condizione di legittimità per l'installazione di cookie o l'uso di altre tecniche di trattaciamento online, secondo la disciplina ePrivacy è indifferente che «*quest'ultimo sia una persona fisica o giuridica*» [v. Considerando (17), dir.

2002/58/CE]. Questo in quanto la tutela della vita privata, per costante giurisprudenza della CGUE, si estende anche alle persone giuridiche.
Anche sotto questo profilo, quindi, la disciplina ePrivacy si differenzia dalla regolamentazione generale sulla protezione dei dati generali (GDPR) la quale prevede che il soggetto "interessato" sia solo la persona fisica (v. la definizione di "dato personale" dell'articolo 4(1) del GDPR).

Informativa sui cookie

Anche riguardo all'informativa, la disciplina ePrivacy fa esplicito rinvio alla regolamentazione generale; recita l'articolo 5, par. 3 della direttiva 2002/58/CE che la norma nazionale dello Stato membro deve assicurare «*che l'archiviazione di informazioni oppure l'accesso a informazioni già archiviate nell'apparecchiatura terminale di un abbonato o di un utente sia consentito unicamente a condizione che l'abbonato o l'utente in questione abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, a norma della direttiva [95/46], tra l'altro sugli scopi del trattamento*».

Invalidità del consenso cookie tramite caselle preselezionate

Uno dei quesiti posti dal giudice tedesco alla CGUE, nella domanda di pronuncia pregiudiziale, ha riguardato la validità del consenso per i cookie ottenuto «*mediante una casella preselezionata che l'utente deve dunque deselezionare al fine di negare il proprio consenso*».
La CGUE evidenzia come sia sotto l'egida della direttiva 95/46/CE sia con la vigenza del GDPR la modalità di raccolta del consenso tramite una casella online preselezionata debba ritenersi illegittima, come specificamente indicato nel regolamento; in quanto «*(a) tal riguardo, risulta praticamente impossibile determinare in modo oggettivo se, non deselezionando una casella preselezionata, l'utente di un sito Internet abbia effettivamente manifestato il proprio consenso al trattamento dei suoi dati personali, nonché, in ogni caso, se tale consenso sia stato manifestato in modo informato. Non può, infatti, essere escluso che detto utente non abbia letto l'informazione che accompagna la casella preselezionata, o addirittura che lo stesso non abbia visto tale casella, prima di continuare la propria attività sul sito Internet che visita.*» (par. 55 della sentenza).
Come si accennava, ora il GDPR al considerando (32) «*esclude invece espressamente che "il silenzio, l'inattività o la preselezione di caselle" configurino consenso*» (par. 62 della sentenza).

Informativa su tempi di conservazione e destinatari

Di contenuto innovativo, in quanto la decisione rappresenta la prima pronuncia in tal senso, è la decisione riferita al contenuto dell'obbligo di informativa nel caso di installazione di cookie.
Argomentando sulle seguenti considerazioni:

- anche l'obbligo di informativa previsto dall'ePrivacy deve essere letto secondo i canoni della regolamentazione generale sulla protezione dei dati personali (cioè, direttiva 95/46/CE e GDPR) in quanto «*l'articolo 5, paragrafo 3, della direttiva 2002/58 esige che l'utente abbia espresso preliminarmente il proprio consenso, dopo essere stato informato in modo chiaro e completo, "a norma della direttiva [95/46]"*» (par. 73 della sentenza);
- «*un'informazione chiara e completa implica che un utente sia in grado di determinare agevolmente le conseguenze di un eventuale consenso prestato e assicurare che questo sia espresso con piena conoscenza di causa. Le informazioni fornite devono essere chiaramente comprensibili e sufficientemente dettagliate, al fine di consentire all'utente di comprendere il funzionamento dei cookie utilizzati*» (par. 74);

- «*il periodo di attività dei cookie, nonché la possibilità o meno per i terzi di avere accesso a tali cookie rientrano nell'informazione chiara e completa da fornire all'utente ai sensi dell'articolo 5, paragrafo 3, della direttiva 2002/58*» (par. 75 della sentenza)

il GDPR [art. 13(1)(e) e (2)(b)] – ed in parte anche l'articolo 10 della direttiva 95/46/CE – menziona rispettivamente, in via esplicita, i destinatari o le categorie di destinatari tra i contenuti da fornire all'interessato nell'informativa e «*prevede che il titolare del trattamento debba fornire all'interessato, per garantire un trattamento corretto e trasparente, informazioni relative, in particolare, al periodo di conservazione dei dati personali oppure, se ciò non è possibile, ai criteri utilizzati per determinare tale periodo*» (par. 79 della sentenza).

Informativa precondizione del consenso valido

La conclusione della CGUE sull'informativa, ancorchè prevedibile in quanto fondata sulla lettera e sulla logica della norma, rende ancora più onerosi gli obblighi dei titolari dei siti web che nella maggioranza dei casi, allo stato attuale, non hanno ancora improntato un adeguato sistema di governo e trasparenza sui cookie e sulle tecniche di tracciamento online.

Ciò, per lo più, getta una preoccupante ombra sulla validità dei consensi cookie che non siano supportati da un'adeguata informativa anche sui citati profili

- della durata di conservazione e;
- degli eventuali destinatari delle informazioni raccolte tramite queste tecnologie.

36.
Accountability, fiducia e prova

Il 15 ottobre 2019 si è tenuto un interessante confronto presso il Parlamento UE, organizzato dal Supervisore europeo (EDPS) e dall'Osservatorio679, sul tema dei modelli di certificazione ai sensi del GDPR, nel contesto del principio di accountability. L'iniziativa italiana aveva come obiettivo quello di dare nuovo impulso alla conclusione dell'articolato processo di impostazione di tutti gli elementi necessari per l'approvazione dei criteri di certificazione da parte delle autorità di supervisione competenti (per l'Italia, il Garante privacy) nonchè per l'accreditamento degli schemi e degli enti di certificazione in tale ambito (in Italia, da parte di Accredia).

Sintesi

Il panel dell'evento su "Data protection certification models".

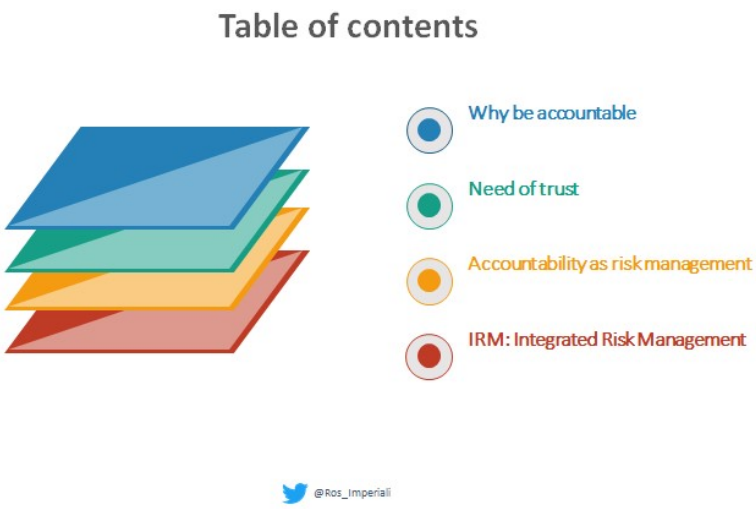
Nella presentazione del programma dell'evento veniva sottolineato come «*(c)on i principi di consapevolezza e accountability, fortemente richiamati dal GDPR, il Titolare è chiamato a "garantire" ed essere in grado di "dimostrare" che il trattamento è conforme al regolamento. Cosa fare per raggiungerlo? Quali elementi dovrebbero essere considerati? Come gestire i rischi impliciti?*
Il rischio è un concetto trasversale nel regolamento, che abbraccia il rischio per i diritti e la libertà e il rischio per le operazioni di trattamento. Come può essere gestito?».

La certificazione "ai sensi" del GDPR, **introdotta dagli artt. 42 e 43 del regolamento**, rappresenta un potente strumento atto ad agevolare la dimostrazione della conformità al GDPR, specie se correttamente interpretata proprio come supporto dell'accountability. In questa prospettiva, la relazione qui riportata aveva l'obiettivo di rispondere a tre domande principali:

- **perchè l'accountability** è stata considerata dal legislatore europeo una pietra fondante della riforma;
- **cos'è in sostanza** l'accountability;
- **qual è il metodo più convincente** per un'azienda, **per provarla** in concreto.

Table of contents

The GDPR is in itself a complex law that addresses many different and articulated issues, some of which – like accountability – are central and raise delicate questions about their proper management.
I was assigned the topic of accountability and the most appropriate ways to prove it.

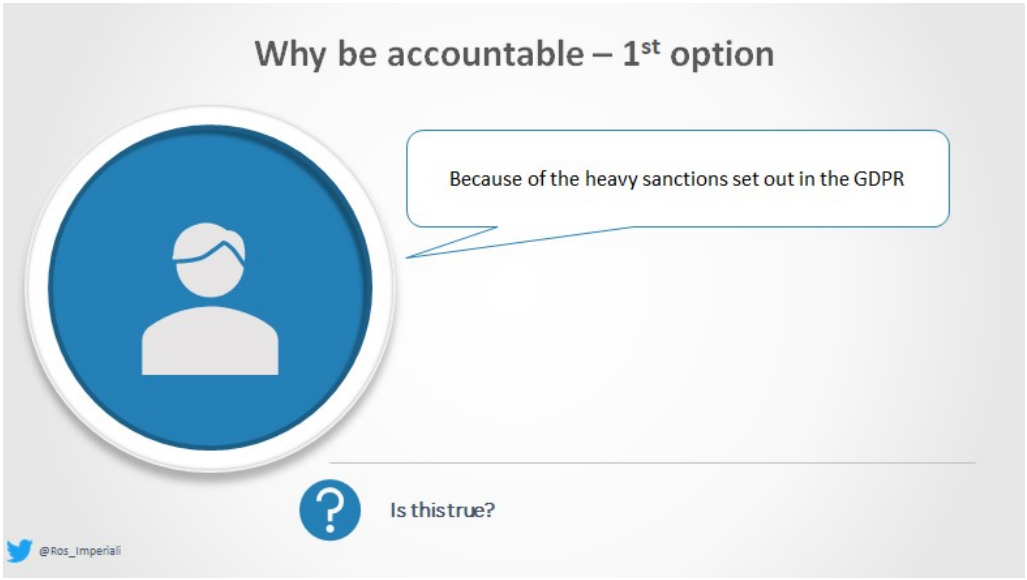


These that you see projected in the slide are the topics I would like to touch on during our talk today on this subject.

Why be accountable

When we talk about GDPR, it is natural to say that one of the fundamental principles underlying the reform is accountability.
On the other hand, it is much less frequent to consider why the EU legislator intended to put accountability as the foundation of the reform.

Avoidance of GDPR sanctions



A first possible answer could be that accountability is a condition to avoid the heavy penalties provided by the GDPR.
In this sense, accountability **would only be a remedy to avoid the worst**.
Can we agree with this vision?

Are sanctions dissuasive enough

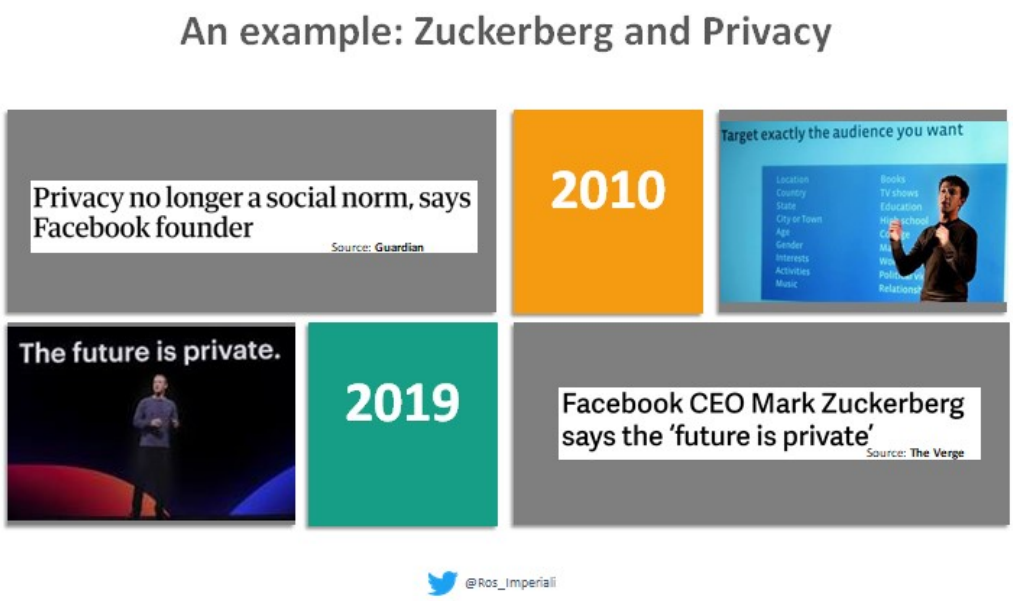
If we look at the value of the GDPR sanctions imposed in recent months, we note that it has gone from the order of thousands of euros, up to millions and even to billions of euros.
The sanction imposed on **Facebook** by the Federal Trade Commission, which technically is not a sanction but a **privacy settlement**, has caused quite a stir:

- on the one hand for the amount in billions;
- on the other hand because it was claimed that nevertheless, it was not sufficiently dissuasive as Facebook can recover this amount in less than a month of activity and, by paying this amount, a pass was guaranteed for its current business model based on the indiscriminate acquisition of users' personal data.

The question remains, therefore, whether the avoidance of sanctions is the actual driver of the GDPR compliance or if, rather, there is **a greater reason**.

Market and consumers expectations

A second option to the question of why it is necessary to be accountable presents us with a **different perspective**: that of the market and consumer expectations.
This second possible justification for the question we asked raises the hypothesis that accountability is the answer to the **current market demand**: this perspective could be the index of a changed collective attitude towards this theme, as symbolically indicates the attitude taken by Zuckerberg, head of Facebook, over the past nine years.



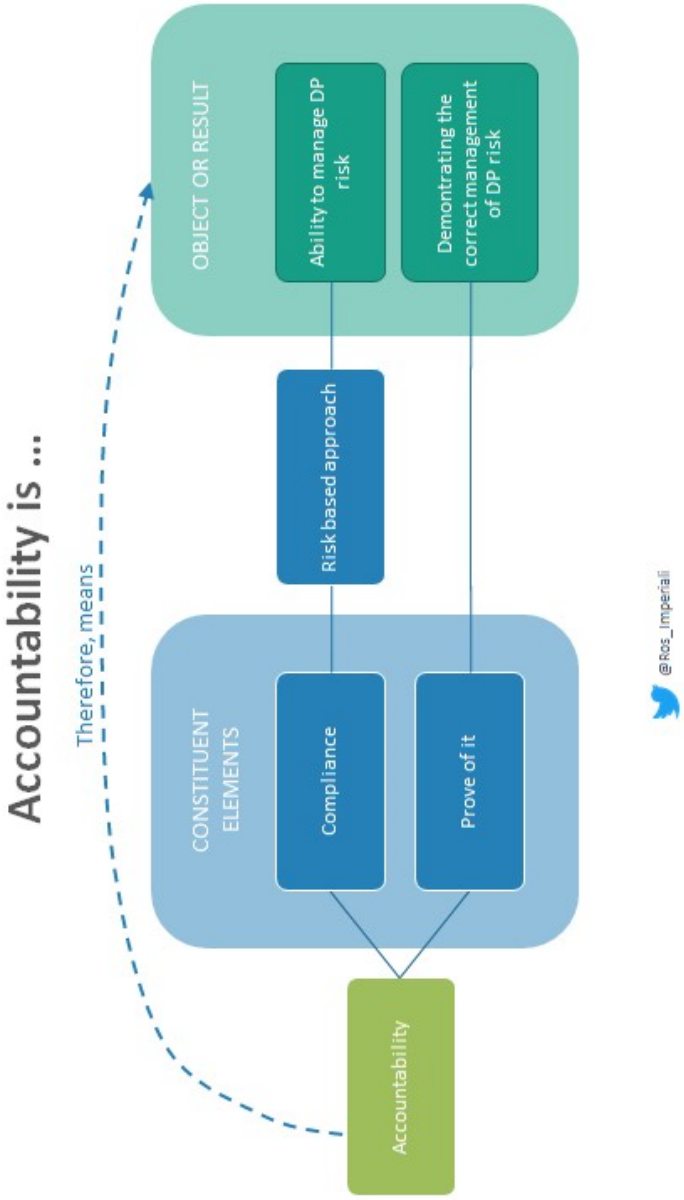
Market needs trust

If we examine this suggestion in more detail, we will note that it highlights the formation of **a virtual agreement between suppliers and consumers, of mutual convenience**: suppliers are accountable to make their customers or prospects feel at ease when they provide personal data and, on the other hand, consumers – if they know that suppliers act correctly – are encouraged to provide their personal data to obtain products and services that better meet their needs.

In other words, **accountability is an essential condition to create that context of trust** that favors the free exchange of personal data for business development, in the mutual interest of suppliers and consumers.

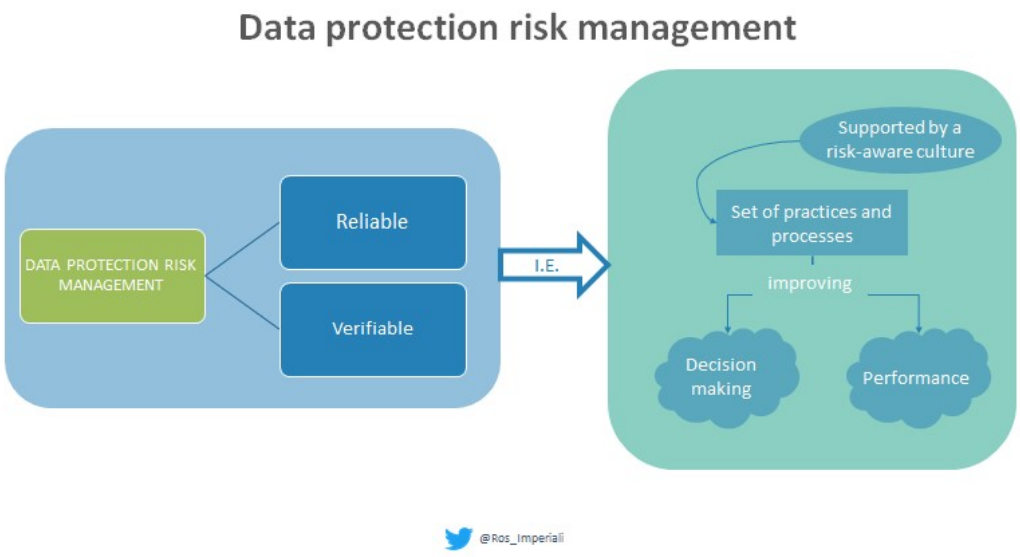
What accountability is

Once we have clarified why we need to be accountable and its significant importance, let's try to better understand what accountability is and how to manage it at its best.



As we know from the definition contained in Article 5 of the GDPR, accountability means being compliant and being able to prove it.
Compliance with the GDPR is closely linked to the risk-based approach that Article 24 of the GDPR presents as an expression of the responsibility of the controller.
Therefore, it can be stated that **compliance with the GDPR is, in essence, the ability to manage risk** to the protection of personal data.
And again, the burden of proof means the ability to demonstrate the correct management of data protection risk.

Data protection risk management



A first conclusion can be drawn: the correct management of data protection risk requires that this management be reliable and verifiable. That is, it consists of a set of practices and processes supported by a risk-aware corporate culture that is able to improve decision-making and performance activities.

Integrated risk management

But, as we will see with the projection of the last slide, for an organization that is data controller or processor, it is not enough to manage the data protection risk with a mono-dedicated tool but something more is needed, as the correct management of personal data is a **crossroads that intersect at least four domains**:

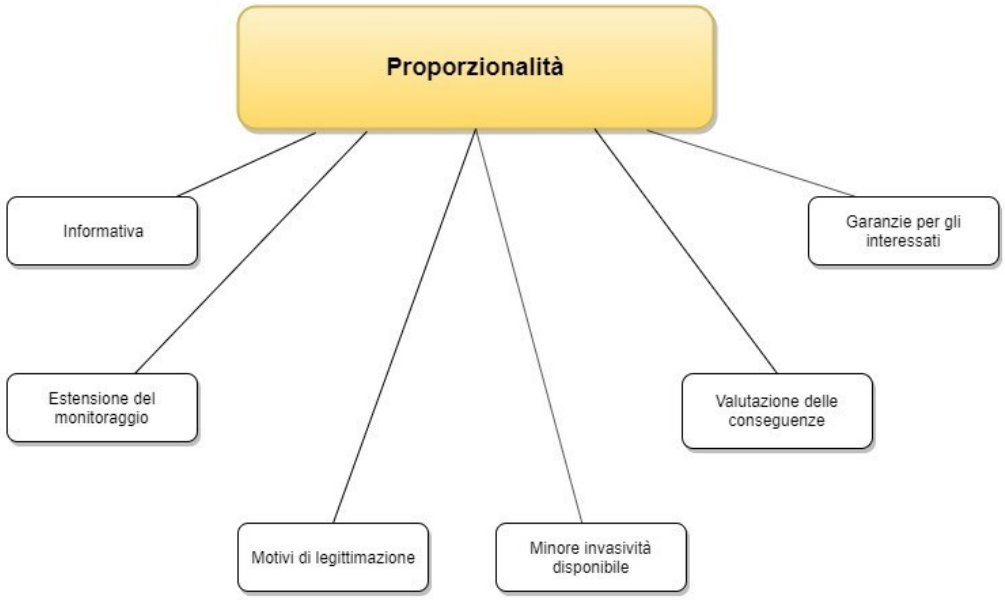
- data protection;
- antitrust;
- consumer protection and;
- intellectual property.

For these reasons, **accountability – understood as a dimension of market trust** – is **achieved** only **through integrated risk management**.

37.
CtEDU e videosorveglianza: chi ruba non è tutelato

Molto clamore ha fatto la sentenza della Corte europea dei diritti umani (CtEDU) – anche grazie alla disinformazione che ne ha formato oggetto – la quale ha ritenuto non violare l'articolo 8 della Convenzione (Convenzione Europea sui Diritti Umani – CEDU), l'installazione di telecamere occulte sul luogo di lavoro per scoprire i responsabili di furti presso le casse di un supermercato. In ambito italiano, la circostanza è nota come "controllo difensivo" ed è considerata legittima – nel rispetto dei principi di proporzionalità e necessità – da costante giurisprudenza di merito e di legittimità. Per un approfondimento vedi la sezione "Controlli a distanza" sul DPtel.

VIDEOSORVEGLIANZA
Criteri determinativi della proporzionalità



CtEDU e CEDU

La CtEDU è il tribunale internazionale di Strasburgo che decide in merito alla corretta applicazione ed interpretazione dei diritti contenuti nella Convenzione Europea dei Diritti dell'Uomo (CEDU).

Articolo 8 - Rispetto della vita privata

Nella circostanza qui commentata (caso Lopez Ribalda e altri contro Spagna, n. 1874/13 e 8567/13), il caso concreto veniva valutato in merito ad una possibile violazione dell'articolo 8 della CEDU che sancisce il rispetto della vita privata («*1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.*»).

Nozione di "vita privata"

La Grande Camera ha ribadito che il **concetto di "vita privata" è un termine generico non suscettibile di una definizione esaustiva**.

- **Copre l'integrità fisica e psicologica** di una persona. Può quindi abbracciare molteplici aspetti dell'identità fisica e sociale della persona (vedi, come esempio recente, Denisov v. Ukraine [GC], n. 76639/11, § 95, 25 settembre 2018).
- Si estende in particolare agli **aspetti relativi all'identità personale**, come il nome o l'immagine di una persona (vedi Schüssel v. Austria (dec.), N. 42409/98, 21 febbraio 2002 e Von Hannover v. Germania (n. 2) [GC], nn. 40660/08 e 60641/08, § 95, CEDU 2012).
- Il concetto di vita privata non si limita a un "cerchio interno" in cui l'individuo può vivere la propria vita personale senza interferenze esterne, ma comprende anche **il diritto di condurre una "vita sociale privata"**, cioè la possibilità di **stabilire e sviluppare relazioni con gli altri e il mondo esterno** (vedi Bărbulescu v. Romania [GC], n. 61496/08, § 70, 5 settembre 2017).
- **Non esclude le attività professionali** a tale proposito (vedi Fernández Martínez contro Spagna [GC], n. 56030/07, § 110, CEDU 2014 (estratti); Köpke contro Germania (dicembre), n. 420/07, 5 ottobre 2010; Bărbulescu, citata sopra, § 71; Antović e Mirković v. Montenegro, n. 70838/13, § 42, 28 novembre 2017; e Denisov, citata sopra, § 100) o **attività che si svolgono in un contesto pubblico** (vedi Von Hannover (n. 2), citata sopra, § 95). Esiste quindi una zona di interazione di una persona con gli altri, anche in un contesto pubblico, che può rientrare nell'ambito di "vita privata" (vedi PG e JH c. Regno Unito, n. 44787/98, § 56, CEDU 2001-IX; Perry c. Regno Unito, n. 63737/00, § 36, CEDU 2003-IX (estratti); e Von Hannover (n. 2), citata sopra, § 95).

Secondo i precedenti del CtEDU l'articolo 8 trova quindi applicazione anche sul luogo di lavoro e in spazi aperti al pubblico, come nel caso di specie: l'ambito di una cassa per pagamenti di un supermercato.

Gradazione dell'aspettativa di riservatezza

La CtEDU con la sentenza del 17 ottobre 2019, ha ribadito che l'aspettativa di riservatezza è elevata nelle aree di lavoro chiuse come gli uffici e può divenire ancora più alta in luoghi di natura privata, come servizi igienici o guardaroba, dove è giustificata una maggiore protezione, tale da indurre ad un divieto assoluto di videosorveglianza, salvo ipotesi eccezionali.

La stessa aspettativa, invece, è «*manifestamente inferiore in luoghi che sono visibili o accessibili ai colleghi o, come nel caso dei ricorrenti, al pubblico in generale*».

Fatti

A seguito di ammanchi di cassa e furti di altro genere desunti da incoerenze tra il livello delle scorte e le cifre delle vendite, il gestore di un supermercato decide di installare una serie di telecamere, alcune visibili ed oggetto di regolare informativa, altre nascoste, che riprendevano l'area delle casse.

Le telecamere occulte sono rimaste in funzione per 10 giorni ed hanno consentito di scoprire i responsabili dei furti (cassieri ed assistenti alle vendite che aiutavano i clienti o altri dipendenti del supermercato a rubare beni e rubare loro stessi beni) e di ottenere le prove da utilizzare in

procedimenti disciplinari nei loro confronti. Secondo il datore di lavoro, questi atti costituivano una grave violazione degli obblighi di buona fede e fedeltà richiesti nel rapporto di lavoro e giustificavano la risoluzione del contratto con effetto immediato.

Impugnative

Alcuni dipendenti coinvolti hanno impugnato il licenziamento ritenendolo ingiusto contestando in particolare l'uso della videosorveglianza nascosta che avrebbe violato il diritto alla protezione della loro privacy. I ricorrenti hanno chiesto che le registrazioni ottenute con tali mezzi non dovessero essere ammesse come prove nel procedimento.

Il giudice del lavoro spagnolo ha ritenuto legittima l'installazione e l'uso di tali telecamere avendo valutato che le modalità seguite operassero un adeguato bilanciamento tra i contrapposti diritti dei lavoratori, alla propria riservatezza sul luogo di lavoro, e del datore alla tutela del patrimonio aziendale. Successivamente, gli interessati hanno proposto appello all'Alta Corte della Catalogna, alla Corte Suprema ed alla Corte Costituzionale, ottenendo sempre il rigetto delle rispettive azioni.

Prima decisione della Camera CtEDU

In precedenza, con una decisione del 9 gennaio 2018, una Camera della CtEDU aveva ritenuto che il comportamento del datore di lavoro avesse violato l'articolo 8 della Convenzione (in particolare, in quanto i diritti del datore di lavoro avrebbero potuto essere garantiti informando i ricorrenti, anche in modo generale, dell'installazione di un sistema di videosorveglianza) per cui, nel maggio dello stesso anno, il governo spagnolo aveva chiesto che la questione fosse portata all'attenzione del Gran Camera della CtEDU (art. 43, CEDU), come avvenne per il precedente caso Barbulescu, commentato nell'Editoriale del 21 settembre 2017.

La Grande Camera ha ribaltato il giudizio precedente, ritenendo che l'installazione ed uso delle telecamere occulte, in questa circostanza non abbia violato l'articolo 8 CEDU per le ragioni indicate di seguito.

Criteri di valutazione della proporzionalità

La Grante Camera ritiene che i principi stabiliti nella sentenza Bărbulescu, che riguardava fatti simili a quelli qui considerati, sono trasponibili alle circostanze in cui un datore di lavoro può attuare misure di videosorveglianza sul posto di lavoro.

«*In tale contesto, al fine di garantire la proporzionalità delle misure di videosorveglianza sul luogo di lavoro, i tribunali nazionali dovrebbero tener conto dei seguenti fattori quando valutano i vari interessi in conflitto*»:

1. **Informativa** - Se il dipendente è stato informato della possibilità di adottare misure di videosorveglianza da parte del datore di lavoro e dell'attuazione di tali misure.
2. **Estensione del monitoraggio** - L'entità del monitoraggio da parte del datore di lavoro e il grado di intrusione nella privacy del dipendente (area monitorata, limitazioni nel tempo e nello spazio, numero di persone che hanno accesso alle immagini).
3. **Motivi di legittimazione** - Se il datore di lavoro ha fornito motivi legittimi per giustificare il controllo e la sua portata (ad esempio, il ragionevole sospetto della commissione di gravi violazioni).
4. **Minore invasività disponibile** - Se sarebbe stato possibile istituire un sistema di monitoraggio basato su metodi e misure meno invadenti.

5. **Valutazione delle conseguenze** - Le conseguenze del monitoraggio per il dipendente ad esso soggetto.
6. **Garanzie per gli interessati** - Se al dipendente sono state fornite garanzie adeguate, in particolare laddove le operazioni di monitoraggio del datore di lavoro siano di natura intrusiva (ad es. mediante informazioni a dipendenti o rappresentanti dei lavoratori per quanto riguarda l'installazione e l'estensione del monitoraggio, la possibilità di presentare un reclamo).

Giudice del lavoro spagnolo

La Grande Camera ha valutato come ragionevole il giudizio di bilanciamento degli interessi in gioco operato dal giudice del lavoro spagnolo, il quale si è basato sui seguenti assunti:

- l'installazione della videosorveglianza era stata giustificata da motivi legittimi, vale a dire il fondato sospetto che fossero stati commessi furti;
- l'obiettivo legittimo perseguito dal datore di lavoro non avrebbe potuto essere conseguito con misure meno invasive per i diritti dei ricorrenti;
- l'estensione del monitoraggio era stata limitata alle aree interessate dagli ammanchi e al relativo personale (limitazione in spazio);
- la sua durata (10 giorni) non aveva superato quanto necessario per confermare i sospetti di furto (limitazione in tempo);
- limitato accesso alle immagini contestate, in quanto solo il gestore del supermercato, il rappresentante legale della società e il rappresentante sindacale avevano visto le registrazioni ottenute, prima di informare gli interessati;
- la videosorveglianza e le registrazioni erano state utilizzate dal datore di lavoro al solo scopo di individuare i responsabili delle perdite registrate di beni, di disporre di prove adeguate e di adottare misure disciplinari nei loro confronti.

Informativa agli interessati

La Grande Camera ha ribadito che Il requisito della trasparenza e il conseguente diritto degli interessati all'informazione sono di natura fondamentale, in particolare nel contesto dei rapporti di lavoro al fine di evitare qualsiasi abuso. Sebbene, la fornitura di informazioni all'individuo da monitorare e la sua portata costituiscono solo uno dei criteri da prendere in considerazione per valutare la proporzionalità di una misura del tipo di quella in oggetto. Tuttavia, la mancanza di informazioni preliminari può giustificarsi solo in presenza di un requisito imperativo relativo alla tutela di interessi pubblici o privati significativi.

Pertanto, «*l'esistenza di un ragionevole sospetto che siano state commesse gravi condotte illecite e l'entità delle perdite identificate nel caso costituiscono una significativa giustificazione*».

38.
Pubblicate le linee guida sulla necessità contrattuale

Terminata la procedura di consultazione pubblica, nel corso della quattordicesima sessione plenaria, l'EDPB ha approvato la versione finale delle «linee guida 2/2019 sul trattamento dei dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del GDPR nel contesto della fornitura di servizi online agli interessati».

Sintesi

Fig. 1 - Le basi giuridiche dell'articolo 6 del GDPR.

Versione finale delle linee guida 2/2019

La versione 2.0 dell'8 ottobre 2019 differisce solo per limitati aspetti formali dalla precedente versione 1.0 del 9/4/2019, sottoposta a consultazione pubblica; pertanto, rimangono validi i commenti oggetto della precedente puntata dell'Editoriale del 2 maggio 2019, cui si rinvia; in questa sede ci soffermeremo su aspetti non affrontati nella precedente tornata.

Principi e basi giuridiche

La base giuridica, come la necessità contrattuale qui esaminata, è una condizione di legittimità del trattamento di dati personali che declina il principio del trattamento lecito [art. 5(1)(a) GDPR]. L'individuazione della base giuridica è operazione fondamentale ma non sufficiente; essa deve essere considerata nel contesto complessivo del GDPR, all'interno della cornice degli obiettivi di tutela della riservatezza e della protezione dei dati personali [art. 1(2)] e «*accanto all'obbligo del titolare del trattamento di trattare i dati personali in conformità con i principi di protezione dei dati ai sensi dell'articolo 5*» tra cui si annoverano la limitazione delle finalità e gli obblighi di minimizzazione dei dati, oltre a quelli di correttezza e trasparenza.
Nel rispetto del principio di liceità, il titolare dovrà conformarsi anche a discipline appartenenti ad altri domini, come quello della legge sui contratti e della protezione dei consumatori;

analogamente, in attuazione del principio di correttezza, egli dovrà riconoscere le «*ragionevoli aspettative degli interessati, considerando le possibili conseguenze negative che il trattamento può avere su di loro e tenendo conto della relazione e dei potenziali effetti di uno squilibrio tra loro e il titolare del trattamento*».
Secondo il principio di trasparenza, il titolare dovrà fornire un'adeguata informativa, comprensiva dei profili indicati negli articoli 13 e 14 del GDPR, anche quando la base giuridica sarà individuata nella necessità contrattuale.
In merito ai rapporti tra principi e basi giuridiche si veda anche quanto indicato nell'Editoriale del 30 maggio 2019. Sui principi di liceità si veda la sezione "Principi" del DPtel.

Libertà di impresa

La base giuridica della necessità contrattuale – che legittima il trattamento di dati personali necessario per dare esecuzione ad un contratto di cui è parte l'interessato – è diretta espressione del diritto fondamentale della libertà di impresa, garantito

- dall'articolo 16 della **Carta di Nizza**;
- dall'articolo 41 della **Costituzione italiana**.

Secondo la Carta dei diritti fondamentali dell'UE «*È riconosciuta la libertà d'impresa, conformemente al diritto comunitario e alle legislazioni e prassi nazionali*»; mentre la costituzione italiana ai primi due capoversi dell'articolo 41 così recita «*L'iniziativa economica privata è libera.*
Non puo` svolgersi in contrasto con l'utilita` sociale o in modo da recare danno alla sicurezza, alla liberta`, alla dignita` umana.»
Una prima considerazione desumibile dal diritto di libertà d'impresa, pertanto, è che il trattamento di dati personali necessario per consentire transazioni commerciali tra fornitore e interessato, trova la propria legittimazione nel permettere l'esercizio del diritto fondamentale all'iniziativa economica privata. La previsione della base giuridica dell'articolo 6(1)(b) del GDPR rappresenta uno dei numerosi esempi di bilanciamento tra diritto alla protezione dei dati personali e altri diritti fondamentali, laddove il primo indietreggia – senza peraltro annullarsi – entro il limite necessario per permettere all'altro diritto fondamentale di compiersi.

Non regolamentare l'ovvio

Una seconda considerazione che può desumersi dalla previsione della base giuridica della necessità contrattuale è che essa è un'ovvia traslazione dell'autodeterminazione informativa dell'interessato. Più semplicemente, se il trattamento dei dati personali dell'interessato

- è necessario per dare esecuzione ad un contratto che lo stesso interessato ha sottoscritto (in quanto ne è parte);
- oppure è necessario per adottare misure precontrattuali richieste dal medesimo soggetto.

risulta ovvio che il conseguente trattamento di dati si desuma acconsentito dall'interessato grazie al pertinente vincolo di necessità: senza l'uso di quei dati non si potrebbe dare esecuzione a (1) un contratto o (2) a misure precontrattuali che lo stesso interessato esige o richiede.

Consenso inequivocabile

Lo sdoganamento della manifestazione del consenso "privacy" tramite "fatti concludenti" trova ora fondamento nel ricorso all'espressione della "inequivocabilità" contenuta nella definizione del consenso operata dal regolamento: «*qualsiasi manifestazione di volontà libera, specifica, informata e*

inequivocabile *dell'interessato, con la quale lo stesso manifesta il proprio assenso,* ***mediante*** *dichiarazione o* ***azione positiva inequivocabile****, che i dati personali che lo riguardano siano oggetto di trattamento*» [evidenze aggiunte, art. 4, punto 11) GDPR]. La prerogativa che l'inequivocabilità sia supportata da una manifestazione attiva o azione positiva dell'interessato è qui suffragata da:

- **la sottoscrizione del contratto** ad opera dell'interessato, per la cui esecuzione sono necessitati i dati personali della parte firmataria;
- **l'espressa richiesta dell'interessato** nell'adozione delle misure precontrattuali che lo riguardano.

In conclusione, come opportunamente osservato nelle linee guida, «è nell'interesse di entrambe le parti elaborare tali dati, altrimenti il servizio non potrebbe essere fornito e il contratto non potrebbe essere eseguito» (§2).
Riguardo al consenso ed ai suoi requisiti si veda la sezione "Consenso" del DPtel.

Vincolo di necessità

Come già indicato, il vincolo di necessità è condizione essenziale di tutte le basi giuridiche elencate nell'articolo 6 del regolamento, con la sola eccezione di quella del consenso dell'interessato.
In aggiunta a quanto già riportato nell'Editoriale del 2/5/2019, il concetto di "necessità" va interpretato nel senso di offrire piena realizzazione allo scopo del GDPR come delineato all'articolo 1(2): «*Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.*» per cui non può avere un contenuto variabile in funzione degli Stati membri, in quanto si tratta di una nozione autonoma del diritto comunitario [v. CGUE del 16/12/2008, C-524/06 (Heinz Huber v Bundesrepublik Deutschland), par. 52].

Definizione di necessità

Come rilevato dalla Corte europea dei diritti dell'uomo (CtEDU), il concetto di necessità non «*ha la flessibilità di termini quali 'ammissibile', 'ordinaria', 'utile', 'ragionevole' o 'auspicabile' […]*» (CtEDU, 25/3/1983, Silver e altri c. Regno Unito, punto 97). Le linee guida 2/2019 evidenziano in proposito che «*(l)'articolo 6, paragrafo 1, lettera b), non riguarderà il trattamento che è* ***utile*** *ma non obiettivamente necessario per eseguire il servizio contrattuale o per adottare le pertinenti misure precontrattuali su richiesta dell'interessato, anche se è necessario per le altre attività di business del titolare del trattamento*» (evidenza aggiunta, §25). Per queste ragioni non soddisferà le condizioni di questa base giuridica la situazione in cui il trattamento, anzichè essere "necessario", venga «*imposto unilateralmente all'interessato dal titolare del trattamento*».

Previsione del trattamento nel contratto

La mera menzione espressa di attività di trattamento nel contratto non le rende, di per sè solo, "necessarie" all'esecuzione del contratto. Il parere 6/2014 sul legittimo interesse (wp217), emesso dal WPArt29, sottolinea come il "test di necessità" non è superato dalla mera constatazione che alcuni trattamenti siano previsti da clausole contrattuali sebbene non facciano parte dello scopo (oggetto e obiettivo fondamentali) dello stesso. Viene fatto l'esempio della creazione di «*un profilo dei gusti e delle scelte di stile di vita dell'utente sulla base della sequenza di clic che ha effettuato su un sito web e degli articoli che ha acquistato*», laddove l'oggetto del contratto è, invece, la fornitura di beni e servizi particolari. Queste considerazioni fanno emergere l'esistenza di «*un chiaro collegamento tra*

*la **valutazione della necessità** e il rispetto del principio di **limitazione delle finalità***» [art. 5(1)(b) GDPR] in quanto entrambi si valutano ricercando la sostanza e l'obiettivo fondamentale perseguiti.

La fase dell'esecuzione

La prima ipotesi della base giuridica della necessità contrattuale (quella dell'esecuzione del contratto) limita la sua portata alla sola fase esecutiva dello stesso per cui, come rilevato nel citato parere wp217, tale base giuridica «*(n)on si applica a tutte le ulteriori azioni avviate a seguito di inosservanza o a tutti gli altri incidenti intervenuti nell'esecuzione di un contratto*».

Fase di eventuale conflitto

Di conseguenza, mentre il trattamento di dati personali del cliente per l'inoltro di un sollecito di pagamento da parte del fornitore può considerarsi rientrare nella fase esecutiva contrattuale [quindi basata sull'art. 6(1)(b) GDPR] altrettanto non dovrebbe potersi sostenere per ipotesi di conflitto che sfociano o meno in azioni giudiziarie; per queste ultime sarebbe più appropriato fare riferimento alla base giuridica del legittimo interesse del titolare del trattamento, «*subordinatamente al soddisfacimento del test comparativo*» tra interessi del titolare e diritti ed interessi degli interessati [art. 6(1)(f) GDPR] [§ III.2.2. punto i), wp217]. L'esercizio del diritto di difesa, infatti, è previsto esplicitamente dal legislatore solo come eccezione al divieto di trattamento delle speciali categorie di dati e non anche come base giuridica di carattere generale [art. 9(2)(f) GDPR].

Misure precontrattuali su richiesta

La seconda ipotesi rientrante sotto l'ombrello della base giuridica dell'articolo 6(1)(b) è quella delle misure precontrattuali richieste dall'interessato (cioè prima che il contratto sia firmato o concluso): qui l'elemento condizionante per la sussistenza della base giuridica contrattuale è il fatto che tali misure siano **richieste dall'interessato**, anzichè essere attuate su iniziativa del titolare del trattamento.
La condizione della "richiesta da parte dell'interessato" porta ad escludere la possibilità di annoverare in questo ambito quelle attività precontrattuali accessorie, propedeutiche alla conclusione del relativo contratto. Il citato parere wp217 fa gli esempi di:

- «*trattamento dei dati relativi a controlli medici prima che una società di assicurazioni stipuli un'assicurazione sulla salute o un'assicurazione sulla vita con un richiedente*»
- «*verifiche delle informazioni creditizie svolte prima della concessione di un prestito*» [entrambe potenzialmente rientranti nell'ambito delle basi giuridiche dell'interesse legittimo o dell'esecuzione di un obbligo legale, secondo le circostanze del caso, art. 6(1)(f) o 6(1)(c) GDPR]
- invio di «*materiale pubblicitario su iniziativa del rivenditore al dettaglio/titolare del trattamento*», nella quale ipotesi, in via prevalente, occorre prendere in considerazione la base legale del consenso di cui all'articolo 6(1)(a) del regolamento.

39.
Whistleblowing: importanti novità

Novità in materia di whistleblowing; in ottemperanza al disposto della legge 179 del 2017 l'Autorità anticorruzione (ANAC) ha posto in consultazione pubblica le nuove linee guida sul whistleblowing ed è prossima alla pubblicazione della loro versione definitiva. Sul versante dell'Unione europea è in corso di pubblicazione sulla Gazzetta Ufficiale dell'UE la nuova direttiva sul tema. Il Garante privacy, dal suo canto, ha reso noto che tra i profili oggetto di ispezione programmata per il secondo semestre luglio-dicembre 2019 vi è quello relativo alle segnalazioni interne di illeciti. In questa tornata facciamo il punto sull'attuale disciplina rinviando, a futuri interventi su queste colonne, l'esame delle novità indicate, alla luce delle implicazioni di interesse per la protezione dei dati personali.

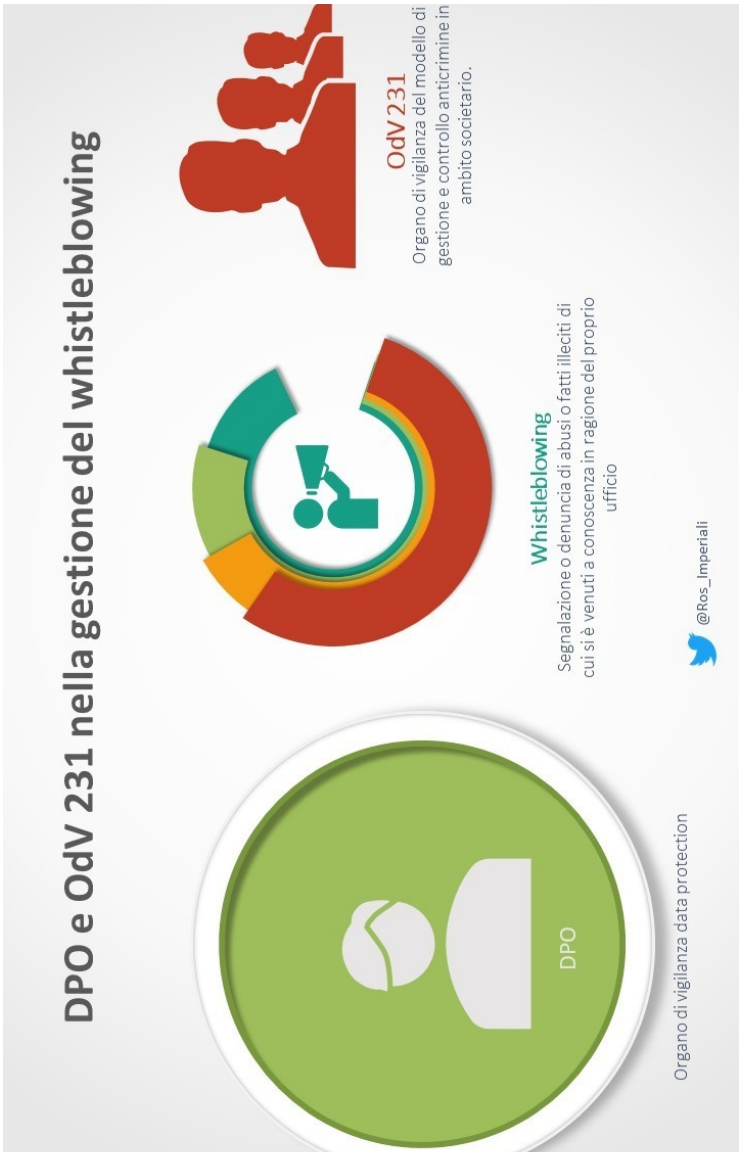


Fig. 1 - Rapporti tra DPO e OdV231 nella gestione del whistleblowing.

La legge 179/2017

Il tema del whistleblowing è stato già affrontato in precedenti puntate come indicato in "Argomenti collegati" in coda a questi commenti.

La tabella seguente riporta in sintesi l'attuale disciplina dettata dalla legge n. 179/2017, presentata tramite la comparazione tra settore pubblico e privato.

Whistleblowing		
Tema	**Settore pubblico**	**Settore privato**
Riferimento modifica norme preesistenti	art. 54-bis dlgs. 165/2001 sostituito integralmente	nuovi commi 2-bis, 2-ter e 2-quater, art. 6, dlgs 231/2001
Soggetto tutelato	inclusi i dipendenti di enti pubblici economici e di enti privati a controllo pubblico, nonchè di fornitori che agiscono per la PA.	coloro che a qualsiasi titolo rappresentino o dirigano l'ente (e coloro che da questi siano sottoposti a direzione o vigilanza).
Ambito della segnalazione	condotte illecite di cui sia venuto a conoscenza	condotte illecite, rilevanti ai sensi del decreto 231/2001 e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente
Oggetto della tutela	Divieto di attività discriminatorie e riservatezza del segnalante	Divieto di attività discriminatorie e riservatezza del segnalante
Inversione dell'onere della prova	spetta all'amministrazione o all'ente l'onere di provare che le misure discriminatorie o ritorsive adottate nei confronti del segnalante sono motivate da ragioni estranee alla segnalazione	è onere del datore di lavoro dimostrare che l'adozione di misure discriminatorie o ritorsive siano estranee alla segnalazione
Obblighi per facilitare la denuncia	Procedure per la presentazione e gestione delle segnalazioni con modalità informatiche e crittografia, secondo le linee guida ANAC	attivazione di canali (almeno uno alternativo con modalità informatiche) che consentano la trasmissione delle segnalazioni stesse a tutela riservatezza del segnalante
Clausola di esclusione della tutela	se accertata la responsabilità penale del segnalante, anche con sentenza di primo grado, per i reati di calunnia o diffamazione o comunque reati commessi con la denuncia del medesimo segnalante ovvero per sua responsabilità civile, nei casi di dolo o colpa grave	sanzioni disciplinari per chi effettua, con dolo o colpa grave, segnalazioni che si rivelino infondate
Limite all'obbligo di non rivelazione della identità del segnalante	tutelata in sede disciplinare, salvo che col consenso del segnalante; estesa anche al procedimento penale (nei limiti del segreto degli atti di indagine) e contabile (fino alla fine della fase istruttoria)	non previsto

Tema	Settore pubblico	Settore privato
Misure a tutela della riservatezza dell'identità del segnalante	le pubbliche amministrazioni sono tenute ad adottare i necessari accorgimenti tecnici a tutela	i canali per le segnalazioni debbono garantire la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione
Destinatari della segnalazione	responsabile della prevenzione della corruzione e trasparenza, o ANAC o autorità giudiziaria	presumibilmente l'OdV
Limiti al diritto di accesso	accesso ai documenti amministrativi della l. 241/1990 e accesso civico	accesso privacy [art. 2-undecies(1)(f) codice privacy]
Sanzioni	l'ANAC applica le seguenti sanzioni amministrative a carico del responsabile: da € 5.000 a 30.000 in caso di attività discriminatorie a danno del segnalante da € 10.000 a 50.000, per assenza o non conformità di procedure di inoltro e gestione delle segnalazioni da € 10.000 a 50.000, per mancato svolgimento di attività di verifica e analisi delle segnalazioni ricevute	sanzioni disciplinari per chi viola le misure di tutela del segnalante e per chi effettua segnalazioni infondate con dolo o colpa grave
Diritti del segnalante licenziato per la segnalazione	reintegra nel posto di lavoro da parte del giudice, al risarcimento del danno subito e al versamento dei contributi previdenziali e assistenziali dovuti dalla data di licenziamento a quella di reintegrazione	nullità del licenziamento ritorsivo o discriminatorio del segnalante, del mutamento di mansioni, di qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante
Scriminante della rivelazione del segreto	la segnalazione o denuncia effettuate nel settore pubblico (art. 54-bis del D.Lgs. 165/2001) o privato (art. 6 del D.Lgs. 231/2001) è giusta causa di rivelazione del segreto d'ufficio (art. 326 c.p.), del segreto professionale (art. 622 c.p.), del segreto scientifico e industriale (art. 623 c.p.) nonché di violazione dell'obbligo di fedeltà all'imprenditore da parte del prestatore di lavoro (art. 2105 c.c.)	la segnalazione o denuncia effettuate nel settore pubblico (art. 54-bis del D.Lgs. 165/2001) o privato (art. 6 del D.Lgs. 231/2001) è giusta causa di rivelazione del segreto d'ufficio (art. 326 c.p.), del segreto professionale (art. 622 c.p.), del segreto scientifico e industriale (art. 623 c.p.) nonché di violazione dell'obbligo di fedeltà all'imprenditore da parte del prestatore di lavoro (art. 2105 c.c.)

La legge 179/2017 in breve

La legge 179 si compone di tre articoli:

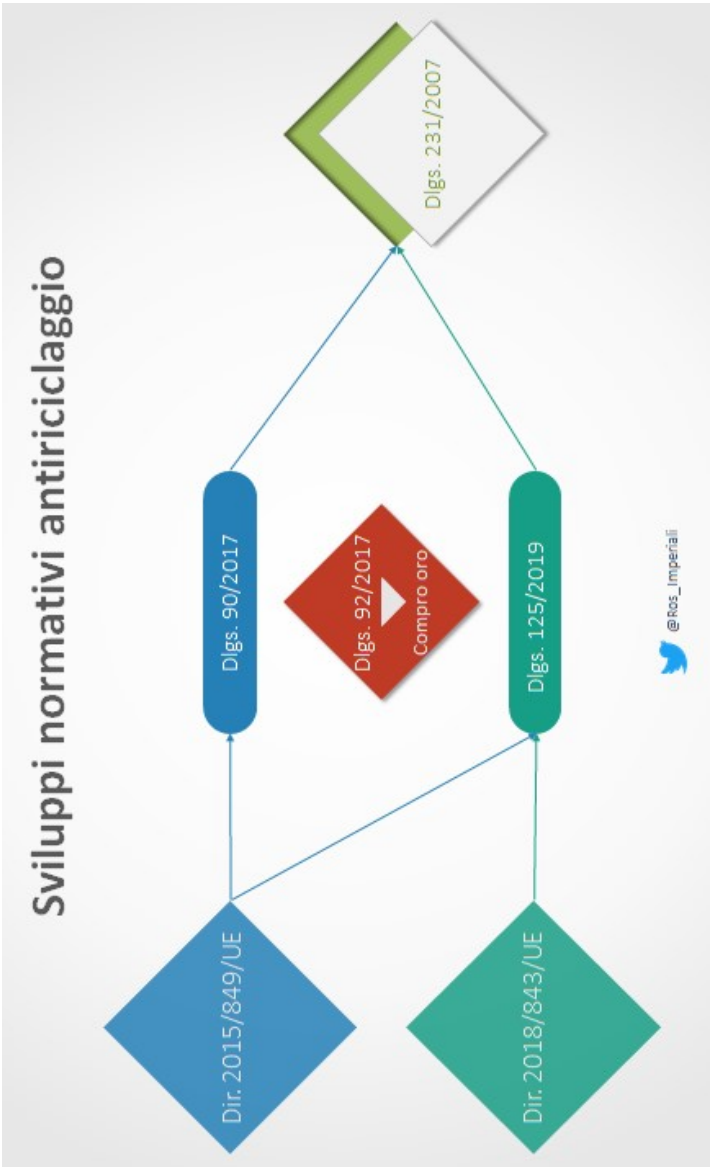
1. Il primo «*Tutela del dipendente pubblico che segnala illeciti*» disciplina la tutela del segnalante nel settore pubblico riscrivendo integralmente l'art. 54-bis del Dlgs. 165/2001.

2. Il secondo «*Tutela del dipendente o collaboratore che segnala illeciti nel settore privato*» introduce, per la prima volta nel nostro ordinamento, la disciplina del whistleblowing nel settore privato, aggiungendo il comma 2-bis all'interno dell'art. 6 del Dlgs. 231/2001, sulla responsabilità amministrativa delle persone giuridiche per i reati commessi da propri dipendenti o collaboratori.
3. Il terzo «*Integrazione della disciplina dell'obbligo di segreto d'ufficio, aziendale, professionale, scientifico e industriale*» contiene una disposizione comune alle segnalazioni effettuate sia nel settore pubblico sia nel settore privato di esonero dalla responsabilità nel caso il segnalante – tramite l'attività di whistleblowing – riveli un segreto d'ufficio, aziendale, professionale, scientifico o industriale o violi il dovere di lealtà e fedeltà (art. 2015 c.c.).

40.
Decreto di recepimento della V Direttiva antiriciclaggio - Prima parte

Il decreto legislativo n. 125 del 2019 ha dato attuazione alla V direttiva antiriciclaggio ed è entrato in vigore il 10 novembre 2019.
Esso contiene ampliamenti richiesti dalla citata direttiva – soprattutto con riferimento ai pagamenti in forma anonima e alle nuove forme di pagamento – e correttivi imposti dalla procedura di infrazione contro l'Italia per l'incompleto recepimento della IV direttiva; ampliamenti e correttivi che vengono inseriti nel nostro ordinamento giuridico, in particolare, integrando e modificando il noto Dlgs. 231 del 2007.

Sintesi



Il decreto legislativo 4 ottobre 2019, n. 125 è stato pubblicato sulla Gazzetta ufficiale n. 252 del 26/10/2019, cui sono seguiti due errata corrige.
Questo decreto recepisce nel nostro ordinamento la V direttiva antiriciclaggio e opera quei correttivi richiesti dalla Commissione europea nel corso della procedura di infrazione contro il nostro Paese per il non completo recepimento della precedente IV direttiva del 2015 sullo stesso tema.
La V direttiva, diversamente dalla IV, viene recepita in corso di piena applicazione del Regolamento privacy, per cui l'attuale disciplina nazionale di recepimento, che già in precedenza mostrava numerosi punti di contatto con quella della protezione dei dati personali, solleva ulteriori interrogativi di corretto bilanciamento tra i due settori.

Precedenti

In materia di contrasto del riciclaggio di danaro di illecita provenienza, sono state emanate – in successione – numerose direttive: da ultimo la direttiva 2015/849/UE (detta IV direttiva) recepita col decreto legislativo n. 90 del 2017 e la 2018/843/UE (del 30 maggio 2018, detta V direttiva) recepita col Dlgs. n. 125/2019 oggetto di questa puntata.

Obblighi antiriciclaggio

L'obiettivo fondamentale della disciplina è la tracciabilità dei flussi finanziari e, a tal fine, sono previsti obblighi (ed eventuali sanzioni con particolare riguardo a violazioni dell'obbligo di adeguata verifica della clientela, di conservazione dei documenti, di segnalazione di operazioni sospette e di controlli interni) a carico di operatori qualificati.
La principale prescrizione, cui i cosiddetti "soggetti obbligati" sono tenuti a ottemperare, è la segnalazione delle operazioni sospette, vale a dire le transazioni a contenuto finanziario che, in base a determinati indicatori prestabiliti, inducano a far ritenere che costituiscano modalità di riciclo o di reimpiego.

Ambito soggettivo

La platea dei soggetti obbligati comprende numerose categorie di titolari (operatori finanziari, revisori legali, liberi professionisti, pubbliche amministrazioni, ecc.) cui si aggiungono, da ultimo, i prestatori di servizi di cambio tra valute virtuali e valute legali, i prestatori di servizi di portafoglio digitale, i soggetti che commerciano opere d'arte o che agiscono in qualità di intermediari.

UIF

L'Unità di Informazione Finanziaria è l'autorità centrale antiriciclaggio, subentrata all'Ufficio Italiano Cambi (UIC), è stata istituita dal Dlgs. 231/2007 ed ha iniziato ad operare nel 2008, in posizione di indipendenza e autonomia funzionale, presso la Banca d'Italia.
L'articolo 13-bis di nuovo conio, che il decreto legislativo n. 125/2019 ha inserito nel Dlgs. 231/2007, nel disciplinare la cooperazione dell'UIF con le Unità di altri Paesi (Financial Intelligence Unit – FIU) sembra non essere del tutto conforme al GDPR – come evidenziato dallo stesso Garante nel parere rilasciato (v. in seguito) – per alcuni profili come:

- la disciplina del trattamento da parte UIF per finalità ulteriori rispetto a quelle per le quali le informazioni sono fornite dalle FIU, previo consenso di queste ultime, in quanto non in

linea col principio di limitazione della finalità [art. 5, par. 1, lett. b) del GDPR];
- la mancata adozione di regole specifiche per l'utilizzo di canali protetti di comunicazione, in ottemperanza al principio di integrità e riservatezza e all'obbligo di garantire un livello di sicurezza adeguato al rischio [artt. 5, par. 1, lett. f), e 32 del GDPR].

Attività consultiva del Garante

Il Garante ha reso a suo tempo parere sullo schema di decreto legislativo con il quale è stato effettuato il primo recepimento della direttiva (UE) 2015/849 (parere n. 125 del 9 marzo 2017, doc. web n. 6124534).
Successivamente, l'Autorità ha rilasciato il parere in merito allo schema del decreto legislativo n. 125/2019 (parere n. 150 del 24 luglio 2019, doc. web n. 9126288).

Antiriciclaggio e data protection

La necessità di incentivare la segnalazione di operazioni sospette, si tutelare i segnalanti e il contenuto delle segnalazioni, di individuare i soggetti coinvolti, di identificare i titolari effettivi pone la disciplina dell'antiriciclaggio in stretto collegamento con quella della protezione dei dati personali.
La direttiva (UE) 2015/849, al riguardo, pone l'accento sulla necessità di rispettare i diritti fondamentali delle persone e i princìpi riconosciuti, in particolare, dalla Carta dei diritti fondamentali dell'Unione europea, il cui articolo 8 garantisce ad ogni individuo il diritto alla protezione dei dati personali che lo riguardano (considerando 43).
Anche la direttiva (UE) 2018/843 richiama il rispetto dell'attuale quadro giuridico dell'Unione in materia di protezione dei dati, con particolare riferimento al Regolamento (UE) 2016/679 (considerando 38 e 40).

Disciplina dei dati personali per finalità antiriciclaggio

Il Dlgs. 231/2007 riporta la clausola generale di rispetto del Codice e impone ai soggetti obbligati di assicurare «*che il trattamento dei dati acquisiti nell'adempimento degli obblighi di cui al presente decreto avvenga, per i soli scopi e per le attività da esso previsti e nel rispetto delle prescrizioni e delle garanzie stabilite dal Codice in materia di protezione dei dati personali*» [art. 3(9)].

GDPR e antiriciclaggio

Il Regolamento (UE) 2016/679, in via speculare, tiene conto della disciplina antiriciclaggio in quanto annovera fra gli «*obiettivi di interesse pubblico generale… di uno Stato membro… un rilevante interesse economico o finanziario… anche in materia monetaria, di bilancio e tributaria*», la cui salvaguardia consente limitazioni ai diritti degli interessati (art. 23, par. 1, lett. e), Reg.).

Base giuridica per le autorità di vigilanza

La direttiva (UE) 2015/849 – la quale espressamente assoggetta il trattamento dei dati personali per finalità di antiriciclaggio alla direttiva 95/46/CE (art. 41 e considerando 41 e 42) – sottolinea che tale trattamento, ai fini della disciplina sulla protezione dei dati personali, trova la propria base giuridica nell'interesse pubblico rilevante da parte di tutti gli Stati membri (art. 43).
Per corrispondere a tale disposizione e ad una precisa richiesta della Commissione europea,

il Dlgs 125/2019 esplicita che il trattamento dei dati personali per finalità di antiriciclaggio è considerato di interesse pubblico nell'ambito delle garanzie previste dal Regolamento (UE) 2016/679 [art. 1(1)(i)]. Pertanto, i trattamenti di dati personali effettuati dalle autorità di vigilanza di settore – mediante l'attribuzione di un profilo di rischio ai soggetti obbligati, anche persone fisiche, per determinare la frequenza e l'intensità dei controlli – si fondano sulla base giuridica della necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri [art. 6(1)(e) del GDPR].

Base giuridica per i soggetti obbligati

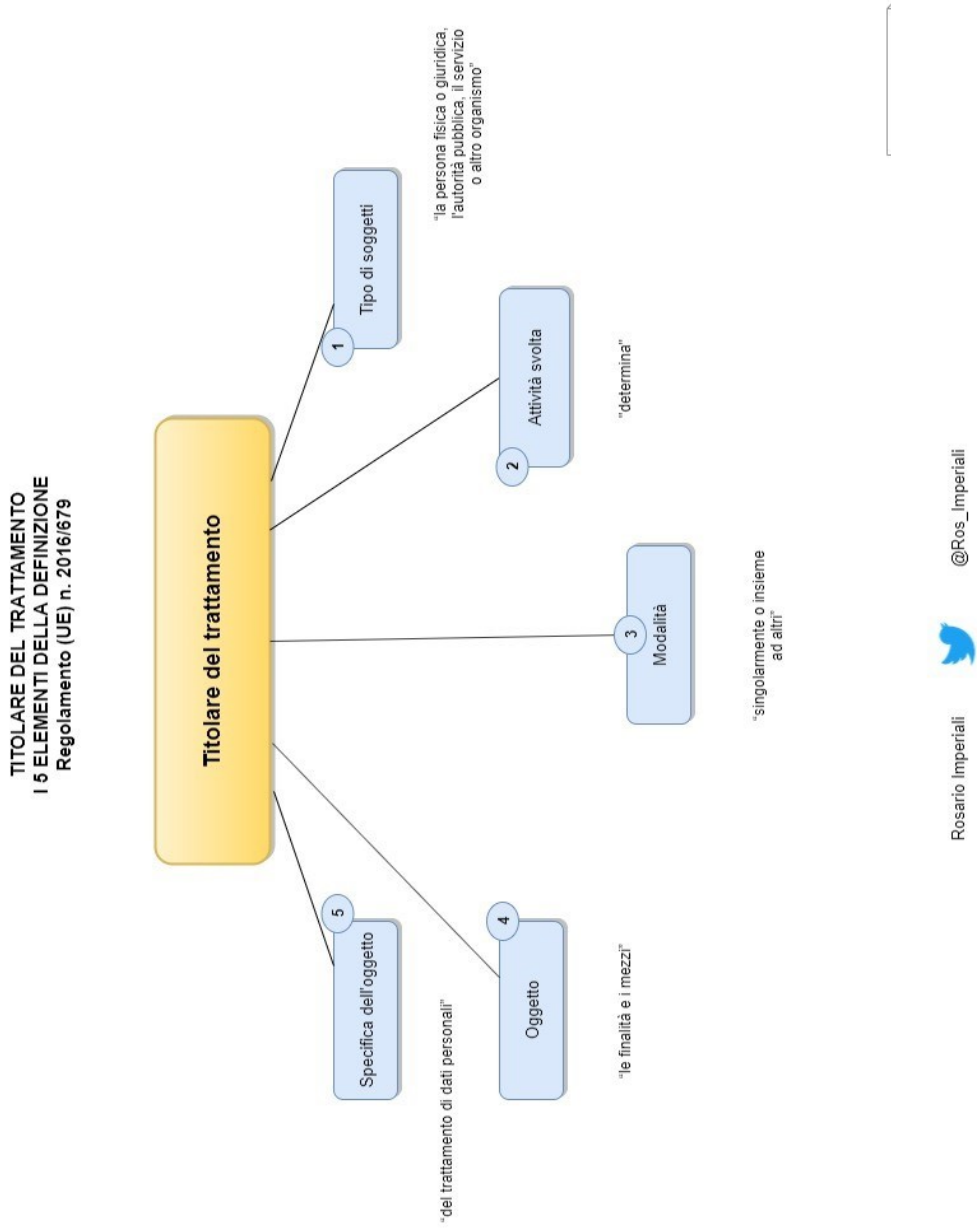
I soggetti obbligati, tenuti a effettuare l'adeguata verifica della propria clientela, sono titolari del trattamento dei pertinenti dati personali per finalità di antiriciclaggio.
L'attività svolta dai soggetti obbligati trova la propria base giuridica nella necessità di adempiere ad un obbligo legale [art. 6(1)(c) GDPR] che si fonda sul diritto dell'Unione e dello Stato membro cui è soggetto il titolare [art. 6(3) GDPR].

Bilanciamento di interessi

Per entrambi i trattamenti delle autorità di vigilanza e per i soggetti obbligati, il GDPR, nel rispetto del principio di liceità del trattamento, impone al legislatore di contemperare l'interesse pubblico del contrasto al riciclaggio o al finanziamento del terrorismo, col diritto alla protezione dei dati [art. 6(3) GDPR].
Il Regolamento prevede che la base giuridica dovrebbe anche «*contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i periodi di conservazione e le operazioni e procedure di trattamento, comprese le misure atte a garantire un trattamento lecito e corretto*».
Di questo specifico bilanciamento – declinato al paragrafo 3 dell'articolo 6 del Regolamento in cui si ricorda che l'obiettivo dell'interesse pubblico deve essere proporzionato all'obiettivo legittimo perseguito – non sembra trovarsi traccia nei decreti attuativi delle direttive europee di settore, incluso il Dlgs 125/2019.

41.
EDPS: linee guida su titolare, contitolare e responsabile

Il 7 novembre 2019 l'European Data Protection Supervisor ("EDPS") ha pubblicato le "Linee guida sui concetti di titolare, contitolare e responsabile in base al Regolamento (UE) 2018/1725. In questa sede affrontiamo i chiarimenti espressi per la figura del titolare del trattamento.



EDPS e Regolamento 2018/1725

L'EDPS è il supervisore europeo che svolge attività di vigilanza, controllo e sanzionatoria – parallelamente a quanto in carico alle autorità di supervisione nazionali ("ASN") per i soggetti pubblici e privati degli Stati membri – riguardo al trattamento di dati personali operato dalle istituzioni comunitarie. Analogamente all'ambito di applicazione del GDPR, il regolamento 2018/1725 disciplina il trattamento di dati personali nel contesto delle istituzioni ed altri organi o agenzie dell'Unione. Si veda, in proposito, l'Alert del 29 novembre 2018.

Linee guida su titolare, contitolare e responsabile

Ancorchè l'ambito applicativo di queste linee guida è differente da quello del GDPR, la stretta corrispondenza tra le due fonti normative (GDPR e regolamento 2018/1725), entrambe incardinate nel diritto dell'Unione, permette di cogliere interessanti spunti ed esempi da questo documento, che risultano utili anche nel più specifico contesto del GDPR.

Sul tema della individuazione e distinzione dei ruoli di titolare, contitolare e responsabile si rinvia alle puntate dell'Editoriale pubblicate tra la fine del 2018 e l'inizio del 2019, rintracciabili mediante i collegamenti in fondo pagina. In questa tornata forniremo una lettura del documento in ottica applicativa GDPR.

Ruolo del titolare

Il GDPR ha come principale interlocutore il titolare del trattamento; al titolare spetta adempiere alla stragrande maggioranza delle prescrizioni contenute nel regolamento con il parallelo dovere di darne testimonianza (**accountability**). Pertanto, eventuali danni causati dal trattamento di dati personali dovranno essere risarciti *in toto*, cioè quelli sia materiali sia immateriali, in primo luogo dal titolare (art. 82 GDPR).

E' responsabilità del titolare dare attuazione pratica al potere di controllo degli interessati sui propri dati, mediante l'esercizio dei diritti privacy previsti dagli articoli da 15 a 22.

5 elementi della definizione di titolare

Le linee guida dell'EDPS evidenziano come il concetto di titolare del trattamento si costruisca attraverso cinque distinti elementi:

1. il **tipo di soggetti** ("la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo");
2. l'**attività svolta** ("determina");
3. la **modalità** ("singolarmente o insieme ad altri");
4. l'**oggetto** ("le finalità e i mezzi");
5. la **specifica dell'oggetto** ("del trattamento di dati personali").

1. Tipo di soggetti

Le categorie soggettive indicate dal legislatore danno indicazione di un'accezione di "titolare" di **ampia portata**, volta a garantire agli interessati una protezione efficace e completa evitando qualsiasi possibile mancanza di responsabilità, come ribadito dalla giurisprudenza più recente della CGUE (Causa C-131/12, Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González cpv. 34. Vedi anche causa C-210/16

Wirtschaftskademie Schleswig-Holstein par. 27-28 e causa C-25/17 Jehovan todistajat par. 66). Titolare è, infatti, «*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo*» [art. 4, punto 7), GDPR]; da tale definizione emerge che la natura giuridica del soggetto è irrilevante ai fini della individuazione del ruolo di titolare.

2. Attività svolta

Il titolare è colui che "determina", cioè che **esercita un'influenza effettiva** sulle operazioni di trattamento mediante l'**esercizio di un potere decisionale**.
Questo potere dispositivo può derivare:

- **direttamente dalla legge**, che espressamente assegna il ruolo di titolare ad un determinato soggetto;
- **indirettamente dalla legge**, se a una parte viene assegnato dalla legge un compito specifico che le richiede necessariamente di svolgere determinati compiti che implicano il trattamento di dati personali, il ruolo del titolare del trattamento risulta in definitiva da tali compiti e doveri assegnati dalla norma a quella parte;
- **valutando le circostanze di fatto** in cui l'entità opera, nel contesto di una specifica operazione di trattamento.

3. Modalità

La definizione di titolare contenuta nel GDPR [art. 4, p.7)], identifica la possibilità che il potere di determinazione sia esercitato «***singolarmente o insieme ad altri***», cioè da più di un attore. Di conseguenza, e come confermato dalla CGUE, ciascuno degli attori coinvolti, in qualità di titolari congiunti o contitolari, ha obblighi ai sensi della legge sulla protezione dei dati.

4. Oggetto

Ulteriore elemento della definizione riguarda l'oggetto dell'influenza del titolare del trattamento, vale a dire la determinazione delle **finalità** (cioè del "**perché**") e dei **mezzi** (cioè del "**come**") di un'operazione di trattamento.

Finalità e mezzi

Come già indicato nel parere 1/2010 wp169 del WPArt29, sebbene finalità e mezzi sono strettamente collegati, non è necessario che una parte determini allo stesso modo entrambi; in linea generale, è la determinazione dello scopo – vale a dire "a cosa serve" un determinato trattamento – a qualificare l'attore come titolare del trattamento.
Per quanto riguarda la determinazione dei mezzi, in particolare alle misure tecniche e organizzative messe in atto durante l'esecuzione di una specifica operazione di trattamento, il livello di dettaglio potrà dipendere dal contesto in cui si svolge il trattamento.

Mezzi

La determinazione dei mezzi da utilizzare implica il ruolo di titolare solo se la parte
decide in merito agli elementi essenziali dei mezzi: secondo il parere wp169, esempi di tali "**elementi essenziali dei mezzi**" comprendono:

- il tipo o i tipi di dati da elaborare;
- il periodo per il quale verrebbero conservati;
- da quali interessati verrebbero raccolti;
- chi avrà accesso ai dati (elenchi di controllo degli accessi, profili utente ecc.) ;
- i destinatari di dati ecc.;
- che di solito sono riservati alla determinazione del titolare del trattamento.

Di converso, identificare **i mezzi non essenziali** delle operazioni di trattamento, come il software da utilizzare o le misure tecniche e organizzative che potrebbero dover essere messe in atto, può essere demandato a terzi responsabili del trattamento che assistono il titolare nel rispetto dei propri obblighi.

Titolare è solo chi accede ai dati personali?

Il materiale **accesso ai dati personali non influisce sulla individuazione della titolarità**, in quanto è sufficiente la constatazione dell'effettiva influenza esercitata sul trattamento, determinandone gli scopi e i mezzi, causando il suo avvio e la possibilità di interromperlo; pertanto, ben può risultare titolare del trattamento (in presenza dei citati presupposti di legge) l'organizzazione che si limita all'eventuale ricezione di statistiche anonime basate sui dati personali raccolti e trattati da un'altra entità.

Questa situazione talvolta si verifica nella gestione di campagne pubblicitarie, laddove l'organizzazione commissiona ad un'agenzia pubblicitaria una determinata campagna – semmai su cluster di dati personali forniti dalla stessa agenzia – limitandosi a richiedere al termine della campagna, statistiche anonime sull'attività svolta.

5. Specifica dell'oggetto

Il potere decisionale del titolare deve essere esercitato su un **trattamento di dati personali**, inteso come «*qualsiasi operazione o insieme di operazioni (...) applicate a dati personali o insiemi di dati personali*». In pratica, le operazioni di trattamento sono raggruppate, secondo un certo margine di apprezzamento del titolare, in serie di operazioni che hanno uno scopo definito e da questi determinato.

L'esercizio del controllo da parte di un titolare può applicarsi all'intero trattamento, ma può anche essere limitato a specifiche operazioni che lo compongono.

Questa operazione ha un risvolto pratico nella impostazione del **registro dei trattamenti**, allorquando spetterà al titolare (in questo caso, obbligazione estesa anche al responsabile per quanto di competenza) stabilire la granularità dei trattamenti da censire nel registro, secondo il livello di impatto e le conseguenti implicazioni che ne derivano.

Lista di controllo della titolarità

Le linee guida dell'EDPS riportano, in conclusione, una lista di controllo che aiuta a individuare gli elementi principali dai quali può desumersi la titolarità: se la maggior parte delle risposte alle dichiarazioni è SÌ, è probabile che l'organizzazione di riferimento sia titolare del relativo trattamento.

Hai deciso di elaborare i dati personali o hai causato il trattamento di un'altra entità.	Sì	No
Hai deciso quale scopo o risultato deve avere l'operazione di trattamento.		
Hai deciso gli elementi essenziali del trattamento, ovvero quali dati personali dovrebbero essere raccolti, su quali soggetti, il periodo di conservazione dei dati, chi ha accesso ai dati, i destinatari ecc.		
Gli interessati delle operazioni di trattamento sono i tuoi dipendenti.		
Eserciti un giudizio professionale sul trattamento dei dati personali.		
Hai una relazione diretta con gli interessati.		
Hai autonomia e indipendenza sul modo in cui i dati personali vengono elaborati		
È stato nominato un responsabile del trattamento per lo svolgimento di attività di elaborazione per tuo conto, anche se l'azienda scelta a tale scopo eventualmente implementa specifici mezzi tecnici e organizzativi (elementi non essenziali).		

Tabella degli indicatori di titolarità del trattamento di dati personali.

42.
EDPB - Linee guida 3/2018, «criterio dello stabilimento»

Dopo circa un anno dalla pubblicazione della prima versione sottoposta a consultazione pubblica, nella quindicesima riunione plenaria l'EDPB ha approvato e rilasciato la versione finale delle linee guida 3/2018 sull'ambito territoriale del GDPR (articolo 3). Il tempo trascorso, alquanto anomalo riguardo al processo di pubblicazione delle linee guida del Comitato europeo, denota sia la complessità della materia affrontata sia, probabilmente, la difficoltà di pervenire ad una posizione condivisa tra tutte le autorità di supervisione nazionali (ASN) riunite all'interno dell'EDPB.
In questa tornata affrontiamo gli aspetti relativi al primo dei criteri che perimetrano l'ambito territoriale del GDPR: il cosiddetto "criterio dello stabilimento"; mentre lasceremo ad un successivo commento l'analisi dell'altro "criterio del bersaglio".

Sintesi

Fig. 1 - I sei elementi indicativi del "criterio dello stabilimento".

Competenza della UE a legiferare in materia di protezione dei dati

L'articolo 16 del trattato sul funzionamento della UE (TFUE) conferisce all'Unione la competenza a legiferare in materia di protezione dei dati in tutte le questioni di competenza dell'UE, compresa la cooperazione di polizia e giudiziaria in materia penale. L'articolo 16, infatti, ha formato la base giuridica per l'adozione del pacchetto di riforma del 2016, vale a dire il GDPR e la direttiva 2016/680 per la protezione dei dati da parte della polizia e delle autorità giudiziarie penali.

Principio di territorialità

Il potere legislativo dell'Unione, la cui funzione è rimessa congiuntamente al Parlamento ed al Consiglio, è soggetto al principio generale di territorialità, secondo cui l'attuazione del potere coercitivo della norma di legge è circoscritta al territorio dello Stato o, in questo caso, dell'Unione. Ciò significa che la norma di legge ha una sfera di efficacia spaziale, nel senso che unicamente atti o fatti che sono collegati al suo territorio hanno rilevanza per il diritto dell'Unione e rientrano nella competenza dei suoi atti legislativi.

Affinchè possa porsi l'interrogativo dell'ambito di applicazione territoriale del GDPR, cioè chiedersi se il GDPR si applica riguardo ad una determinata situazione, il fatto considerato deve avere qualche elemento che esula dai confini territoriali dell'Unione. In altri termini, qualora un trattamento di dati personali fosse interamente realizzato presso uno stabilimento di un titolare o responsabile ubicato sul territorio dell'Unione, il medesimo trattamento sarebbe certamente soggetto al GDPR, in quanto non vi sarebbe alcun dubbio in merito al suo legame territoriale.

Applicabilità riferita al trattamento anziché ai soggetti

Sulla base di quanto appena affermato, se è incontrovertibile che tutti i trattamenti effettuati da uno stabilimento UE di un titolare o di un responsabile dell'Unione sono soggetti al GDPR, lo stesso non può dirsi nel caso in cui il titolare o il responsabile siano soggetti extra-Ue ma con stabilimento nella UE. In tal caso, l'eventuale legame di uno specifico trattamento allo stabilimento UE, attrarrà quel solo trattamento alla disciplina del regolamento; in quanto le prescrizioni dell'articolo 3 del GDPR hanno come riferimento i trattamenti anziché i soggetti che assumono il ruolo di titolare o responsabile. Cioè, entrambi i criteri "dello stabilimento" e "del bersaglio" – in presenza delle condizioni ivi indicate – assoggettano al GDPR il solo trattamento "catturato" dalle rispettive condizioni invece che tutti i trattamenti posti in essere dal medesimo titolare o responsabile extra-UE.

Ambito di applicazione territoriale

L'articolo 3 del GDPR fornisce risposta all'interrogativo relativo all'individuazione del legame che collega gli atti o fatti (cioè i trattamenti di dati personali) al territorio dell'Unione, così da assoggettarli al regolamento e, di conseguenza, stabilire quale sia l'ambito di applicazione territoriale del GDPR. Siccome tale ambito deve rispondere al citato principio di territorialità, occorre che i criteri indicati dal legislatore individuino pur sempre il collegamento dei trattamenti di dati al territorio dell'Unione.

Riguardo all'applicabilità del GDPR per le imprese extra-UE, si veda la corrispondente sezione "Imprese extra-UE" nel DPtel.

Due criteri dell'ambito territoriale

La prescrizione dell'articolo 3 del regolamento indica due criteri territoriali che fanno scattare l'applicazione del GDPR, cosiddetti:

1. "criterio dello stabilimento";
2. "criterio del bersaglio".

Entrambi i criteri individuano un legame del trattamento di dati al territorio dell'Unione.

Criterio dello stabilimento

Nel primo caso (criterio dello stabilimento) il legame è dato, come si vedrà in dettaglio più avanti, dalla presenza di uno stabilimento sul territorio UE, col quale il trattamento di dati è in correlazione.

Criterio del bersaglio

Col "criterio del bersaglio" il legame tra il trattamento ed il territorio UE è fornito dalla presenza degli interessati nella Unione

- verso i quali sono rivolte offerte di beni o servizi (mediante il trattamento dei relativi dati) ;
- oggetto di monitoraggio dei loro comportamenti nella UE.

Nell'ipotesi del monitoraggio, quindi, il legame territoriale risulta duplice:

1. deve trattarsi di individui che si trovano nella UE;
2. l'ambito applicativo riguarda solo il monitoraggio di comportamenti che si realizzano nella UE.

I sei elementi del "criterio dello stabilimento"

Il "criterio dello stabilimento" è specificato al primo paragrafo dell'articolo 3 del GDPR che così recita: *«1. Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione.».*

Da tale formulazione possono trarsi sei distinti elementi la cui interazione consente di stabilire se il GDPR sia applicabile ad un determinato trattamento di dati personali secondo il "criterio dello stabilimento".

1. Un trattamento di dati personali;
2. effettuato nell'ambito delle attività di;
3. uno stabilimento;
4. situato nell'Unione;
5. di un titolare o responsabile del trattamento;
6. a prescindere che il trattamento sia effettuato o meno nell'Unione.

Trattamento di dati personali riferito a uno stabilimento nella UE

In primo luogo è bene ricordare, anche se ciò sembrerebbe pleonastico, che l'interrogativo in merito all'applicabilità territoriale del GDPR può sussistere solo nel caso in cui si sia in presenza di un trattamento di dati personali, secondo le definizioni contenute all'articolo 4, punti 1) e 2) del regolamento. Qualora le operazioni in esame, invece, dovessero riguardare, ad esempio, dati anonimi ovvero dati riferibili a persone giuridiche, non si sarebbe in presenza di un trattamento

di "dati personali" e, pertanto, non si porrebbe il problema dell'eventuale applicabilità territoriale del GDPR ai fatti considerati.
In aggiunta, affinchè il trattamento in questione possa essere attratto dal "criterio dello stabilimento" e, quindi, vedersi assoggettato al GDPR, occorre che esso sia in relazione con uno stabilimento situato nella UE. E' lo stabilimento stabilito nella UE, l'elemento territoriale che attrae il trattamento in questione nell'ambito applicativo del GDPR, grazie al legame che collega il trattamento stesso allo stabilimento UE, come si vedrà più avanti.

Irrilevanza dell'ubicazione degli interessati

Poiché nel "criterio dello stabilimento" l'elemento territoriale trova riscontro nello stabilimento situato nell'Unione, la presenza degli interessati sul suolo dell'Unione non è rilevante, diversamente da quanto risulterà per l'altro "criterio del bersaglio". Ne consegue che, qualora sussistano gli elementi della formulazione dell'articolo 3(1), sarà soggetto al GDPR anche un trattamento di dati personali, ad esempio, di consumatori brasiliani che si trovano in Brasile.

Irrilevanza del luogo in cui è effettuato il trattamento

Sempre secondo il "criterio dello stabilimento", parimenti irrilevante è il luogo dove effettivamente si effettua il trattamento, visto che l'elemento territoriale è già soddisfatto dallo stabilimento ubicato nell'Unione. Pertanto, a condizione che sussistano tutti gli elementi del citato "criterio dello stabilimento", ben può essere attratto alla disciplina del GDPR un trattamento di dati personali che sia effettuato fuori dal territorio dell'Unione.

Concetto di "stabilimento"

Il GDPR definisce lo «stabilimento principale» ai fini dell'individuazione dell'autorità capofila [art. 4, p.16)] ma non anche lo «stabilimento» che entra in gioco riguardo all'ambito di applicazione territoriale (art. 3). In merito allo «stabilimento principale» si veda l'Editoriale del 6 luglio 2017.
Tuttavia, al considerando (22) – come già avvenuto nella direttiva 95/46/CE al considerando (19) della stessa – viene precisato che *«(l)o stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica.»* (v. anche Weltimmo, p. 28 e Google Spain p. 48).
Quindi, come rilevato nella causa Weltimmo, si è passati da un'impostazione formalistica secondo cui un'impresa sarebbe stabilita esclusivamente nel luogo in cui è registrata, ad una concezione flessibile della nozione di stabilimento (Weltimmo, p.29).
Per determinare se una società extra-Ue, titolare di un trattamento dei dati, dispone di uno stabilimento nella UE, *«occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni di servizi in questione».*
Nel caso Weltimmo, così come ribadito nelle linee guida 3/2018, si fa rilevare che alla luce dell'obiettivo perseguito dalla normativa comunitaria, *«consistente nel garantire una tutela efficace e completa del diritto alla vita privata e nell'evitare che le disposizioni vengano eluse, (...) la presenza di un unico rappresentante, in talune circostanze, può essere sufficiente a costituire un'organizzazione stabile se il medesimo opera con un grado di stabilità sufficiente con l'ausilio dei mezzi necessari per la fornitura dei servizi concreti di cui*

trattasi nello Stato membro in questione» e «la nozione di «stabilimento» (...) si estende a qualsiasi attività reale ed effettiva, anche minima, esercitata tramite un'organizzazione stabile».

Di un titolare o responsabile

Ulteriore elemento del "criterio dello stabilimento" è che lo stabilimento, situato nella UE, sia del titolare o del responsabile del trattamento. La precisazione porta in evidenza come non sia solo lo stabilimento UE del titolare a poter attrarre il trattamento alla disciplina del GDPR, ma anche quello del responsabile del trattamento. L'attrazione della disciplina del regolamento riguarderà le sole prescrizioni riferibili al titolare o al responsabile rispettivamente; nel senso che se è lo stabilimento UE del responsabile a far scattare l'applicabilità del regolamento al trattamento in questione, riguardo ad esso troveranno attuazione le sole prescrizioni direttamente indirizzate al responsabile del trattamento anzichè tutte quelle contenute nel GDPR.

Legame tra trattamento e stabilimento: «l'ambito delle attività»

Si è già detto che:

- il trattamento di dati personali;
- deve essere collegato a;
- uno stabilimento;
- situato nell'Unione;
- di un titolare o responsabile del trattamento.

Il legame che collega il trattamento allo stabilimento UE richiede che esso sia «effettuato nell'ambito delle attività» dello stabilimento. Da questa formulazione emergono due importanti conseguenze:

- la non necessità che il trattamento sia effettuato dallo stesso stabilimento;
- l'irrilevanza del luogo in cui sia effettuato il trattamento (cioè, esso potrebbe persino effettuarsi fuori della UE).

«Ambito delle attività»: significato

Il GDPR non spiega il significato della locuzione «*nell'ambito delle attività*», peraltro già presente nell'abrogata direttiva 95/46/CE.

L'EDPB, nelle linee guida 3/2018, raccomanda che la verifica se "il trattamento sia effettuato nell'ambito delle attività di uno stabilimento UE del titolare o del responsabile del trattamento" venga espletata caso per caso, considerando le specificità della fattispecie e tenendo conto delle indicazioni provenienti dai precedenti presso la Corte di Giustizia (CtGUE); si vedano, al riguardo, i casi Google Spain SL, Google Inc. contro AEPD, Mario Costeja González (C-131/12), nonchè Weltimmo contro NAIH (C-230/14).

Al fine di raggiungere l'obiettivo di garantire una protezione efficace e completa, il significato di «*nel contesto delle attività di uno stabilimento*» non può essere interpretato in modo restrittivo; per aiutare ad individuare la sussistenza di questo legame di "stretta connessione", secondo le linee guida dell'EDPB, vengono in soccorso due fattori:

- la relazione esistente tra il titolare o responsabile e il suo stabilimento locale;
- la raccolta di entrate nell'Unione.

Sul concetto di «ambito delle attività» e sul caso Google Spain, si veda l'Editoriale del 6 luglio 2017.

Relazione tra titolare/responsabile e suo stabilimento UE

Nel caso di un titolare o responsabile extra-UE, le attività di trattamento di dati personali devono essere "strettamente collegate" alle attività del proprio stabilimento nella UE. In tal caso al trattamento in questione si applica il GDPR anche nell'ipotesi in cui lo stabilimento UE non abbia alcun ruolo nella realizzazione del trattamento.
Per un'applicazione del concetto di "stretta connessione" al caso di Facebook Italy dinanzi all'autorità Garante, si veda l'Alert del 19 maggio 2016.

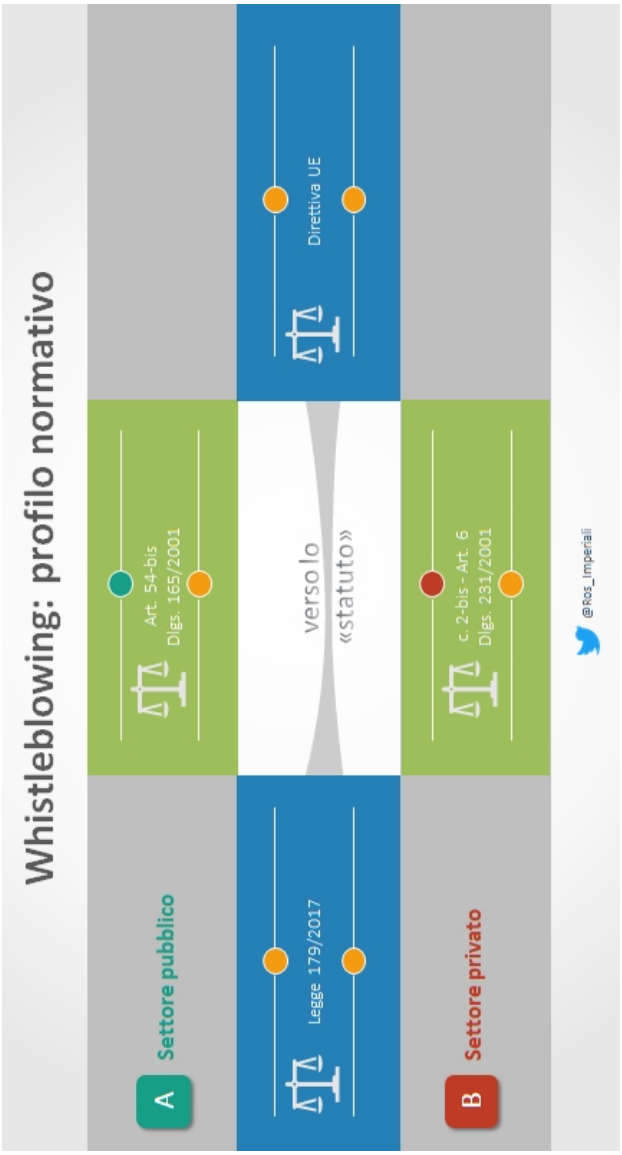
Raccolta di entrate nell'UE

Se la raccolta di entrate effettuata da uno stabilimento nell'Unione è "strettamente connessa" al trattamento di dati personali realizzato fuori della UE, essa può essere indicativa del fatto che il trattamento di dati personali del titolare o responsabile extra-UE sia realizzato «nell'ambito delle attività dello stabilimento UE».

43.
Whistleblowing: linee guida ANAC

Ritorniamo sul tema del whistleblowing a seguito delle due importanti novità dovute alla prossima pubblicazione da parte dell'Autorità anticorruzione (ANAC) delle nuove linee guida sul whistleblowing, conclusasi la procedura di consultazione pubblica, nonchè la nuova direttiva UE sul whistleblowing in corso di pubblicazione sulla Gazzetta Ufficiale dell'UE. In questa tornata facciamo il punto sui numerosi punti di intersezione tra l'attuale disciplina dettata dalla legge 179/2017 e quella sulla protezione dei dati personali. Il tema del whistleblowing è stato già affrontato in precedenti puntate come indicato in "Argomenti collegati" in coda a questi commenti.

La legge 179/2017 in breve



La legge 179 si compone di tre articoli:

1. Il primo «*Tutela del dipendente pubblico che segnala illeciti*» disciplina la tutela del segnalante nel settore pubblico **riscrivendo integralmente l'art. 54-bis del Dlgs. 165/2001**.
2. Il secondo «*Tutela del dipendente o collaboratore che segnala illeciti nel settore privato*» introduce, per la prima volta nel nostro ordinamento, la disciplina del whistleblowing nel settore privato, **aggiungendo il comma 2-bis all'interno dell'art. 6 del Dlgs. 231/2001**, sulla responsabilità amministrativa delle persone giuridiche per i reati commessi da propri dipendenti o collaboratori.
3. Il terzo «*Integrazione della disciplina dell'obbligo di segreto d'ufficio, aziendale, professionale, scientifico e industriale*» contiene una disposizione comune alle segnalazioni effettuate sia nel settore pubblico sia nel settore privato di esonero dalla responsabilità nel caso il segnalante – tramite l'attività di whistleblowing – riveli un segreto d'ufficio, aziendale, professionale, scientifico o industriale o violi il dovere di lealtà e fedeltà (art. 2015 c.c.).

Importanza del whistleblowing

L'istituto del whistleblowing, vale a dire la gestione delle segnalazioni o denunce di informazioni relative a abusi o illeciti, ottenute nel contesto lavorativo, costituisce un importante strumento di salvaguardia di molteplici interessi sia pubblici sia privati. Esso, infatti, contribuisce «*a prevenire danni e ad individuare minacce o pregiudizi al pubblico interesse che non verrebbero altrimenti alla luce*».
D'altro canto, la necessità di proteggere in modo efficace gli informatori rappresenta una forma di tutela della libertà di espressione e della libertà dei mezzi di comunicazione, sancite dall'articolo 21 della costituzione italiana e 11 della Carta dei diritti fondamentali dell'UE ("Carta").
Nella relazione della Commissione alla proposta di Direttiva UE si evidenzia come la (proposta) Direttiva avrà un impatto positivo anche su altri diritti fondamentali quali

- «**diritto a condizioni di lavoro giuste ed eque** (articoli 30 e 31 della Carta): creando appositi canali di comunicazione e migliorando la tutela da eventuali ritorsioni sul lavoro»;
- **rispetto della vita privata**, della **protezione dei dati personali**, della **protezione della salute**, della **tutela dell'ambiente**, della **protezione dei consumatori** «(rispettivamente, articoli 7, 8, 35, 37 e 38 della Carta) e sul principio generale di una **buona amministrazione** (articolo 41)».

ANAC e le linee guida

L'autorità nazionale anticorruzione è il soggetto destinatario delle segnalazioni di condotte illecite del settore pubblico sia provenienti dal proprio interno sia da altre amministrazioni pubbliche (in via alternativa al Responsabile della prevenzione della corruzione e della trasparenza "RPCT", per le segnalazioni, ed in via esclusiva per le comunicazioni di atti ritorsivi a danno del segnalante); l'ANAC, inoltre, emana linee guida sul tema, come prescritto dall'articolo 54-bis del Dlgs. 165/2001 da ultimo modificato dalla legge 179/2017.
Una prima versione delle linee guida è stata pubblicata dall'ANAC nel 2015, con la Determinazione n.6; il 24 luglio 2019 è stata pubblicata una seconda versione del documento, sottoposta a procedura di consultazione pubblica che è terminata il 15 settembre 2019.

Ambito soggettivo

I soggetti tenuti a attuare misure di tutela per il dipendente che denuncia gli illeciti sono:

1. **secondo la disciplina pubblicistica** (art. 54-bis Dlgs. 165/2001) le amministrazioni pubbliche, gli ordini professionali, gli enti pubblici economici, gli enti di diritto privato sottoposti a controllo pubblico e, secondo l'interpretazione dell'ANAC, le autorità amministrative indipendenti come il Garante privacy, considerato che la tutela si estende ai dipendenti delle amministrazioni pubbliche il cui rapporto di lavoro è assoggettato al regime pubblicistico; a questi si aggiungono le «*imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica*»
2. **in ambito privatistico**, le imprese soggette al Dlgs. 231/2001: enti forniti di personalità giuridica e società e associazioni anche prive di personalità giuridica (art.1).

Ambito oggettivo

La disciplina del whistleblowing dettata dal Dlgs. 179/2017 riguarda le segnalazioni e le comunicazioni:

- **le segnalazioni** di condotte illecite possono essere inoltrate, **nel settore pubblico**, alternativamente al RPCT o all'ANAC oppure all'autorità giudiziaria ordinaria sotto forma di denuncia; **nel settore privato**, il legislatore non indica espressamente chi debba essere il destinatario delle segnalazioni che, a livello interpretativo si ritiene che vadano inoltrate all'Organismo di vigilanza in quanto l'OdV è il soggetto che meglio può garantire il vincolo di riservatezza richiesto dalla norma; infatti, la riservatezza dell'identità del segnalante è prescritta anche al fine di evitare l'esposizione dello stesso a misure ritorsive che l'ente di appartenenza potrebbe adottare a seguito della segnalazione
- **le comunicazioni** di atti ritorsivi a danno del segnalante, in ragione della segnalazione; **nel settore pubblico**, esse vanno indirizzate esclusivamente all'ANAC, mentre **nel settore privato** seguono le medesime modalità già previste per le segnalazioni.

Soggetti tutelati

Soggetti tutelati sono:

- i pubblici dipendenti;
- i dipendenti e collaboratori di imprese fornitrici delle amministrazioni pubbliche o che realizzano opere in favore di queste;
- le persone che rivestono funzioni apicali nelle aziende private e persone sottoposte alla direzione o alla vigilanza dei precedenti che segnalano condotte illecite di cui sono venuti a conoscenza in ragione del loro ufficio.

Tutela del segnalante

L'attuale disciplina del whistleblowing (Dlgs. 179/2017) ha il proprio asse nel sistema generale di tutela e protezione del segnalante che comprende

- la garanzia di riservatezza sull'identità;
- la protezione da eventuali misure ritorsive adottate dalle amministrazioni o aziende private a causa della segnalazione;

- la qualificazione della segnalazione del whistleblower come "esimente" del divieto di rivelazione di un segreto d'ufficio, aziendale, professionale, scientifico o industriale o di violazione del dovere di lealtà e fedeltà.

Riservatezza sull'identità del segnalante

La riservatezza sull'identità del segnalante è prescritta **per entrambi i settori pubblico e privato** (comma 3 dell'articolo 54-bis del Dlgs. 165/2001 e comma 2-bis, lettere a) e b), dell'articolo 6 del Dlgs. 231/2001).

Come correttamente sottolineato dall'ANAC nelle sue linee guida del 2019, «*il divieto di rilevare l'identità del segnalante (...) è da riferirsi non solo al nominativo del segnalante ma anche a tutti gli elementi della segnalazione, inclusa la documentazione ad essa allegata, nella misura in cui il loro disvelamento, anche indirettamente, possa consentire l'identificazione del segnalante. Il trattamento di tali elementi va quindi improntato alla massima cautela, a cominciare dall'oscuramento dei dati qualora per ragioni istruttorie altri soggetti ne debbano essere messi a conoscenza.*».

La violazione della riservatezza dell'identità del segnalante è fonte di responsabilità disciplinare.

Tutela della riservatezza del segnalato

La legge non fa menzione dei profili di riservatezza del segnalato sebbene esso goda di tutela in qualità di interessato, alla stessa stregua del segnalante, ai sensi della disciplina sulla protezione dei dati personali. L'ANAC, nelle sue linee guida del 2019, prevede che «*nella trattazione e gestione delle segnalazioni devono essere anche adottate le necessarie cautele per la tutela della riservatezza del soggetto segnalato. Ciò al fine di evitare conseguenze pregiudiziali, anche solo di carattere reputazionale, all'interno del contesto lavorativo in cui il soggetto segnalato è inserito. Pertanto, conformemente ai principi stabiliti dalla Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, l'Amministrazione o l'ente tenuto dovrà aver cura, fin dalla fase di ricezione della segnalazione, di calibrare la tutela della riservatezza accordata al segnalante con quella del segnalato al fine di proteggere entrambi dai rischi cui in concreto tali soggetti sono esposti, avendo particolare riguardo a tale aspetto nella fase di inoltro della segnalazione a terzi.*».

Il nominativo del soggetto segnalato sospettato di essere responsabile della violazione potrà essere comunicato secondo le previsioni di legge, ad esempio su richiesta dell'Autorità giudiziaria.

Oggetto della segnalazione

Condizioni per poter godere della tutela apprestata dalla norma sono:

1. **per il settore pubblico** che
   a. la segnalazione provenga da dipendenti pubblici o ad essi equiparati;
   b. la segnalazione sia effettuata «*nell'interesse all'integrità della pubblica amministrazione*», cioè non per esclusivo interesse personale;
   c. la segnalazione abbia ad oggetto «*condotte illecite*»;
   d. che il dipendente sia venuto a conoscenza di tali illeciti «*in ragione del proprio rapporto di lavoro*».
2. **per il settore privato** che:
   a. la segnalazione provenga da soggetti apicali o sottoposti alla loro direzione o vigilanza;
   b. la segnalazione sia effettuata «a tutela dell'integrità dell'ente»;

c. la segnalazione abbia ad oggetto «condotte illecite rilevanti» ai sensi del decreto 231, cioè riconducenti al portafoglio dei reati 231, «o … violazioni del modello di organizzazione e gestione dell'ente»;
d. che il segnalante sia venuto a conoscenza di tali illeciti e violazioni «*in ragione delle funzioni svolte*».

Nozione di "condotte illecite"

Il concetto di "condotte illecite" per la disciplina del whistleblowing nel settore pubblico richiede una precisazione interpretativa; secondo l'ANAC «*(i) fatti illeciti oggetto delle segnalazioni whistleblowing comprendono, quindi, non solo l'intera gamma dei delitti contro la pubblica amministrazione di cui al Titolo II, Capo I, del codice penale, ma tutte le situazioni in cui, nel corso dell'attività amministrativa si riscontri un abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati.*
Si pensi a titolo meramente esemplificativo ai casi di sprechi, nepotismo, ripetuto mancato rispetto dei tempi procedimentali, assunzioni non trasparenti, irregolarità contabili, false dichiarazioni, violazione delle norme ambientali e di sicurezza sul lavoro.».
Diversamente, la nozione di "condotte illecite" riguardo al settore privato non presenta dubbi interpretativi, grazie al riferimento nella norma a quelle condotte rilevanti ai sensi del decreto 231.

Nesso con il rapporto di lavoro

Le condotte illecite segnalate devono riguardare situazioni, fatti, circostanze, di cui il soggetto sia venuto a conoscenza «*in ragione del rapporto di lavoro*» pubblico o «*in ragione delle funzioni svolte*» in ambito privato.
Secondo le linee guida ANAC, «*(v)i rientrano pertanto fatti appresi in virtù dell'ufficio rivestito ma anche notizie acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative, sia pure in modo casuale.*».
Ovviamente la tutela non opera nei confronti del segnalante, pubblico o privato che sia, che violi la legge, come quella a protezione dei dati personali, al fine di raccogliere informazioni sugli illeciti segnalati; come nel caso di Cassazione penale n. 35792 del 21 maggio 2018, in cui il segnalante aveva acquisito le informazioni realizzando un accesso abusivo a banca dati della pubblica amministrazione.

Segnalazioni anonime

La legge non disciplina espressamente il caso delle segnalazioni anonime le quali, tuttavia, sembrano essere fuori dall'ambito applicativo della norma. Secondo l'ANAC, «*La ratio della richiamata disposizione è quella di offrire tutela, tra cui la riservatezza dell'identità, a chi faccia emergere condotte e fatti illeciti. Tale tutela opera, quindi, solo nei confronti di soggetti individuabili e riconoscibili. Ciò in quanto, da un lato, non può proteggersi la riservatezza di chi non si conosce; dall'altro, se il segnalante non svela la propria identità*» non si può accertare se il segnalante appartiene alle medesime categorie soggettive per cui la norma dispone la tutela (cioè dipendenti pubblici, apicali e loro sottoposti).
Ciò precisato, i destinatari delle segnalazioni anonime possono comunque tenere in considerazione le segnalazioni anonime che, secondo l'ANAC, vanno «*trattate attraverso canali distinti e differenti da quelli approntati per le segnalazioni di whistleblowing*».

Limiti ai diritti di accesso

Diretta conseguenza della tutela dell'identità del segnalante sono i limiti imposti dalla norma all'esercizio dei diritti di accesso:

- quello ai documenti amministrativi previsto dalla legge 241/1990, secondo la previsione contenuta all'articolo 54-bis, comma 4, del Dlgs. 165/2001;
- quello dell'accesso civico generalizzato (art. 5.2 del Dlgs. 33/2013), secondo l'interpretazione ANAC;
- quello dell'accesso privacy, secondo la specifica previsione dell'art. 2-undecies, comma 1, lett. f) del codice privacy.

44.
“Prassi di riferimento” e simili come «meccanismi di certificazione della protezione dei dati»

Come noto il Regolamento (UE) 2016/679 ("GDPR") riconosce ai «meccanismi di certificazione di cui all'articolo 42» (o «meccanismi di certificazione della protezione dei dati») specifiche funzioni all'interno del quadro regolatorio introdotto dalla riforma.
I «meccanismi di certificazione della protezione dei dati» sono un valido strumento di regolamentazione volontaria da cui si fanno discendere importanti effetti di accountability e di affidabilità che non possono essere compromessi da iniziative collaterali che non soddisfano le prescrizioni normative e, quindi, non possono sortire i medesimi effetti dei «meccanismi di certificazione della protezione dei dati». Sul mercato si è assistito ad un fiorire di certificazioni in ambito GDPR che, tuttavia, non potevano considerarsi «meccanismi di certificazione della protezione dei dati» per le ragioni anzidette, creando una pericolosa confusione proprio in danno dei profili di accountability e affidabilità citati in precedenza.
Questa puntata si sofferma sulle distinzioni che intercorrono tra i «meccanismi di certificazione della protezione dei dati» ed il collaterale fenomeno di accordi e prassi che non costituiscono "norme tecniche".

Sintesi

Fig. 1 - Il ruolo dei meccanismi di certificazione della protezione dei dati in ambito GDPR.

Considerate le numerose e delicate funzioni svolte dai «meccanismi di certificazione della protezione dei dati» – importante strumento di *soft law* – il legislatore ha disciplinato con prescrizioni tassative, l'intero procedimento dall'ideazione, vaglio e accreditamento dei pertinenti schemi di certificazione, sino all'individuazione dei soggetti titolati ed alla conseguente procedura di accreditamento degli organismi di certificazione.

Sistemi di certificazione che indirizzano il tema del GDPR, ma che non rispondono esattamente alle prescrizioni in esso previste – così come altri modelli analoghi ma non rispondenti alle caratteristiche dettate dal regolamento per tali strumenti – non possono qualificarsi come «meccanismi di certificazione della protezione dei dati» e, di conseguenza, non possono produrre i medesimi effetti che il GDPR ricollega a questi ultimi. Questa conclusione vale anche per prassi o accordi e simili che si vorrebbe far rientrare tra i «meccanismi di certificazione della protezione dei dati», considerata la maggiore semplicità del relativo procedimento di realizzazione.

Funzioni dei «meccanismi di certificazione della protezione dei dati»

Secondo il GDPR, l'adesione a un meccanismo di certificazione «*ai sensi dell'articolo 42*» ha lo «*scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento*» e, in particolare:

«*può essere utilizzat(o) come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento*» (art. 24(3), GDPR)

- «*può essere utilizzato come elemento per dimostrare la conformità ai requisiti*» della protezione dei dati by design e by default (art. 25(3), GDPR);
- «*può essere utilizzat(o) come elemento per dimostrare le garanzie sufficienti*» che i responsabili del trattamento ed i sub-responsabili sono tenuti a prestare (art. 28(5), GDPR);
- «*può essere utilizzat(o) come elemento per dimostrare la conformità ai requisiti*» per l'adozione di un adeguato livello di sicurezza (art. 32(3), GDPR);
- costituisce una garanzia adeguata ai sensi dell'articolo 46 per legittimare il flusso di dati personali verso paesi extra-UE che, viceversa, non forniscono garanzie adeguate (art. 46(2)(f), GDPR);
- rappresenta un elemento da tenere in debito conto da parte dell'autorità di controllo nazionale «*(a)l momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso*» (art. 83(2)(j), GDPR).

Di conseguenza, anche se le norme tecniche nascono come norme volontarie, il «meccanismo di certificazione per la protezione dei dati», essendo regolato dal GDPR, ha natura vincolante riguardo alla procedura di formazione ed ai suoi criteri e requisiti.

Accountability

Principio fondante della riforma è la cosiddetta accountability (art. 5(2), GDPR). La versione italiana del regolamento («*Il titolare del trattamento* è competente per il rispetto *(...) e in grado di comprovarlo*», enfasi aggiunta) non aiuta a "sdoganare" questo concetto non facilmente traducibile nella nostra lingua: un misto di responsabilizzazione, affidabilità, attendibilità, assicurazione, rendicontabilità. Il parere 3/2010 del WPArt29 del luglio 2010 (wp173) si era già posto il problema terminologico precisando che tramite questo termine, «*(i)n generale, comunque,* ***l'accento è posto sulla dimostrazione di come viene esercitata la responsabilità*** *e sulla sua verificabilità. La responsabilità e l'obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance. Solo quando si dimostra che la responsabilità funziona effettivamente nella pratica può instaurarsi una fiducia sufficiente.*». Il parere wp173 va dritto al punto quando afferma che tale principio contribuisce «*a passare "dalla teoria alla pratica"*» ed aumenta il livello di responsabilità del titolare.

Certificazioni GDPR come strumento di accountability

Quindi, punto centrale dell'accountability è la «*dimostrazione di come viene esercitata la responsabilità*», cioè di come si rispettano prescrizioni e garanzie poste dal regolamento.

Dalle funzioni affidate allo strumento dei «meccanismi di certificazione della protezione dei dati», come sopra rilevato, emerge che le certificazioni GDPR sono «*element(i) per dimostrare*»

- «*il rispetto degli obblighi del titolare*»;
- «*la conformità ai requisiti*»;
- «*le garanzie sufficienti*».

In breve, i «meccanismi di certificazione della protezione dei dati» contribuiscono a dimostrare il rispetto della norma, cioè che l'organizzazione di riferimento sia effettivamente "*accountable*".

Certificazioni GDPR e valutazione sanzionatoria

Ulteriore funzione svolta dai «meccanismi di certificazione della protezione dei dati» si ha nell'ambito sanzionatorio: «*(a)l momento di decidere se infliggere una sanzione amministrativa pecuniaria e di fissare l'ammontare della stessa in ogni singolo caso* ***si tiene debito conto*** *(...) (del)l'adesione ai meccanismi di certificazione* ***approvati ai sensi dell'articolo 42***» [art. 83(2)(j), GDPR, enfasi aggiunta].

"Tenere in debito conto" è espressione analoga a "tenere nella dovuta considerazione", cioè in ambito sanzionatorio l'autorità di supervisione "deve considerare attentamente" l'influenza dell'eventuale adesione dell'organizzazione a «*meccanismi di certificazione approvati ai sensi dell'articolo 42*» sia per stabilire il livello della sanzione ma financo per decidere se irrogare o meno la sanzione stessa. Vale a dire che tali strumenti, allorquando rispondono ai requisiti del GDPR, hanno valenza di esimente totale o parziale dell'eventuale illecito in materia di protezione dei dati personali; ancorchè soggetta all'apprezzamento dell'autorità, in quanto «*(l)a certificazione ai sensi del presente articolo non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al presente regolamento e lascia impregiudicati i compiti e i poteri delle autorità di controllo competenti*», [art. 42(4), GDPR].

Certificazioni GDPR come garanzie adeguate

Diversamente dalle casistiche indicate in precedenza, laddove i «meccanismi di certificazione della protezione dei dati» costituiscono un elemento di valutazione indicativo di un'evidenza di conformità, i medesimi «meccanismi di certificazione della protezione dei dati» «*unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate*», assumono essi stessi il valore giuridico di garanzie adeguate a legittimare il flusso internazionale di dati personali [art. 46(2)(f), GDPR].

In tale circostanza, pertanto, il legislatore sottrae la determinazione del valore giuridico dello strumento, alla valutazione dell'autorità di supervisione o, in ultima analisi, del giudice competente: è lo stesso GDPR a stabilire l'effetto giuridico dei «meccanismi di certificazione della protezione dei dati» in questo contesto.

Incoraggiamento all'istituzione e sanzioni per violazioni

Questa breve ricostruzione denota l'importante funzione che il legislatore del regolamento attribuisce ai meccanismi di certificazione "ai sensi dell'articolo 42" tanto che

- impone agli Stati membri e alla Commissione di incoraggiare «*in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati*»;

- impone alle autorità di controllo nazionali di «*incoraggia(re) l'istituzione di meccanismi di certificazione della protezione dei dati (...) a norma dell'articolo 42, paragrafo 1*» (art. 57(1)(n), GDPR);
- impone al comitato europeo di «*incoraggia(re) (...) l'istituzione di meccanismi di certificazione della protezione dei dati*» ai sensi dell'articolo 42;
- sanziona con pena pecuniaria amministrativa «*fino a 10.000.000 EUR, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore*», la violazione degli «*obblighi dell'organismo di certificazione a norma degli articoli 42 e 43*» [art. 83(4)(b), GDPR].

Condizioni e requisiti dei «meccanismi di certificazione della protezione dei dati»

In considerazione di quanto sopra, il legislatore del regolamento si è premurato di stabilire in dettaglio quali siano condizioni e requisiti dei «meccanismi di certificazione della protezione dei dati» idonei a legittimare le molteplici funzioni ad essi assegnate, come sopra rappresentato. In breve, solo i meccanismi di certificazione che rispondono alle precise condizioni indicate agli articoli 42 e 43 possono qualificarsi come «*meccanismi di certificazione della protezione dei dati, ai sensi dell'articolo 42*» del GDPR e svolgere le funzioni previste dal regolamento. Eventuali ulteriori iniziative provenienti dall'ambito della normazione tecnica nel contesto data protection potranno comunque essere espletate, non essendovi al riguardo alcun divieto normativo ostativo, ma non potranno essere equiparate ai «*meccanismi di certificazione della protezione dei dati, ai sensi dell'articolo 42*» nè svolgere le funzioni che il GDPR assegna a questi ultimi.

Condizioni dell'articolo 43

Tra le ulteriori condizioni che l'articolo detta per i «meccanismi di certificazione della protezione dei dati», l'articolo 43 rubricato "Organismi di certificazione" prescrive che:

- la certificazione (cioè l'oggetto principale del meccanismo di certificazione) sia rilasciata e rinnovata dagli «*organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati*» (art. 43(1), GDPR);
- gli organismi di certificazione siano accreditati dall'autorità di controllo nazionale o dall'organismo nazionale di accreditamento (il codice privacy italiano si è orientato verso l'accreditamento da parte di Accredia, salvo casi particolari; art. 2-septiesdecies, cod. privacy);
- che allorquando gli organismi di certificazione siano accreditati dall'organismo nazionale di accreditamento ciò avvenga «*conformemente alla norma EN-ISO/IEC 17065/2012 e ai requisiti aggiuntivi stabiliti dall'autorità di controllo competente ai sensi degli articoli 55 o 56*» [art. 43(1)(b), GDPR].

Richiamo alla norma EN-ISO/IEC 17065/2012

Da tale ricostruzione si deduce che il richiamo «*alla norma EN-ISO/IEC 17065/2012*» non si riferisce alla sola procedura di accreditamento dell'organismo di certificazione ma si estende anche (se non soprattutto) allo **schema di certificazione** (per accertarne la validità), su cui si basa la certificazione che l'organismo stesso rilascerà ai titolari del trattamento o ai responsabili che dimostrino il rispetto dei requisiti in esso previsti. Tale rispetto (o conformità) viene appunto attestato nella certificazione «ai sensi dell'articolo 42» rilasciata dall'organismo di certificazione accreditato da Accredia.

Fig. 2 - I simboli sulla certificazione GDPR già presenti sul mercato ma non il linea col GDPR.

Da tale osservazione ne consegue che eventuali schemi di certificazione che si basassero su normazioni differenti dalla EN-ISO/IEC 17065/2012 – come ISO 27001, ISO 27701 e BS10012 – sarebbero fuori dall'ambito degli articoli 42 e 43 del GDPR e, quindi, non qualificabili come «meccanismi di certificazione della protezione dei dati» da cui far scaturire gli effetti previsti dal GDPR.

Processo del meccanismo di certificazione GDPR

Come si nota, quindi, il processo del «meccanismo di certificazione della protezione dei dati» prevede una serie di passaggi (prescrizioni di legge) tutti parimenti essenziali per il raggiungimento dell'obiettivo finale: l'istituzione di un «meccanismo di certificazione della protezione dei dati» ai sensi dell'articolo 42 GDPR, suscettibile di rilasciare una certificazione che sia idonea a svolgere tutte le citate funzioni previste dal GDPR.

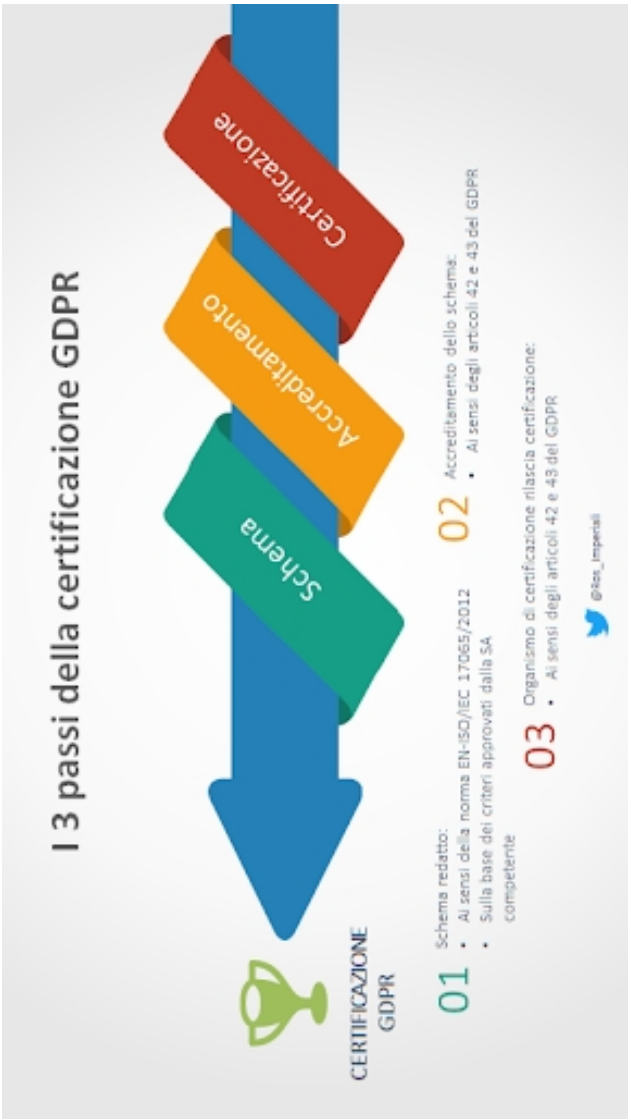


Fig. 3 - Le distinte fasi del «meccanismo di certificazione della protezione dei dati».

Approvazione dei criteri da parte dell'autorità di supervisione

Nella fase iniziale del procedimento per la certificazione GDPR – come indicato nella figura 3 – vi è l'approvazione dei criteri in esso contenuti da parte dell'autorità di supervisione competente, cioè di quella «*del luogo in cui l'organismo di certificazione intende offrire la certificazione e ottiene l'accreditamento*» (linee guida 1/2018, §34).

L'EDPB ha già rilasciato apposite linee guida sia «*relative alla certificazione e all'identificazione di criteri di certificazione*» (1/2018) sia «*relative all'accreditamento degli organismi di certificazione ai sensi dell'articolo 43*» (4/2018).

Peraltro, anche nel caso in cui l'organismo di certificazione intendesse ottenere l'approvazione dei criteri relativi al "sigillo europeo" da parte dell'EDPB (cioè per un meccanismo di certificazione a livello europeo), la domanda per l'approvazione dei criteri da parte del Comitato andrebbe pur sempre presentata per il tramite dell'ASN competente, la quale trasmette il progetto al Comitato, «*se ritiene che i criteri possono essere approvati*» dallo stesso (linee guida 1/2018, § 36).

Criteri di certificazione

Le linee guida 1/2018 sottolineano che i criteri di certificazione sono parte integrante del meccanismo di certificazione e sono suscettibili di approvazione se e quando essi «*rispecchiano perfettamente il requisito del*» GDPR «*per cui il meccanismo di certificazione consente (...) di dimostrare la conformità al regolamento*». Inoltre, «*(i) criteri di certificazione devono essere approvati dall'autorità di controllo competente prima del processo di accreditamento di un organismo di certificazione o nel corso dello stesso.*».

Tempestività dell'approvazione dei criteri incide su competitività e accountability

Le singole autorità di supervisione nazionali (ASN) sono già nelle condizioni di poter esaminare gli schemi e valutarne l'aderenza dei criteri in essi contenuti rispetto alle indicazioni formulate dall'EDPB. Risulta chiaro che tale attività, essendo pregiudiziale per l'accreditamento e la successiva certificazione, incide significativamente sui livelli di competitività degli organismi interessati: chi prima otterrà l'approvazione dei criteri del proprio schema dall'ASN competente, avrà un vantaggio competitivo sul mercato rispetto ai concorrenti. Per le implicazioni economiche che ne possono derivare, l'EDPB sottolinea che «*(l)e autorità di controllo sono tenute a trattare tutte le richieste di approvazione dei criteri di certificazione in modo equo e non discriminatorio, in conformità di una procedura pubblica che specifichi le condizioni generali che dovranno essere soddisfatte e che descriva il processo di approvazione.*» (linee guida 1/2018, §33).

Sinora si è a conoscenza della presentazione presso le ASN di taluni schemi per la relativa approvazione dei criteri (es. in Lussemburgo, Germania, Italia) ma non si ha contezza di approvazioni già rilasciate da parte di una ASN.

Meccanismi di certificazione della protezione dei dati e "prassi di riferimento"

Sulla base della ricostruzione normativa e sulle argomentazioni che ne discendono non sembra potersi aderire alla proposta di istituire «meccanismi di certificazione della protezione dei dati», ai sensi dell'articolo 42 GDPR, facendo ricorso alle cosiddette "prassi di riferimento" e similari quale nuova tipologia di documento sia a livello italiano (UNI – Ente nazionale italiano di unificazione) che internazionale (per l'ISO – International Organization for Standardization, le PAS – Publicly Available Specifications; per il CEN – Comitato europeo di normazione, il CWA – CEN Workshop Agreement).

Le PAS dell'ISO

Le PAS sono pubblicate per rispondere a un'esigenza urgente del mercato, che rappresenta alternativamente l'accordo degli esperti all'interno di un gruppo di lavoro o il consenso raggiunto in un'organizzazione esterna all'ISO. Le PAS «*sono pubblicate per l'uso immediato e servono anche come mezzo per ottenere feedback per un'eventuale trasformazione in uno standard internazionale, (esse) hanno una durata massima di sei anni, dopo di che possono essere trasformate in uno standard internazionale o ritirate*» (fonte ISO).

Il CWA del CEN

Un CWA è un accordo sviluppato e approvato in un seminario CEN aperto alla partecipazione diretta di chiunque abbia interesse nello sviluppo dell'accordo, ma non ha lo stato di uno standard europeo e non può confliggere con uno standard europeo. Lo sviluppo di un CWA dura in media tra 10-12 mesi ed esso non può durare più di 6 anni.

Natura delle "prassi di riferimento"

Le "prassi di riferimento" ("PdR") non sono "norme tecniche" ma «*una forma di documento para-normativo nazionale*» finalizzata a «*consentire in tempi brevi la definizione di accordi specifici, formalizzati sotto forma di disciplinari coordinati dall'intervento strategico dell'UNI*» (fonte: UNI).
«*In sintesi, le prassi di riferimento sono documenti che introducono prescrizioni tecniche o modelli applicativi settoriali di norme tecniche, elaborati sulla base di un rapido (al massimo 8 mesi dall'approvazione della richiesta) processo di condivisione ristretto ai soli autori, verificata l'assenza di norme o progetti di norma allo studio sullo stesso argomento.*». Le PdR durano al massimo due anni.

Caratteristiche comuni di PAS, CWA e PdR

Se ne deduce, pertanto, che PAS, CWA e PdR sono soluzioni adottate dai diversi organismi per rispondere ad esigenze di opportunità e che hanno alcune comuni caratteristiche:

- essi non sono una normazione tecnica ma documenti **para-normativi** che eventualmente possono anticipare una futura normazione tecnica;
- **non si basano su alcuna normazione tecnica** di riferimento;
- **non possono** innovare o **contrastare norme tecniche** esistenti;
- il **processo di condivisione (è) ristretto ai soli autori,** proponenti o partecipanti anzichè a tutti i portatori di interesse, come per le norme tecniche;
- il loro **periodo di vigenza è temporalmente limitato**.

Conclusioni

Da tali indicazioni emerge chiaramente che PAS, CWA e PdR non possono essere equiparate ai «meccanismi di certificazione della protezione dei dati», ai sensi dell'articolo 42 GDPR,

- «non essendo documenti normativi» (Fonte: ISO, CEN, UNI) laddove, invece, gli articoli 42 e 43 del regolamento chiaramente indicano la volontà del legislatore a che il «meccanismi di certificazione della protezione dei dati» faccia affidamento su (cioè porti in dote) le garanzie di una tipica norma tecnica che passa attraverso una serie di fasi di analisi e accreditamento;
- non essendo basati su alcuna norma tecnica, mentre i «meccanismi di certificazione per la protezione dei dati», accreditati presso l'organismo nazionale di accreditamento, si fondano sulla norma EN-ISO/IEC 17065/2012 [art. 43(1)(b), GDPR];
- avendo un periodo di vigenza temporalmente limitato (massimo 6 anni per PAS, 3+3 anni per CWA, 2 anni per PdR).

In aggiunta, uno dei presupposti che giustificano il ricorso alle "prassi di riferimento" è «l'**assenza di norme o progetti di norma allo studio sullo stesso argomento**», circostanza questa che appare destituita di fondamento per quanto attiene il tema della protezione dei dati avendo il legislatore fatto ricorso alla citata EN-ISO/IEC 17065/2012 ed essendo stata riconosciuta a

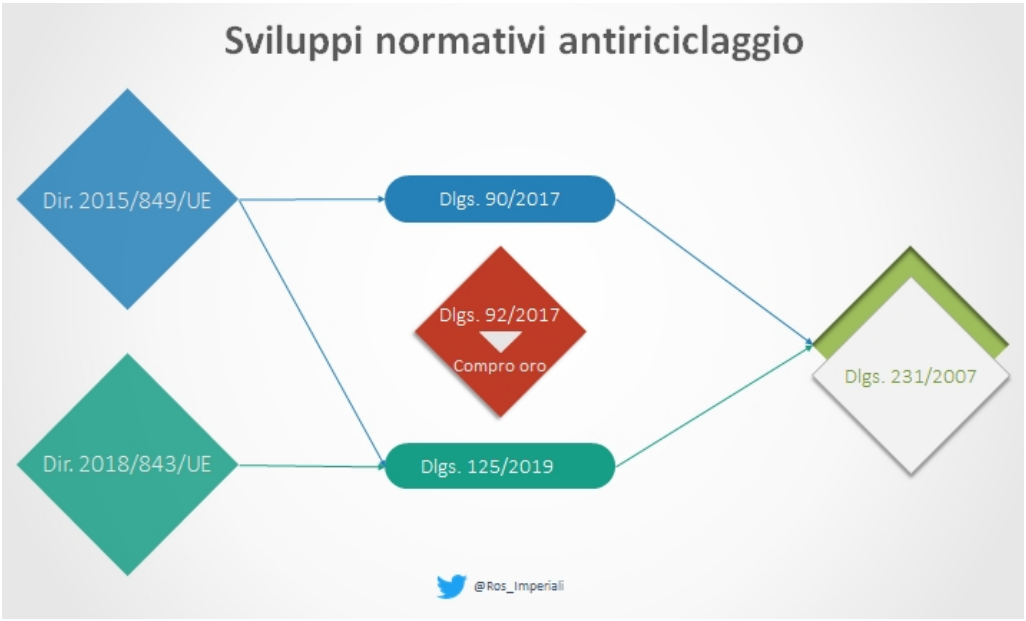
livello internazionale (v. studio Università di Tillsburgh) la presenza, allo stato, di due schemi che rispondono al richiamo dell'ISO 17065: uno italiano (ISDP 10003) e l'altro tedesco (EuroPrise).

45.
V Direttiva antiriciclaggio e impatti data protection

Il decreto legislativo n. 125 del 2019 ha dato attuazione alla V direttiva antiriciclaggio ed è entrato in vigore il 10 novembre 2019.

La disciplina antiriciclaggio ha numerosi punti di contatto e provoca impatti in relazione alla normativa sulla protezione dei dati personali. Il bilanciamento reso necessario trova esplicitazione al comma 9 dell'articolo 3 del dlgs. 231/2007 che così recita: «*9. I soggetti obbligati assicurano che il trattamento dei dati acquisiti nell'adempimento degli obblighi di cui al presente decreto avvenga, per i soli scopi e per le attività da esso previsti e nel rispetto delle prescrizioni e delle garanzie stabilite dal Codice in materia di protezione dei dati personali.*»; il riferimento al codice va interpretato in senso comprensivo del GDPR come indicato all'articolo 1 del medesimo codice privacy («*Il trattamento dei dati personali avviene secondo le norme del regolamento (UE) 2016/679 (...) e del presente codice*»).

Gli obblighi di informativa privacy e circa l'uso dei dati relativi a condanne penali e reati, l'esternalizzazione a terzi di specifiche attività antiriciclaggio, la limitazione dei diritti privacy, le operazioni di profilazione della clientela e la sottoposizione di tali attività alla preventiva DPIA, sono solo alcuni dei principali punti di intersezione tra le due discipline che esamineremo in questa tornata.



Informativa

Anche per i trattamenti per finalità di antiriciclaggio vige il rispetto del principio di trasparenza: i soggetti obbligati sono tenuti a fornire ai clienti le informazioni previste dal GDPR (artt. 13 e 14) prima di instaurare un rapporto d'affari o eseguire un'operazione occasionale.

La direttiva (UE) 2015/849 prevedeva espressamente tale obbligo [«*I soggetti obbligati forniscono ai nuovi clienti le informazioni di cui all'articolo 10 della direttiva 95/46/CE prima di instaurare un rapporto d'affari o eseguire un'operazione occasionale. Tali informazioni includono, in particolare, una comunicazione generale sugli obblighi giuridici imposti ai soggetti obbligati ai sensi della presente direttiva in ordine al trattamento dei dati personali ai fini della prevenzione del riciclaggio e del finanziamento del terrorismo*» art. 41(3)]; l'assenza

di tale previsione nella norma di attuazione italiana ha formato oggetto di contestazione da parte della Commissione nella procedura di infrazione.
Il governo italiano, in risposta, ha ritenuto sufficiente la vigenza dell'art. 13 del Regolamento, nonché la clausola generale contenuta nel Dlgs. 231/2007 e sopra riportata.
Ad ogni buon conto, occorre tener presente che, come indicato nella direttiva 2015/849, le informazioni previste dal GDPR dovranno essere integrate dai titolari del trattamento, con le informazioni sugli obblighi giuridici imposti ai soggetti obbligati, anche con riferimento all'adeguata verifica della clientela attraverso indicatori ed alla valutazione del rischio di riciclaggio e finanziamento del terrorismo. Si veda, in proposito, anche quanto indicato in seguito in relazione alle limitazioni all'esercizio dei diritti privacy.

Dati relativi a condanne penali e reati

Il Codice privacy, fa esplicito riferimento ai trattamenti per finalità di antiriciclaggio in relazione ai cosiddetti dati giudiziari, sancendo che "*l'adempimento degli obblighi previsti dalle normative vigenti in materia di prevenzione dell'uso del sistema finanziario a scopo di riciclaggio*" legittima il trattamento di dati relativi a condanne penali o reati [art. 2-octies(3)(m), Codice].
Ne consegue che, mentre per la piena legittimazione dell'utilizzo di tali dati nella maggioranza dei casi si attende ancora il decreto del ministro della giustizia (art. 2-octies, comma 2, codice privacy), l'uso dei dati giudiziari per finalità antiriciclaggio trova la sua fonte di legittimità nella citata specifica previsione normativa.

Esternalizzazione a terzi delle fasi di identificazione e verifica d'identità

Il decreto attuativo della V direttiva apre alla possibilità che si realizzi un'esternalizzazione a terzi non appartenenti al gruppo delle fasi dell'identificazione e della verifica dell'identità (mentre resta escluso il monitoraggio dell'operatività). Questa possibilità è condizionata al rispetto delle cautele che verranno individuate dalle autorità di vigilanza di settore e richiede un opportuno coordinamento con la disciplina del GDPR per quanto attiene l'affidamento di operazioni di trattamento di dati personali a terzi (art. 28, GDPR).

Limitazioni ai diritti privacy

L'articolo 2, comma 3, lett. a), del Dlgs. 125/2019, interviene a modifica dell'articolo 39, del Dlgs. n. 231/2007, prevedendo che il trattamento dei dati personali connesso alle attività di segnalazione e comunicazione sia soggetto alle disposizioni di cui all'articolo 2-undecies del Codice. L'articolo 2-undecies disciplina le limitazioni ai diritti dell'interessato (art. 15-22) quando vengono perseguiti altri interessi meritevoli di considerazione, tra cui quelli in materia di riciclaggio, in applicazione di quanto previsto dal GDPR (art. 23).
Più chiaramente, in tal modo si tutela la riservatezza dell'identità del segnalante e del contenuto delle comunicazioni da parte dell'interessato.
In base a quest'ultima disposizione il ritardo, la limitazione o l'eventuale esclusione da questi diritti va resa nota all'interessato con comunicazione da rilasciare senza ritardo, «*a meno che la comunicazione possa compromettere la finalità della limitazione*».
È previsto, comunque, che i diritti dell'interessato possano essere esercitati per il tramite del Garante e di tale facoltà il titolare deve darne informativa all'interessato.

Profilazione

In base alla normativa, i soggetti obbligati sono tenuti ad effettuare trattamenti automatizzati di dati personali della propria clientela, consistenti nella profilazione sistematica secondo gli elementi di rischio di riciclaggio o terrorismo identificati dall'UIF, i cui esiti sono resi disponibili alle autorità di vigilanza di settore. Le autorità di vigilanza realizzano analoghi trattamenti di dati per il controllo dei soggetti obbligati mediante una profilazione automatizzata del rischio ad essi associato.

Questi trattamenti, che riguardano la formulazione degli indicatori di anomalia per la creazione di profili di rischio, si attuano mediante processi decisionali automatizzati per la cui legittimità il GDPR richiede l'autorizzazione «dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato» [art. 22(2)(b) GDPR].

Queste misure di garanzia di fonte normativa devono ancora essere individuate.

Valutazione d'impatto

Le descritte tipologie di trattamenti presentano rischi elevati per i diritti e le libertà e sono soggette a valutazione d'impatto obbligatoria volta a individuare le misure di mitigazione a tutela degli interessati.

Il GDPR consente che per i trattamenti che si fondano sulla necessità dell'obbligo legale e dell'interesse pubblico e che trovino la propria base giuridica nel diritto dell'Unione o dello Stato membro del titolare, la valutazione di impatto generale eventualmente realizzata nel contesto di tale base giuridica, può far venir meno l'obbligo della DPIA da parte dei singoli titolari. Nell'attuale assenza di questa DPIA incardinata nella norma di legge, l'obbligo della DPIA per ciascun titolare – soggetto obbligato e autorità di vigilanza – permane.

Accesso alle informazioni sulla titolarità effettiva

La disciplina dell'antiriciclaggio prevede un regime di libera accessibilità alle informazioni contenute nel registro delle imprese, per la verifica della titolarità effettiva delle imprese dotate di personalità giuridica e delle persone giuridiche private; l'accesso deve essere conforme alle norme sulla protezione dei dati, come esplicitamente indicato nella IV direttiva, sulla base di modalità di consultazione che saranno dettate con decreto del Ministro dell'economia e delle finanze, su parere del Garante (articoli 21 e 22 del d. lgs. n. 231/2007, come modificati).

La lettera f) del comma 2 dell'articolo 21 – che sopprime il riferimento al fatto che le informazioni sulla titolarità vengano conservate in una sezione del Registro delle imprese ad accesso riservato – prevede che il "pubblico" in generale – e non più i soli portatori di interessi – possa accedere a nome e cognome, mese e anno di nascita, paese di residenza e cittadinanza del titolare effettivo e conoscere le condizioni «*in forza delle quali il titolare effettivo è tale*». L'accesso è escluso «*in tutto o in parte, qualora l'accesso esponga il titolare effettivo a un rischio sproporzionato di frode, rapimento, ricatto, estorsione, molestia, violenza o intimidazione ovvero qualora il titolare effettivo sia una persona incapace o minore d'età*».

Un più ampio accesso alle informazioni sulla titolarità effettiva riguarda anche i trust includendo, tra coloro ai quali è consentito l'accesso, oltre alle autorità competenti e ai soggetti obbligati ad effettuare le verifiche sulla clientela, i soggetti privati titolari di un interesse giuridico rilevante e differenziato (art. 21.4, nuova lettera d-bis) del dlgs. 231/2007).

Whistleblowing

Nella procedura di infrazione la Commissione aveva rilevato, tra l'altro, la mancata attuazione delle norme d'incoraggiamento delle segnalazioni e del whistleblowing riportate all'art. 61, commi 1 e 2, della IV direttiva.

Il citato articolo impone agli Stati membri l'attuazione di meccanismi efficaci e affidabili per incoraggiare la segnalazione alle autorità competenti di violazioni potenziali o effettive delle disposizioni nazionali di recepimento della direttiva. Questi meccanismi devono includere almeno:

- procedure per il ricevimento di segnalazioni;
- adeguata tutela dei dipendenti di soggetti obbligati che segnalano violazioni commesse all'interno;
- adeguata tutela della persona accusata;
- protezione dei dati personali concernenti sia la persona che segnala le violazioni sia la persona fisica sospettata di essere responsabile della violazione;
- norme chiare che garantiscano la riservatezza dell'identità del segnalante;
- uno specifico canale di comunicazione anonimo e indipendente, proporzionato alla natura e alla dimensione del soggetto obbligato interessato.

Il Governo italiano replica che queste disposizioni trovano attuazione nell'art. 52-ter del TUB il quale, tuttavia, non riguarda la totalità dei soggetti sottoposti agli obblighi antiriciclaggio. In ogni caso, è in corso di pubblicazione la nuova direttiva europea sul whistleblowing che introduce una disciplina generale e orizzontale sul tema, superando l'attuale frammentarietà settoriale. Questa direttiva dovrà essere recepita dagli Stati membri entro due anni dalla sua entrata in vigore.

Si ricorda, inoltre, che la regolamentazione del whistleblowing nel settore antiriciclaggio, è materia diversa dalle disposizioni a tutela del segnalante delle operazioni sospette, già contenute all'articolo 38 del dlgs. 231/2007.

Conservazione delle verifiche

I soggetti obbligati sono tenuti alla conservazione dei documenti, dei dati e delle informazioni utili per accertare eventuali attività di riciclaggio o di finanziamento del terrorismo per «dieci anni dalla cessazione del rapporto continuativo, della prestazione professionale o dall'esecuzione dell'operazione occasionale». La norma richiede che siano conservati almeno, tra l'altro, i dati identificativi del cliente, del titolare effettivo e dell'esecutore, nonchè gli estremi della consultazione, ove effettuata, dell'apposita sezione del Registro delle imprese.

Questa prescrizione normativa sulla conservazione temporale delle informazioni, va tenuta presente nel dizionario dei tempi di conservazione dei dati personali richiesto dal GDPR.

Approccio basato sul rischio

Un ulteriore punto di contatto tra normativa antiriciclaggio e data protection è l'approccio basato sul rischio. Come nel GDPR, dove al titolare viene richiesto di adottare misure tecnico-organizzative commisurate al rischio per i diritti e le libertà delle persone (art. 24 e 32), così i destinatari degli obblighi antiriciclaggio, secondo un approccio scalare, sono chiamati a valutare i rischi cui sono esposti e a dotarsi di presidi commisurati alle proprie caratteristiche (art. 17.3, dlgs 231/2007); questo aspetto va correlato al principio di minimizzazione del GDPR, secondo

cui occorre raccogliere solo i dati personali che risultano necessari e non eccedenti rispetto al perseguimento della legittima finalità dichiarata: ne consegue che un basso rischio antiriciclaggio giustificherà una minore raccolta di dati personali dei soggetti coinvolti. Così come – si ricorda – sono esclusi dagli obblighi di adeguata verifica della clientela le trasmissioni di fondi derivanti da obblighi fiscali e per gli adempimenti in materia di amministrazione del personale: per tali attività, pertanto, non troverebbe alcuna giustificazione il più pervasivo trattamento di dati personali a fini antiriciclaggio.

Formazione

Infine, si ricorda che in base all'articolo 16 del dlgs. 231/2007 – rubricato "Procedure di mitigazione del rischio" – si prescrive che «*i soggetti obbligati garantiscono lo svolgimento di programmi permanenti di formazione*» e che gli stessi soggetti adottano misure proporzionate ai propri rischi, natura e dimensioni, idonee a rendere note al proprio personale gli obblighi dell'antiriciclaggio e di quelli in materia di protezione dei dati personali (art. 16.3, dlgs. 231/2007).

Indice analitico

A

Accountability 210 e ss., *v. anche Certificazioni*
- Motivazioni 211 e ss.
- Significato 215

Accreditamento 86, *v. anche Certificazione*
- Allegato alle linee guida 4/2018 131

Antiriciclaggio 234 e ss., 269 e ss.
- Approccio basato sul rischio 271
- Base giuridica 236
- Bilanciamento di interessi 237
- Conservazione delle verifiche 272
- Data protection (Antiriciclaggio e) 236
- Dati relativi a condanne penali e reati 270
- Decreto legislativo n. 125/2019 *v. in questa voce V Direttiva*
- Diritti privacy (Limitazione ai) 270
- Esternalizzazione a terzi 270
- Formazione 273
- Garante (Attività consultiva del) 236
- Obblighi antiriciclaggio 235
- Profilazione 271
- UIF
- V Direttiva (Decreto di recepimento della) 234 e ss.
  - Ambito soggettivo 235
  - Decreto legislativo n. 125/2019 234 e ss., 269 e ss.
  - Precedenti 235
- Valutazione d'impatto (DPIA) 271
- Whistleblowing 272

Autorizzazioni generali 2 e ss.
- Cessazione effetti 3
- Disciplina transitoria 2 e ss.

B

Base giuridica 113 e ss., *v. anche Antiriciclaggio, Videosorveglianza*
- Assenza di 22
- Obbligo contrattuale 84, 91 e ss.
  - Libertà di impresa 225
  - Linee guida 2/2019 91 e ss., 224 e ss.
    - Fase dell'esecuzione 227
    - Fase di eventuale conflitto 227
    - Misure precontrattuali su richiesta 227
    - Servizi on line *v. in questa voce Servizi on line*
    - Situazioni specifiche *v. in questa voce Situazioni specifiche*
  - Necessità contrattuale (Requisiti per la) 93, 226
    - Necessità (Concetto di) 93

Servizi on line 91
Situazioni specifiche
Miglioramento del servizio 94
Pubblicità comportamentale 94
Trattamenti per fini anti-frode 94
Trattamenti per personalizzazione dei contenuti 95
Big data 146 e ss.
Indagine conoscitiva congiunta di Garante, AGCM e AGCOM 146 e ss.
Antitrust, privacy e pluralismo 147
Asimmetria informativa 149
Dimensione globale 149
Economia dei dati 149
Opt-in 150
Portabilità del dato 150
Profilazione algoritmica, sfruttamento economico e concentrazione di potere 148
Promozione del pluralismo online 150
Brexit 21, 30, 42
FAQ di ICO sul dopo-Brexit) 25
British Airways *v. Sanzioni*

C

Cambridge Analytica *v. Facebook*
Campagne elettorali 63
Carte fedeltà *v. Marketing*
CEN *v. Certificazione/Prassi e simili*
Certificazione 75 e ss., *v. anche Accreditamento e Cybersecurity Act*
Accountability (In relazione alla) 260
Certificazioni per DPO
Condizioni e requisiti 262
Condizioni dell'articolo 43 262
Criteri di certificazione 65
Approvazione dei criteri da parte dell'ASN 264
Richiamo alla norma EN-ISO/IEC 17065/2012 262
Convenzione Garante-Accredia 76
Distinzioni tra requisiti e criteri 89
Garanzie adeguate (In relazione alle) 261
Influenza delle certificazioni 8, 260
Linee guida 1/2018 33, 84 e ss., 132 e ss.
Allegato 2 76, 132
Ruoli dell'ASN (Possibili) 86
Meccanismi di certificazione data protection (Pubblicazione su) 77
Oggetto della certificazione 89
Prassi e simili 259 e ss.
CWA del CEN
PAS dell'ISO 265
Processo del meccanismo di certificazione 263
Sanzioni (In relazione alle) 261

CGUE (v. anche Schrems II)
Appello delle decisioni di rinvio 122
Causa C-673/17 *v. in questa voce Planet49*
Giurisdizione esclusiva CGUE 121
Planet49 67, 205 e ss.
Tipi di rinvio alla CGUE 122
Clausole contrattuali tipo o SCC *v. SCC*
CNIL sanziona Google per 50 milioni 21, 148
Autorità capofila 21
Base giuridica (Assenza di) 22
Consenso non informato 22
Consenso non specifico né inequivocabile 23
Informativa multi-strato 22
Informative carenti e di non agevole accesso 22
Sanzione (Determinazione della) 23
Stabilimento principale 21
Cloud Act 156
Codice di condotta SIC 191 e ss.
Ambito oggettivo 192
Ambito soggettivo 193
Distinte responsabilità dei titolari 193
Ruoli soggettivi 193
Ambito territoriale 192
Organismo di monitoraggio 195
Prescrizioni 194
Base giuridica 194
Data breach (In caso di) 195
Decisioni automatizzate di scoring 195
Diritti dell'interessato 195
Informativa 194
Misure di sicurezza 195
Preavviso di registrazione 194
Procedimento di approvazione 192
Codice di condotta su informazioni commerciali 134 e ss.
Ambito di applicazione 137
Base giuridica 138
Data breach 139
Dati sensibili e giudiziari 138
Informativa agli interessati 138
Organismo di monitoraggio e accreditamento 137
Soggetti committenti 138
Criteri di accreditamento 156
Criteri per l'approvazione 48
Codici deontologici previgenti 16, *v. anche Regole deontologiche*
Codici di condotta 45 e ss., 131, 135 e ss., *v. anche Regole deontologiche*
Linee guida 1/2019 EDPB 43, 45 e ss., 131 e ss., 136 e ss.
Approvazione dei codici di condotta(Procedura di) 50 e ss.

Autorità di controllo competente (Individuazione della) 49
Fasi del processo di approvazione 47
Finalità dei codici 46
Nazionali ed europei 47
Organismo di monitoraggio 49, 137
Organismo di monitoraggio: Accreditamento 49 e ss.
Procedura 136
Rilevanza dei codici 47

Consenso 66 e ss., 197 e ss., *v. anche CNIL, Marketing, Videosorveglianza*
Casella di spunta preselezionata 72
Concetto 199
Condizioni di validità 197 e ss.
Consenso "a pagamento" 197 e ss.
Merce di scambio (Come) 201
Trasparenza 201
Consenso condizionato 70
Consenso cookie 71, 207
Caselle preselezionate 207
Consenso cookie e consenso GDPR 69
Consenso cookie richiesto insieme ad altre finalità 72
Modalità di raccolta del consenso 62 e ss.
Quando occorre il consenso per i cookie 71
Consenso libero 197 e ss.
Consenso oggetto di vendita di dati 70 e ss.
Contratto (Consenso legato a un) 199 e ss.
Distinzione tra consenso, rifiuto e opposizione 71
Marketing (Consenso per il) *v. Marketing*
Consulenti del lavoro *v. Responsabile*
Convenzione 108 53 e ss.
Argentina ratifica 53
Paesi adeguati *v. Trasferimenti internazionali di dati*
Convenzione 108+ 53 e ss.
Cookie 68, *v. anche CGUE/Planet49*
Consenso cookie *v. Consenso*
Cookies wall 62
Informativa per i cookie 68, 207
Destinatari 207
Precondizione del consenso 208
Tempi di conservazione 207
Cooperazione tra ASN 63, *v. anche Meccanismo di coerenza*
CtEDU (Corte Europea dei Diritti Umani) 219 e ss.
Articolo 8 Rispetto della vita privata 219 e ss.
Caso Lopez Ribalda *v. Videosorveglianza/CtEDU*
CtEDU e CEDU 219
Cybersecurity Act 125 e ss.
Certificazioni 127

Obiettivi 128
Processo di certificazione 128
Valore dei certificati sulla sicurezza 129
Contenuti 127
ENISA *v. ENISA*
Iter 127
Obiettivi 126
Sicurezza by design e by default *v. Sicurezza*
CWA *v. Certificazione/Prassi e simili*

D

Data breach (primo provvedimento del Garante su) 25 e ss.
Comunicazione agli interessati 26
Notifiche 33
Provvedimento n. 157 180
Come si effettua la notificazione 182
Informazioni da comunicare nella notifica 181
Modello di notificazione 181
Obblighi di notificazione derivanti dal provvedimento 181
Scheda informativa sul data breach 182
Valutazione del rischio 27
Valutazione di "elevato rischio" 27
Dati giudiziari *v. Dati relativi a condanne penali e reati*
Dati personali
Commerciabilità 202, *v. anche Consenso*
Linee guida wp259 rev.01
Spunti regolatori 202
Weople (Il caso) 203
Dati relativi a condanne penali e reati 180, *v. anche Antiriciclaggio*
Dati sensibili *v. Speciali categorie di dati personali*
Direct marketing *v. Marketing*
Direttiva NIS 126
Diritti degli interessati 55
DPIA *v. anche Antiriciclaggio, Videosorveglianza*
Liste 32
DPO
Esempi di certificazioni 75
Germania modifica condizioni per l'obbligatorietà 155

E

EDPB
Programma biennale 2019-2020 41
Linee guida codici di condotta *v. Codici di condotta*
EDPS
Linee guida su Titolare, contitolare e responsabile 239 e ss.
ENISA 127
Relazione annuale incidenti sicurezza nei servizi fiduciari 154

ePrivacy 42, 67, 205
Autorità competente 61
Consenso ePrivacy 62, 206
Modalità di raccolta *v. Cookie*
Cookie *v. Cookie*
Garante in materia ePrivacy 61
GDPR (Interrelazione con) 61, 206
Informazioni oggetto di tutela (Natura delle) 206
Legge speciale 205
Regolamento ePrivacy 61
Dichiarazione EDPB 61
Segretezza delle comunicazioni 62
Soggetti (Natura dei … cui si riferiscono le informazioni) 206
Eurobarometro 141
Eurobarometro 2019 141 e ss.
Consapevolezza del GDPR 141
Consapevolezza dell'authority nazionale 142
Informativa (Ottenimento della) 145
Policy privacy (La lettura delle) 144

F

Facebook *v. anche Big Data e Sanzioni*
Condanna antitrust italiana 110 e ss.
Condotta ingannevole 111
Pratica aggressiva 111
Condanna antitrust tedesca 109 e ss.
Posizione dominante 110
Garante privacy contro Fb (Cambridge Analytica) 148
Finalità del trattamento 113 e ss.
Disciplina applicabile (Parametro della) 115
Limitazione della finalità (Principio della) 115
Titolarità (In relazione alla) 114
Trattamento (Come elemento qualificante il) 115
Flusso estero di dati 56
Giappone *v. Giappone*
Paesi adeguati 24
Paesi adeguati (Correlazione tra white list e Convenzione 108) 54
Privacy Shield *v. "Privacy Shield"*

G

GDPR
Ambito applicativo 22, 245 e ss.
Ambito territoriale 246
Bersaglio (Criterio del) 247
Luogo di effettuazione del trattamento (Irrilevanza del) 248
Stabilimento (Criterio dello) *v. in questa voce Stabilimento*
Ubicazione degli interessati (Irrilevanza della) 248

Linee guida EDPB 3/2018 245 e ss.
Trattamento (Riferimento al) 246
Territorialità (Principio di) 246
Obiettivo 28
Primi risultati 28
Stabilimento 245 e ss.
Concetto 248
Titolare o responsabili (Di) 249
Relazione tra titolare/responsabile e stabilimento UE 250
Trattamento e stabilimento: legame dello "ambito delle attività" 249
"Ambito delle attività" (Significato dello) 249
Trattamento riferito a uno stabilimento UE 247
Giappone
Libero flusso di dati 24
Mutuo riconoscimento UE-Giappone 23
Partenariato economico 23
Google *v. anche Sanzioni*
CNIL (Sanzione per 50 milioni) *v. CNIL*

I
ICO *v. anche Sanzioni*
E-mail marketing (Sanzione per) 79
Linee guida direct marketing 80
Informative 22, *v. anche CNIL, Eurobarometro*
Carenti (Informative) 22
Multi-strato (Informative) 22
ISO *v. Certificazione*

L
Legittimo interesse *v. Videosorveglianza*

M
Marketing *v. anche ICO, RPO, Videosorveglianza*
Carte fedeltà 167 e ss.
Consenso marketing 80, 167
Consenso informato (Condizioni del) 81
Individuazione dei terzi 81
Verifica della validità del consenso 80
E-mail marketing 79, 167
Soft opt-in 79
Fidelizzazione (Finalità di) 167
Opposizione 168 e ss.
Documentazione probatoria 170
Mancato riscontro 170
Riscontro 169
Marriott International *v. Sanzioni*
Meccanismi di certificazione *v. Certificazione*

Meccanismo di coerenza 64
Modello organizzativo DP 102
Autonomia organizzativa dell'imprenditore 102
Designati al trattamento (incaricati) 103
Art. 29 del GDPR 104
Comparazione art. 29 e 32(4) GDPR 104
Operazioni di trattamento oltre le istruzioni 106
Ruoli DP 105
Medico competente 107

N
NIS *v. Direttiva NIS*

O
OdV231 (Ruolo privacy dell') 97 e ss., 101 e ss.
OdV autonomo titolare 98
OdV parte dell'azienda 97, 101
Critica 104
OdV responsabile del trattamento 99
Soggetti designati al trattamento 97

P
Planet49 *v. CGUE*
Policy privacy *v. Eurobarometro*
Principi data protection 113 e ss.
Privacy Shield 24 e ss., 30, 119
Schrems II *v. Schrems II*
Accesso da parte delle autorità pubbliche 25
Aspetti commerciali 24
Secondo rapporto congiunto annuale 24

R
Registro Pubblico delle Opposizioni (RPO) 17 e ss.
Consultazione del RPO e periodo di efficacia 18
Utilizzo degli indirizzi sugli elenchi telefonici per marketing postale 17
Prossimi sviluppi del RPO 18
Sanzioni 18
Regole deontologiche 14 e ss.
Dai codici deontologici alle regole deontologiche 15
Differenze con codici deontologici e regole deontologiche 135 e ss.
Pubblicazione in Gazzetta Ufficiale 14
Sanzioni per violazioni 17
Responsabile del trattamento 8 e ss.
Che agisce come titolare 8, 10
Consulenti del lavoro 35 e ss.
Distribuzione di compiti nell'assetto organizzativo del (…) 39
Esempio di ISP 11

Esempio fornitori di messaggistica online 11
Unico rapporto giuridico, più ruoli 37
Rischio nel GDPR 57 e ss., *v. anche Data breach, Valutazione del rischio*
Bene soggetto a rischio 57
Misure di contrasto 57

S

Safe Harbour, *v. Schrems I*
Sanzioni 152 e ss.
British Airways 153
Cambridge Analytica *v. Facebook*
Call center 152
Facebook 154, *v. anche Facebook*
Google *v. CNIL*
Marriott International 153
Wind Tre 152
SCC 118 e ss., *v. anche Schrems II*
Schrems I 119
Decisione autorità irlandese 119
Safe Harbour (Invalidazione del) 119
Schrems II 120
Dubbi di legittimità 121
Giurisdizione esclusiva CGUE 121
Legge applicabile 121
Tipi di rinvio alla CGUE *v. CGUE*
Sicurezza
Sicurezza by design e by default 129
Speciali categorie di dati personali 179 e ss.
Provvedimento n. 146 del Garante 179
Ambito di intervento 179
Durata delle prescrizioni 180
Struttura del provvedimento 180
Sperimentazioni cliniche 11, 30 e ss.
Base giuridica 31 e ss.
Regolamento CTR (2018/1725) 31
Differenze con GDPR 31
Correlazioni con GDPR 31
Stabilimento (Principio dello) *v. GDPR/Ambito applicativo*
Stabilimento principale 21
Sub-responsabili 38

T

Titolari del trattamento 8, *v. anche EDPS*
5 elementi della definizione di titolare 240
1. Tipo di soggetti 240
2. Attività svolta 241
3. Modalità 241

4. Oggetto 241
5. Specifica dell'oggetto 242
Esempio servizi professionali 8 e ss.
Esempio avvocati 9
Esempio contabili 9
Esempio organi indipendenti 9
Esempio agenzia di reclutamento 10
Esempio di società di pagamento online 12
Esempio di sperimentazioni cliniche 11
Lista di controllo della titolarità 242
Trasferimenti internazionali di dati *v. Flusso estero di dati*

U
UIF *v. Antiriciclaggio*

V
Valutazione del rischio 56 e ss.
Aggiornamento 58
Elevato rischio 59
Black list o lista del Garante 59
Criteri di determinazione 59
Metodologia 58
Oggetto di valutazione 58
Valutazione di adeguatezza 56
Valutazione prima della DPIA 57 e ss.
Prima fase 58
Videosorveglianza 156 e ss., 159 e ss., 172 e ss., 184 e ss.
Basi giuridiche 164
Consenso 164
CtEDU caso Lopez Ribalda 219 e ss.
Fatti 220
Impugnative 221
Informativa 222
Prima decisione della Camera CtEDU 221
Proporzionalità (Criteri di valutazione della) 221
Fuori ambito GDPR 161
Finalità anti-crimine 161
Finalità personali o domestiche 161
Immagini non identificative 161
Liceità del trattamento 163
Legge concretezza (l. n. 56/2019) 163
Linee guida 3/2019 156 e ss., 159 e ss., 172 e ss.
Comunicazione a terzi 185
Comunicazione alle Forze dell'ordine 185
Conservazione dei dati 188
Contenuti 162
Dati biometrici (Videosorveglianza con) 174, 185

Informativa 175
Cartellonistica 175
Contenuto del cartello 176
Multilivello 175
Posizionamento 175
Diritti 186
Diritto di accesso 186
Diritto di cancellazione 187
Diritto di opposizione 187
Richieste eccessive 187
DPIA per videosorveglianza 189
Finalità di marketing (Videosorveglianza per) 188
Misure tecnico-organizzative 188
By default 189
By design 188
Riconoscimento facciale *v. in questa voce Linee guida 3/2019/Dati biometrici*
Speciali categorie di dati 173
Legittimo interesse 164
Nei diversi ambiti 160
Identificazione di individui 162
In ambito lavorativo 161
In aree pubbliche 160
Parere 4/2007 WPArt29
Provvedimento generale del 2010 161

W

Weople *v. Dati personali/Commerciabilità*
Whistleblowing 18, 229 e ss., *v. anche Antiriciclaggio*
Diritti di accesso (Limiti ai) 257
Importanza del whistleblowing 253
Legge n. 179/2017 230 e ss., 252 e ss.
Linee guida ANAC 2019 252 e ss.
Ambito oggettivo 254
Ambito soggettivo 254
Oggetto della segnalazione 255
Nesso con il rapporto di lavoro 256
Nozione di “condotte illecite” 256
Segnalazioni anonime 256
Soggetti tutelati 254
Tutela del segnalante 254
Riservatezza sull’identità del segnalante 255
Tutela della riservatezza del segnalato 255