Delibera del Garante Privacy e DPIA

Apprendo da una delle tante newsletter fornite dalle banche dati giuridiche alle quali sono abbonato che il Garante ha appena approvato la "**Delibera del Garante Privacy dell'11 ottobre 2018, n. 467; in G.U. del 19 novembre 2018, n. 269 – Valutazione d'impatto**"

Orbene tale delibera concerne o, meglio, individua, come esplicitamente scritto nella medesima delibera, quali siano i trattamenti e/o le tipologie di trattamenti da sottoporre a preventiva Valutazione di Impatto (ar.35 e 36 GDPR)

Partiamo dall'analisi dell'art.35, riportato nella tabella che segue:

1.	Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.	

2.	Il titolare del trattamento, allorquando svolge una valutazione d’impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.	
3.	La valutazione d’impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:	
3.		a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
3.		b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all’articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all’articolo 10; o

3.		c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
4.	L’autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d’impatto sulla protezione dei dati ai sensi del paragrafo 1. L’autorità di controllo comunica tali elenchi al comitato di cui all’articolo 68.	
5.	L’autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d’impatto sulla protezione dei dati. L’autorità di controllo comunica tali elenchi al comitato.	

6.	Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l’autorità di controllo competente applica il meccanismo di coerenza di cui all’articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all’offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all’interno dell’Unione.	
7.	**La valutazione contiene almeno:**	
7.		a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l’interesse legittimo perseguito dal titolare del trattamento;
7.		b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

7.		c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e
7.		d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
8.	Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.	

9.	Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.	
10.	Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.	

11.	Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.	

Orbene, la delibera in questione specifica:

…omissis…

Tutto cio' premesso:

- *ai sensi degli articoli 35, paragrafo 4, e 57, paragrafo 1, lettera k), del RGPD fermo restando quanto indicato nel richiamato WP 248, rev. 01, individua l'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto, riportate nell'allegato 1 facente parte integrante del presente provvedimento, che specificano quanto riportato nel citato WP 248, rev. 01;*

…omissis…

Conseguentemente, l'articolo di riferimento è il 35 del GDPR, oltre all'art.57 del GDPR medesimo, che è quello che concerne i compiti in generale dell'Autorità di Controllo, ossia del Garante per il trattamento dei dati personali nel nostro paese.

Poi, però, prima di passare all'analisi pratica della questione, occorre NON DIMENTICARE cosa afferma l'art.36 del GDPR, che concerne la c.d. "consultazione preventiva", ossia **l'obbligo per i soggetti individuati** di sottoporre i

trattamenti da essi effettuati al **previo controllo** dell’Autorità Garante:

1	Il titolare del trattamento, prima di procedere al trattamento, consulta l’autorità di controllo qualora la valutazione d’impatto sulla protezione dei dati a norma dell’articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.	

2	Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.	
3	Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:	

3		a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell’ambito di un gruppo imprenditoriale;
3		b) le finalità e i mezzi del trattamento previsto;
3		c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;
3		d) ove applicabile, i dati di contatto del responsabile della protezione dei dati;
3		e) la valutazione d’impatto sulla protezione dei dati di cui all’articolo 35;

3		f) ogni altra informazione richiesta dall'autorità di controllo.
4	Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.	
5	Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.	

Ed infatti in questo senso deve essere intesa la delibera, non nella ***esenzione*** per i soggetti NON indicati nella delibera medesima dall'obbligo di valutazione preventiva, e questo per alcuni semplicissimi motivi:

- *La delibera medesima precisa che …omissis… Rilevato che tale elenco e' riferito esclusivamente a tipologie di trattamento soggette al meccanismo di coerenza e che non e' esaustivo, restando fermo quindi l'obbligo di adottare una valutazione d'impatto sulla protezione dei dati laddove ricorrano due o più dei criteri individuati*

dal WP 248, rev. 01 e che in taluni casi «un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno [dei predetti] criteri richieda una valutazione d'impatto sulla protezione dei dati» (cfr. WP 248, rev. 01, pag. 11) …omissis…;

- Il riferimento nella Delibera all'art.35 e non ad altri articoli dovrebbe togliere ogni dubbio sulla necessità per tutti di effettuare comunque una DPIA, nella maggior parte dei casi anche semplicemente perché se non si effettua una corretta DPIA non si può essere certi che i trattamenti effettuati rientrino o meno nell'elenco collegato alla cennata Delibera del Garante;
- La delibera medesima, nella propria parte introduttiva, in un certo senso spiega perché venga emanata, e la ragione è quella di individuare specificatamente e direi per dettato normativo le tipologie di trattamenti ed i trattamenti per i quali i titolari (ovvero i responsabili per la parte loro concernente) debbano **necessariamente** procedere ad una valutazione di impatto **preventiva**.

Passiamo ora ad esaminare le singole ipotesi previste dalla Delibera, con riserva di una più approfondita analisi nel prosieguo.

TESTO DELIBERA	COMMENTO

*1. Trattamenti valutativi o di scoring su **larga scala**, nonche' trattamenti che comportano la profilazione degli interessati nonche' lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad «aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato».*	La prima obiezione che a mio parere salta subito agli occhi è la mancanza di una definizione normativa del concetto di "larga scala", peraltro già più volte sollecitata da più parti, in quanto senza che tale concetto sia definito – giusto o sbagliato, ma definito – in qualche modo, l'interprete (ossia il consulente che debba applicare **nella realtà** la normativa, si trova privo di strumenti stabili e deve necessariamente ricorrere alla propria esperienza e conoscenza, ampliando però il margine di errore. Per il resto mi sembra chiaro il riferimento alle varie "centrali rischi", ove confluiscono i nostri dati relativi all'essere o meno "buoni pagatori".
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono «effetti giuridici» oppure che incidono «in modo analogo significativamente» sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).	Anche qui mi sembra chiaro il riferimento alle varie "centrali rischi", ove confluiscono i nostri dati relativi all'essere o meno "buoni pagatori". **Ritengo che però tutto l'ambito relativo a questo aspetto dovrebbe, per un principio di correttezza generale, essere integrato anche dalle notizie sulla esistenza di eventuali cause promosse dai c.d. "cattivi pagatori" nei confronti dei soggetti che hanno dato origine a tale "marchio".**

3. Trattamenti che prevedono un utilizzo sistematico di dati per ***l'osservazione, il monitoraggio o il controllo degli interessati****, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonche' il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma piu' in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.*	Qual è il significato preciso di "***l'osservazione, il monitoraggio o il controllo degli interessati***"? Non mi sembra che gli esempi siano così chiari. A volere essere pignoli la norma sembra stabilire che sono sottoposti alla Delibera tutti i trattamenti che non sfocino specificatamente nella profilazione, **ma anche** …omissis… ma piu' in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza …omissis… Il che lascia ben poco spazio alla fantasia!

4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).	Quali sono "*dati aventi carattere estremamente personale*"? Una cosa sono i dati relativi alla ubicazione, già oggetto della notificazione del trattamento al Garante nel codice previgente, ben altra cosa sono i dati *la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato.* Qual sono?

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri numeri 3, 7 e 8).	Qui il riferimento è e rimane la legge n.300/1970 art. 4 ed 8, pur con le opportune circoscrizioni effettuate nel corso degli anni dalla giurisprudenza.
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).	In pratica si vuole affermare che qualunque tipo di trattamento che NON SIA OCCASIONALE e che concerna determinate categorie di persone *più vulnerabili*¸ è soggetto alla applicazione della Delibera.

7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.	Qui si fa semplicemente riferimento alla utilizzazione di tecnologie molto avanzate, quasi *auto-decidenti*. Per il contenuto del documento,tra gli altri: https://www.privacy.it/2017/10/04/wp248-rev01/
*8. Trattamenti che comportano lo scambio tra diversi titolari di dati **su larga scala** con modalità telematiche.*	Anche qui la mancanza di una definizione normativa del concetto di "larga scala", peraltro già più volte sollecitata da più parti, in quanto senza che tale concetto sia definito – giusto o sbagliato, ma definito – in qualche modo, l'interprete (ossia il consulente che debba applicare **nella realtà** la normativa, si trova privo di strumenti stabili e deve necessariamente ricorrere alla propria esperienza e conoscenza, ampliando però il margine di errore.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).	In questo caso ritengo che la Delibera colga nel segno, anche perché la realtà ci ha spesso portati a scontrarci con situazioni simili che risultavano di palmare evidenza ma conto le quali non si avevano molte armi

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.	In questo caso ritengo che la Delibera colga nel segno, anche perché la realtà ci ha spesso portati a scontrarci con situazioni simili che risultavano di palmare evidenza ma conto le quali non si avevano molte armi; in pratica si vuol dire che se si trattano dati **sensibili o dati giudiziari** per finalità che non siano **strettamente connesse all'oggetto della prestazione**, si ricade nell'ambito di applicazione della Delibera.
*11. Trattamenti sistematici di dati **biometrici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.*	In questo caso ritengo che la Delibera colga nel segno, proprio in relazione alla grande possibilità di incrociare facilmente (=*interconnessione, combinazione o raffronto di informazioni*) molti dati e/o metadati
*12. Trattamenti sistematici di dati **genetici**, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.*	In questo caso ritengo che la Delibera colga nel segno, proprio in relazione alla grande possibilità di incrociare facilmente (=*interconnessione, combinazione o raffronto di informazioni*) molti dati e/o metadati

Continuerò questa disamina nei prossimi articoli.

Articolo a cura di **Luca-M. de Grazia**

L'articolo Delibera del Garante Privacy e DPIA proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/delibera-del-garante-privacy-e-dpia/