TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI

Segnalazioni giuridiche a cura del Servizio Centrale Legale

N. 07 / 08 Anno XXIV
Luglio / Agosto 2019

INDICE:

CONCORRENZA

BIG DATA – LE AUTORITÀ INDIPENDENTI PER LA TUTELA DELLA CONCORRENZA, DELLE COMUNICAZIONI E DELLA PROTEZIONE DEI DATI PERSONALI ADOTTANO CONGIUNTAMENTE DELLE LINEE GUIDA E RACCOMANDAZIONI DI POLICY SUL FENOMENO DEI BIG DATA

Il 2 luglio 2019 sono state finalmente pubblicate le Linee Guida e Raccomandazioni di Policy (***Linee Guida***) che anticipano la pubblicazione del rapporto finale dell'Indagine Conoscitiva sui c.d. Big Data (***Indagine***) condotta congiuntamente dall'Autorità Garante della Concorrenza e del Mercato (***AGCM***), dall'Autorità per le Garanzie nelle Comunicazioni (***AGCom***) e dal Garante per la protezione dei dati personali (***Garante***) (congiuntamente, le ***Autorità***), ed avviata il 30 maggio del 2017. L'indagine ha visto il coinvolgimento attivo delle Autorità in ragione delle implicazioni trasversali proprie del fenomeno dei Big Data, inerenti il funzionamento dei mercati, il benessere dei consumatori, nonché profili relativi al pluralismo. Le Linee Guida sono articolate in 11 diversi punti.

Anzitutto, viene caldeggiata una riflessione da parte del Governo e del Parlamento con riguardo alla necessità di approntare un quadro normativo adeguato che affronti la questione della piena ed effettiva trasparenza nell'uso delle informazioni personali. In particolare, sebbene le Autorità riconoscano che l'attuale assetto istituzionale appare 'adeguato' a tutelare le libertà fondamentali e nello specifico la protezione dei dati personali e della concorrenza, non sembra potersi affermare lo stesso in relazione alla protezione del pluralismo informativo. Ciò in ragione della difficoltà di applicare l'approccio tradizionale a questioni quali la limitata trasparenza circa l'origine delle informazioni e la loro natura editoriale, nonché gli effetti della profilazione sulla selezione dei contenuti proposti agli utenti. Sul punto, le Linee Guida auspicano iniziative legislative che assicurino alle autorità indipendenti preposte alla tutela del pluralismo "*...poteri di* audit *e* inspection *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* hatespeech...".

Inoltre, il carattere transnazionale insito nel fenomeno dei Big Data è alla base dell'auspicato rafforzamento delle forme di cooperazione esistenti a livello europeo e in alcuni casi internazionale) tra le Autorità e i loro omologhi europei.

Più in generale, le Linee Guida ritengono opportuno, tanto nell'ottica del rafforzamento della sicurezza del trattamento dei dati personali che in quella di un'azione coerente con la strategia nazionale di sicurezza cibernetica, che chiunque intenda procedere al trattamento dei dati secondo le modalità dei Big Data ne identifichi la natura – personale o meno – e le proprietà, anche allo scopo di valutare la possibilità di identificazione della persona a partire da dati 'anonimizzati'. Invece, con specifico riferimento all'utilizzo dei Big Data da parte di soggetti pubblici nello svolgimento delle loro attività istituzionali, viene caldeggiata l'adozione di una *policy* unica e trasparente in merito all'estrazione, accessibilità e utilizzo dei dati pubblici ai fini della determinazione delle politiche pubbliche a vantaggio di imprese e cittadini. Con riguardo al rapporto tra operatori digitali e utenti, le Linee Guida auspicano, inoltre, la riduzione delle asimmetrie informative esistenti, ipotizzando l'adozione di misure volte a rendere maggiormente consapevoli i consumatori nel momento in cui prestano il consenso al trattamento dei propri dati, aumentare la trasparenza dei criteri con cui tali dati vengono elaborati e favorire l'ingresso sul mercato di nuovi intermediari dei dati i quali, su mandato degli utenti, negozino con accresciuto potere commerciale con le piattaforme globali il valore del dato e il suo impiego a fini commerciali. Inoltre, con l'obiettivo di sviluppare la concorrenza nei vari ambiti di valorizzazione economica dei dati ed una conseguente maggior tutela del consumatore-utente, le Linee Guida suggeriscono iniziative regolamentari per l'adozione di *standard* aperti e interoperabili che agevolino la portabilità e mobilità dei dati tra diverse piattaforme.

Con specifico riguardo all'attività dell'AGCM, le nuove sfide poste dall'utilizzo dei Big Data si avvertono con particolare evidenza in relazione a (i) potenziali comportamenti abusivi da parte dei principali operatori di mercato, con riferimento ai quali le Linee Guida ritengono opportuno ripensare il tradizionale approccio alla definizione del mercato rilevante, tenendo in considerazione anche elementi ulteriori; nonché (ii) possibili pratiche collusive la cui realizzazione appare facilitata da algoritmi, a cui occorre prestare particolare attenzione, in quanto in grado di determinare effetti restrittivi della concorrenza.

Inoltre, con riferimento al controllo delle concentrazioni, le Linee Guida auspicano una riforma a livello nazionale e internazionale delle soglie richieste per la comunicazione preventiva, così da poter valutare anche quelle operazioni – altrimenti non soggette

all'obbligo di notifica – che sarebbero in grado di ridurre importanti forme di concorrenza potenziale (ad es. in relazione all'acquisizione di *start-up* particolarmente innovative). Parimenti, viene caldeggiata l'introduzione dello *standard* valutativo già previsto nel Regolamento comunitario sulle concentrazioni, ossia il criterio dell'impedimento significativo della concorrenza effettiva (in luogo di quello della creazione o rafforzamento di una posizione dominante), ritenuto maggiormente idoneo a fronteggiare le sfide poste dall'economia digitale. Le Linee Guida ritengono altresì appropriato fare ricorso agli strumenti propri del diritto antitrust, non confinando l'analisi ai soli parametri tradizionali di prezzo e quantità ma adoperando anche i criteri della qualità dei servizi, dell'innovazione e dell'equità. Inoltre, quantomeno con riferimento alle piattaforme digitali globali, viene auspicata l'adozione di misure che incrementino la trasparenza nei confronti dell'utente circa la profilazione in merito ai contenuti ricevuti dall'utente e meccanismi di *opt-in* in relazione al grado di profilazione prescelto.
Sempre nell'ottica di un'effettiva tutela del consumatore, le Linee Guida auspicano quindi un rafforzamento dei poteri di acquisizione delle informazioni da parte dell'AGCM e dell'AGCom al di fuori dei procedimenti istruttori, anche attraverso l'introduzione di sanzioni in caso di rifiuto o ritardo nel fornire le informazioni richieste, nonché in presenza di informazioni ingannevoli od omissive. Inoltre, a fronte delle significative dimensioni degli operatori digitali, le Linee Guida ritengono necessario anche un innalzamento del massimo edittale delle sanzioni previste al fine di assicurare l'effetto deterrente delle norme in materia di pratiche commerciali scorrette.
Infine, le Linee Guida prevedono l'istituzione di un 'coordinamento permanente' tra le Autorità al fine di garantire un proficuo sfruttamento delle sinergie esistenti tra strumentazione *ex ante* ed *ex post* per la tutela della *privacy*, della concorrenza e del consumatore e del pluralismo.

Con le Linee guida in commento le Autorità forniscono quindi, in primo luogo al legislatore, molteplici spunti ed esplicite raccomandazioni di *policy* in relazione al fenomeno dei Big Data. Resta ora da vedere in primo luogo come questi punto sono stati trattati nel dettaglio nel testo della relazione finale dell'indagine conoscitiva in commento, che secondo quanto annunciati dovrebbe essere pubblicata in tempi relativamente brevi. Inoltre, sarà interessante vedere quali e quanti di questi spunti si tradurranno nell'adozione di misure concrete e se queste ultime si dimostreranno adeguate a garantire la tutela della concorrenza, del pluralismo e della *privacy*, senza scoraggiare i processi innovativi.

Avv. Roberta Laghi
Freshfields Bruckhaus Deringer

CONTRATTUALISTICA

IL NUOVO "CONTRATTO DI ESPANSIONE"

Il 29 giugno scorso è stato pubblicato in Gazzetta Ufficiale il tanto atteso "Decreto Crescita" (Legge 28 giugno 2019, n. 58, dal titolo "**Conversione in legge, con modificazioni, del decreto-legge 30 aprile 2019, n. 34, recante misure urgenti di crescita economica e per la risoluzione di specifiche situazioni di crisi**").

Tra le varie novità, il Decreto Crescita ha introdotto, in via sperimentale per gli anni 2019-2020, il "Contratto di Espansione": una nuova opportunità per le imprese di grandi dimensioni che intendono avviare processi di reindustrializzazione e riorganizzazione mirati al progresso e allo sviluppo tecnologico.
Il Contratto di Espansione sostituisce i contratti di solidarietà espansivi ed è finalizzato a sostenere le aziende nella gestione efficiente del cambiamento dei processi produttivi attraverso l'acquisizione di nuove competenze, la riqualificazione del personale e l'uscita anticipata dei lavoratori prossimi alla pensione.
E' uno strumento rivolto alle imprese con un organico superiore a 1.000 unità, che intendono avviare piani di reindustrializzazione e riorganizzazione che comportano, in tutto o in parte, una strutturale modifica dei processi aziendali finalizzati al progresso e allo sviluppo tecnologico dell'attività.
In particolare, l'attivazione di un Contratto di Espansione presuppone l'esigenza di gestire in modo più efficiente le competenze professionali in organico al fine di agevolare lo sviluppo aziendale, prevedendo d'altro canto l'assunzione di nuove figure professionali.
Nello specifico, l'introduzione del Contratto di Espansione consente di anticipare il pensionamento per quei lavoratori che si trovano non oltre 60 mesi dal raggiungimento dei requisiti anagrafici previsti per l'età pensionabile ed abbiano raggiunto il requisito contributivo versando almeno 20 anni di contributi.
Nel periodo che intercorre tra l'uscita anticipata e il pensionamento, l'azienda sarà tenuta a corrispondere al lavoratore l'ammontare dell'assegno pensionistico lordo, comprensivo di indennità Naspi.
Il vantaggio per le aziende che decideranno di ricorrere al Contratto di Espansione sarà quello di facilitare il turn over generazionale, promuovendo il passaggio a

nuove tecnologie e favorendo l'ingresso in azienda di professionalità specifiche e adeguatamente formate. Inoltre, è prevista anche la possibilità, per i lavoratori che non hanno maturato i requisiti per l'accesso allo scivolo pensionistico di cinque anni, di ridurre l'orario di lavoro (nel limite del 30% dell'orario dei lavoratori interessati dal Contratto di Espansione) per favorire l'ingresso in azienda di nuovi professionisti.
In questo caso, la riduzione di stipendio determinata dalla riduzione di orario sarà compensata con una integrazione salariale a carico dell'INPS.
Dal lato pratico, il datore di lavoro che intende sottoscrivere un contratto di espansione dovrà avviare una procedura di consultazione sindacale (ai sensi dell'art. 24 D. Lgs. 148/2015), finalizzata a sottoscrivere in sede governativa il Contratto di Espansione con il Ministero delle Politiche Economiche e Sociali e le associazioni sindacali comparativamente più rappresentative sul piano nazionale, ovvero con le RSA o le RSU.

Il Contratto di Espansione dovrà prevedere:

- il numero di lavoratori da assumere e relativi profili professionali;
- la programmazione temporale delle assunzioni;
- l'indicazione della durata a tempo indeterminato dei contratti di lavoro (incluso l'apprendistato professionalizzante);
- la riduzione di orario prevista e i dipendenti coinvolti;
- il numero di dipendenti che hanno aderito al piano di pensionamento;
- un progetto di formazione e riqualificazione dei lavoratori.

Infine, con l'approvazione del Contratto di Espansione, il datore di lavoro potrà richiedere l'intervento straordinario di integrazione salariale per un massimo di 18 mesi, anche non continuativi.
Il Contratto di Espansione si prospetta, dunque, un utile strumento volto a favorire il ricambio generazionale, a promuovere lo sviluppo produttivo e a migliorare la competitività aziendale. Considerato che in Italia si stimano almeno 381 aziende sopra i 1.000 dipendenti che potrebbero pertanto beneficiare del Contratto di Espansione, restiamo in attesa di valutarne l'impatto sul mercato del lavoro nell'arco dei prossimi mesi.

Avv. Ottavia Colnago
Cocuzza & Associati, Studio Legale

DIRETTORE RESPONSABILE
Maria Antonietta Portaluri

REDAZIONE
Alessandra Toncelli – Mirella Cignoni – Mattia Ciribifera

LA REDAZIONE RINGRAZIA PER LA COLLABORAZIONE

Avv. Ottavia Colnago, Cocuzza & Associati, Studio Legale (Milano) - Avv. Riccardo Fadiga, Avv. Roberta Laghi, Avv. Gloria Panaccione, Freshfields Bruckhaus Deringer (Milano) – Ing. Cecilia Cantaluppi, IMQ International Services Area (Milano) - Avv. Claudio Gabriele, Studio Associato Oddo Lora Gabriele (Milano) - Avv. Marco Soffientini, Studio Legale Rosadi Soffientini Associati (Arezzo)

Proprietario ed editore:
Federazione ANIE
Viale Lancetti 43, 20158, MI
Telefono (02) 3264.1
Direttore Responsabile
Maria Antonietta Portaluri
Registrazione del Tribunale
di Milano al n° 116 del
19/2/1996

***Te*Lex Anie**
Lancetti 43, 20158, MI Telefono (02) 3264.246 e-mail legale@anie.it *Diffusione via web www.anie.it*

Pubblicazione a cura di:
Servizio Centrale Legale Viale

La valutazione di impatto privacy

(pubblicato su Diritto & Pratica del lavoro 2019, 22, 1385)

Disciplina applicabile

Il regolamento generale sulla protezione dei dati non definisce formalmente il concetto di "valutazione d'impatto sulla protezione dei dati" (c.d. Data Protection Impact Assessment - DPIA) come tale [(1)], ma lo disciplina all'articolo 35, paragrafo 7, del Regolamento Ue 2016/679 (RGPD, in inglese GDPR) in modo che debba contenere:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati per-sonali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre perso-ne in questione.

Il valore e il ruolo della DPIA sono chiariti dal Considerando n. 84, secondo il quale: *"[p]er potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisi-che, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio".*

Inoltre, il Considerando n. 90 precisa che la valutazione di impatto dovrebbe vertere, in particolare, anche sulle misure, sulle garanzie e sui meccanismi previsti per attenuare tale rischio, assicurando la protezione dei dati personali e dimostrando la conformità al presente regolamento. La Valutazione di impatto privacy sostituisce di fatto l'obbligo generale della notificazione preventiva, prevista dalla precedente disciplina, e della verifica preliminare (vedi Considerando n. 89). In tali casi, (precisa il Considerando n. 90) è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio.

La disciplina sulla valutazione di impatto privacy deve, anche, tenere conto delle Linee Guida con-cernenti la valutazione di impatto sulla protezione dei dati, nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679, adottate dal Gruppo di Lavoro "Articolo 29" il 4 aprile 2017 e successivamente emendate e adottate il 4 ottobre 2017 [(2)].

Da ultimo, recentemente, l'Autorità Garante per la protezione dei dati personali ha predisposto, come stabilito per le Autorità di controllo nazionali dal regolamento europeo nell'ambito dei trattamenti transfrontalieri, un elenco delle tipologie di trattamento soggette al meccanismo di coerenza che i soggetti pubblici e privati dovranno sottoporre a valutazione di impatto. L'elenco recepisce le osservazioni del Comitato europeo per la protezione dei dati, al quale era stato sotto-posto dal Garante per il prescritto parere. [doc. web n. 9058979]. Si tratta di uno strumento in più per le aziende e le pubbliche amministrazioni che effettuano trattamenti di dati volti ad offrire beni e servizi anche a persone residenti in altri Paesi dell'Unione.

Accountability

Il regolamento generale sulla protezione dei dati prevede che i titolari del trattamento attuino misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto regolamento, tenendo conto tra l'altro dei *"rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche"* (articolo 24, paragrafo 1 RGPD).

Qualsiasi trattamento, che presenti un rischio elevato per i diritti, le libertà fondamentali e la dignità delle persone interessate, deve essere oggetto di una valutazione di impatto, prima di darvi inizio, da parte dei Titolari (art. 35, paragrafo 1 RGPD), consultando l'Autorità Garante in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti, cioè, quando *il **rischio residuale** per i diritti e le libertà degli interessati resti elevato* (art. 36, paragrafo 1 RGPD) [(3)].
Si tratta di uno degli elementi di maggiore rilevanza nel nuovo quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati. I titolari sono, infatti, tenuti non soltanto a garantire il rispetto del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

Cosa si intende per "rischio elevato per i diritti e le libertà delle persone fisiche"

Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di **gravità** e **probabilità**. Il riferimento ai "diritti e libertà" degli interessati va inteso in primo luogo come relativo al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.
Ad esempio, va sottoposto a DPIA un trattamento che presenti un rischio elevato per i diritti, le libertà fondamentali e la dignità delle persone interessate a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono trattati dati sensibili, o anche per una combinazione di questi e altri fattori.

In cosa consiste la valutazione di impatto privacy

La valutazione di impatto privacy (Data Protection Impact Assessment - DPIA) consiste in una procedura finalizzata ad esaminare un trattamento di dati per valutarne il rispetto ai principi privacy, nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli.
Osservano i Garanti Europei [(4)] che "una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). *In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità con le norme".*

Da Chi e quando va condotta una DPIA

La responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare ne monitora lo svolgimento consultandosi con il responsabile della protezione dei dati (RPD, in inglese DPO) e acquisendo - se i tratta-menti lo richiedono - il parere di esperti di setto-re, del responsabile della sicurezza dei sistemi informativi (Chief Information Security Officer) e del responsabile IT.
La DPIA deve essere condotta prima di procede-re al trattamento. Dovrebbe, comunque, essere previsto un riesame continuo della DPIA, ripe-tendo la valutazione a intervalli regolari.

Valutazione di impatto di un nuovo dispositivo tecnologico

La valutazione di impatto - precisa il primo paragrafo dell'articolo 35 RGPD - è obbligatoria quando il trattamento dei dati - per l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto o le finalità - può presentare un rischio elevato per i diritti e le libertà delle persone. Gli esempi possono essere molteplici; si pensi ai sistemi di videosorveglianza "face detection" per finalità di marketing, o di "face recognition" per motivi di sicurezza, o all'utilizzo di tecnologie sul controllo accessi basate sulle biometrie e/o la geolocalizzazione.
Premesso che il Titolare del trattamento che utilizza detto prodotto resta soggetto all'obbligo di svolgere la propria valutazione d'impatto sulla protezione dei dati in relazione all'attuazione specifica, tuttavia, esso nella propria valutazione potrà acquisire le informazioni eventualmente provenienti dalla valutazione d'impatto preparata dal fornitore del prodotto.
Si tratta di un aspetto importante perché la DPIA del fornitore potrà contenere dettagli in merito alle misure di sicurezza presenti nel dispositivo tecnologico oggetto della valutazione del titolare utilizzatore che, quindi, se opportunamente configurato gli consentirà una adeguata gestione dei rischi e la dimostrazione del rispetto dei principi della privacy by design e by default. Sarà proprio la DPIA del fornitore/produttore della nuova tecnologia ad essere esaminata, oltre che dal Data Protection Officer, anche dal Chief Information Security Officer e/o responsabile IT.

Oggetto della DPIA sono i trattamenti

Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi (Vedi Considerando n. 92).
Non devono essere sottoposti a DPIA tutti i trattamenti del Titolare, ma è necessaria solo se il trattamento "può comportare un rischio elevato per i diritti e le libertà delle persone fisiche". Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.

Quando la DPIA è obbligatoria

La DPIA è obbligatoria in tutti i casi in cui un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. L'articolo 35, paragrafo 3 cita alcuni esempi che generalmente hanno un notevole impatto sui diritti e le libertà fondamentali degli interessati:

a) La 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;
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;
c) La sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Come si evince dall'utilizzo della locuzione "in particolare" nella prima parte del paragrafo 3 [(5)], l'elenco di cui sopra non ha pretese di esaustività [(6)]. Possono esservi trattamenti "a rischio elevato" che non sono ricompresi nell'elenco in questione; anche questi trattamenti dovrebbero essere oggetto di DPIA.
Per tale motivo, le linee Guida WP 248, allo scopo di fornire indicazioni concrete rispetto ai trattamenti che richiedono una DPIA per il rischio inerentemente elevato, e tenendo conto degli elementi specifici contenuti negli articoli 35, paragrafo 1, e 35, paragrafo 3, lettere a)-c), nonché degli elenchi di cui è prevista l'adozione a livello nazionale in base all'art. 35, paragrafo 4, dei considerando 71, 75 e 91, e degli altri riferimenti contenuti nel regolamento a trattamenti "che possono presentare un rischio elevato", hanno sviluppato nove criteri:

1) trattamenti valutativi o di scoring, compresa la profilazione [(7)];
2) decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);

3) monitoraggio sistematico (es: videosorveglianza);

4) trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
5) trattamenti di dati personali su larga scala (8);
6) combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
7) dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
8) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
9) trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la con-cessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

Il concetto di "larga scala"

Il regolamento non offre definizioni del concetto di "larga scala", anche se il considerando 91 (v. nota 8) fornisce indicazioni in merito. In ogni caso, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei seguenti fattori individuati in WP 243 (9), al fine di stabilire se un trattamento sia svolto su larga scala:

a) numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;
b) volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento;
c) durata, o persistenza, dell'attività del trattamento;
d) ambito geografico dell'attività di trattamento.

DPIA facoltativa

Secondo le Linee guida WP 248, la DPIA **non** è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche (vedi infra "Trattamenti autorizzati dal Garante");
- sono compresi nell'elenco facoltativo dei tratta-menti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno Stato membro, per la cui definizione è stata condotta una DPIA.

Trattamenti autorizzati dal Garante

Non è necessario condurre una DPIA per quei trattamenti che siano stati oggetto di verifica preliminare ai sensi dell'abrogato articolo 17, D.Lgs. n. 196/2003 da parte dell'Autorità Garante e che proseguano con le stesse modalità oggetto di verifica.
Come indicato nel considerando 171, "Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/Ce rimangono in vigore fino a quando non verranno modificate, sostituite o abrogate".

Elenco dei trattamenti transfrontalieri da sottoporre a DPIA

L'art. 35, par. 4, rimette alle autorità di controllo nazionali il compito di redigere e rendere pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto e di comunicarlo al Comitato europeo per la protezione dei dati di cui all'art. 68 del RGPD.
L'elenco (non esaustivo) creato dall'Autorità Garante ai sensi della suindicata normativa è stato predisposto riprendendo i nove criteri proposti da WP 248 allo scopo di ulteriormente specificarne il contenuto e riguarda esclusivamente tipologie di trattamento soggette al meccanismo di coerenza.
Il par. 6 del citato art. 35 stabilisce l'applicazione del meccanismo di coerenza di cui all'art. 63 del RGPD [(10)], da parte della singola autorità di controllo competente, qualora l'elenco comprenda "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 per-sonali all'interno dell'Unione".
L'elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto contempla:

1) trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profila-zione degli interessati nonché 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";
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);
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, nonché 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 tratta-menti di metadati, ad es. in ambito di telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza, etc.;
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 (come i dati relativi alle comunicazioni elettroniche, dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (i dati sull'ubica-zione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (i dati finanziari, che potrebbero essere utilizzati per commettere frodi in materia di pagamenti);
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 nn. 3, 7 e 8);
6) trattamenti *non occasionali* di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);
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;
8) trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;

9) trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedo-no l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);
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;
11) trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza dell'attività di trattamento;
12) trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza dell'attività di trattamento.

L'Autorità Garante, con riferimento ai trattamenti di cui ai punti 6, 11 e 12, ha precisato che le espressioni trattamenti "sistematici" e "non occasionali" sono riconducibili al criterio della larga scala, mentre l'espressione "dati biometrici" va intesa come "dati biometrici trattati per identificare univocamente una persona fisica".

Criteri e metodologia di una DPIA

Il regolamento non specifica quale procedura debba essere seguita ai fini della DPIA, lasciando ai titolari la definizione di uno schema che integri le rispettive prassi e che deve, tuttavia, te-nere conto delle componenti di cui all'art. 35, paragrafo 7.
L'importante è che la metodologia prescelta soddisfi i criteri riportati nell'Allegato 2 delle linee Guida WP 248 (in calce al presente articolo).

Come si fa una DPIA

Il Titolare che intenda svolgere una DPIA, dovrà:

- adottare una metodologia conforme ai criteri contenuti nell'Allegato 2 delle Linee Guida;
- coinvolgere i soggetti interessati (titolare, RPD/DPO, interessati o loro rappresentanti, area business, servizi tecnici, responsabili del tratta-mento, responsabile della sicurezza informativa, ecc.);
- fornire all'Autorità di controllo competente, ove previsto, la relazione sulla DPIA svolta; consultare l'Autorità di controllo se non è stato in grado di individuare misure sufficienti ad attenuare i rischi elevati;
- riesaminare periodicamente la DPIA.

Pubblicazione della DPIA e Modello organizzativo

La pubblicazione di una valutazione d'impatto sulla protezione dei dati non è un requisito giuridico sancito dal regolamento generale sulla protezione dei dati.
La sua pubblicazione è una decisione dei titolari del trattamento anche se - raccomandano i Garanti Europei (Wp 248) - sarebbe auspicabile che quest'ultimi prendessero in considerazione la pubblicazione di almeno alcune parti, ad esempio di una sintesi o della conclusione della loro valutazione d'impatto sulla protezione dei dati.
La DPIA deve essere inserita e gestita nel modello organizzativo di cui ciascun Titolare si è dotato ed è consigliabile anche l'istituzione di un manuale di gestione che precisi la metodologia applicata.

Sanzioni per omessa DPIA

La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati, nei casi in cui il trattamento è soggetto alla stessa (articolo 35,paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) oppure la mancata consultazione dell'autorità di controllo, laddove richiesto (articolo 36, paragrafo 3, lettera e), possono comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di euro oppure, nel caso di un'impresa, pari a fino il 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore.

Avv. Marco Soffientini
Studio Legale Rosadi Soffientini Associati

NOTE:

(1) In questi termini Linee Guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679, adottate il 4 aprile 2017 e successivamente emendate e adottate il 4 ottobre 2017,WP 248. Pag. 3 nota 4.

(2) Esse sono emanate ai sensi dell'articolo 70, paragrafo 1, lettera e) RGPD per il quale, come noto, il Comitato Europeo per la protezione dei dati può pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del regolamento generale sulla protezione dei dati.

(3) Con la piena attuazione del GDPR l'intervento delle autorità di controllo avviene principalmente "ex post", ossia si colloca successivamente alle determinazioni assunte autonomamente dal titolare; ciò **spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dalla direttiva del 1995 e dal Codice italiano**, come la **notifica preventiva dei trattamenti** all'autorità di controllo e il cosiddetto prior checking (o verifica preliminare: si veda art. 17 Codice), sostituiti da obblighi di tenuta di un registro dei trattamenti da parte del titolare/responsabile e di effettuazione di valutazioni di impatto in piena autonomia.

(4) WP 248, cit. pag. 3

(5) La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: [OMISSIS]

(6) As the words "in particular" in the introductory sentence of Article 35(3) GDPR indicate, this is meant as a non-exhaustive list. (WP cit. pag. 8).

(7) Sul punto si veda il Considerando n. 91 secondo il quale opportuno altresì effettuare una valutazione d'impatto sulla protezione dei dati nei casi in cui i dati personali sono trattati per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati.

(8) Sempre il Considerando n. 91 precisa che la valutazione di impatto dovrebbe applicarsi ai trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti. procedere a una valutazione d'impatto sulla protezione dei dati.

(9) Linee Guida sul Responsabile della Protezione dei dati – WP 243, rev. 01

(10) Si veda il Considerando n. 135: *È opportuno istituire un meccanismo di coerenza per la cooperazione tra le autorità di controllo, al fine di assicurare un'applicazione coerente del presente regolamento in tutta l'Unione. Tale meccanismo dovrebbe applicarsi in particolare quando un'autorità di controllo intenda adottare una misura intesa a produrre effetti giuridici con riguardo ad attività di trattamento che incidono in modo sostanziale su un numero significativo di interessati in vari Stati membri. È opportuno che il meccanismo si attivi anche quando un' autorità di controllo interessata o la Commissione chiede che tale questione sia trattata nell'ambito del meccanismo di coerenza. Tale meccanismo non dovrebbe pregiudicare le misure che la Commissione può adottare nell'esercizio dei suoi poteri a norma dei trattati.*