1. I principi e l'applicazione extraterritoriale del Regolamento: focus sulla accountability

Entro il prossimo 25 maggio 2018, tutte le organizzazioni, pubbliche e private, che trattano dati personali dovranno adeguarsi al Nuovo Regolamento Europeo in materia di Protezione dei Dati Personali.

La nuova normativa comunitaria segna un cambio di paradigma nell'approccio alla privacy ed alla tutela dei dati delle persone, sia per l'estensione territoriale dei propri effetti, con il superamento di alcuni anacronistici limiti della regolamentazione previgente, sia, più in generale, per il cambio di mentalità che esso impone a tutti gli operatori.

In primo luogo, sotto il profilo territoriale, il Nuovo Regolamento estende la propria sfera applicativa al trattamento di dati personali relativi a soggetti che si trovano nel territorio dell'Unione Europea, anche laddove tali dati siano trattati da un soggetto non stabilito nell'Unione. In particolare, qualsiasi società stabilita in un Paese extra UE, che offra sul territorio europeo, anche a titolo gratuito, beni o servizi o che, comunque, monitori il comportamento sul territorio dell'Unione di persone fisiche (ad esempio, utenti o consumatori), sarà tenuta ad adeguarsi alla nuova normativa.

Cardine del Nuovo Regolamento è il principio di accountability, che, per un verso, offre maggiore flessibilità nel trattamento dei dati personali, superando alcune rigidità tipiche della normativa previgente, ma che, per altro verso, impone l'adozione di comportamenti proattivi, volti a garantire il rispetto delle prescrizioni e dei principi sanciti dal Regolamento.

A tal fine, ciascuna organizzazione sarà tenuta a mappare i trattamenti di dati personali dei quali è responsabile e, quindi, a valutarne il profilo di rischio, individuando le misure tecniche ed organizzative più idonee ad assicurare il rispetto delle garanzie previste dal Regolamento.

Altri due principi chiave sono riassunti dall'espressione inglese "*data protection by design e by default* ", ovvero la necessità che ciascun processo così come ciascuna tecnologia che comporti un trattamento di dati personali, sin dal momento della progettazione, sia elaborato in modo tale da garantire il rispetto delle prescrizioni in materia di privacy e sia impostato di *default* in modo tale da limitare il trattamento ai soli dati strettamente indispensabili. Accorgimenti che naturalmente andranno implementati a monte, prima, quindi, che il trattamento dei dati abbia inizio.

2. La classificazione dei dati, anonimizzazione e pseudonimizzazione

Secondo la definizione fornita dal Regolamento per dato personale si intende: *"qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)"*.

Affinché una persona possa essere considerata identificabile ai sensi del Regolamento, può ritenersi sufficiente anche un codice identificativo, i dati relativi all'ubicazione, o uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Tra i dati personali, una tutela rafforzata è garantita dal Regolamento a categorie particolari di dati personali, che includono oltre a quelli che il Codice Privacy definiva dati sensibili, quali, ad esempio, quelli relativi allo stato di salute, all'origine razziale o etnica, alle opinioni politiche, alle convinzioni religiose o filosofiche, o all'appartenenza sindacale, anche i dati genetici (relativi, quindi, al nostro DNA) ed i dati biometrici (come ad esempio, l'impronta digitale o il riconoscimento facciale).

Non rientrano, invece, nell'ambito di applicazione del Regolamento i cosiddetti dati anonimi, ovvero quei dati che non consentono – neppure in via indiretta - l'identificazione della persona a cui si riferiscono.

Non sempre è, tuttavia, agevole stabilire se un set di informazioni possa essere considerato o meno anonimo e, quindi, non consenta di risalire alla identità dell'interessato.

Al fine di poter condurre una simile valutazione, uno strumento utile può senz'altro essere il provvedimento n. 5/2014 pubblicato dall'Article 29 Working Party, che illustra, in modo dettagliato, quali sono le principali tecniche di anonimizzazione e quali sono i criteri per poter stabilire se un dato possa essere considerato o meno anonimo.

Il dato anonimo non va infatti confuso con il dato pseudonimo, ovvero il dato personale che, anziché essere collegato ad un nome e ad un cognome, è collegato ad un codice identificativo (ad esempio, quello di un tablet o di uno smartphone o di una carta fedeltà).

Tali dati continuano, infatti, a rientrare nella categoria dei dati personali, sebbene presentino un minor livello di rischio, potendo essere attribuiti ad un interessato specifico solo attraverso un passaggio supplementare, ovvero l'incrocio con informazioni aggiuntive, le quali dovranno essere conservate separatamente e sottoposte ad adeguate misure di sicurezza tecniche ed organizzative.

La pseudonimizzazione non costituisce, come si è detto, una tecnica di anonimizzazione, ma una misura di sicurezza, utile per ridurre i possibili rischi per gli interessati ed aiutare così i titolari del trattamento ed i responsabili del trattamento all'assolvimento degli obblighi di protezione dei dati personali prescritti dal Regolamento.

3. Il consenso: focus sui consensi già ottenuti sulla base del Codice Privacy

Il consenso dell'interessato al trattamento dei propri dati personali continua ad essere uno dei punti focali della disciplina sulla privacy anche a seguito dell'adozione del Regolamento.

Il Regolamento definisce il consenso come qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso - mediante una dichiarazione o un'azione positiva inequivocabile - affinché i dati personali che lo riguardano siano oggetto di trattamento.

Non è, quindi, ammesso un consenso tacito o presunto.

La richiesta di consenso dovrà essere comprensibile, semplice, chiara e preceduta da una valida informativa. Occorrerà, quindi, evitare formulazioni ambigue o eccessivamente complesse. Inoltre, tale richiesta dovrà essere chiaramente distinguibile da eventuali altre richieste o dichiarazioni rivolte all'interessato, per esempio all'interno di modulistica contrattuale.

Quali sono, quindi, le principali novità?

- Con riguardo ai minori, il Regolamento precisa che il consenso del minore è valido a partire dall'età di 16 anni; prima, occorrerà raccogliere il consenso dei genitori o di chi ne fa le veci.

- Per i dati "sensibili", viene meno, invece, l'obbligo della forma scritta. Sarà sufficiente un consenso esplicito, consistente, quindi, in una manifestazione di volontà espressa, così come un consenso esplicito dell'interessato sarà richiesto per i trattamenti automatizzati (compresi la profilazione), che possano produrre effetti giuridici sulla sua persona (ad esempio, un licenziamento o la revisione delle condizioni di una polizza assicurativa) o che, comunque, possano incidere in modo significativo sulla persona (ad esempio, attraverso effetti di natura discriminatoria).

Il titolare del trattamento, per poter fare affidamento su tale base giuridica, dovrà, in ogni caso, essere in grado di dimostrare che l'interessato ha prestato il proprio valido consenso a uno specifico trattamento.

A tal riguardo, rilevante è il tema della efficacia dei consensi acquisiti precedentemente al **25 maggio 2018**, rispetto ai quali, il Garante ha precisato che essi restano validi nella misura in cui hanno tutte le caratteristiche previste dal Regolamento.

In caso contrario, il titolare – ove intenda continuare a fare ricorso a tale base giuridica - dovrà adoperarsi prima di tale data per raccogliere nuovamente il consenso degli interessati, nel rispetto delle previsioni introdotte dalla nuova normativa.

4. I trattamenti per finalità di profilazione

Tra i trattamenti rispetto ai quali il Regolamento introduce novità meritevoli di attenzione vi è sicuramente la profilazione: un'attività molto comune nel mondo del marketing, ma con molteplici applicazioni anche in altri settori.

Per profilazione si intende qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare, per analizzare o

prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.

Sotto il profilo degli obblighi informativi, il titolare dovrà comunicare agli interessati l'esistenza di un'attività automatizzata di profilazione, fornendo informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze che tale trattamento può comportare per l'interessato.

L'interessato ha, inoltre, il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato (ivi inclusa, quindi, la profilazione), ove tale decisione sia idonea a produrre effetti giuridici che lo riguardano (ad esempio, il rifiuto di una domanda di finanziamento o la modifica delle condizioni di una polizza assicurativa) o, comunque, ad incidere significativamente sulla sua persona, a meno che tale decisione:

a) sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e il titolare del trattamento;
b) sia autorizzata dalla legge nazionale o comunitaria;
c) si basi sul consenso esplicito dell'interessato.

Un simile trattamento è, inoltre, indicato dal Regolamento tra quelli che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e che, pertanto, richiedono l'attivazione in via preventiva di una procedura di *data protection impact assessment*.

Il titolare del trattamento dovrà, in ogni caso, assicurare all'interessato il diritto di ottenere l'intervento umano da parte del titolare del trattamento ed evitare così una decisione completamente automatizzata e, ancora, il diritto di esprimere la propria opinione ed eventualmente contestare la decisione.

Va, peraltro, osservato che non sempre la profilazione comporta l'assunzione, in modo automatizzato, di decisioni tali da incidere in modo significativo sulla persona de titolare.

Ad esempio – come osservato dall'Article 29 Working Party - in molti casi, la pubblicità comportamentale – basata sulla profilazione di utenti e clienti - non comporta effetti significativi su questi ultimi, per quanto ciò non possa essere escluso a priori, dovendosi considerare tutte le specificità del caso concreto, tra cui:

- il carattere più o meno intrusivo del trattamento
- le aspettative dei soggetti coinvolti nel trattamento
- le modalità attraverso cui la pubblicità è veicolata
- la particolare vulnerabilità dei soggetti interessati.

Va, infine, considerato che – in base alla nuova normativa, diversamente da quanto accade ora - l'attività di profilazione, in linea di principio, potrebbe anche trovare la sua base giuridica nell'interesse legittimo del titolare o di una terza parte e, quindi, non richiedere il consenso dell'interessato.

Per poter fare affidamento sull'interesse legittimo, il titolare sarà, in ogni caso, tenuto a porre in essere – in via preventiva - un serio bilanciamento degli interessi in gioco, volto a valutare se il proprio interesse possa essere ritenuto o meno prevalente rispetto agli interessi, ai diritti ed alle libertà dei soggetti i cui dati vengono trattati.

5. Il registro dei trattamenti

Tra i nuovi obblighi previsti dal Regolamento, una menzione particolare merita l'istituzione del registro dei trattamenti. Si tratta, infatti, di uno strumento fondamentale, per una corretta osservanza del principio di "*accountability*", non solo ai fini della mappatura dei trattamenti in essere presso qualsiasi organizzazione, ma anche al fine di individuare ed analizzare i profili di rischio e procedere, quindi, alla adozione delle misure necessarie al fine di garantire il rispetto dei requisiti prescritti dal Regolamento.

Ove il titolare o il responsabile non abbiano un quadro preciso ed aggiornato dei trattamenti in essere presso la propria struttura, appare, infatti, alquanto improbabile che essi riescano a dimostrare di avere osservato un comportamento responsabile a tutela dei dati personali trattati.

Anche per tale ragione, il Garante per la Privacy ha avuto modo di precisare che la tenuta del registro dei trattamenti (che, per alcuni versi, sembra richiamare il vecchio DPS) non costituisce un mero adempimento di natura formale, ma,

al contrario, è parte integrante di un sistema di corretta gestione dei dati personali, raccomandando, per tale motivo, a tutti i titolari del trattamento ed ai responsabili - a prescindere dalle dimensioni dell'organizzazione ed indipendentemente dall'esistenza di un obbligo di legge – l'adozione di tale registro e, in ogni caso, l'effettuazione di un'accurata ricognizione dei trattamenti svolti e delle rispettive caratteristiche.

Ciò detto, l'adozione di tale registro non sarà, comunque, obbligatorio per tutti. Un obbligo in tal senso non sussiste, infatti, per le organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa comportare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o riguardi categorie particolari di dati (i cosiddetti dati "sensibili") o dati personali relativi a condanne penali e a reati.

Il registro deve avere forma scritta, anche elettronica, e dovrà essere esibito al Garante nel caso di richiesta da parte dell'Autorità. Il contenuto minimo del registro è previsto dal Regolamento ed è differenziato per il titolare ed il responsabile del trattamento. Nello specifico, si richiama l'attenzione sulla sostanziale coincidenza fra i contenuti della notifica dei trattamenti di cui all'art. 38 del Codice Privacy e quelli prescritti dal Regolamento per il registro dei trattamenti.

Nulla vieta, peraltro, a titolare e responsabile di inserire ulteriori informazioni ove lo ritengano opportuno, proprio nell'ottica di una massima trasparenza in relazione ai trattamenti svolti.

Al fine di agevolare il lavoro di quanti dovranno dotarsi di tale strumento entro il 25 maggio 2018, il Garante sta valutando di mettere a disposizione sul proprio sito un modello di registro dei trattamenti, che i singoli titolari potranno integrare nei modi ritenuti più opportuni.

6. Responsabili e Sub-responsabili

Un altro aspetto chiave del Regolamento è la disciplina dei rapporti tra titolare e responsabile del trattamento, con implicazioni non marginali sia per quanto concerne il processo di selezione, sia per quanto riguarda la regolamentazione dei rapporti.

Nella scelta del responsabile, il titolare dovrà, infatti, ricorrere unicamente a soggetti che offrano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate al fine di rispettare le prescrizioni del Regolamento.

Obbligo che impone al titolare di svolgere una vera e propria *due diligence* prima di procedere all'affidamento dell'incarico.
In tale scenario, i codici di condotta e gli schemi di certificazione, conformi alle previsioni del Regolamento, potranno essere strumenti estremamente importanti, per un verso, al fine di agevolare il titolare nel processo di selezione, e, per altro verso, al fine di offrire ai responsabili un efficace elemento di accreditamento.

Anche ai fini della formalizzazione del rapporto, non sarà più sufficiente un mero atto di nomina, ma occorrerà un vero e proprio contratto, che obblighi il Responsabile e dare esecuzione alle istruzioni documentate del titolare e disciplini - tenendo conto dei compiti e responsabilità specifici del responsabile nel contesto del trattamento da eseguire e del rischio in relazione ai diritti e alle libertà dell'interessato - la durata, la natura e le finalità del trattamento, il tipo di dati e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Se un responsabile del trattamento viola il Regolamento, sostituendosi al titolare nel determinare le finalità e i mezzi del trattamento, sarà considerato a sua volta titolare del trattamento in questione, assumendosene le relative responsabilità.

Ove, poi, il responsabile del trattamento intenda affidare una parte del trattamento ad un sub-responsabile, sarà necessaria l'autorizzazione scritta del titolare. Anche in questo caso, il rapporto dovrà essere disciplinato sulla base di un contratto scritto tra responsabile e sub-responsabile, tramite il quale dovranno essere posti a carico del sub-responsabile i medesimi obblighi di cui al contratto tra responsabile e titolare.

Il Responsabile, in ogni caso, conserva nei confronti del titolare del trattamento la piena responsabilità dell'adempimento degli obblighi del sub-responsabile.

Alla luce di quanto esposto, in vista del 25 maggio 2018, i titolari di trattamento dovrebbero verificare in modo scrupoloso che i contratti o gli altri atti giuridici che attualmente disciplinano i rapporti con i rispettivi responsabili siano conformi a quanto previsto dal Regolamento.

La Commissione e le autorità nazionali di controllo (fra cui il Garante) stanno valutando la definizione di clausole contrattuali standard da utilizzare a questo scopo.

7. Il Data Protection Officer (DPO)

Uno degli aspetti più dibattuti del Nuovo Regolamento à senz'altro la figura del DPO, ovvero del "responsabile della protezione dati", da non confondere con il "responsabile del trattamento".

Il DPO è un professionista (o un team di professionisti), nelle intenzioni del legislatore, destinato a favorire una corretta attuazione del Regolamento da parte del titolare e del responsabile. E', infatti, chiamato a svolgere funzioni di supporto al titolare ed al responsabile, assicurando il rispetto del Regolamento e fungendo da punto di contatto per gli interessati e per l'autorità di controllo.

Il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni inerenti la protezione dei dati personali, nonché sostenuto nell'esecuzione dei suoi compiti dal titolare e dal responsabile del trattamento, i quali gli devono fornire tutte risorse adeguate per poter svolgere il proprio lavoro.

La designazione di un DPO in alcuni casi è obbligatoria. In particolare, nel settore privato, tale obbligo sussiste allorché le attività principali di titolare o responsabile comportino un monitoraggio regolare e sistematico degli interessati su larga scala o un trattamento relativo a particolari categorie di dati, condotto su larga scala.

Al fine di poter chiarire cosa si intenda per "attività principale" di titolare o responsabile, cosa si intenda per "trattamenti su larga scala" e cosa per "monitoraggio regolare o sistematico", molto utili sono gli spunti interpretativi contenuti nelle linee guida pubblicate dall'Article 29 Working Party. Spunti che non esimono, tuttavia, titolare e responsabile da una severa valutazione dei trattamenti, da condurre caso per caso, proprio al fine di accertare se la nomina di un DPO possa reputarsi una misura organizzativa necessaria per la propria organizzazione, in considerazione del livello di rischio che determinati trattamenti possono comportare.

Nell'ambito di gruppi di imprese, potrà essere nominato anche un solo DPO, a condizione che quest'ultimo sia "*facilmente raggiungibile da ciascuno stabilimento*" e possa, quindi, rappresentare un valido punto di contatto per gli interessati, le autorità di controllo ed i dipendenti del gruppo.

Il DPO potrà essere un lavoratore dipendente o anche un soggetto esterno, incaricato sulla base di un contratto di servizi. Il Regolamento tratteggia anche le caratteristiche soggettive e oggettive che questa figura deve garantire, tra le quali spiccano l'indipendenza (e, quindi, l'assenza di conflitti di interesse) e la competenza, da misurare anche in materia di protezione dei dati personali.

Anche per i casi in cui il Regolamento non impone in modo specifico la designazione di un DPO, la nomina potrà comunque avvenire su base volontaria. Scelta che in molti casi, in special modo per organizzazioni complesse, è certamente consigliabile.

8. Il Data Protection Impact Assessment (DPIA)

La valutazione del rischio è sicuramente un passaggio fondamentale ai fini dell'adeguamento al Nuovo Regolamento.

Pertanto, laddove un determinato trattamento possa comportare un rischio elevato per le libertà ed i diritti degli interessati, il Regolamento prevede come obbligatorio un apposito processo di valutazione: il cosiddetto *Data Protection Impact Assessment*.

Le linee-guida in materia di valutazione di impatto sulla protezione dei dati recentemente pubblicate dal WP29, identificano alcuni fattori che possono rappresentare un indice di un elevato livello di rischio, tra i quali, ad esempio, l'utilizzo di modalità di trattamento automatizzate idonee a produrre in capo all'interessato effetti legali o simili effetti sostanziali, un'attività di monitoraggio sistematico, il trattamento di dati sensibili o il trattamento di dati personali su larga scala.

Maggiore sarà la ricorrenza dei fattori sopra indicati, maggiore potrà essere considerato il rischio per i diritti e le libertà delle persone fisiche. La valutazione dovrà, in ogni caso, essere condotta caso per caso, sulla base delle specifiche caratteristiche di ciascun trattamento. Infatti, in ipotesi, anche la ricorrenza di un singolo fattore di rischio potrebbe comportare l'obbligo di procedere alla valutazione d'impatto.

Tale procedura comporta una descrizione del trattamento, la valutazione della necessità e proporzionalità dello stesso rispetto alle sue finalità, la descrizione delle misure tecniche ed organizzative adottate a protezione dei diritti e delle libertà degli interessati, l'individuazione dei possibili rischi, l'individuazione di misure supplementari idonee a mitigare tali rischi e, quindi, la valutazione circa la sussistenza di rischi residui, anche a seguito della implementazione di tali ultime misure.

All'esito di questa valutazione d'impatto il titolare potrà decidere in autonomia se iniziare il trattamento (ove ritenga le misure adottate idonee a mitigare sufficientemente il rischio) ovvero – ove il livello di rischio continui ad essere elevato - consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale.

Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare; ciò spiega l'abolizione a partire dal 25 maggio 2018 di alcuni istituti previsti dal Codice Privacy, come la notifica preventiva dei trattamenti all'autorità di controllo ed il cosiddetto procedimento di *prior checking* (ovvero, di verifica preliminare), sostituiti dall'obbligo di tenuta di un registro dei trattamenti da parte del titolare/responsabile e, appunto, dall'obbligo di effettuazione di una valutazione di impatto nei termini brevemente illustrati.

9. La data breach notification

Nel caso di violazione dei dati personali, il Regolamento prevede a carico del titolare l'obbligo di seguire una specifica procedura.

A partire dal 25 maggio 2018, tutti i titolari del trattamento – e non soltanto i fornitori di servizi di comunicazione elettronica accessibili al pubblico, come avviene oggi – dovranno, infatti, notificare all'autorità di controllo le violazioni di dati personali di cui vengano a conoscenza.

Ciò dovrà avvenire in un termine molto breve: entro 72 ore e comunque "senza ingiustificato ritardo".

Tale notificazione dovrà avvenire ogniqualvolta i titolari ritengano probabile che da tale violazione possano derivare rischi per i diritti e le libertà degli interessati.

Pertanto, la notifica all'autorità dell'avvenuta violazione non è obbligatoria, in ogni caso di *data breach*, ma anche in tal caso sarà subordinata ad una preventiva valutazione del rischio per gli interessati, che dovrà essere comunque condotta in tempi molto rapidi.

Laddove, poi, la probabilità di tale rischio sia considerata elevata, le violazioni dovranno essere comunicate non solo all'autorità di controllo, ma anche agli interessati ed anche in questo caso, senza ingiustificato ritardo.

L'obbligo di notificazione non sussisterà, ad esempio, nel caso in cui il titolare del trattamento abbia messo in atto le idonee misure tecniche e organizzative e tali misure di protezione siano state applicate ai dati personali oggetto della violazione, quali ad esempio quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, come la cifratura dei dati.

I contenuti minimi obbligatori della notifica all'autorità e della comunicazione agli interessati sono indicati dal Regolamento.

Tutti i titolari di trattamento dovranno in ogni caso documentare tutte le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze, le conseguenze ed i provvedimenti adottati.

Il Garante ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico. Il modello verrà rielaborato al fine di renderlo utilizzabile da tutti i titolari di trattamento secondo quanto prevede il Regolamento.

10. I diritti degli interessati: il diritto all'oblio

Tra i diritti degli interessati particolare rilievo ha il diritto alla cancellazione, definito dal Regolamento anche come "diritto all'oblio".

In particolare, il Regolamento prevede specifici casi in cui l'interessato può esercitare il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano.

Si è molto parlato di diritto all'oblio in questi anni, a seguito della famosa pronuncia della Corte di Giustizia nel caso Google Spain che ha previsto la facoltà di richiedere ai motori di ricerca la deindicizzazione. Oggi il Regolamento prevede il diritto di ottenere la cancellazione dei dati personali spingendosi oltre la mera deindicizzazione delle pagine lesive dei diritti e travalicando il confine tra l'online e l'offline.

Secondo il Regolamento, il diritto cosiddetto "all'oblio" si configura come un diritto rafforzato alla cancellazione dei propri dati personali. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione".

L'ambito di applicazione è più esteso di quello di cui all'art. 7 del Codice Privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati, per esempio, anche dopo revoca del consenso al trattamento.

Il Regolamento prevede anche specifiche eccezioni al diritto alla cancellazione, ad esempio, nel caso in cui il trattamento sia necessario per l'esercizio del diritto alla libertà di espressione e di informazione; per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

A questo punto, ci si chiede quale valore avranno le indicazioni del WP29 ai tempi della pronuncia Google Spain. In particolare, con riferimento all'oggetto della rimozione, il parere del WP29 precisa che la pronuncia della Corte di Giustizia concerne soltanto i risultati ottenuti attraverso ricerche svolte sulla base del nome di una determinata persona. In questo senso, l'informazione originale potrà essere ancora accessibile sul web impiegando altri termini di ricerca o attraverso un accesso diretto alla fonte originale dell'informazione. Il Regolamento al contrario prevede un espresso diritto alla cancellazione dei dati dell'interessato.

Un altro punto rilevante dell'interpretazione del diritto all'oblio riguarda la sua limitazione per particolari categorie di soggetti quali quelle che svolgono funzioni pubbliche. Il Regolamento non si esprime sul punto lasciando agli interpreti la soluzione di tale quesito.

11. I diritti degli interessati: la portabilità dei dati

Tra i nuovi diritti degli interessati previsti dal Regolamento, vi è il diritto alla portabilità dei dati.

La portabilità dei dati sostanzialmente permette agli interessati di ottenere e riutilizzare i "propri" dati per i propri scopi e attraverso servizi diversi. In questo senso, facilita la circolazione, la copia o il trasferimento dei dati personali da un ambiente informatico all'altro senza impedimenti.

In primo luogo, l'interessato ha il diritto di ricevere dati personali ("in un formato strutturato, di uso comune e leggibile meccanicamente") trattati da un titolare e di memorizzarli su un dispositivo nella propria disponibilità in vista di un successivo utilizzo personale, senza trasferirli a un diverso titolare.

Si tratta, dunque, di un diritto che facilita la gestione diretta dei propri dati personali.

In secondo luogo, si ha il diritto di trasmettere i propri dati personali "senza impedimenti". A tali fini, occorre che siano soddisfatte tre condizioni.

In primo luogo, i dati personali devono essere trattati, attraverso strumenti automatizzati (quindi escludendo gli archivi cartacei), sulla base del consenso preventivo dell'interessato o per l'esecuzione di un contratto di cui è parte l'interessato.

In secondo luogo, i dati personali di cui si chiede la portabilità devono riguardare l'interessato ed essere quelli forniti dall'interessato.

Il WP29 raccomanda ai titolari di non interpretare l'espressione "dati personali che riguardano l'interessato" in modo eccessivamente restrittivo, qualora vi siano dati personali di terzi all'interno di un insieme di dati che riguardano l'interessato e sono stati forniti da quest'ultimo, e che l'interessato utilizza per scopi personali. Ne sono un esempio, tipicamente, i tabulati telefonici, che contengono le chiamate in entrata e quelle in uscita, oppure il prospetto dei movimenti sul proprio conto corrente bancario, in cui sono riportati anche gli accrediti effettuati da soggetti terzi. Si può ritenere che un dato personale sia fornito dall'interessato se quest'ultimo lo "fornisce" consapevolmente e in modo attivo: è il caso, per esempio, dei dati di registrazione (indirizzo postale, nome utente, età, ecc.) inseriti compilando un modulo online. Tuttavia, la definizione comprende anche i dati generati e raccolti attraverso le attività dell'utente che fruisce di un servizio o utilizza un dispositivo.

Viceversa, il diritto alla portabilità non si applica ai dati personali che sono derivati o dedotti dalle informazioni fornite dall'interessato (per esempio, il profilo-utente creato analizzando i dati grezzi di uno smart meter), poiché non si tratta di dati forniti dall'interessato bensì creati dal titolare del trattamento.

In terzo luogo, l'esercizio del diritto alla portabilità non deve ledere i diritti e le libertà altrui. Per esempio, se l'insieme dei dati trasferiti su richiesta dell'interessato contiene dati personali che riguardano altre persone fisiche, il nuovo titolare dovrebbe trattare tali dati solo in presenza di un idoneo fondamento giuridico. È questo il caso di un trattamento che sia svolto direttamente dall'interessato nell'ambito di attività esclusivamente personali o domestiche.

Certamente questo diritto rappresenta una opportunità per gli interessati ma è facile immaginarne anche un uso che va oltre la ratio di questo istituto. In ogni caso è immaginabile che possa tenere molto occupati gli avvocati…

12. Le sanzioni introdotte dalla GDPR: nuovi scenari

Il Regolamento ha uniformato le sanzioni per le violazioni delle regole sulla privacy prevedendo l'applicazione di sanzioni che possono arrivare fino ai 20 milioni di euro. Il marcato approccio volto alla responsabilizzazione del titolare del trattamento rende il meccanismo sanzionatorio del Regolamento un argomento molto delicato.

In particolare, le autorità di vigilanza dovranno seguire per ogni singolo caso determinati principi che conducano all'applicazione di una sanzione effettiva, proporzionata e dissuasiva. Tale valutazione deve essere condotta sulla base di parametri tra i quali la natura, la gravità e la durata della violazione, anche in considerazione del numero degli interessati e dei danni da questi subiti; il carattere intenzionale o colposo dell'infrazione; le azioni intraprese dal Titolare o dal Responsabile per mitigare i danni subiti dagli interessati.

Tuttavia, l'importo totale della sanzione non dovrà superare l'importo indicato per la violazione più grave in caso di più violazione connesse ad unico trattamento.

Il Regolamento prevede l'applicazione di sanzioni amministrative fino a 10 milioni di euro, o in caso di un'impresa, fino al 2% del fatturato totale annuo mondiale dell'esercizio precedente, se superiore, per specifici casi di violazione. Ad esempio, rilevano, in particolare, la violazione dei principi di privacy by design e privacy by default o le regole sul consenso del minore.

Mentre, per le violazioni in materia di principi base del trattamento, condizioni per il consenso, diritti degli interessati, trasferimento di dati personali all'estero, mancata ottemperanza a un ordine o a una limitazione temporanea o definitiva del trattamento disposti dall'autorità di vigilanza le sanzioni amministrative sono applicabili fino a 20 milioni di euro, o in caso di un'impresa, fino al 4% del fatturato totale annuo mondiale dell'esercizio precedente, se superiore.

13. Adempimenti: cosa è necessario fare e cosa non è più richiesto dal Regolamento

Non è possibile individuare in linea generale quali adempimenti siano richiesti ad un titolare: il principio di responsabilizzazione comporta che spesso sia il titolare stesso a dover decidere se svolgere determinate attività ai fini di assicurare il rispetto delle regole previste dal Regolamento.

Per quanto riguarda la governance occorrerà definire – anche attraverso la delega di funzioni - ruoli e responsabilità per la protezione dei dati all'interno dell'organizzazione aziendale. Occorrerà, in particolare, valutare la obbligatorietà o meno della nomina di un DPO, regolare contrattualmente i rapporti con gli eventuali contitolari, rivedere i criteri di selezione adottati per la nomina dei Responsabili del trattamento, sulla base dei criteri indicati dal Regolamento, e rivedere i contratti in essere, anche con riguardo alla eventuale nomina di sub-responsabili.

Occorrerà inoltre procedere alla predisposizione del registro dei trattamenti sulla base delle regole stabilite dal Regolamento.

In materia di consenso, sarà necessario rivedere ed integrare le Informative Privacy in conformità alle nuove prescrizioni del Regolamento nonché verificare che i consensi eventualmente già acquisiti riflettano i requisiti prescritti dal Regolamento e, in caso negativo, procedere alla acquisizione di un nuovo consenso.

Riguardo la valutazione d'impatto e la gestione di eventuali *data breach*, sarà opportuno sviluppare una procedura interna che disciplini i meccanismi di attivazione di una DPIA identificando in modo specifico ruoli e responsabilità nella effettuazione di una DPIA, sia con riguardo ai soggetti interni (funzioni aziendali coinvolte, DPO), sia con riguardo ai soggetti esterni (responsabili e consulenti). Inoltre, è consigliabile disporre di procedure interne per dare esecuzione agli obblighi di notificazione previsti in caso di *data breach*, predisponendo ad esempio un *incident response plan*.

Occorrerà inoltre rivedere le misure di sicurezza tecniche e organizzative, sulla base del livello di rischio, tenendo in considerazione stato dell'arte e costi di attuazione; natura, oggetto, contesto e finalità del trattamento; il rischio di violazione di diritti e libertà delle persone fisiche. Valutare la possibilità di utilizzare l'adesione ai codici di condotta o schemi di certificazione - che saranno emanati - per attestare l'adeguatezza delle misure di sicurezza adottate rispetto al livello di rischio.

Inoltre, al fine di garantire i diritti degli interessati, bisognerà predisporre procedure interne che garantiscano che i diritti degli interessati possano essere soddisfatti nei termini previsti dal Regolamento.

Attività di particolare rilievo ai fini del rispetto degli obblighi del Regolamento consisterà nel monitoraggio costante delle proprie attività di trattamento al fine di poter assicurare un costante aggiornamento dei meccanismi interni di *compliance*.

Sparisce, invece, l'obbligo di notifica dei trattamenti al Garante previsto dal Codice Privacy in Italia.