Trattamento di dati sensibili

Informatica Giuridica
Università degli Studi di Milano (UNIMI)
34 pag.

TRATTAMENTO DI DATI SENSIBILI

Sommario

INTRODUZIONE STORICA

Prima di una specifica normativa, l'unica tutela era fornita dalla giurisprudenza della Suprema Corte di Cassazione; per rispettare gli Accordi di Schengen e per dare attuazione alla direttiva dell'Unione Europea 95/46/CE del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali venne emanata la legge 31 dicembre 1996 n. 675, che entrò in vigore nel maggio 1997.

Col passare del tempo, a tale norma si erano affiancate ulteriori leggi, riguardanti singoli e specifici aspetti del trattamento dei dati. La sopravvenuta complessità normativa creatasi in seguito all'approvazione di diverse disposizioni portò all'emanazione del d.lgs. 30 giugno 2003, n. 196 che ha riordinato interamente la materia. Nel 2011 e 2012 altre disposizioni hanno emendato il codice del 2003, in particolare abolendo alcuni passaggi burocratici (tipo il DPS) oppure le regole per le informazioni sensibili fornite spontaneamente mediante il proprio CV.

In data 25 gennaio 2012 la Commissione Europea ha approvato la proposta di un regolamento sulla protezione dei dati personali,[5] in sostituzione della direttiva 95/46/CE. Il 4 maggio 2016 è stato poi emanato il regolamento dell'Unione Europea n. 2016/679 (direttamente applicabile senza necessità di una legge di trasposizione), la cui entrata in vigore definitiva è avvenuta il 25 maggio 2018.

Warren e Brandeis: diritto di essere lasciati in pace, la privacy nasce come modo di intendere la libertà, di limitare l'ingresso nello spazio altrui.
Quindi per:
Borghesia: evitare scandali e diffusione di informazioni riservate riguardanti la vita privata
Cittadino: diritto a mantenere la riservatezza su aspetti sensibili della propria vita privata (religione, politica, salute) per evitare discriminazione.

PRINCIPI

Il GDPR delinea sei principi della protezione dei dati personali:
Liceità, correttezza e trasparenza. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
Limitazione della finalità. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali.

Minimizzazione dei dati. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
Esattezza. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
Limitazione della conservazione. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato.
Integrità e riservatezza. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

TITOLARE, RESPONSABILE E ISTITUTO

Il TITOLARE DEL TRATTAMENTO è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

Il RESPONSABILE DEL TRATTAMENTO è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

L'INCARICATO è Il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri;

Il DESTINATARIO è la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
Il TERZO è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

I CONTITOLARI Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento. Essi determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.

IL TRATTAMENTO

Il TRATTAMENTO è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

In base a che dati trattiamo possiamo avere diversi modi di trattare i dati:

- **Trattamento di categorie particolari di dati personali.** È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Trattamento dei dati personali a condanne penale e reati.** Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.
- **Trattamento di dati pseudonimizzati.** il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
    - **Considerando 26:** Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe

prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici.

- **Trattamento di dati anonimi.**
  - **Considerando 26:** I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca.
- **Trattamento "domestico".** Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.

IL CONSENSO E LE CONDIZIONI DI LICEITA'

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

Qualora il trattamento sia basato sul consenso, il titolare del **trattamento deve essere in grado di dimostrare** che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante.

L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto.

Il **trattamento è lecito** solo se nella misura in cui è attuato ricorre almeno una delle seguenti condizioni:

- l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
- il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica;
- il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
- il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore.

L'INFORMATIVA – art. 13

1. In caso di raccolta presso l'interessato di dati che lo riguardano, il titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti informazioni:
    a. L'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
    b. I dati di contatto del responsabile della protezione dei dati, ove applicabile;
    c. Le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
    d. Qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
    e. Gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
    f. Ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili.

2. In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente:
    a. Il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;

b. L'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
c. Qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
d. Il diritto di proporre reclamo a un'autorità di controllo;
e. Se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
f. L'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Il Titolare ha già predisposto delle informative. Queste devono essere rese prima del trattamento. Il canale e-mail appare preferibile, in quanto è tracciato, ma possono essere rese in via cartacea. Il consenso deve essere raccolto dopo l'informativa e ne deve essere tenuta evidenza documentale.

DPIA

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.

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.

L'inosservanza dei requisiti stabiliti per la valutazione d'impatto sulla protezione dei dati può portare a sanzioni pecuniarie imposte dall'autorità di controllo competente.
Non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Infatti, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

Il regolamento generale sulla protezione dei dati prevede che i titolari del trattamento attuino misure adeguate a 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".

Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "gestione dei rischi", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.
Una valutazione d'impatto sulla protezione dei dati può riguardare una singola operazione di trattamento dei dati. Si potrebbe ricorrere a una singola valutazione d'impatto sulla protezione dei dati nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. Questo potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Ciò può essere applicabile anche a trattamenti simili attuati da vari titolari del trattamento di dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile una valutazione d'impatto sulla protezione dei dati di riferimento, attuare le misure descritte nella stessa, e fornire una giustificazione per la realizzazione di una singola valutazione d'impatto sulla protezione dei dati. Qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti o divulgare vulnerabilità.
Una valutazione d'impatto sulla protezione dei dati può essere altresì utile per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico.
Fatti salvi i casi in cui un trattamento rientra nel campo di applicazione di un'eccezione (III.B.a), è necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento "possa presentare un rischio elevato" (III.B.b).
Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, il WP29 raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.
L'articolo 35, paragrafo 3, fornisce alcuni esempi di casi nei quali un trattamento "possa presentare rischi elevati":

- 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;
- 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
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".

Questo va inteso come un elenco non esaustivo. Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati.

Al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio elevato intrinseco, tenendo conto degli elementi particolari di cui all'articolo 35, paragrafo 1 e all'articolo 35, paragrafo 3, lettere da a) a c), l'elenco da adottare a livello nazionale ai sensi

dell'articolo 35, paragrafo 4, e dei considerando 71, 75 e 91, e di altri riferimenti del regolamento generale sulla protezione dei dati a trattamenti che "possono presentare un rischio elevato"14, si devono considerare i seguenti nove criteri.

1. Valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "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. processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a))
3. monitoraggio sistematico: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c))
4. dati sensibili o dati aventi carattere altamente personale: questo criterio include categorie particolari di dati personali così come definite all'articolo 9, nonché dati personali relativi a condanne penali o reati di cui all'articolo 10.
5. trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:
    a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
    b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
    c. la durata, ovvero la persistenza, dell'attività di trattamento;
    d. la portata geografica dell'attività di trattamento;
6. creazione di corrispondenze o combinazione di insiemi di dati;
7. dati relativi a interessati vulnerabili (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;
8. uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e

91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone.

9. quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto" (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto.

Nella maggior parte dei casi, un titolare del trattamento può considerare che un trattamento che soddisfi due criteri debba formare oggetto di una valutazione d'impatto sulla protezione dei dati. Tuttavia, in alcuni casi, un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.

Un trattamento può essere comunque considerato dal titolare del trattamento un trattamento tale da non "presentare un rischio elevato". In tali casi il titolare del trattamento deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati, nonché includere/registrare i punti di vista del responsabile della protezione dei dati.

Il WP29 ritiene che una valutazione d'impatto sulla protezione dei dati non sia richiesta nei seguenti casi:

- quando il trattamento non è tale da "presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1);
- quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 119);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate (cfr. III.C);
- qualora un trattamento, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi una base giuridica nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10), a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;
- qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5). Tale

elenco può contenere attività di trattamento conformi alle condizioni specificate da detta autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (ad esempio in Francia, autorizzazioni, esenzioni, norme semplificate, pacchetti di conformità, ecc.). In tali casi e a condizione che venga eseguita una nuova valutazione da parte dell'autorità di controllo competente, non è richiesta una valutazione d'impatto sulla protezione dei dati, ma soltanto se il trattamento rientra a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco e continua a rispettare pienamente tutti i requisiti pertinenti del regolamento generale sulla protezione dei dati.

L'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati si applica alle operazioni di trattamento esistenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per le quali vi è stata una variazione dei rischi, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. Secondo le buone prassi, una valutazione d'impatto sulla protezione dei dati va riesaminata continuamente e rivalutata con regolarità. La valutazione d'impatto sulla protezione dei dati va effettuata "prima del trattamento" (articolo 35, paragrafi 1 e 10, considerando 90 e 93). Ciò è coerente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (articolo 25 e considerando 78). La valutazione d'impatto sulla protezione dei dati va considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento. Al titolare del trattamento spetta assicurare che la valutazione d'impatto sulla protezione dei dati sia eseguita (articolo 35, paragrafo 2). Inoltre, il titolare del trattamento deve consultarsi con il responsabile della protezione dei dati (RPD), quest'ultimo deve assistere il titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati.
Il titolare del trattamento deve "raccoglie[re] le opinioni degli interessati o dei loro rappresentanti" (articolo 35, paragrafo 9), "se del caso". Spetta al titolare del trattamento scegliere una metodologia che, comunque, deve essere conforme ai criteri di cui all'allegato 2.
La pubblicazione di una valutazione d'impatto sulla protezione dei dati non è un requisito giuridico sancito dal regolamento generale sulla protezione dei dati, è una decisione dei titolari del trattamento procedere in tal senso. Tuttavia, i titolari del trattamento dovrebbero prendere 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.
Ogniqualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo.

Le valutazioni d'impatto sulla protezione dei dati sono uno strumento utile di cui dispongono i titolari del trattamento per attuare sistemi di trattamento dei dati conformi al regolamento generale sulla protezione dei dati e possono essere obbligatorie per talune tipologie di trattamenti. Hanno natura modulabile e possono assumere forme diverse, tuttavia il regolamento generale sulla protezione dei dati stabilisce i requisiti essenziali di

una valutazione d'impatto sulla protezione dei dati efficace. I titolari del trattamento dovrebbero considerare la realizzazione di una valutazione d'impatto sulla protezione dei dati come un'attività utile e positiva che contribuisce alla conformità giuridica.

L'articolo 24, paragrafo 1, definisce la responsabilità fondamentale del titolare del trattamento in termini di rispetto del regolamento generale sulla protezione dei dati: "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*".

La valutazione d'impatto sulla protezione dei dati è un aspetto fondamentale del rispetto del regolamento laddove si preveda di svolgere o si stia svolgendo un trattamento di dati soggetto a rischio elevato. Ciò significa che i titolari del trattamento dovrebbero utilizzare i criteri stabiliti nel presente documento per stabilire se devono realizzare una valutazione d'impatto sulla protezione dei dati o meno. La politica interna dei titolari del trattamento potrebbe estendere questo elenco andando oltre i requisiti giuridici sanciti dal regolamento generale sulla protezione dei dati. Ciò dovrebbe suscitare un maggior senso di fiducia e riservatezza negli interessati e in altri titolari del trattamento.
Qualora si preveda di effettuare un trattamento che possa presentare un rischio elevato, il titolare del trattamento deve:

- scegliere una metodologia per la valutazione d'impatto sulla protezione dei dati (esempi riportati nell'allegato 1) che soddisfi i criteri di cui all'allegato 2, oppure specificare ed attuare un processo sistematico di valutazione d'impatto sulla protezione dei dati che:
    - sia conforme ai criteri di cui all'allegato 2;
    - sia integrata nei processi in materia di progettazione, sviluppo, cambiamento, rischio e riesame operativo in conformità con i processi, il contesto e la cultura interni;
    - coinvolga le parti interessate appropriate e definisca chiaramente le loro responsabilità (titolare del trattamento, responsabile della protezione dei dati, interessati o loro rappresentanti, imprese, servizi tecnici, responsabili del trattamento, responsabile della sicurezza dei sistemi d'informazione, ecc.);
- fornire la relazione relativa alla valutazione d'impatto sulla protezione dei dati all'autorità di controllo, laddove gli venga richiesto di procedere in tal senso;
- consultare l'autorità di controllo, qualora il titolare del trattamento non sia riuscito a determinare misure sufficienti per attenuare i rischi elevati;
- riesaminare periodicamente la valutazione d'impatto sulla protezione dei dati e il trattamento che essa valuta, almeno quando si registra una variazione del rischio posto dal trattamento;

- documentare le decisioni prese.

IL REGISTRO DEI TRATTAMENTI

Bisognerà mantenere aggiornati dei registri del trattamento (art 30 GDPR) contenenti:

a) *Il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;*
b) *Le finalità del trattamento;*
c) *una descrizione delle categorie di interessati e delle categorie di dati personali;*
d) *le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49 del GDPR, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati (attenzione non solo fascicolo sanitario);
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del GDPR.

In aggiunta:

- Verifica delle informative rese;
- Risultati dell'eventuale PIA;
- Verifica informative e consensi;

LE BRECCE NELLA SICUREZZA

Notifica di una violazione dei dati personali all'autorità di controllo (art 33)

1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.
2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
3. La notifica di cui al paragrafo 1 deve almeno:
    a. descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;

   b. comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
   c. descrivere le probabili conseguenze della violazione dei dati personali;
   d. descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.
4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.
5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo.

Comunicazione di una violazione dei dati personali all'interessato (art 34)

1. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.
2. La comunicazione all'interessato di cui al paragrafo 1 del presente articolo descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure di cui all'articolo 33, paragrafo 3, lettere b), c) e d).
3. Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni:
   a. il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
   b. il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1;
   c. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.
4. Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda o può decidere che una delle condizioni di cui al paragrafo 3 è soddisfatta.

IL GARANTE PRIVACY

Il **Garante per la protezione dei dati personali** è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice in materia di protezione dei dati personali (d.lg. 30 giugno 2003 n. 196), come modificato dal Decreto legislativo 10 agosto 2018, n. 101. Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51).

Art. 154-bis (Poteri) Oltre a quanto previsto da specifiche disposizioni, dalla Sezione II del Capo VI del Regolamento e dal presente codice, ai sensi dell'articolo 58, paragrafo 6, del Regolamento medesimo, il Garante ha il potere di:

- adottare linee guida di indirizzo riguardanti le misure organizzative e tecniche di attuazione dei principi del Regolamento, anche per singoli settori e in applicazione dei principi di cui all'articolo 25 del Regolamento; b) approvare le regole deontologiche di c)

Oltre a quanto previsto da specifiche disposizioni e dalla Sezione II del Capo VI del regolamento, il Garante, ai sensi dell'articolo 57, paragrafo 1, lettera v), del Regolamento medesimo, anche di propria iniziativa e avvalendosi dell'Ufficio, in conformità alla disciplina vigente e nei confronti di uno o più titolari del trattamento, ha il compito di:

a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico;
b) trattare i reclami presentati ai sensi del regolamento, e delle disposizioni del presente codice, anche individuando con proprio regolamento modalità specifiche per la trattazione, nonché fissando annualmente le priorità delle questioni emergenti dai reclami che potranno essere istruite nel corso dell'anno di riferimento;
c) promuovere l'adozione di regole deontologiche, nei casi di cui all'articolo 2- quater;
d) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni;
e) trasmettere la relazione, predisposta annualmente ai sensi dell'articolo 59 del Regolamento, al Parlamento e al Governo entro il 31 maggio dell'anno successivo a quello cui si riferisce;
f) assicurare la tutela dei diritti e delle libertà fondamentali degli individui dando idonea attuazione al Regolamento e al presente codice;
g) provvedere altresì all'espletamento dei compiti ad esso attribuiti dal diritto dell'Unione europea o dello Stato e svolgere le ulteriori funzioni previste dall'ordinamento.

Articolo 51 Autorità di controllo

1. Ogni Stato membro dispone che una o più autorità pubbliche indipendenti siano incaricate di sorvegliare l'applicazione del presente regolamento al fine di tutelare i diritti e le libertà fondamentali delle persone fisiche con riguardo al trattamento e di

agevolare la libera circolazione dei dati personali all'interno dell'Unione (l'«autorità di controllo»).
2. Ogni autorità di controllo contribuisce alla coerente applicazione del presente regolamento in tutta l'Unione. A tale scopo, le autorità di controllo cooperano tra loro e con la Commissione, conformemente al capo VII.
3. Qualora in uno Stato membro siano istituite più autorità di controllo, detto Stato membro designa l'autorità di controllo che rappresenta tali autorità nel comitato e stabilisce il meccanismo in base al quale le altre autorità si conformano alle norme relative al meccanismo di coerenza di cui all'articolo 63.
4. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del presente capo al più tardi entro 25 maggio 2018, e comunica senza ritardo ogni successiva modifica.

IL DPO

In base all'articolo 37, primo paragrafo, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici:

a) *se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;*
b) *Se le attività principali del titolare o del responsabile consistono in trattamenti che* ***richiedono il monitoraggio regolare e sistematico di interessati su larga scala****; oppure*
c) *Se le attività principali del titolare o del responsabile consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.*

Attività Principali

L'articolo 37, paragrafo 1, lettere b) e c) del RGPD contiene un riferimento alle "attività principali del titolare del trattamento o del responsabile del trattamento". Nel considerando 97 si afferma che le attività principali di un titolare del trattamento "riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria". Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare o dal responsabile del trattamento. Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare o dal responsabile. Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un RPD.

Larga Scala

- A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- Il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- Il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- **La durata, ovvero la persistenza, dell'attività di trattamento;**
- **La portata geografica dell'attività di trattamento**.

Regolare e sistematico

L'aggettivo **"regolare"** ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo **"sistematico"** ha almeno uno dei seguenti significati a giudizio del WP29:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

La funzione di DPO può essere esercitata anche in base a un **contratto di servizi stipulato con una persona fisica o giuridica esterna** all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che **ciascun soggetto appartenente alla persona giuridica e operante quale DPO soddisfi tutti i requisiti applicabili come fissati nella Sezione 4 del RGPD**; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi. Pari importanza riveste il fatto che ciascuno dei soggetti in questione godono delle tutele previste dal RGPD: per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto RPD, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di RPD.
Al contempo, si potranno associare le competenze e le capacità individuali affinché il contributo collettivo fornito da più soggetti consenta di rendere alla clientela un servizio più efficiente.
Per favorire una corretta e trasparente organizzazione interna, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del gruppo di lavoro RPD e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

Posizione

- Coinvolgimento del DPO in tutte le questioni riguardanti la protezione dei dati personali
- Risorse necessarie
- Istruzioni e "indipendenza della condotta"
- Rimozione o penalizzazioni in rapporto all'adempimento dei compiti

Compiti

- Sorvegliare l'osservanza GDPR
- Effettuare valutazione di impatto sulla protezione dei dati
- Mantenere del registro delle attività di trattamento

DIRITTO ALL'OBLIO

Art. 17 GDPR - Diritto alla cancellazione («diritto all'oblio»)

1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti:

a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;

b)l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c)l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;

d) i dati personali sono stati trattati illecitamente;

e) I dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;

f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.

Aspetti definitori

"Il diritto ad essere sé stessi" (cfr. Piraino Leto, 1990)

*"**il diritto a che fatti, pure pubblici, attinenti al soggetto, con il decorso del tempo cessino di avere tale qualità**" (Zencovich, 1986)*

"non si nega la possibilità di rendere pubbliche informazioni [...] ma solo che queste siano corrispondenti alla situazione concreta" (Corte Cost.13/1994)

"Si tutela identità-verità, anche senza violazione di privacy" (Ferri, 1981)

*Il concetto di oblio è **proprio dei modelli cognitivi**.*

*Il problema principale del diritto all'oblio consiste nell'esportate il concetto di oblio da un modello **tipicamente cognitivo** all'interno di un sistema **non cognitivo**, quale la Rete.*

PRIVACY BY DESIGN & DEFAULT

Necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.
Tutto questo deve avvenire a **monte, prima di procedere al trattamento dei dati vero e proprio** ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25 del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

LA PORTABILITÀ DEI DATI

1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:
   a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e

   b) il trattamento sia effettuato con mezzi automatizzati.
2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.
3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.
4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.

I DIRITTI

Cancellazione

Il titolare del trattamento potrebbe dover cancellare, previa richiesta, i dati personali in diverse ipotesi -ad esempio, nel caso in cui i dati non siano più necessari per la loro finalità originaria o allorché venga revocato il consenso al trattamento.

L'opposizione

- Gli individui godono del diritto di opporsi al trattamento basato su legittimi interessi (compresa la profilazione), marketing diretto, ricerca e statistiche.
- Se esercitata, questa richiesta deve essere rispettata, salvo il caso in cui l'organizzazione non dimostri l'esistenza di validi motivi che ne richiedono il proseguimento e che prevalgono sui diritti dei suddetti individui, ovvero nei casi in cui il trattamento si renda necessario per stabilire, esercitare o difendere un diritto legale.

Portabilità

Questo diritto consente agli interessati di ricevere i dati personali "in un formato strutturato, di uso comune e leggibile da dispositivo automatico" e di trasmettere i dati in quel formato a un altro titolare del trattamento.

La responsabilizzazione in azienda

Il Regolamento generale sulla protezione dei dati stabilisce un nuovo principio di responsabilizzazione, per cui il titolare del trattamento è tenuto a dimostrare la conformità con gli obblighi legali a proprio carico.

LA PROFILAZIONE

La profilazione è una qualsiasi forma di trattamento automatizzato di dati personali, consistente nell'utilizzo di tali dati 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.
Le decisioni automatizzate sono consentite nella misura necessaria alla conclusione o esecuzione di un contratto con l'individuo, ovvero nelle ipotesi previste dalla legge o sulla base del consenso esplicito dell'individuo.
Negli altri casi, sono necessari ulteriori controlli incrociati, ai fini di tutelare i diritti degli individui.

Cosa fare?

- *Analizzare le procedure lavorative in cui ci si avvale della profilazione.*
- *Garantire fondamenti giuridici adeguati a sostegno di una profilazione conforme alla legge.*
- *Rispettare i requisiti di trasmissione di informazioni relative all'uso di un processo decisionale automatizzato e, ove applicabile, introdurre l'intervento umano nel processo decisionale*

IL MONITORAGGIO A DISTANZA (VIDEOSORVEGLIANZA)

La raccolta, la registrazione, la conservazione e, in generale, l' utilizzo di immagini configura un trattamento di dati personali (*art. 4, comma 1, lett. b), del Codice*). È considerato dato

personale, infatti, qualunque informazione relativa a persona fisica identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione. L'utilizzo della videosorveglianza è atto per:

1. protezione e incolumità degli individui, ivi ricompresi i profili attinenti alla sicurezza urbana, all'ordine e sicurezza pubblica, alla prevenzione, accertamento o repressione dei reati svolti dai soggetti pubblici, alla razionalizzazione e miglioramento dei servizi volti al pubblico anche ad accrescere la sicurezza degli utenti, nel quadro delle competenze ad essi attribuite dalla legge;
2. protezione della proprietà;
3. rilevazione, prevenzione e controllo delle infrazioni svolti dai soggetti pubblici, nel quadro delle competenze ad essi attribuite dalla legge;
4. acquisizione di prove.

Per far uso di sistemi di sorveglianza bisogna attenersi a ciò che è scritto di seguito:

a) il trattamento dei dati attraverso sistemi di videosorveglianza sia fondato su uno dei presupposti di liceità che il Codice prevede espressamente per i soggetti pubblici da un lato (svolgimento di funzioni istituzionali: artt. 18-22 del Codice) e, dall'altro, per soggetti privati ed enti pubblici economici (es. adempimento ad un obbligo di legge, provvedimento del Garante di c.d. "bilanciamento di interessi" -v., in proposito, punto 6.2.- o consenso libero ed espresso: artt. 23-27 del Codice). Si tratta di presupposti operanti in settori diversi e che sono pertanto richiamati separatamente nei successivi paragrafi del presente provvedimento relativi, rispettivamente, all'ambito pubblico e a quello privato;
b) ciascun sistema informativo ed il relativo programma informatico vengano conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate impiegando solo dati anonimi (es., configurando il programma informatico in modo da consentire, per monitorare il traffico, solo riprese generali che escludano la possibilità di ingrandire le immagini e rendere identificabili le persone). Lo impone il principio di necessità, il quale comporta un obbligo di attenta configurazione di sistemi informativi e di programmi informatici per ridurre al minimo l'utilizzazione di dati personali (art. 3 del Codice);
c) l'attività di videosorveglianza venga effettuata nel rispetto del c.d. principio di proporzionalità nella scelta delle modalità di ripresa e dislocazione (es. tramite telecamere fisse o brandeggiabili, dotate o meno di zoom), nonché nelle varie fasi del trattamento che deve comportare, comunque, un trattamento di dati pertinenti e non eccedenti rispetto alle finalità perseguite (art. 11, comma 1, lett. d) del Codice).

L'installazione di sistemi di rilevazione delle immagini deve avvenire nel rispetto, oltre che della disciplina in materia di protezione dei dati personali, anche delle altre disposizioni dell'ordinamento applicabili, quali ad es. le vigenti norme dell'ordinamento civile e penale in materia di interferenze illecite nella vita privata, sul controllo a distanza dei lavoratori, in materia di sicurezza presso stadi e impianti sportivi, o con

riferimento a musei, biblioteche statali e archivi di Stato, in relazione ad impianti di ripresa sulle navi da passeggeri adibite a viaggi nazionali e, ancora, nell'ambito dei porti, delle stazioni ferroviarie, delle stazioni delle ferrovie metropolitane e nell'ambito delle linee di trasporto urbano.

Per utilizzare sistemi di videosorveglianza bisogna seguire alcuni punti:

- *Liceità e bilanciamento degli interessi*
- *Principio di necessità (e minimizzazione)*
- *Proporzionalità*
- *Valutazione d'impatto (art. 35 GDPR)*
- *Misure di sicurezza*
- *Nomina dei responsabili*
- *Informativa (minima ed estesa)*

Eccezioni?

- finalità di tutela dell'ordine e della sicurezza pubblica, prevenzione, accertamento o repressione dei reati;
- il trattamento deve comunque essere effettuato in base ad espressa disposizione di legge che lo preveda specificamente

Il supporto con l'informativa:

- deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;
- deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;
- può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate o anche registrate.

a. in presenza di differenti competenze specificatamente attribuite ai singoli operatori devono essere configurati diversi livelli di visibilità e trattamento delle immagini (v. punto 3.3.2). Laddove tecnicamente possibile, in base alle caratteristiche dei sistemi utilizzati, i già menzionati soggetti, designati incaricati o, eventualmente, responsabili del trattamento, devono essere in possesso di credenziali di autenticazione che permettano di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza;
b. laddove i sistemi siano configurati per la registrazione e successiva conservazione delle immagini rilevate, deve essere altresì attentamente limitata la possibilità, per i soggetti abilitati, di visionare non solo in sincronia con la ripresa, ma anche in tempo differito, le immagini registrate e di effettuare sulle medesime operazioni di cancellazione o duplicazione;

c. per quanto riguarda il periodo di conservazione delle immagini devono essere predisposte misure tecniche od organizzative per la cancellazione, anche in forma automatica, delle registrazioni, allo scadere del termine previsto (v. punto 3.4.);
d. nel caso di interventi derivanti da esigenze di manutenzione, occorre adottare specifiche cautele; in particolare, i soggetti preposti alle già menzionate operazioni possono accedere alle immagini solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche ed in presenza dei soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini;
e. qualora si utilizzino apparati di ripresa digitali connessi a reti informatiche, gli apparati medesimi devono essere protetti contro i rischi di accesso abusivo di cui all'art. 615-ter del Codice penale;
f. la trasmissione tramite una rete pubblica di comunicazioni di immagini riprese da apparati di videosorveglianza deve essere effettuata previa applicazione di tecniche crittografiche che ne garantiscano la riservatezza; le stesse cautele sono richieste per la trasmissione di immagini da punti di ripresa dotati di connessioni wireless (tecnologie Wi-Fi, wi-max, Gprs).

Esclusione dell'applicazione del GDPR

Il RGPD non è applicabile alle fotocamere false (vale a dire a qualsiasi fotocamera che non funziona come una fotocamera e quindi non elabora alcun dato personale). Tuttavia, in alcuni Stati membri potrebbero essere applicabili altre normative.

Le registrazioni ad alta quota rientrano nell'ambito di applicazione del RGPD solo se, in queste circostanze, i dati trattati possono essere correlati a una determinata persona.

Una videocamera è integrata in un'automobile per fornire assistenza al parcheggio. Se la videocamera è costruita o regolata in modo tale da non raccogliere alcuna informazione relativa a persona fisica, il RGPD non è applicabile.

Per documentare le sue vacanze, un turista registra video sia con il suo cellulare sia con una videocamera. Mostra il filmato ad amici e familiari, ma non lo rende accessibile a un numero indefinito di persone. Questo caso rientrerebbe nella deroga relativa alle attività a carattere domestico.

Una ciclista in mountain bike vuole registrare il suo percorso in discesa con una telecamera sportiva. Attraversa una zona isolata e prevede di utilizzare le registrazioni solo per intrattenimento personale e nel suo domicilio. Questo caso rientrerebbe nella deroga relativa alle attività a carattere domestico anche se vi fosse in una certa misura un trattamento di dati personali.

Qualcuno sorveglia e registra il proprio giardino. La proprietà è recintata e soltanto il titolare del trattamento e la sua famiglia entrano regolarmente in giardino. Questo caso rientrerebbe nella deroga relativa alle attività a carattere domestico, a condizione che la videosorveglianza non si estenda, neppure parzialmente, a uno spazio pubblico o a una

proprietà confinanti.

Il legittimo interesse deve essere esistente e attuale

Un negoziante vuole aprire un nuovo esercizio commerciale e installare un sistema di videosorveglianza per prevenire atti vandalici. Può dimostrare, presentando delle statistiche, che nel quartiere è alta la probabilità di eventi vandalici. È utile anche l'esperienza degli esercizi commerciali posti in prossimità. Non è necessario che il titolare del trattamento in questione abbia subito un danno. Nella misura in cui dai danni subiti nel quartiere emerga una situazione di pericolo o comunque analoga, può esservi un'indicazione dell'esistenza di un legittimo interesse. Tuttavia, non è sufficiente presentare statistiche nazionali o generali sulla criminalità senza analizzare l'area in questione o i pericoli per lo specifico esercizio commerciale.

Necessità del trattamento

Una libreria vuole proteggere la propria sede contro atti di vandalismo. In linea generale, le telecamere dovrebbero riprendere soltanto i locali in senso stretto; non è infatti necessario sorvegliare i locali adiacenti o le zone pubbliche circostanti la sede della libreria per tale scopo.

Bilanciamento degli interessi

Una società che gestisce un parcheggio privato ha registrato problemi ricorrenti di furti nelle auto parcheggiate. Il parcheggio è uno spazio aperto e facilmente accessibile da chiunque, ma è chiaramente contrassegnato con cartelli e dissuasori che circondano l'area interessata. La società di parcheggio ha un legittimo interesse (prevenire i furti nelle auto dei clienti a monitorare l'area durante le ore del giorno in cui si verificano problemi. Gli interessati sono sorvegliati per un arco di tempo limitato, non si trovano nella zona per scopi ricreativi ed è anche nel loro interesse prevenire i furti. In questo caso, sull'interesse degli interessati a non essere sottoposti a monitoraggio prevale il legittimo interesse del titolare del trattamento.

Un ristorante decide di installare videocamere nei bagni per controllare la pulizia dei servizi igienici. In questo caso i diritti degli interessati prevalgono chiaramente sull'interesse del titolare del trattamento; pertanto, le telecamere non possono essere installate.

Se è installata una telecamera da cruscotto (dash cam) – ad esempio, allo scopo di raccogliere prove in caso di incidente – è importante assicurarsi che la telecamera non registri costantemente il traffico, così come le persone che si trovano vicino a una strada. In caso contrario, l'interesse ad avere le videoregistrazioni come elemento di prova ipotetico di un incidente stradale non può giustificare questa grave interferenza nei diritti degli interessati.

Nei servizi igienici gli interessati si aspettano di non essere sorvegliati. La videosorveglianza, ad esempio, per prevenire incidenti non è uno strumento proporzionato.

Consenso

Gli atleti possono chiedere di essere monitorati durante gli esercizi individuali al fine di analizzare tecniche e prestazioni. D'altra parte, quando una società sportiva prende l'iniziativa di monitorare un'intera squadra per la stessa finalità. Il consenso spesso non sarà valido, in quanto i singoli atleti possono sentirsi costretti a prestare il proprio consenso per evitare che un loro eventuale rifiuto si ripercuota negativamente sui compagni di squadra.

Dati particolari

Si potrebbero, ad esempio, dedurre le opinioni politiche da immagini che mostrano interessati identificabili mentre partecipano a un evento, a uno sciopero, ecc. Questo caso rientrerebbe nell'ambito di applicazione dell'articolo 9.

Un ospedale che installa una videocamera per monitorare le condizioni di salute di un paziente effettua un trattamento di categorie particolari di dati personali (art. 9).

Un datore di lavoro non deve utilizzare registrazioni di videosorveglianza che mostrano una manifestazione al fine di identificare scioperanti.

Trattamento dei dati biometrici

Per migliorare il servizio, un'impresa privata sostituisce i posti di controllo per l'identificazione dei passeggeri all'interno di un aeroporto (consegna bagagli, imbarco) con sistemi di videosorveglianza che utilizzano tecniche di riconoscimento facciale per verificare l'identità dei passeggeri che hanno scelto di acconsentire a tale procedura. Poiché il trattamento rientra nel campo di applicazione dell'articolo 9, i passeggeri che avranno precedentemente prestato il consenso esplicito e informato dovranno registrarsi, ad esempio, presso un terminale automatico per creare e registrare il rispettivo modello facciale associato alla carta d'imbarco e al documento d'identità. I posti di controllo con riconoscimento facciale devono essere mantenuti chiaramente separati: ad esempio, il sistema deve essere installato all'interno di un varco di sicurezza, in modo da non acquisire i modelli biometrici delle persone che non hanno prestato il consenso. Solo i passeggeri che avranno preventivamente prestato il loro consenso e proceduto alla registrazione utilizzeranno il varco dotato del sistema biometrico.

Un titolare del trattamento gestisce l'accesso al proprio edificio utilizzando un metodo di riconoscimento facciale. L'utilizzo di questa modalità di accesso è possibile solo se gli interessati hanno preventivamente prestato il loro consenso informato ed esplicito (ai sensi dell'articolo 9, paragrafo 2, lettera a)). Tuttavia, al fine di garantire che non vengano acquisiti i dati di coloro che non abbiano precedentemente prestato il consenso, il riconoscimento facciale dovrebbe essere attivato dall'interessato stesso, ad esempio

premendo un pulsante. Per assicurare la liceità del trattamento, il titolare deve sempre offrire una modalità alternativa di accesso all'edificio senza trattamento biometrico, ad esempio tramite badge o chiavi.

Il proprietario di un esercizio commerciale vorrebbe personalizzare la propria pubblicità in base al genere e all'età dei clienti, acquisendo tali caratteristiche attraverso un sistema di videosorveglianza. Se tale sistema non genera modelli biometrici al fine di identificare in modo univoco le persone, ma semplicemente rileva tali caratteristiche fisiche al fine di classificare le persone, il trattamento non ricade nel campo di applicazione dell'articolo 9 (purché non siano trattate altre categorie particolari di dati).

Un negoziante ha installato un sistema di riconoscimento facciale all'interno del proprio negozio al fine di personalizzare la pubblicità rivolta ai clienti. Il titolare del trattamento deve ottenere il consenso esplicito e informato di tutti gli interessati prima di utilizzare questo sistema biometrico e trasmettere pubblicità personalizzata. Il sistema sarebbe illegale se acquisisse i dati dei visitatori o dei passanti che non hanno acconsentito alla creazione di un modello biometrico, anche se quest'ultimo venisse eliminato nel più breve tempo possibile. Infatti, questi modelli temporanei costituiscono dati biometrici trattati al fine di identificare in modo univoco una persona che potrebbe non voler ricevere pubblicità mirata.

Esercizio dei diritti degli interessati

Qualora l'interessato richieda una copia dei propri dati personali trattati mediante videosorveglianza all'ingresso di un centro commerciale con 30 000 visitatori al giorno, deve specificare quando ha acceduto alla zona monitorata indicando una finestra di circa un'ora. Se il titolare del trattamento stesse ancora trattando il materiale, dovrebbe fornirgli una copia del filmato. Se altri interessati possono essere identificati nello stesso materiale, allora quella parte del materiale deve essere anonimizzata (ad esempio sfocando la copia o parti di essa) prima che la copia sia consegnata all'interessato che ha presentato la richiesta.

Se il titolare del trattamento cancella automaticamente tutte le riprese, ad esempio entro due giorni, non sarà in grado di fornire le riprese all'interessato dopo tale lasso di tempo. Se il titolare del trattamento riceve una richiesta successivamente, l'interessato dovrebbe esserne informato di conseguenza.

Un minimarket ha subito atti vandalici, in particolare sull'esterno del negozio, e utilizza quindi la videosorveglianza al di fuori dell'entrata, con la telecamera che riprende l'area prossima alle pareti. Un passante chiede che vengano cancellati i suoi dati personali a partire da quel momento. Il titolare del trattamento è tenuto a rispondere alla richiesta senza ingiustificato ritardo e al più tardi entro un mese. Poiché il filmato in questione non soddisfa più lo scopo per il quale è stato inizialmente conservato (non si è verificato alcun atto vandalico durante il periodo in cui l'interessato è transitato nei pressi del negozio), al momento della richiesta non vi è alcun interesse legittimo a conservare i dati tale da

prevalere sugli interessi degli interessati. Il titolare del trattamento deve cancellare i dati personali.

Informativa

Un negoziante videosorveglia il suo esercizio commerciale. Ai fini del rispetto delle disposizioni dell'articolo 13, è sufficiente che collochi un cartello di avvertimento in un punto facilmente visibile all'ingresso dell'esercizio commerciale, contenente le informazioni di primo livello. Dovrà poi fornire le informazioni di secondo livello attraverso un foglio informativo disponibile presso la cassa o qualsiasi altro punto centrale e facilmente accessibile all'interno dell'esercizio.

Periodo di conservazione e obbligo di cancellazione

Normalmente, il titolare di un piccolo esercizio commerciale si accorgerebbe di eventuali atti vandalici il giorno stesso in cui si verificassero. Un periodo di conservazione di 24 ore è quindi sufficiente. La chiusura nei fine settimana o in periodi festivi più lunghi potrebbe tuttavia giustificare un periodo di conservazione più prolungato. Se viene rilevato un danno, può essere anche necessario conservare il filmato per un periodo più lungo al fine di intraprendere un'azione legale contro l'autore del reato.

I SEGRETI INDUSTRIALI

1. *Per segreti commerciali si intendono le informazioni aziendali e le esperienze tecnico-industriali, comprese quelle commerciali, soggette al legittimo controllo del detentore, ove tali informazioni:*
    a. *siano segrete, nel senso che non siano nel loro insieme o nella precisa configurazione e combinazione dei loro elementi generalmente note o facilmente accessibili agli esperti ed agli operatori del settore;*
    b. *abbiano valore economico in quanto segrete;*
    c. ***siano sottoposte, da parte delle persone al cui legittimo controllo sono soggette, a misure da ritenersi ragionevolmente adeguate a mantenerle segrete***
2. *Costituiscono altresì oggetto di protezione i dati relativi a prove o altri dati segreti, la cui elaborazione comporti un considerevole impegno ed alla cui presentazione sia subordinata l'autorizzazione dell'immissione in commercio di prodotti chimici, farmaceutici o agricoli implicanti l'uso di nuove sostanze chimiche.*

L'art. 99 cpi, a sua volta, prevede al comma 1) che ferma la disciplina della concorrenza sleale, il legittimo detentore dei segreti commerciali di cui all'articolo 98 cpi, ha il diritto di vietare ai terzi, salvo proprio consenso, di acquisire, rivelare a terzi od utilizzare, in modo abusivo, tali segreti, salvo il caso in cui essi siano stati conseguiti in modo indipendente dal terzo, mentre il comma 1-quater del medesimo articolo fissa un termine prescrizionale di cinque anni per i diritti e le azioni derivanti dalle condotte illecite di cui ai commi 1, 1-bis e 1-ter dell'art. 99 cpi.
L'art. 99 cpi, al comma 1-bis. introduce una importante novità: l'acquisizione, l'utilizzazione o la rivelazione dei segreti commerciali di cui all'articolo 98 si considerano illecite anche

quando il soggetto, al momento dell'acquisizione, dell'utilizzazione o della rivelazione, era a conoscenza o, secondo le circostanze, avrebbe dovuto essere a conoscenza del fatto che i segreti commerciali erano stati ottenuti direttamente o indirettamente da un terzo che li utilizzava o rivelava illecitamente ai sensi del comma 1.

Art 623 c.p.

*Il nuovo testo sanziona ora la condotta di "chiunque, venuto a cognizione per ragioni del suo stato o ufficio, o della sua professione o arte, di segreti commerciali o di notizie destinate a rimanere segrete, sopra scoperte o invenzioni scientifiche, li rivela o li impiega a proprio o altrui profitto", punendolo con **la reclusione fino a due anni**; il colpevole potrà essere punibile solo a seguito della **querela** della persona offesa. La stessa pena si applica altresì a "chiunque, avendo acquisito in modo abusivo segreti commerciali, li rivela o li impiega a proprio o altrui profitto". Il comma tre dell'art. in esame, tuttavia, prevede una curiosa aggravante "Se il fatto relativo ai segreti commerciali è commesso tramite qualsiasi strumento informatico la pena è aumentata".*

I CONTRATTI AD OGGETTO INFORMATICO

- ***contratti informatici*** *(termine generale, spesso riferito ai contratti conclusi mediante strumenti informatici),*
- ***contratti di informatica*** *(termine generale),*
- ***contratti ad oggetto informatico*** *(contratti aventi ad oggetto hardware, software, sistemi e servizi informatici).*
- *In origine:* ***contratti unitari*** *in cui il computer era il bene principale, mentre i programmi e i servizi di assistenza e manutenzione erano solo accessori (sistema bundling).*
- ***1969*** *– L'autorità antitrust americana impone ad IBM di commercializzare hardware e software separatamente.*
- *Contratto di sviluppo software*
- *Contratto di licenza software*
- *Contratto di manutenzione software*
- *...Ma anche*
- *T&C di social network*
- *Contratto ad oggetto cloud*
- *Contratto di sviluppo di APP*

DIRITTI DELLA PERSONALITÀ

Con il termine "diritti della personalità" si intendono quei diritti soggettivi ed assoluti volti a garantire le ragioni fondamentali della vita e dello sviluppo, fisico e morale, dell'esistenza della persona. Tali diritti si caratterizzano per non avere carattere patrimoniale, per essere inalienabili, intrasmissibili, irrinunziabili, imprescrittibili.

Diritto alla identità personale

diritto all'identità personale può essere definito ***come l'interesse di ogni persona a non vedere travisato o alterato all'esterno il proprio patrimonio intellettuale, politico, sociale, religioso, professionale, a causa dell'attribuzione di idee, opinioni, o comportamenti differenti da quelli che l'interessato ritenga propri e abbia manifestato nella vita di relazione.***

Diritto alla reputazione

*È possibile definire il concetto di reputazione quale "****la rappresentazione della personalità di un soggetto in una cerchia di consociati****" ().*
Secondo tale impostazione essa "viene lesa da quegli addebiti o quelle offese che colpiscono un rapporto di stima esistente o fanno sorgere un rapporto di disistima".

Altri diritti

Diritto al nome;
Diritto alla privacy ed alla riservatezza;
Diritto all'oblio;

DIRITTO D'AUTORE

Il **diritto d'autore** *è l'istituto giuridico che ha lo scopo di tutelare i frutti dell'attività intellettuale mediante il riconoscimento di una serie di diritti (di carattere morale e patrimoniale) all'autore originario dell'opera. L'esercizio in forma esclusiva di questi diritti da parte dell'autore permette di remunerarsi per un periodo limitato nel tempo attraverso lo sfruttamento commerciale dell'opera.*

Opere protette

Art. 1

Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione.
Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.
In particolare, sono comprese nella protezione:

1. *le opere letterarie, drammatiche, scientifiche, didattiche, religiose, tanto se in forma scritta quanto se orale;*
2. *le opere e le composizioni musicali, con o senza parole, le opere drammatico-musicali e le variazioni musicali costituenti di per sé opera originale;*
3. *le opere coreografiche e pantomimiche, delle quali sia fissata la traccia per iscritto o altrimenti;*
4. *le opere della scultura, della pittura, dell'arte del disegno, della incisione e delle arti figurative similari, compresa la scenografia (1)*

5. *i disegni e le opere dell'architettura;*
6. *le opere dell'arte cinematografica, muta o sonora, sempreché non si tratti di semplice documentazione protetta ai sensi delle norme del capo quinto del titolo secondo;*
7. *le opere fotografiche e quelle espresse con procedimento analogo a quello della fotografia sempre che non si tratti di semplice fotografia protetta ai sensi delle norme del capo V del titolo II;*
8. *i programmi per elaboratore, in qualsiasi forma espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso;*
9. *Le banche di dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto;*
10. *le opere del disegno industriale che presentino di per sé carattere creativo e valore artistico (2)*

Diritto morale d'autore

Il diritto morale d'autore nasce dal momento in cui l'opera creativa si manifesta. È una forma di diritto la cui durata di tempo è illimitata. All'autore contraente tale diritto spettano diritti inalienabili quali facoltà di rivendicare la ***paternità*** *dell'opera.*

Legge 22 aprile 1941 n. 633

Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione.
Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

> Art.2: *In particolare sono comprese nella protezione:1) le opere letterarie, drammatiche, scientifiche, didattiche, religiose, tanto se in forma scritta quanto se orale;2) le opere e le composizioni musicali, con o senza parole, le opere drammatico-musicali e le variazioni musicali costituenti di per sé opera originale;3) le opere coreografiche e pantomimiche, delle quali sia fissata la traccia per iscritto o altrimenti;4) le opere della scultura, della pittura, dell'arte del disegno, della incisione e delle arti figurative similari, compresa la scenografia;5) i disegni e le opere dell'architettura;6) le opere dell'arte cinematografica, muta o sonora, sempreché non si tratti di semplice documentazione protetta ai sensi delle norme del Capo V del Titolo II;7) le opere fotografiche e quelle espresse con procedimento analogo a quello della fotografia sempre che non si tratti di semplice fotografia protetta ai sensi delle norme del Capo V del Titolo II;8) i programmi per elaboratore, in qualsiasi forma*

espressi purché originali quale risultato di creazione intellettuale dell'autore. Restano esclusi dalla tutela accordata dalla presente legge le idee e i principi che stanno alla base di qualsiasi elemento di un programma, compresi quelli alla base delle sue interfacce. Il termine programma comprende anche il materiale preparatorio per la progettazione del programma stesso.9) le banche di dati di cui al secondo comma dell'articolo 1, intese come raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo. La tutela delle banche di dati non si estende al loro contenuto e lascia impregiudicati diritti esistenti su tale contenuto.10) Le opere del disegno industriale che presentino di per sé carattere creativo e valore artistico.

Le opere collettive, costituite dalla riunione di opere o di parti di opere, che hanno carattere di creazione autonoma, come risultato della scelta e del coordinamento ad un determinato fine letterario, scientifico didattico, religioso, politico od artistico, quali le enciclopedie, i dizionari, le antologie, le riviste e i giornali sono protette come opere originali, indipendentemente e senza pregiudizio dei diritti di autore sulle opere o sulle parti di opere di cui sono composte.
Senza pregiudizio dei diritti esistenti sull'opera originaria, sono altresì protette le elaborazioni di carattere creativo dell'opera stessa, quali le traduzioni in altra lingua, le trasformazioni da una in altra forma letteraria od artistica, le modificazioni ed aggiunte che costituiscono un rifacimento sostanziale dell'opera originaria, gli adattamenti, le riduzioni, i compendi, le variazioni non costituenti opera originale.

ALCUNI PROVVEDIMENTI DEL GARANTE

Il dipendente deconcentrato

- *Il dipendente lavora come centralinista presso la vostra azienda.*
- *I dirigenti lo sorprendono, più volte, a visitare siti a carattere pornografico.*
- *Numerosi computer vengono infettati da virus dopo aver ricevuto file dal computer del dipendente.*
- *L'amministratore delegato viene da voi, dicendo che vuole licenziarlo.*
- *Ha bisogno di prove: il dipendente, infatti ha negato ogni addebito.*

Per contestare l'indebito utilizzo di beni aziendali, (...) sarebbe stato in questo caso sufficiente verificare gli avvenuti accessi a Internet e i tempi di connessione senza indagare sui contenuti dei siti. Insomma, altri tipi di controlli sarebbero stati proporzionati rispetto alla verifica del comportamento del dipendente. (...) Va rilevato sotto altro profilo che non risulta che il ricorrente avesse necessità di accedere ad Internet per svolgere le proprie prestazioni. La resistente avrebbe potuto quindi dimostrare l'illiceità del suo comportamento in rapporto al corretto uso degli strumenti affidati sul luogo di lavoro limitandosi a provare in altro modo l'esistenza di accessi indebiti alla rete e i relativi tempi di collegamento. La società ha invece operato un trattamento diffuso di numerose altre informazioni indicative anche degli specifici "contenuti" degli accessi dei singoli siti web

visitati nel corso delle varie navigazioni, operando -in modo peraltro non trasparente- un trattamento di dati eccedente rispetto alle finalità perseguite".

(...)Per ciò che concerne il merito va rilevato che la società, (...) ha esperito dettagliati accertamenti in assenza di una previa informativa all'interessato relativa al trattamento dei dati personali, nonché in difformità dall'art. 11 del Codice nella parte in cui prevede che i dati siano trattati in modo lecito e secondo correttezza, nel rispetto dei principi di pertinenza e non eccedenza rispetto alle finalità perseguite.

l'Autorità dispone quindi, ai sensi dell'art. 150, comma 2, del Codice, quale misura a tutela dei diritti dell'interessato, **il divieto per la società resistente di trattare ulteriormente i dati personali raccolti nei modi contestati con il ricorso.**

Illecito spiare il contenuto della navigazione in internet del dipendente"

Il Garante: "L'uso indebito del computer può essere contestato senza indagare sui siti visitati" - (Comunicato stampa - 14 febbraio 2006)

Una corretta informativa

La casa di cura per ciechi Curas III. È stata sanzionata perché ha adottato una informativa completa, in quanto questa non era evidentemente visibile dagli ospiti.
Soluzione
«L'art. 12, par. 1, del Regolamento richiede, invece, che le informazioni di cui all'art. 13 siano rese in forma "trasparente, intelligibile e facilmente accessibile". Pertanto, allorquando il titolare del trattamento sia "consapevole che i suoi beni/servizi sono utilizzati da (o destinati ad) altri soggetti vulnerabili della società, tra cui persone con disabilità o persone che possono incontrare difficoltà ad accedere alle informazioni, [si dovrebbe] tenere conto delle vulnerabilità di tali interessati nella valutazione del modo in cui assolvere gli obblighi di trasparenza nei loro confronti. Ciò si ricollega alla necessità che il titolare del trattamento valuti il probabile livello di comprensione del proprio pubblico [...]" (Gruppo di Lavoro Articolo 29, "Linee guida sulla trasparenza ai sensi del regolamento 2016/679" dell'11 aprile 2018, WP260 rev.01, par. 16».

I GARANTI EUROPEI

Articolo 68 Comitato europeo per la protezione dei dati

1. Il comitato europeo per la protezione dei dati («comitato») è istituito quale organismo dell'Unione ed è dotato di personalità giuridica.
2. Il comitato è rappresentato dal suo presidente.
3. Il comitato è composto dalla figura di vertice di un'autorità di controllo per ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti.
4. Qualora, in uno Stato membro, più autorità di controllo siano incaricate di sorvegliare l'applicazione delle disposizioni del presente regolamento, è designato un rappresentante comune conformemente al diritto di tale Stato membro.

5. La Commissione ha il diritto di partecipare alle attività e alle riunioni del comitato senza diritto di voto. La Commissione designa un rappresentante. Il presidente del comitato comunica alla Commissione le attività del comitato.
6. Nei casi di cui all'articolo 65, il garante europeo della protezione dei dati ha diritto di voto solo per decisioni che riguardano principi e norme applicabili a istituzioni, organi, uffici e agenzie dell'Unione che corrispondono nella sostanza a quelli del presente regolamento.

Articolo 70 Compiti del comitato

Il comitato garantisce l'applicazione coerente del presente regolamento. A tal fine, il comitato, di propria iniziativa o, se del caso, su richiesta della Commissione, in particolare:
(...)
d) **pubblica linee guida, raccomandazioni e migliori prassi in materia di procedure** per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico di cui all'articolo 17, paragrafo 2;
e) esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del presente regolamento e pubblica linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del presente regolamento;
f) Fornisce alla Commissione **un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale**, così come per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione. A tal fine, la Commissione fornisce al comitato tutta la documentazione necessaria, inclusa la corrispondenza con il governo del paese terzo, con riguardo a tale paese terzo, territorio o settore specifico, o con l'organizzazione internazionale;