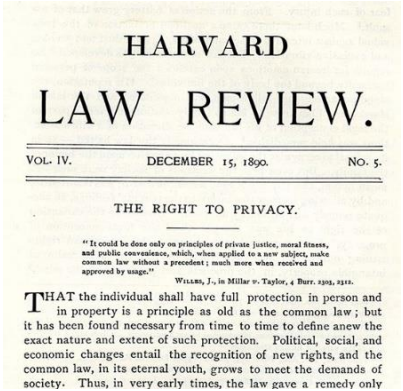
UNIVERSITÀ DEGLI STUDI DI SALERNO

UNISA D G

CONSIGLIO PROVINCIALE DELL'ORDINE DEI CONSULENTI DEL LAVORO DI SALERNO

Salerno 07/10/2025	XL Corso formativo per praticanti Consulenti del lavoro 2025
Docenti	Prof. avv. Giorgio Giannone Codiglione
Argomento	Privacy e tutela del lavoratore

Le origini del «Right to privacy»



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar v. Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only

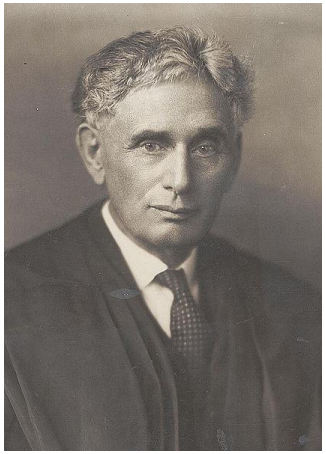
S. WARREN – L. BRANDEIS,
***The Right to Privacy*, 4 *Harvard L.R.* 193 (Dec. 15, 1890)**

"*The press is **overstepping in every direction the obvious bounds of propriety and of decency**. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. To satisfy a prurient taste the details of sexual relations are spread broadcast in the columns of the daily papers. To occupy the indolent, column upon column is filled with idle gossip, which can only be procured by **intrusion upon the domestic circle**".*

***Olmstead v. United States*, 277 U.S. 438 (1928)**

«*Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet*»

(La scoperta e l'invenzione hanno fornito al Governo mezzi molto più efficaci che origliare oltre gli scaffali, per rivelare in pubblico ciò che viene sussurrato in privato"

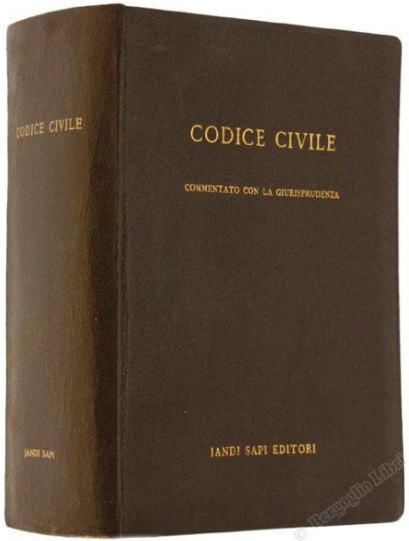


Libertà negativa

«Libertà come assenza di impedimento o di costrizione): situazione in cui un soggetto ha la possibilità di agire senza essere impedito, o di non agire senza essere costretto, da altri soggetti».

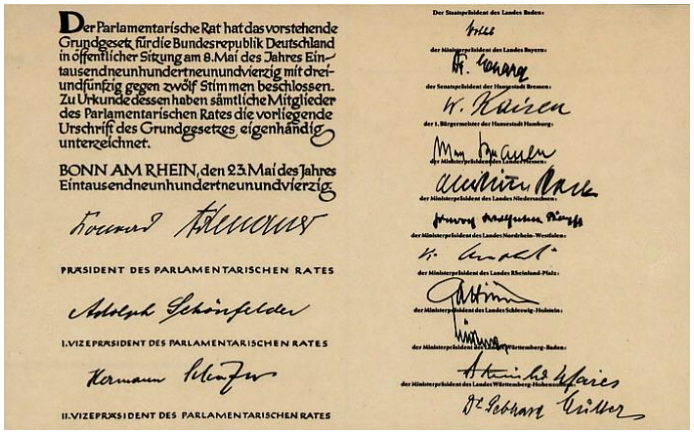
Il cammino europeo del diritto alla riservatezza

- Anche il cammino del diritto alla riservatezza nell'ordinamento europeo trova una prima base teorica nella protezione giuridica degli attributi della **personalità umana**.
- Nella Germania di fine secolo XIX, la dottrina formula il fondamentale dualismo tra i **diritti individuali o della personalità** – inalienabili e personalissimi – e i diritti sui c.d. **beni immateriali**, suscettibili di essere incorporati materialmente (ad es. attraverso la pubblicazione di un libro o la realizzazione di un ritratto o di una fotografia) e con ciò trasferibili.



- Queste tecniche di protezione non contemplavano espressamente la riservatezza come **diritto autonomo**, ma riconoscevano appunto la protezione di **taluni aspetti della personalità umana.**
- Ad esempio, il **Codice civile italiano** del 1942 tutela l'integrità fisica (art. 5), il nome (artt. 6, 7 e 8), lo pseudonimo (art. 9), l'immagine (art. 10 cod. civ. e artt. 96-98 l. n. 633/1941 sul diritto d'autore), come le prerogative morali dell'autore di un'opera dell'ingegno (art. 2577 cod. civ.).

- Neppure la **Carta costituzionale** del 1948 contiene un espresso riferimento alla riservatezza: l'art. 2 afferma che "*la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità*", mentre l'art. 15 tutela la **libertà e la segretezza della corrispondenza e delle comunicazioni** e gli artt. 13 e 14 affermano l'inviolabilità **libertà personale e del domicilio.**
- Analogamente, il ***Grundgesetz*** **tedesco** tutela la dignità umana (art. 1), la vita, l'integrità fisica e l'inviolabilità della libertà della persona (art. 2, par. 2) nonché il segreto della corrispondenza (art. 10) e l'inviolabilità del domicilio (art. 13).


Der Parlamentarische Rat hat das vorstehende Grundgesetz für die Bundesrepublik Deutschland in öffentlicher Sitzung am 8. Mai des Jahres Eintausendneunhundertneunundvierzig mit dreiundfünfzig gegen zwölf Stimmen beschlossen. Zu Urkunde dessen haben sämtliche Mitglieder des Parlamentarischen Rates die vorliegende Urschrift des Grundgesetzes eigenhändig unterzeichnet.

BONN AM RHEIN, den 23. Mai des Jahres Eintausendneunhundertneunundvierzig

PRÄSIDENT DES PARLAMENTARISCHEN RATES

I. VIZEPRÄSIDENT DES PARLAMENTARISCHEN RATES

II. VIZEPRÄSIDENT DES PARLAMENTARISCHEN RATES

- A livello normativo, un primo tentativo di positivizzazione del diritto alla riservatezza si registra con l'entrata in vigore del c.d. **Statuto dei lavoratori** (legge 20 maggio 1970, n. 300): nel pieno dell'espansione industriale, viene introdotta un'innovativa forma di tutela preventiva della privacy della classe operaia.
- Lo Statuto, tuttora in vigore con alcune modifiche, **consente l'impiego di impianti audiovisivi e altri strumenti di controllo a distanza dell'attività dei lavoratori esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, previo accordo sindacale** (art. 4).

- La l. n. 300/1970 vieta inoltre lo svolgimento di accertamenti sanitari da parte del datore di lavoro, indicando quali soggetti competenti i servizi ispettivi degli istituti previdenziali (art. 5), limita le visite personali di controllo sul lavoratore (art. 6) e impone il divieto "*di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore*" (art. 8).

Il Regolamento UE 2016/679 – *General Data Protection Regulation* (GDPR)

- La direttiva 95/46 è stata sostituita dal **25 maggio del 2018** dal Regolamento generale sulla protezione dei dati personali 2016/679/UE (*General Data Protection Regulation*, o GDPR)
- Diversamente dalla direttiva, il regolamento è un atto normativo di matrice comunitaria direttamente applicabile negli Stati membri (c.d. ***self executing***), non richiedendo in linea generale l'adozione di disposizioni attuative.

- Ad esempio, il legislatore italiano ha emanato il **d.lgs. n. 101/2018** con lo scopo di abrogare gli articoli del Codice privacy non conformi al GDPR e adeguare la normativa nazionale.

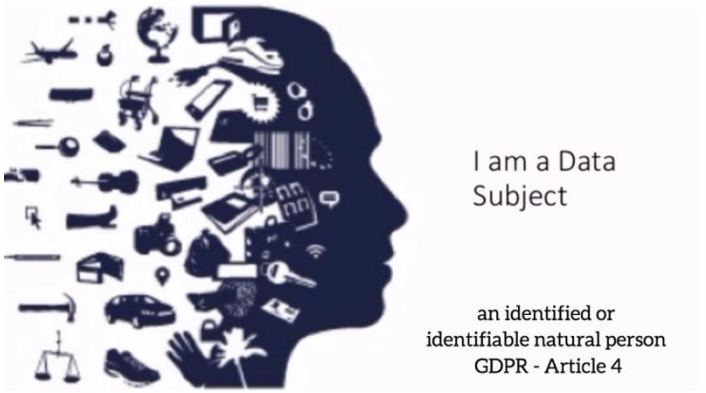
La nozione di «dato personale»

- Ai sensi dell'art. 4, n. 1) del GDPR per "dato personale" deve intendersi non soltanto **qualsiasi informazione concernente una persona fisica identificata o identificabile** (c.d. interessato), ma **tutto l'insieme delle informazioni relative a una persona fisica** come gli identificativi prodotti da dispositivi on line (indirizzo IP, cookies, ecc.) o quei dati che, sottoposti a procedimenti atti a nascondere le generalità dell'interessato (c.d. pseudonomizzazione), possano comunque essere oggetto di combinazione con ulteriori informazioni in modo da renderne possibile, direttamente o indirettamente, l'identificazione.

- Leggendo l'art. 4, n. 1) del GDPR si può osservare come vengano coperte per via normativa **tutte le forme di trattamento multiplo di dati** che conducono, anche astrattamente, all'**identificazione di una persona fisica**, con l'esclusione dei dati anonimi (ovvero le informazioni che non si riferiscono a una persona fisica identificata o identificabile) e dei dati personali trattati in maniera tale da impedire o da non consentire l'identificazione dell'interessato.

- La **forma** in cui i dati personali sono conservati o utilizzati non è rilevante ai fini dell'applicazione delle norme in materia di protezione dei dati. I dati personali possono essere inclusi in comunicazioni scritte o parlate, così come in immagini, incluse le riprese o i suoni di un sistema televisivo a circuito chiuso (CCTV).
- Le informazioni registrate in formato elettronico, così come le informazioni su carta, possono costituire dati personali. I dati biometrici, come le impronte digitali o finanche i campioni di cellule di tessuto umano, possono costituire dati personali, al pari del DNA di una persona.
- Le **informazioni generiche** riguardo alle retribuzioni in una determinata società non costituiscono dati personali. Tuttavia, se un singolo individuo è impiegato in una posizione determinata, le informazioni concernenti la retribuzione per quella specifica posizione lavorativa costituiscono dati personali relativi al dipendente che occupa tale posizione.

- Una persona si considera **identificabile** se un'informazione contiene elementi di identificazione attraverso i quali la persona può essere identificata direttamente o indirettamente. Conseguentemente, se il contenuto dell'informazione (alla quale non è associato un nominativo) rende possibile stabilire l'identità di una persona attraverso ulteriori ricerche, si potrà comunque trattare di dati personali.
- Un esempio tipico di dati personali sono i **numeri assegnati a ciascuna persona in molti Paesi.** Un altro esempio può essere il **nome** della persona, anche se spesso i nomi non sono unici e pertanto l'identificazione può richiedere ulteriori elementi identificativi coma la data e il luogo di nascita. In alcuni casi, altri elementi identificativi possono avere un effetto simile al nome. Ad esempio, per i personaggi pubblici, può essere sufficiente riferirsi alla loro posizione, come, ad esempio, "attuale Presidente della Commissione europea".



- In alcuni casi, **anche le bollette dei cellulari, gli indirizzi IP, i dati relativi all'ubicazione o le informazioni concernenti la condotta di una persona** possono costituire dati personali. Un'analisi individuale di ogni singolo caso specifico è spesso richiesta al fine di determinare se una certa informazione costituisca un dato personale. Come punto di partenza, è possibile prendere in considerazione i **mezzi** che sono a disposizione per l'identificazione e la **facilità** con cui la persona che intende procedere all'identificazione può ricorrere a tali mezzi.

- Applicare il parametro per l'identificabilità consiste nel valutare la probabilità che mezzi ragionevoli di identificazione siano a disposizione e utilizzabili dal responsabile del trattamento o da altri. La persona è identificabile solo se informazioni ulteriori possono essere ottenute senza sforzi irragionevoli (un irragionevole lasso di tempo, risorse umane, ecc...),permettendo l'identificazione dell'interessato. L'identificazione richiede elementi che descrivano una persona in modo tale che lei o lui sia distinguibile da tutte le altre persone e riconoscibile come individuo.

La nozione di «dato sensibile» nell'evoluzione normativa

- L'articolo 8, paragrafo 2 della direttiva 95/46/CE vietava, in linea di principio, il trattamento di categorie particolari di dati personali, ovvero q**uelle informazioni che rivelano un particolare e intimo aspetto della persona interessata o della propria vita** (l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici e i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona).
- Un'eccezione a questa regola si verificava qualora la persona interessata avesse prestato il proprio **consenso** esplicito al trattamento di dati sensibili (salvo nei casi in cui la legislazione dello Stato membro preveda che il consenso della persona interessata non sia sufficiente per derogare al divieto).
- Il trattamento di dati personali sensibili era altresì ammesso, ad esempio, quando: è necessario per assolvere gli obblighi e i diritti specifici del titolare del trattamento in materia di diritto del lavoro o è necessario per salvaguardare un interesse vitale della persona interessata o di un terzo nel caso in cui la persona interessata si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso.

- Norme simili sono contenute nel GDPR (articolo 9, paragrafo 2) che riproduce in gran parte le disposizioni della direttiva 95/46. L'art. 9 del GDPR impone infatti un **divieto generale di trattamento per particolari tipologie di dati personali.**
- Il divieto è temperato da alcune eccezioni:

  a) il consenso esplicito dell'interessato, fatta salva la revoca

  e, ancora le ipotesi in cui il trattamento sia necessario per:

  b) assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;

  c) tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;

  d) perseguire finalità politiche, filosofiche, religiose o sindacali da parte di una fondazione, associazione o altro organismo senza scopo di lucro;

  e) accertare, esercitare o difendere un diritto in sede giudiziaria;

  f) motivi di interesse pubblico rilevante;

  g) finalità di medicina preventiva o di medicina del lavoro;

  h) motivi di interesse pubblico nel settore della sanità pubblica;

  i) archiviare nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

I dati relativi a condanne penali e reati

- Si tratta dei dati c.d. "**giudiziari**", cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.
- Il GDPR (articolo 10) ricomprende in tale nozione i dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

La nozione di «trattamento»

- Per trattamento dei dati personali deve intendersi invece "***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*" [art. 4, n. 2)], con l'aggiunta della c.d. profilazione [art. 4, n. 4)] e dei c.d. trattamenti transfrontalieri, svolti in più paesi dell'Unione [art. 4, n. 23)].

- La **profilazione** rappresenta una tipologia di trattamento automatizzato di dati personali svolta per **valutare ai fini predittivi** un particolare aspetto di una persona fisica quali il rendimento professionale, la situazione economica, la salute, le preferenze, gli interessi, l'affidabilità, il comportamento o gli spostamenti.
- Il GDPR offre protezione avverso tutte le tecniche di **trattamento multiplo** di dati che conducono, anche in astratto, all'identificazione di una persona fisica, con **l'esclusione dei dati anonimi** (ovvero le informazioni che non si riferiscono a una persona fisica identificata o identificabile) e **dei dati personali trattati in maniera tale da impedire o da non consentire l'identificazione dell'interessato**.

La nozione di «interessato»

- In base al diritto dell'Unione, i beneficiari delle norme in materia di protezione dei dati sono, in linea di principio, le **persone fisiche**. Se i dati relativi a una persona fisica sono oggetto di trattamento, questa persona è chiamata "la persona interessata".
- In generale, le norme UE in materia di protezione dei dati non apprestano alcuna tutela per le persone giuridiche con riferimento al trattamento di dati che le riguardano. I legislatori nazionali sono tuttavia liberi di disciplinare tale aspetto.
- Parimenti, in base alla Convenzione n. 108, la protezione dei dati riguarda, principalmente, la tutela delle persone fisiche. Ciò nonostante, le parti contraenti possono estendere la tutela in materia di protezione dei dati anche alle persone giuridiche, come società commerciali e associazioni, nel proprio diritto interno (articolo 3.2(b) della Convenzione n. 108).
- Mentre il testo originario del Codice Privacy includeva nella definizione di dati personale "**qualunque informazione relativa a persona fisica, persona giuridica, ente o associazione**", con il D.L. n. 201/2011 l'Italia ha recepito il principio secondo cui **le imprese, gli enti e le associazioni non possono più essere considerati interessati al trattamento.**

I ruoli soggettivi

- **Titolare:** la persona fisica o giuridica che determina le finalità e i mezzi del trattamento di dati personali (sono qualificabili, ad es., come titolare la società, l'associazione professionale, l'avvocato, il commercialista, la fondazione, il consiglio dell'ordine, ecc.).
- **Contitolare**: l'art. 26 del GDPR prevede che in ogni caso in cui le **finalità ed i mezzi del trattamento vengano determinati congiuntamente** da parte di più titolari, potrà essere nominato uno o più "contitolare/i" del trattamento: il rapporto interno tra contitolari deve essere disciplinato da apposito accordo.
- **Responsabile**: la persona fisica o giuridica che tratta dati personali per conto del Titolare del trattamento. La nomina del Responsabile del trattamento deve avvenire con apposito atto scritto, contratto, o comunque per clausole tipizzate, e deve contenere gli elementi individuati dall'art. 28 del GDPR e tassativamente almeno le materie riportate al paragrafo 3 della medesima disposizione, al fine di dimostrare che il responsabile fornisce "garanzie sufficienti" – quali, in particolare, la natura, durata e finalità del trattamento o dei trattamenti assegnati, e categorie di dati oggetto di trattamento; le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel GDPR.
- Il Titolare e il Responsabile possono avvalersi **di persone autorizzate "*al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*"** e secondo le finalità e le istruzioni da essi impartite.

Il sub-responsabile del trattamento

2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.

Il dipendente: inquadramento ai sensi di GDPR e del Codice privacy

- Il GDPR e il Codice privacy prevedono la possibilità per il Titolare e per il Responsabile di avvalersi di persone autorizzate "*al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile*".
- Ci si riferisce a categorie di soggetti interni, che ben potrebbero figurare nell'organigramma come dipendenti e collaboratori, i quali sono tenuti ad eseguire le operazioni di trattamento secondo le finalità e le istruzioni impartite, ad assicurarsi che l'esecuzione delle operazioni di trattamento avvenga nel pieno rispetto dei principi generali del GDPR e ad adottare tutte le cautele necessarie ad evitare rischi di violazioni di dati (pertanto, anche nel caso di *data breach*).
- Il Titolare e il Responsabile devono preoccuparsi anche di formare ciclicamente le persone autorizzate sul GDPR.

Art. 29 GDPR

Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento

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

Art. 2-*quaterdecies* dCodice privacy

(Attribuzione di funzioni e compiti a soggetti designati)

1. Il titolare o il responsabile del trattamento possono prevedere**, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.**
2. Il titolare o il responsabile del trattamento **individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.**

I principi generali
in materia di trattamento dei dati personali

- Secondo i **principi generali** del GDPR (art. 5), i dati personali devono essere:

a) trattati in modo lecito, corretto e trasparente;
b) raccolti per finalità determinate, esplicite e legittime e trattati in maniera compatibile con queste ultime;
c) adeguati ed esatti;
d) conservati in modo tale da rendere identificabile l'interessato solo per il lasso di tempo necessario ai fini del perseguimento delle finalità, eccetto nelle ipotesi di conservazione per interesse pubblico, scientifico, storico o statistico;
e) trattati in maniera sicura.

La c.d. *Accountability* (Responsabilizzazione) del titolare o del responsabile del trattamento

- Il titolare del trattamento è chiamato a dare prova in ogni momento dell'adempimento di tali obblighi, in virtù del principio di responsabilizzazione o *accountability*.
- La responsabilizzazione richiede **l'adozione attiva di misure da parte dei titolari del trattamento dei dati** per la promozione e la salvaguardia della protezione dei dati nel corso delle loro attività di trattamento.
- Esempi di tali nuove misure sono:

1) L'obbligo di tenuta del **registro dei trattamenti** (+ 250 dipendenti, trattamenti rischiosi per i diritti e la libertà dell'interessato, non occasionale e avente come oggetto particolari tipologie di dati);
2) Obbligo di designazione del **Responsabile della protezione dei dati personali** (v. *infra*).

- I titolari del trattamento **sono responsabili per e devono essere in grado di provare in ogni momento l'osservanza dei principi in materia di protezione dei dati alle persone interessate, al pubblico in generale e alle autorità di controllo.**
- Il GDPR stabilisce inoltre nuovi obblighi in termini di responsabilizzazione che richiedono altresì l'adozione di **nuove significative misure di carattere tecnico e organizzativo per dimostrare il rispetto del GDPR.**

Il principio del trattamento lecito

- Nella normativa in materia di protezione dei dati nell'ambito dell'UE e del CoE, il principio del trattamento lecito è il primo principio a essere nominato; esso è espresso in modo pressoché identico nell'articolo 5 della Convenzione n. 108 del CoE e nell'articolo 5 del GDPR.
- Non esiste una definizione precisa di cosa si intenda per trattamento lecito e, per determinarlo, occorre fare riferimento alle ingerenze ammissibili ai sensi dell'articolo 8, paragrafo2 della CEDU, per come interpretate nella giurisprudenza della Corte EDU, e alle condizioni per le limitazioni legittime ai sensi dell'articolo 52 della Carta dei diritti fondamentali dell'UE.
- In base all'articolo 52, paragrafo 1, il trattamento dei dati personali è ammissibile solo se:
    - è previsto dalla legge
    - rispetta il contenuto essenziale del diritto alla protezione dei dati
    - è necessario, nel rispetto del principio di proporzionalità
    - risponde effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui.

- I motivi di **liceità del trattamento** possono derivare, oltre che:

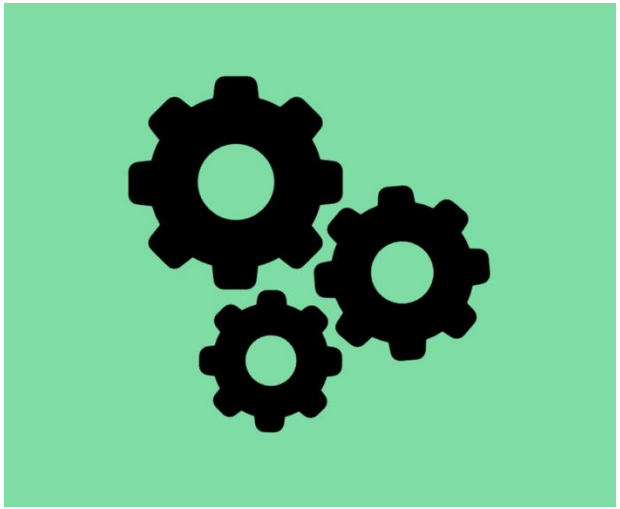
a1) dall'integrità e validità del consenso prestato dall'interessato,

anche da **altri fattori**, quali:

a2) **l'esecuzione di un contratto** in cui una delle parti coincide con l'interessato;

a3) **l'adempimento di un obbligo legale** da parte del titolare o il **perseguimento di un legittimo interesse** del titolare o di un terzo, a patto che esso non prevalga sulle prerogative dell'interessato;

a4) **l'esecuzione di un compito di interesse pubblico** o, ancora, la **salvaguardia degli interessi vitali** dell'interessato o dei consociati.



Il consenso al trattamento dei dati personali

- Ai sensi dell'art. 7 del GDPR, il titolare del trattamento deve essere in grado di **dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei dati personali**. Esso deve essere libero, specifico, informato ed inequivocabile. Nel caso di dichiarazione scritta, il consenso deve essere distinto chiaramente dalle eventuali altre dichiarazioni rese dall'interessato, in forma comprensibile e facilmente accessibile, con un linguaggio semplice e chiaro. L'interessato può revocare il proprio consenso in qualsiasi momento.
- Un'importante novità normativa è poi prevista dall'art. 8: nel caso di **offerta diretta ai minori di servizi on line** (ad es. social network), il trattamento di dati personali del minore è lecito **soltanto se il minore ha compiuto 16 anni** (il GDPR autorizza gli Stati membri a stabilire per legge un'età ancora inferiore, sino a un limite di 13 anni). In caso di minore di sedici anni, il trattamento è comunque lecito **se il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale**.
- Sulla falsariga dell'esperienza statunitense del *Children Online Privacy Protection Act* entrato in vigore nel 2000, l'art. 8, par. 2 del GDPR obbliga i titolari/gestori di siti e piattaforme on line accessibili ai minori a predisporre sistemi di verifica della genuinità del consenso o dell'autorizzazione del genitore "in considerazione delle tecnologie disponibili", ad esempio basati sull'identificazione dei tratti somatici associata alla lettura dei documenti rilasciati dagli enti governativi (Carta d'identità elettronica).

Considerando n. 43: è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica. **Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.**

Il principio di trattamento corretto e trasparente dei dati personali

- **Trattamento corretto** significa trasparenza del trattamento e ragioni legittime per la raccolta e l'utilizzo dei dati, specialmente in rapporto alle persone interessate. Questo significa che non ci devono essere conseguenze negative ingiustificate per gli individui coinvolti.
- I titolari del trattamento dei dati devono informare le persone interessate prima di trattare i loro dati, quantomeno con riferimento alla finalità del trattamento e all'identità e all'indirizzo del titolare del trattamento.
- A meno che ciò non sia specificatamente autorizzato dalla legge, il trattamento dei dati non può essere coperto da segreto.
- Nel sistema europeo, la persona interessata ha il diritto di accedere ai propri dati ogni qualvolta siano elaborati.
- Il **principio di trasparenza** disciplina, in particolare, il rapporto tra il titolare del trattamento dei dati e la persona interessata. Le attività di trattamento devono essere spiegate alle persone interessate in una maniera facilmente accessibile che assicuri la piena comprensione di cosa accadrà ai loro dati. Clicca qui per maggiori dettagli.

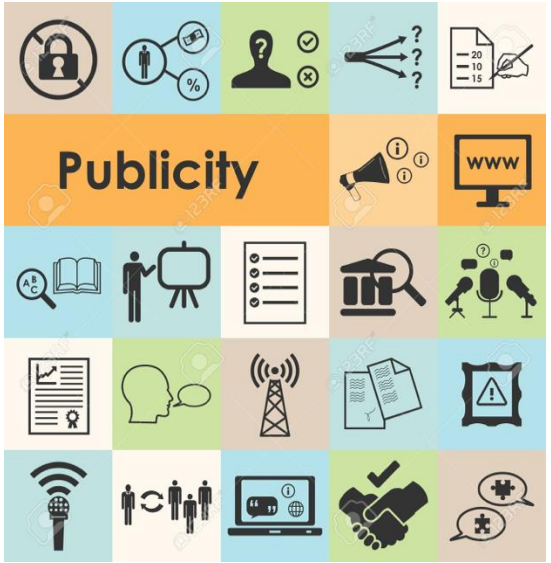
- Nel GDPR, i principi di **correttezza e trasparenza** del trattamento (art. 5 GDPR) trovano compiuta espressione nel rapporto sussistente tra l'eventuale consenso dell'interessato (o altra causa di liceità del trattamento) e l'obbligo d'informazione posto in capo al titolare.
- L'art. 12 del GDPR obbliga il titolare ad adottare misure appropriate al fine di fornire all'interessato **tutte le informazioni relative al trattamento**. Le informative devono essere rese in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, per iscritto o con mezzi elettronici.
- I successivi artt. 13 e 14 del GDPR introducono dei requisiti obbligatori delle informative nei casi in cui i dati personali vengano raccolti o meno presso l'interessato.

- L'interessato dovrebbe ricevere le informazioni relative al trattamento di dati personali che lo riguardano **al momento della raccolta presso l'interessato** o, se i dati sono ottenuti da altra fonte, entro un termine ragionevole, in funzione delle circostanze del caso.
- Se i dati personali possono essere **legittimamente comunicati** a un altro destinatario, l'interessato dovrebbe esserne informato nel momento in cui il destinatario riceve la prima comunicazione dei dati personali.
- Il titolare del trattamento, qualora intenda trattare i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, dovrebbe fornire all'interessato, prima di tale ulteriore trattamento, informazioni in merito a tale finalità diversa e altre informazioni necessarie.

- Qualora non sia possibile comunicare all'interessato l'origine dei dati personali, perché sono state utilizzate varie fonti, dovrebbe essere fornita un'informazione di carattere generale.
- Per contro, non è necessario imporre l'obbligo di fornire l'informazione se l'interessato dispone già dell'informazione, se la registrazione o la comunicazione dei dati personali sono previste per legge o se informare l'interessato si rivela impossibile o richiederebbe uno sforzo sproporzionato. Quest'ultima eventualità potrebbe verificarsi, ad esempio, nei trattamenti eseguiti a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi si può tener conto del numero di interessati, dell'antichità dei dati e di eventuali garanzie adeguate in essere.

Informativa e Informazioni: Codice privacy *vs*. GDPR

- Dall'assolvimento di un **mero obbligo burocratico** (l'informativa) all'attuazione di un **costante obbligo di informazione** in tutte le fasi dello svolgimento del trattamento dei dati personali (le informative);
- **Intuitività ed intellegibilità** (ad es. icone standardizzate ex art. 12, par. 7);
- **Gratuità** delle attività di informazione (art. 12, par. 5) eccetto nei casi di richieste eccessive, ripetitive o infondate da parte dell'interessato;
- Art. 12 (attività come procedimento) – artt. 13 e 14 (atti di informazione)



Il principio di limitazione delle finalità

- La finalità del trattamento dei dati deve essere chiaramente definita prima che il trattamento abbia inizio.
- In base al diritto dell'Unione europea, la finalità del trattamento deve essere definita espressamente; la normativa CoE rimette la disciplina di tale aspetto al diritto interno.
- Il trattamento per finalità indefinite non rispetta la normativa in materia di protezione dei dati.
- L'utilizzo ulteriore dei dati per un'altra finalità richiede una base giuridica supplementare se la nuova finalità del trattamento è incompatibile con quella originaria.
- Il trasferimento di dati a terzi è una finalità nuova che richiede una base giuridica supplementare.
- Questo principio indica che la legittimità del trattamento dei dati personali dipende dalla finalità del trattamento ("limitazione della finalità").
- Il titolare del trattamento dei dati deve precisare la finalità del trattamento dei dati personali (ad esempio, attraverso una comunicazione).
- È illegale trattare dati personali per finalità illimitate e indefinite.
- Il trattamento secondario di dati personali deve avere la sua specifica base giuridica e non può fondarsi sul fatto che i dati erano stati inizialmente acquisiti o trattati per un'altra finalità legittima.
- Il trattamento ulteriore di dati per un interesse pubblico o per finalità storiche, statistiche o scientifiche è ammesso purché gli Stati membri prevedano garanzie appropriate.

Il principio di minimizzazione ed esattezza dei dati

- I principi relativi ai dati ("minimizzazione dei dati", esattezza e limitazione della conservazione) devono essere rispettati dal titolare del trattamento in tutte le attività di trattamento.
- Il principio della **limitazione della conservazione** richiede la cancellazione dei dati non appena questi non siano più necessari per il conseguimento delle finalità per le quali sono stati raccolti.
- Deroghe al principio della limitazione della conservazione possono essere stabilite per legge e richiedono speciali garanzie per la protezione delle persone interessate.
- In ossequio al **principio di minimizzazione**, possono essere trattati solo i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati e/o ulteriormente elaborati. Le categorie di dati scelti per il trattamento devono essere necessarie al fine di conseguire la finalità generale dichiarata delle attività di trattamento.
- Quanto alla durata del trattamento e alla relativa conservazione dei dati da parte del titolare (principi di adeguatezza e limitazione del trattamento), il GDPR specifica come **tali processi debbano essere limitati al tempo necessario per il perseguimento delle finalità del trattamento**.
- È possibile fissare un termine per la definitiva eliminazione delle informazioni o, ancora, ai fini dell'espletamento di una verifica periodica e di un'eventuale rettifica.

Il principio di integrità e sicurezza

I dati personali devono essere trattati in modo da garantire un'adeguata sicurezza dei dati personali, compresa la protezione da:

- trattamenti non autorizzati o illeciti
- perdita accidentale
- distruzione
- danno

mediante misure tecniche e organizzative adeguate.

- **Liceità, correttezza, trasparenza**: obbligo di svolgere un trattamento dei dati personali lecito, corretto e trasparente nei confronti dell'interessato;
- **Minimizzazione:** i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- **Limitazione delle finalità**: i dati personali devono essere raccolti per finalità limitate, esplicite e legittime e trattati in modo compatibile con tali finalità;
- **Esattezza:** i dati personali devono essere esatti e, se necessario, aggiornati; se inesatti rispetto le finalità devono essere modificati, rettificati e/o cancellati tempestivamente con tutte le misure idonee;
- **Integrità e riservatezza**: i dati vanno trattati in maniera tale da garantire un'adeguata sicurezza compresa la protezione, mediante misure tecniche e organizzative adeguati, al fin di non configurare trattamenti illecite e non autorizzati e non causarne la perdita, la distruzione o danni accidentali;
- **Limitazione della conservazione**: i dati personali vanno conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al perseguimento delle finalità per le quali sono trattati.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Case-study: *Privacy* e tutela del lavoratore

Videosorveglianza sul luogo di lavoro (1) - GPDP, provv. 10 aprile 2025 [10144203]

- Con un reclamo pervenuto a questa Autorità in data 20/04/2023, veniva segnalata la presenza di un sistema di videosorveglianza presso la sede di XXXXXXXX, in violazione della disciplina in materia di protezione dei dati personali.

- In base a quanto rappresentato nel reclamo, l'impianto non era adeguatamente segnalato mediante le informative e veniva utilizzato anche per finalità di controllo dei dipendenti, le cui immagini erano visionabili anche da remoto da parte del titolare del trattamento.

- In primo luogo, occorre rilevare che l'impianto di videosorveglianza (costituito dalle telecamere presenti nella sede legale e nei due esercizi commerciali), secondo quanto dichiarato, è stato installato dalla Società verso la fine del 2022 e inizio del 2023.

- Da quel momento e fino alla data dell'accertamento ispettivo (eseguito a luglio 2023), le informative presenti erano inidonee e, in un caso, l'informativa era addirittura assente.

Videosorveglianza sul luogo di lavoro (2) - GPDP, provv. 10 aprile 2025 [10144203]

- Rispetto a tale violazione, preso atto del tempestivo intervento della Società che ha integrato le informative inidonee, già durante l'accertamento ispettivo, deve rilevarsi che l'utilizzo di sistemi di videosorveglianza determina un trattamento di dati personali ai sensi dell'art. 4, par. 1, n. 2, del Regolamento, rispetto al quale trovano applicazione i principi generali contenuti nell'art. 5 del Regolamento. Tra questi, in particolare, il principio di trasparenza che presuppone che "gli interessati devono essere sempre informati che stanno per accedere in una zona videosorvegliata".

- Le Linee guida n. 3/2019 per la protezione dei dati sul trattamento dei dati personali attraverso dispositivi video (adottate dall'EDPB il 29/01/2020), chiariscono che "le informazioni più importanti devono essere indicate [dal titolare] sul segnale di avvertimento stesso (primo livello) mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello)" (par. 111 delle Linee guida). "Tali informazioni possono essere fornite in combinazione con un'icona per dare, in modo ben visibile, intelligibile e chiaramente leggibile, un quadro d'insieme del trattamento previsto (articolo 12, paragrafo 7, del RGPD). Il formato delle informazioni dovrà adeguarsi alle varie ubicazioni" (par. 112).

Videosorveglianza sul luogo di lavoro (3) - GPDP, provv. 10 aprile 2025 [10144203]

- Nell'informativa fornita ai dipendenti, inoltre, veniva rappresentato che i tempi di conservazione delle immagini erano di 24 ore, contrariamente a quanto verificato nel corso dell'accertamento.

- Su questo specifico aspetto, si osserva, in via generale, che i dati personali non possono essere conservati più a lungo di quanto necessario per le finalità per le quali sono trattati (art. 5, par. 1, lett. c) ed e), Regolamento).

- Tenendo conto dei principi di minimizzazione dei dati e di limitazione della loro conservazione, i dati personali dovrebbero essere cancellati dopo alcuni giorni, preferibilmente tramite meccanismi automatici.

- Nel caso di specie, risulta invece accertato che la conservazione delle immagini era prolungata, senza che vi fosse una reale esigenza o necessità. Anche su questo punto, la Società ha comunque provveduto, nel corso del procedimento, a ridurre il tempo di conservazione delle immagini a 48 ore.

Videosorveglianza sul luogo di lavoro (4) - GPDP, provv. 10 aprile 2025 [10144203]

- In ultimo, rispetto all'ulteriore profilo di illiceità relativo alla rilevazione dell'audio attraverso le telecamere presenti nei due negozi, si osserva che tale trattamento, particolarmente invasivo non solo nei confronti dei dipendenti ma anche dei terzi in generale, risulta del tutto sproporzionato rispetto alla dichiarata finalità di sicurezza del patrimonio aziendale. Tale trattamento è dunque avvenuto in violazione del principio di minimizzazione di cui al richiamato art. 5, par. 1, lett. c), del Regolamento.

- Secondo quanto accertato nel corso delle operazioni svolte dal Nucleo privacy, le telecamere interne presenti presso i due negozi, oltre ad avere il microfono incorporato, erano installate in modo tale da riprendere anche l'attività lavorativa delle dipendenti, senza che fosse stata attivata la procedura di garanzia prevista dall'art. 4 della legge n. 300/1970.

- A tal proposito, si osserva che i trattamenti di dati personali effettuati nell'ambito del rapporto di lavoro, se necessari per la finalità di gestione del rapporto stesso (v. artt. 6, par. 1, lett. b) e c); 9, par. 2, lett. b) del Regolamento), devono svolgersi sempre nel rispetto dei principi generali indicati dall'art. 5 del Regolamento, ed in particolare del principio di liceità, in base al quale il trattamento è lecito se è conforme alle discipline di settore applicabili (art. 5, par. 1, lett. a) del Regolamento).

Videosorveglianza sul luogo di lavoro (5) - GPDP, provv. 10 aprile 2025 [10144203]

- Coerentemente con tale impostazione, l'art. 88 del Regolamento ha fatto salve le norme nazionali di maggior tutela ("norme più specifiche") volte ad assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei lavoratori. Il legislatore nazionale ha approvato, quale disposizione più specifica, l'art. 114 del Codice che tra le condizioni di liceità del trattamento ha stabilito l'osservanza di quanto prescritto dall'art. 4, legge n. 300/1970.

- Tale disposizione prevede che gli apparati di videosorveglianza, qualora dagli stessi derivi "anche la possibilità di controllo a distanza" dell'attività dei dipendenti, "*possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale*" **e la relativa installazione deve, in ogni caso, essere eseguita previa stipulazione di un accordo collettivo con la rappresentanza sindacale unitaria o con le rappresentanze sindacali aziendali o, ove non sia stato possibile raggiungere tale accordo o in caso di assenza delle rappresentanze, solo in quanto preceduta dal rilascio di apposita autorizzazione da parte dell'Ispettorato del lavoro**.

- **Risulta accertato, nel caso di specie, che l'autorizzazione da parte dell'ITL competente sia stata rilasciata solo in data 09/10/2023, quindi in epoca successiva alla installazione delle telecamere, con conseguente violazione degli artt. 5, par. 1, lett. a) in relazione all'art. 114 del Codice, e dell'art. 88 del Regolamento**.

Controllo delle presenze e dati biometrici (1) - GPDP, provv. 27 marzo 2025 [10138981]

- Con reclamo presentato ai sensi dell'art. 77 del Regolamento, i Sig.ri XX, XX e XX hanno lamentato, per il tramite del proprio difensore, una presunta violazione della disciplina in materia di protezione dei dati personali con riguardo all'impiego, presso le sedi dell'Istituto di Istruzione Superiore XXXXX, di un sistema di rilevazione delle presenze del personale dipendente amministrativo che, richiedendo l'utilizzo delle impronte digitali dei lavoratori, implicherebbe il trattamento dei relativi dati biometrici al fine di identificarli in modo univoco.

- Il trattamento di dati biometrici, di regola vietato per effetto del disposto di cui all'art. 9, par. 1, del Regolamento, è consentito esclusivamente al ricorrere di una delle condizioni indicate dell'art. 9, par. 2 del Regolamento e, in ambito lavorativo, solo quando sia "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato" (art. 9, par. 2, lett. b), del Regolamento; v. pure, art. 88, par. 1 e cons. 51-53 del Regolamento).

Controllo delle presenze e dati biometrici (2) - GPDP, provv. 27 marzo 2025 [10138981]

- Il quadro normativo vigente prevede inoltre che il trattamento di dati biometrici, per poter essere lecitamente posto in essere, avvenga nel rispetto di "*ulteriori condizioni, comprese limitazioni*" (cfr. art. 9, par. 4, del Regolamento); a tale disposizione è stata data attuazione, nell'ordinamento nazionale, con l'art. 2-septies (Misure di garanzia per il trattamento dei dati genetici, biometrici e relativi alla salute) del Codice (come modificato dal decreto legislativo 10 agosto 2018 n. 101 di adeguamento della normativa nazionale alle disposizioni del Regolamento). La norma prevede che è lecito il trattamento di tali categorie di dati al ricorrere di una delle condizioni di cui all'art. 9, par. 2, del Regolamento "ed in conformità alle misure di garanzia disposte dal Garante", in relazione a ciascuna categoria dei dati.

- Il datore di lavoro, titolare del trattamento, è, in ogni caso, tenuto a rispettare i principi di protezione dei dati personali, tra cui in particolare quelli di "liceità, correttezza e trasparenza", "minimizzazione" e protezione dei dati "fin dalla progettazione" e "per impostazione predefinita" (artt. 5 e 25 del Regolamento).

Controllo delle presenze e dati biometrici (3) - GPDP, provv. 27 marzo 2025 [10138981]

- In particolare, è stato accertato che il predetto sistema, elaborando le caratteristiche dell'impronta digitale acquisita, permette di creare un modello matematico che, venendo associato al codice identificativo del singolo interessato, costituisce il termine di raffronto delle successive verifiche all'atto della timbratura dei dipendenti.

- Ancorché lo stesso non mantenga traccia dei dati anagrafici dei dipendenti, dell'immagine o di "dati fisici diretti o deducibili" delle relative impronte digitali e, per altro verso, "*la "ricostruzione dell'impronta digitale" partendo dal modello non [… sia] possibile, nemmeno conoscendo l'algoritmo di elaborazione*" (cfr. nota del XX), si osserva quanto segue.

- Le informazioni trattate per il tramite di tale sistema r**isultano comunque riconducibili ad un codice direttamente identificativo del singolo dipendente, ne consentono o confermano l'identificazione univoca e costituiscono pertanto dati personali biometrici** (cfr. art. 4, nn. 1) e 14), del Regolamento).

Controllo delle presenze e dati biometrici (4) - GPDP, provv. 27 marzo 2025 [10138981]

- Ciò premesso, si fa presente che la finalità di rilevazione delle presenze in servizio dei dipendenti, funzionale all'attestazione dell'osservanza dell'orario di lavoro alla sua contabilizzazione, che, in generale, nell'ambito del pubblico impiego, è prevista da un quadro normativo stratificatosi nel tempo (v. ad esempio, art. 22, comma 3 della l. 23.12.1994, n. 724; art. 3 della l. 24.12.2007, n. 244; art. 7 del d.P.R. 1.02.1986, n. 13), è riconducibile nell'ambito di applicazione dell'articolo 9 par. 2, lett. b) del Regolamento poiché implica un trattamento "*necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro* […]" (v. pure art. 88, par. 1, Regolamento).
- Tuttavia, l'impiego di sistemi di rilevazione delle presenze che comportano anche il trattamento di dati biometrici richiede, nel sistema del Regolamento e del Codice, un'espressa previsione normativa e specifiche garanzie per i diritti degli interessati (il trattamento è infatti consentito "*nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri […] in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato", art. 9, par. 2, lett. b), del Regolamento e cons. 51-53, e "nel rispetto delle misure di garanzia*" individuate dal Garante ai sensi dell'art. 9, par. 4, del Regolamento e dell'art. 2-septies del Codice).

Controllo delle presenze e dati biometrici (5) - GPDP, provv. 27 marzo 2025 [10138981]

- Nel contesto lavorativo il trattamento avente a oggetto dati biometrici può essere lecitamente posto in essere solo ove lo stesso trovi il proprio fondamento in una disposizione normativa che possa essere ritenuta base giuridica del trattamento "idonea" anche alla luce dell'assetto delle fonti dell'"ordinamento costituzionale" dello Stato membro (v. considerando 41 del Regolamento e v. anche Corte Cost. sent. n. 271/2005, in base alla quale la disciplina di protezione dei dati personali rientra fra la materia di competenza esclusiva statale riferita all'"ordinamento civile").

- Tale disposizione deve, infatti, avere le caratteristiche richieste dalla disciplina di protezione dei dati e soddisfare specifici requisiti, sia in termini di qualità della fonte, contenuti necessari e misure appropriate e specifiche per tutelare i diritti e le libertà degli interessati, sia in termini di proporzionalità dell'intervento regolatorio rispetto alle finalità che si intendono perseguire (art. 6, parr. 2 e 3, lett. b), del Regolamento). Ciò in quanto, la base giuridica del trattamento, per poter essere considerata una valida condizione di liceità del trattamento, deve, tra l'altro, "*persegu[ire] un obiettivo di interesse pubblico ed [essere] proporzionato all'obiettivo legittimo perseguito*" (art. 6, par. 3, lett. b), del Regolamento).

Controllo delle presenze e dati biometrici (6) - GPDP, provv. 27 marzo 2025 [10138981]

- Al riguardo, si fa presente inoltre che l'art. 2 della l. 19 giugno 2019, n. 56, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo", aveva previsto una generalizzata sostituzione dei sistemi di rilevazione automatica delle presenze con sistemi di rilevazione di dati biometrici unitamente all'impiego di sistemi di videosorveglianza prevedendo che, "*ai fini della verifica dell'osservanza dell'orario di lavoro*", le amministrazioni pubbliche - individuate ai sensi dell'art. 1, comma 2, del d.lgs. n. 165/2001, ad esclusione del "personale in regime di diritto pubblico" (cfr. art. 3, comma 2, d.lgs. n. 165/2001), e quello sottoposto alla disciplina del lavoro agile di cui all'articolo 18 della legge 22 maggio 2017, n. 81 - "introducono sistemi di identificazione biometrica e di videosorveglianza in sostituzione dei diversi sistemi di rilevazione automatica attualmente in uso" ma prevede anche che le "modalità attuative" della norma – nel rispetto dell'art. 9 del Regolamento e delle misure di garanzia definite dal Garante ai sensi dell'art. 2-septies del Codice – siano individuate con d.P.C.M., su proposta del Ministro della funzione pubblica, previa intesa con la conferenza unificata (stato regioni e autonomie locali) e "*previo parere del Garante ai sensi dell'art. 154 del Codice sulle modalità del trattamento dei dati biometrici*".

Controllo delle presenze e dati biometrici (7) - GPDP, provv. 27 marzo 2025 [10138981]

- Nell'esercizio dei propri poteri consultivi sugli atti normativi (artt. 36, par. 4 e 58, par. 3 del Regolamento nonché art. 154 del Codice), il Garante aveva, a suo tempo, segnalato al legislatore nazionale le criticità della norma evidenziando, in particolare, "*l'eccedenza rispetto alle finalità che si intendono perseguire, anche sotto il profilo della gradualità delle misure limitative che possono essere adottate nei confronti dei lavoratori*" (cfr. provv. 11 ottobre 2018, n. 464, doc. web n. 9051774) e - confermando quanto già rilevato nel corso delle audizioni dinanzi alle Commissioni parlamentari competenti (audizioni presso le Commissioni riunite I e XI, Affari Costituzionali e Lavoro, della Camera dei Deputati il 6 febbraio 2019, doc. web n. 9080870) -, ha ribadito, anche in relazione allo schema di regolamento di attuazione, peraltro mai adottato, che "*non può ritenersi in alcun modo conforme al canone di proporzionalità- come declinato dalla giurisprudenza europea e interna– l'ipotizzata introduzione sistematica, generalizzata e indifferenziata per tutte le pubbliche amministrazioni di sistemi di rilevazione biometrica delle presenze, in ragione dei vincoli posti dall'ordinamento europeo sul punto, a motivo dell'invasività di tali forme di verifica e delle implicazioni derivanti dalla particolare natura del dato*" (provv. 19 settembre 2019, n. 167, doc. web n. 9147290).

Controllo delle presenze e dati biometrici (8) - GPDP, provv. 27 marzo 2025 [10138981]

- Le disposizioni che prevedevano l'introduzione di sistemi di rilevazione biometrica delle presenze, in ambito pubblico, contenute nei commi da 1 a 4 dell'art. 2 della l. 19 giugno 2019, n. 56, **sono state da ultimo abrogate** dalla l. 30 dicembre 2020, n. 178 (c.d. Legge di Bilancio 2021, art. 1, comma 958).

- **Per tali ragioni, si evidenzia che, in assenza di specifiche disposizioni che prevedano il trattamento dei dati biometrici per finalità di rilevazione delle presenze e delle relative garanzie, il relativo trattamento non può essere lecitamente effettuato, non sussistendo base giuridica.**

Privacy e procedimento disciplinare (1) - GPDP, provv. 20 maggio 2024 [10060901]

- Il Sig. XX il 18 ottobre 2021, ha presentato un reclamo con cui sono state lamentate presunte violazioni del Regolamento, con particolare riferimento al trattamento di dati effettuato mediante l'attività di una agenzia investigativa, svolta su incarico della sede XX della Società, al fine di verificare il corretto uso dei permessi previsti dalla l. 104 del 1992, e il successivo utilizzo dei dati raccolti nell'ambito di un procedimento disciplinare conclusosi con il licenziamento del reclamante.

- In particolare, con il reclamo è stato lamentato che all'interno della relazione investigativa e della contestazione disciplinare sono presenti riferimenti a soggetti terzi, identificati con nome e cognome, nonché la "descrizione di atteggiamenti e relazionalità" con i predetti terzi, senza che ciò sia necessario per le conclusioni dell'investigazione e pertanto in violazione del principio di pertinenza e proporzionalità.

Privacy e procedimento disciplinare (2) - GPDP, provv. 20 maggio 2024 [10060901]

- Nel merito, con esclusivo riferimento ai trattamenti effettuati dalla Società, è accertato che quest'ultima ha notificato al reclamante il 7 settembre 2021 una contestazione disciplinare, ai sensi dell'art. 7, l. n. 300 del 1970, relativa alla violazione delle condizioni di fruizione dei permessi ex l. n. 104 del 1992.

- **Il riferimento esplicito all'identità della reclamante e l'allusione all'esistenza di una relazione personale e intima tra la stessa e il reclamante**, che emerge in particolare dalle espressioni sopra riportate nonché dalla identificazione della reclamante come la medesima accompagnatrice di molteplici attività quotidiane svolte in comune, **non è conforme ai principi di liceità, correttezza e minimizzazione**, posto che la necessità per il datore di lavoro di contestare dettagliatamente la condotta ascritta al dipendente poteva ben essere utilmente effettuata senza riportare il nome della persona oggetto di osservazione da parte degli investigatori e, a maggior ragione, senza esplicitare l'esistenza di una relazione privata con la medesima.

Privacy e procedimento disciplinare (3) - GPDP, provv. 20 maggio 2024 [10060901]

- Infatti **sarebbe stato sufficiente limitarsi a riportare nella contestazione che trattavasi di persona evidentemente estranea all'attività di assistenza e cura del parente disabile**, posto peraltro che tale circostanza risultava facilmente desumibile dalla stessa natura di alcune delle attività osservate dagli investigatori e riportate dettagliatamente nella contestazione: pesca con muta subacquea, passeggiate a piedi, spostamenti in macchina da e verso l'abitazione del reclamante, prelievi da sportelli bancomat e altro.

- La circostanza, poi, evidenziata dalla Società nelle proprie memorie, che l'atto di contestazione disciplinare non abbia riportato per intero il contenuto della relazione investigativa non esclude, di per sé, che i dati riportati risultino in concreto non adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento, nei termini sopra indicati.

Privacy e procedimento disciplinare (4) - GPDP, provv. 20 maggio 2024 [10060901]

- Né il fatto che i dati di cui si discute non siano stati riportati (anche) nella lettera di licenziamento del reclamante può essere preso in considerazione, come sostenuto dalla Società, per attestare l'osservanza da parte di quest'ultima del principio di minimizzazione anche con riguardo all'atto di contestazione disciplinare, posto che gli stessi sono atti distinti.

- I trattamenti di dati personali devono in primo luogo osservare il principio generale di proporzionalità, sancito dall'art. 52 della Carta dei diritti fondamentali dell'Unione europea ("*Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*").

- In proposito la Corte Cost. 21/2/2019, n. 20, punto 3.1, ha rammentato che "*La Corte di Giustizia dell'Unione europea ha ripetutamente affermato che le esigenze di controllo democratico non possono travolgere il diritto fondamentale alla riservatezza delle persone fisiche, dovendo sempre essere rispettato il principio di proporzionalità, definito cardine della tutela dei dati personali*".

Grazie per l'attenzione!!

ggiannonecodiglione@unisa.it