«GOVERNARE L'INTELLIGENZA ARTIFICIALE NELLE PUBBLICHE AMMINISTRAZIONI»
Università Politecnica delle Marche - 26 giugno 2026

Intelligenza artificiale e protezione dei dati personali nella p.a.

dott. Lorenzo Madau

Assegnista di ricerca in Istituzioni di Diritto pubblico

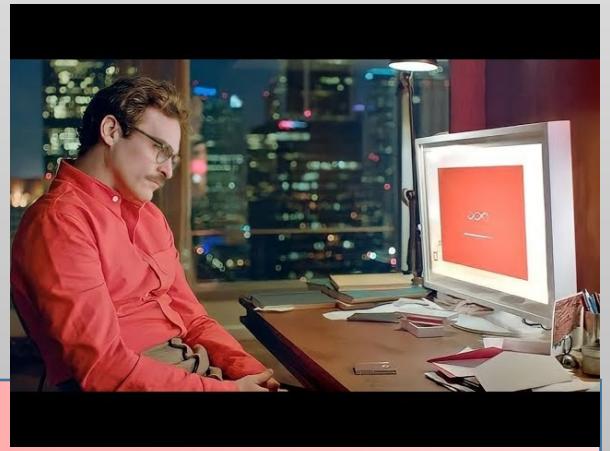
Università Politecnica delle Marche

«Her» («Lei») di Spike Jonze, 2013

UNIVERSITÀ POLITECNICA DELLE MARCHE

- Her | Installing OS

Già in questa scena ci sono molti dei temi coinvolti nel rapporto tra I.A. e dati personali: -domande personali all'utente per impostare assistente IA; -raccolta dati personali milioni di personalità umane per addestrare l'IA (web scraping); -capacità machine learning IA che apprende e si evolve grazie a parole, tono, esperienze dell'utente;
-accesso al pc utente e suoi contenuti per fare ordine in modo mirato e «intelligente»



Rapporto tra I.A. e dati personali

Relazione strettissima: come noto, infatti, il funzionamento dei sistemi di I.A. si basa su uso massiccio di dati, anche personali. I dati sono il «motore» del suo sviluppo

Non a caso Discorso del Presidente del Garante per la protezione dei dati personali in occasione della presentazione della relazione annuale 2024 dedicato in gran parte proprio alle sfide poste dall'I.A.

Difficoltà regolare il fenomeno con gli strumenti tradizionali è emersa in modo esemplare nella vicenda del procedimento sanzionatorio del Garante nei confronti di Open AI per Chatgpt, terminata al momento con annullamento provvedimento sanzionatorio da parte Tribunale di Roma con sentenza n. 4153 del 2026

Di conseguenza, **strettissima connessione anche tra i diversi strumenti normativi** che UE e Italia hanno adottato per disciplinare le due tematiche:

GDPR

Codice privacy (d.lgs. 196/2003 e ss.mm.)

AI ACT

legge n. 132/2025

Difficile ma necessaria cultura della protezione dei dati

Non sempre è semplice il coordinamento tra le diverse normative

(**ora v. proposta della Commissione UE di un nuovo regolamento c.d. «Digital omnibus»** che rivede parti sia dell'AI Act che del GDPR in ottica di semplificazione e razionalizzazione normativa)

Sicuramente non agevole per privati e p.a. navigare e orientarsi in questo mare

MA

indispensabile «cultura della protezione dei dati» (così Presidente del Garante Privacy nella relazione annuale 2024) come parte della più generale «cultura del digitale»

AI ACT e GDPR

- **Art. 2.7 AI ACT:** «*Il diritto dell'Unione in materia di protezione dei dati personali, della vita privata e della riservatezza delle comunicazioni si applica ai dati personali trattati in relazione ai diritti e agli obblighi stabiliti dal presente regolamento. Il presente regolamento lascia impregiudicati il regolamento (UE) 2016/679 o (UE) 2018/1725 o la direttiva 2002/58/CE o (UE) 2016/680, fatti salvi l'articolo 10, paragrafo 5, e l'articolo 59 del presente regolamento*».

= protezione dati personali rimane centrale e il GDPR continua a rimanere punto di riferimento normativo per trattamento dati, che prevale e a cui rinvia l'AI ACT, quando utilizzo I.A. comporti un trattamento dati personali

GDPR: normativa «orizzontale», si applica in ogni settore, ogniqualvolta venga in rilievo un «trattamento» di «dati personali»

AI ACT: disciplina specificamente sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di IA

Sono strumenti complementari, cumulativi e non alternativi tra loro: di qui necessaria c.d. «doppia conformità», sia all'AI ACT che al GDPR, quando un sistema di IA comporta trattamento di dati personali

Prime questioni da porsi

- L'utilizzo dell'I.A. determina o meno un «trattamento» di «dati personali»?
- Se sì, che tipologia di dati personali coinvolge: dati comuni, categorie particolari di dati (art. 9 GDPR) o dati giudiziari (art. 10 GDPR)?

Queste risposte non le fornisce l'AI Act, ma il GDPR, è lì, alle sue definizioni e ai suoi principi fondamentali che bisogna fare riferimento

Art. 4 GDPR (Definizioni) cos'è il dato personale

Definizione di «dato personale»: «**qualsiasi informazione riguardante una persona fisica identificata o identificabile** («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»

- Vi rientrano, per es., anche gli identificativi online (indirizzi IP, *cookies*) e i dati «pseudonimizzati» (= quelli conservati in una forma che impedisce l'identificazione del soggetto senza l'utilizzo di informazioni aggiuntive) - V. i **Considerando nn. 26 e 30**
- Non vi rientrano i dati anonimi (= quelli che in origine o a seguito di trattamento non possono essere associati ad un interessato identificato o identificabile)

La proposta di modifica della nozione di «dato personale» nel digital omnibus

UNIVERSITÀ POLITECNICA DELLE MARCHE

Articolo 3

Modifiche del regolamento (UE) 2016/679 (GDPR)

Il regolamento (UE) 2016/679 è così modificato:

1. l'articolo 4 è così modificato:

(a) al punto 1) sono aggiunte le frasi seguenti:

"le informazioni relative a una persona fisica non sono necessariamente dati personali per qualsiasi altra persona o entità per il solo fatto che un'altra entità può identificare tale persona fisica. Le informazioni non sono personali per una determinata entità se quest'ultima non è in grado di identificare la persona fisica cui si riferiscono le informazioni, tenendo conto dei mezzi di cui tale entità si può ragionevolmente avvalere. Tali informazioni non diventano personali per tale entità per il solo fatto che un potenziale destinatario successivo dispone di mezzi di cui si può ragionevolmente avvalere per identificare la persona fisica cui le informazioni si riferiscono;";

Il dato «relativamente» personale nella proposta della Commissione

si restringe perimetro di cosa è «dato personale»

Cambia la stessa definizione di «dato personale» verso un "*approccio soggettivo*": se una specifica informazione non permette a un soggetto di identificare direttamente una persona, il dato non deve essere considerato "personale" per il soggetto che lo tratta, e resta fuori dal campo di applicazione del GDPR

- inoltre, si prevede rinvio all'adozione di atti di esecuzione della Commissione per stabilire quando i dati pseudonimizzati non costituiscano più dati personali per determinati soggetti

Forti critiche nel parere congiunto dell'11 febbraio 2026 di EDPS (European Data Protection Supervisor) **ed EDPB** (European Data Protection Board) edpb_edps_jointopinion_202602_digitalomnibus_en.pdf : si incide direttamente, in modo restrittivo, sull'ambito di applicazione di un diritto fondamentale protetto dall'art. 8 CDFUE

segue

«La questione assume una dimensione ulteriore se letta in connessione con l'evoluzione dell'intelligenza artificiale. I modelli di apprendimento automatico operano per inferenza statistica: estraggono correlazioni, costruiscono profili, anticipano comportamenti a partire da dati che, considerati singolarmente, potrebbero apparire irrilevanti o anonimi.

Un indirizzo IP, un pattern di navigazione, la frequenza di accesso a determinati servizi: nessuno di questi elementi, preso isolatamente, identifica una persona. Ma la loro combinazione algoritmica può produrre un'identificazione più precisa di qualsiasi nome o codice fiscale.

In un ecosistema in cui l'identificabilità non è più una proprietà statica dell'informazione ma un risultato dinamico della capacità computazionale, ancorare la protezione alla posizione conoscitiva del singolo titolare significa creare una zona d'ombra crescente, nella quale enormi masse di informazioni sfuggono alla tutela proprio perché chi le tratta non è – o non è ancora – in grado di ricollegarle a individui specifici.» (M. Iaselli, *Dal dato personale al dato relativo*)

Art. 9: Tutela di particolari categorie di dati personali

UNIVERSITÀ POLITECNICA DELLE MARCHE

• par. 1: 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 e 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

La regola è il DIVIETO di trattamento di tali categorie di dati. MA:

DEROGHE previste dall'art. 9, par. 2. Esempi:

- consenso esplicito

- trattamento riguarda dati personali resi manifestamente pubblici dall'interessato

- il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri

- finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali (Finalità di cura)

- motivi di interesse pubblico nel settore della sanità pubblica

• Tutela rafforzata con riguardo ai dati genetici, biometrici e dati relativi alla salute (ulteriori condizioni limiti, come le «misure di garanzia», che possono essere previste da Stati nazionali)

Deroga all'art. 9 GDPR da parte dell'art. 10, par. 5, AI ACT

«Nella misura in cui ciò sia **strettamente necessario al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio … i fornitori di tali sistemi possono eccezionalmente trattare categorie particolari di dati personali**, fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche»
Oltre alle disposizioni di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 e alla direttiva (UE) 2016/680, devono essere soddisfatte le condizioni indicate dallo stesso par. 5 (necessità, minimizzazione, limitazione, sicurezza…)

Art. 4 definizione di «**trattamento**»

Anche qui nozione amplissima e onnicomprensiva:

«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»

AGID: Bozza di linee guida per l'adozione di IA nella pubblica amministrazione

Ai sensi del D.P.C.M. 12 gennaio 2024, recante "Piano triennale per l'informatica nella pubblica amministrazione 2024-2026"

Attualmente in fase di approvazione dopo consultazione pubblica svoltasi dal 12 marzo all'11 aprile 2026

Conosciamo il testo della versione attuale, anche se ancora in itinere

v. spec. Paragrafo 10. «Protezione dei dati personali»:

«I sistemi di IA, nel contesto delle presenti Linee guida, possono essere utilizzati per lo svolgimento e/o il supporto di attività che comportano il trattamento di dati anche personali: l'adozione di tali sistemi da parte delle PA, pertanto, DEVE intervenire nel rispetto del diritto fondamentale alla protezione dei dati personali.

In tale ottica, al momento dell'adozione, la PA DEVE porre un'attenzione primaria alla valutazione e alla verifica della conformità normativa del sistema di IA e all'impatto che questo avrà sui diritti degli interessati coinvolti, anche adeguando il proprio modello organizzativo e le correlate misure tecniche e organizzative di sicurezza.»

segue

La PA, in particolare, DEVE verificare il rispetto dei principi enunciati all'art. 5 del GDPR, compresa la responsabilizzazione della PA stessa che ne farà uso in qualità di titolare del trattamento, nel rispetto della normativa unionale e nazionale in materia di protezione dei dati personali e dei provvedimenti e pareri emessi dall'European Data Protection Board e dal Garante per la protezione dei dati personali. Qualora il sistema di IA sia adottato per lo svolgimento di attività che comportano il trattamento di dati personali, risulta di primaria rilevanza che la PA effettui un'analisi di tale sistema sotto lo specifico profilo della protezione dei dati personali, al fine di garantire e dimostrare il rispetto di quanto segue:

segue

- il trattamento dei dati personali mediante il sistema di IA avviene in modo **lecito, corretto e trasparente** nei confronti dell'interessato (principio di liceità);
- i dati personali sono raccolti mediante il sistema di IA **per finalità determinate, esplicite e legittime** e, successivamente, sono trattati compatibilmente con tali finalità (principio di finalità);
- i dati personali trattati a mezzo del sistema di IA sono **adeguati, pertinenti e limitati a quanto necessario** rispetto alle finalità per cui sono trattati (principio di minimizzazione e necessità);
- i dati personali trattati a mezzo del sistema di IA sono **esatti e, se necessario, aggiornati**, adottando la PA tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per cui sono trattati (principio di esattezza);
- i dati personali trattati a mezzo del sistema di IA sono **conservati** in una forma che consenta l'identificazione degli interessati **per un arco di tempo non superiore al conseguimento delle finalità** per cui sono trattati (principio di limitazione della conservazione);

segue

- la PA utilizza il sistema di IA in modo da garantire un **livello di sicurezza dei dati personali adeguato al rischio**, individuando e attuando misure tecniche e organizzative adeguate a proteggere i dati da violazioni di sicurezza che possano comportare, illecitamente o accidentalmente, la perdita, la modifica, la divulgazione non autorizzata, l'accesso ai dati personali trasmessi, conservati o comunque trattati (principio di integrità e riservatezza);

- la PA garantisce sempre all'interessato **l'esercizio dei propri diritti** in materia di protezione dei dati personali; (= diritto di accesso, di rettifica, opposizione, limitazione, cancellazione, portabilità dei dati, non sottoposizione a processo decisionale automatizzato)

- prima di procedere al trattamento di dati personali mediante il sistema di IA adottato e altresì periodicamente, la PA effettua una **valutazione d'impatto** sulla protezione dei dati personali ai sensi dell'art. 35 del GDPR…individuando i rischi e le misure tecniche e organizzative idonee a mitigarli e, qualora risulti un rischio elevato in assenza di misure di attenuazione, consulta il Garante per la protezione dei dati personali;

- le **categorie particolari di dati personali**, come individuate agli artt. 9-10 del GDPR, sono trattate a mezzo di sistemi di IA solo nel rispetto di quanto stabilito dalla normativa unionale e nazionale in materia di protezione dei dati personali e ai sensi dello stesso AI Act»

segue

- Richiamo a indicazioni date dal Garante nel Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di I.A (*in quanto contenente principi validi in generale per una corretta gestione di algoritmi e sistemi di IA nell'attività amministrativa*): «la PA DEVE porre la massima attenzione a tre principi cardine che devono necessariamente governare l'utilizzo di algoritmi e sistemi di IA nell'esecuzione di compiti di rilevante interesse pubblico
- 1. **il principio di conoscibilità**, in base al quale l'interessato ha il diritto di conoscere l'esistenza di processi decisionali basati su trattamenti automatizzati e, in tal caso, di ricevere informazioni significative sulla logica utilizzata, sì da poterla comprendere;
- 2. il **principio di non esclusività della decisione algoritmica**, secondo cui deve comunque esistere nel processo decisionale un intervento umano capace di controllare, validare ovvero smentire la decisione automatica (c.d. human in the loop);
- 3. il **principio di non discriminazione algoritmica**, secondo cui è opportuno che il titolare del trattamento utilizzi sistemi di IA affidabili che riducano le opacità, gli errori dovuti a cause tecnologiche e/o umane, verificandone periodicamente l'efficacia anche alla luce della rapida evoluzione delle tecnologie impiegate, delle procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate.»

= sono i principi riconosciuti già dalla giurisprudenza del Consiglio di Stato

Articolo 22 GDPR
Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione

1. L'interessato ha il **diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona**.

2. Il **paragrafo 1 non si applica** nel caso in cui la decisione:

a) sia necessaria per la conclusione o l'esecuzione di un **contratto** tra l'interessato e un titolare del trattamento;

b) sia autorizzata dal **diritto** dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato;

c) si basi sul **consenso** esplicito dell'interessato.

3. Nei casi di cui al paragrafo 2, lettere a) e c), il titolare del trattamento attua **misure appropriate** per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il **diritto di ottenere l'intervento umano** da parte del titolare del trattamento, di **esprimere la propria opinione e di contestare la decisione**.

4. Le decisioni di cui al paragrafo 2 non si basano sulle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, a meno che non sia d'applicazione l'articolo 9, paragrafo 2, lettere a) o g), e non siano in vigore misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato.

Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di I.A.

Settembre 2023: Decalogo del Garante in 10 punti su quali sono regole che Governo e regioni devono rispettare per poter trattare dati sanitari tramite sistemi i.a.:

1: serve una norma che costituisca base giuridica trattamento (che deve passare per parere Garante) e che specifica tipo dati, operazioni eseguibili, motivi interesse pubblico rilevanti, misure appropriate e specifiche per diritti e interessi, anche perché si tratta di “profilazione” (creazione profili rischio sanitario) sulla base processi automatizzati

2: principi accountability e privacy by design e by default: realizzazione sistemi di i.a. devono integrare sin dall’inizio tutte le misure a tutela dati sanitari e rispetto principio proporzionalità trattamento rispetto all’interesse perseguito

segue

3: corretta individuazione ruoli nella governance dei dati (titolare e responsabile)

4: rispetto principi di conoscibilità, non esclusività e non discriminazione algoritmica (v. Consiglio di Stato)

5: obbligo valutazione d'impatto su protezione dati

6: qualità dei dati utilizzati da IA: dato deve essere esatto, aggiornato, adeguato, pertinente. Banca dati utilizzata deve essere dinamica e aggiornata. Dato inesatto o non aggiornato influenza negativamente efficacia e correttezza risultati algoritmi

7: integrità e riservatezza dati

8: obblighi di correttezza e trasparenza

9: ruolo supervisione umana

10: dignità e identità personale. Possibili conflitti d'interessi con principi etici e obblighi deontologici che vanno tenuti in consideraz.

Artt. 5 e 6 GDPR: Il principio di liceità del trattamento

Il trattamento di dati personali è **lecito se trova fondamento in una delle basi giuridiche** indicate dall'art. 6 GDPR:

a) l'interessato ha espresso il **consenso** al trattamento dei propri dati personali per una o più specifiche finalità;

b) 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;

c) il trattamento è necessario per adempiere un **obbligo legale** al quale è soggetto il titolare del trattamento;

d) il trattamento è necessario per la **salvaguardia degli interessi vitali** dell'interessato o di un'altra persona fisica;

e) 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;

f) 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 (= **bilanciamento rimesso alla responsabilità del titolare**)

Proposta «digital omnibus»: Legittimo interesse come base giuridica addestramento algoritmi I.A.

Articolo 88 quater

Trattamento nel contesto dello sviluppo e del funzionamento dell'IA

Qualora il trattamento dei dati personali sia necessario al fine di tutelare gli interessi del titolare del trattamento nel contesto dello sviluppo e del funzionamento di un sistema di IA quale definito all'articolo 3, punto 1), del regolamento (UE) 2024/1689 o di un modello di IA, tale trattamento può essere effettuato per il perseguimento di interessi legittimi ai sensi dell'articolo 6, paragrafo 1, lettera f), del regolamento (UE) 2016/679, se del caso, tranne qualora altre normative dell'Unione o nazionali richiedano esplicitamente il consenso e qualora su tali interessi prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che prevedono la protezione dei dati personali, in particolare se l'interessato è un minore.

Qualsiasi trattamento di questo tipo è soggetto a misure organizzative e tecniche nonché a garanzie adeguate per la tutela dei diritti e delle libertà dell'interessato, ad esempio per garantire il rispetto del principio della minimizzazione dei dati durante la fase di selezione delle fonti e la fase di addestramento e di prova di un sistema di IA o di un modello di IA e per evitare che non siano divulgati i dati rimasti nel sistema di IA o nel modello di IA al fine di garantire una maggiore trasparenza agli interessati e assicurare a questi ultimi il diritto incondizionato di opporsi al trattamento dei loro dati personali.".

Il consenso

Secondo la definizione dell'art. 4 GDPR, per **consenso** si intende «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»

- Il **consenso dei minori** è valido, in Italia, a partire dai **14 anni**. Sotto tale età occorre il consenso dei genitori o di chi ne fa le veci (artt. 8 GDPR e 2-*quinquies* d.lgs. 196/2003)
- Per il trattamento delle «particolari categorie di dati» (dati sensibili) di cui all'art. 9 GDPR e per le decisioni basate unicamente su trattamenti automatizzati (per es. profilazione) il consenso deve essere **esplicito**, non basta neanche l'inequivocabilità

Art. 5 GDPR: Principio di correttezza e trasparenza

Lo strumento per assicurare il rispetto di tali principi è

l'INFORMATIVA

- deve avere **forma concisa, trasparente, intelligibile** per l'interessato e **facilmente accessibile**, scritta con **linguaggio chiaro e semplice** (art. 12, par. 1), in particolar modo quando destinata ai minori (considerando 58)
- è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, soprattutto nel contesto di servizi online (art. 12, par.1 e considerando 58), anche se sono ammessi "altri mezzi"
- L'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati, se raccolti direttamente presso l'interessato (art. 13).
- Nel caso di dati personali non raccolti direttamente presso l'interessato (art. 14), l'informativa deve essere fornita entro un termine ragionevole (che non può superare 1 mese dalla raccolta), oppure al momento della comunicazione dei dati

Contenuto dell'informativa

Deve contenere tassativamente:

- i dati di contatto del Titolare, del suo rappresentante e del Responsabile della protezione dei dati, se vi sono;
- finalità e base giuridica del trattamento (in caso sia il legittimo interesse, va indicato qual è)
- eventuali destinatari o categorie di destinatari;
- se trasferisce i dati personali in Paesi terzi e, in caso, attraverso quali strumenti
- il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo;
- la possibilità di revocare in qualsiasi momento il consenso al trattamento;
- I diritti e gli strumenti di tutela dell'interessato;

Gli altri principi fondamentali del GDPR

UNIVERSITÀ POLITECNICA DELLE MARCHE

- **PRINCIPIO DI FINALITA' DEL TRATTAMENTO** (artt. 5 e 6): i dati devono essere trattati esclusivamente nell'ambito delle finalità (determinate, esplicite e legittime) che si intendono perseguire e che sono state dichiarate nell'informativa. Divieto di trattamenti incompatibili con tali finalità
- **PRINCIPIO DI NECESSITA' E MINIMIZZAZIONE DEL TRATTAMENTO**: il trattamento deve ridurre al minimo l'utilizzo dei dati personali, i quali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati
- **PRINCIPIO DI LIMITAZIONE DELLA CONSERVAZIONE**: i dati devono essere conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati
- **PRINCIPIO DI ESATTEZZA**: i dati trattati devono essere esatti e aggiornati e deve essere sempre possibile rettifica o cancellazione dei dati inesatti
- **PRINCIPIO DI INTEGRITA' E RISERVATEZZA**: il trattamento deve 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

Il principio di responsabilizzazione del titolare del trattamento

È una delle principali novità del GDPR, la cui filosofia complessiva è pervasa da tale approccio, secondo il quale **è compito del titolare individuare le soluzioni maggiormente adeguate al fine di garantire il rispetto dei principi e delle norme del GDPR e dei diritti degli interessati** (**c.d. *accountability***)

- Ne sono espressione principale i criteri della **privacy *by default* e *by design*,** ossia la necessità di configurare il trattamento prevedendo fin dalla fase di progettazione e per impostazione predefinita le garanzie indispensabili al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo nel quale il trattamento viene svolto e dei rischi per i diritti e le libertà degli interessati (art. 25 GDPR)

art 30: Registro delle attività di trattamento

«Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità.»

Sostituisce precedente obbligo notifica preventiva al Garante di particolari tipologie di trattamento = ottica responsabilizzante e semplificatoria

impone una mappatura di tutte le attività di trattamento, utile sia per titolare sia per eventuali controlli Garante

- **Obbligatorio se** il trattamento:

- presenta un rischio per i diritti e le libertà dell'interessato
- non è occasionale
- include dati personali appartenenti a particolari categorie di dati
- include dati personali relativi a condanne penali e reati

Art. 35: Valutazione d'impatto sulla protezione dati personali (DPIA)

Deve essere effettuata quando trattamento che si intende svolgere è connotato da particolari rischi per i diritti e libertà fondamentali persone (necessaria quindi valutazione preliminare al riguardo in sede progettazione trattamento)

Trattamenti in cui è **obbligatoria:**

a) **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) 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) sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Il Garante ha predisposto apposito documento orientativo: ALLEGATO 1 Elenco delle tipologie di trattamenti soggetti al meccanismo di coerenza da sottoporre a valutazione di impatto.pdf

Se all'esito DPIA emerge elevato rischio per diritti e libertà: necessaria **consultazione preventiva Garante**

artt. 37-39: Responsabile della Protezione dei dati (RDP)

È un soggetto designato dal titolare o dal responsabile del trattamento per assolvere a **funzioni di supporto e di controllo, consultive, formative e informative relativamente all'applicazione del GDPR**. A tal fine, deve essere "tempestivamente e adeguatamente" coinvolto in tutte le questioni riguardanti la protezione dei dati personali anche con riferimento ad attività di interlocuzione con l'Autorità garante. Coopera, inoltre, con l'Autorità e costituisce il punto di contatto rispetto a quest'ultima e agli interessati, in merito alle questioni connesse al trattamento dei dati personali

v. le FAQ del Garante

Deve essere dotato delle **qualità professionali e culturali idonee** per il ruolo svolto e deve avere necessaria **indipendenza** dal titolare:

- Titolare non deve dare istruzioni al RPD né può rimuoverlo o penalizzarlo
- Può essere una figura esterna alla struttura
- Può svolgere altri incarichi, purché non in conflitto d'interessi
- Deve avere risorse necessarie all'esecuzione dei suoi compiti

Art 33-34 Violazione di dati personali (c.d. data breach)

In caso di violazione dei dati personali, il titolare del trattamento **notifica** la violazione **all'autorità di controllo competente (= il Garante)**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.

Contenuto della notifica al Garante:

- descrivere la natura della violazione
- categorie e numero di interessati
- dati di contatto del DPO
- probabili conseguenze della violazione
- misure adottate o che si intende adottare per attenuare le conseguenze

Home - Notifica di una violazione dei dati personali (data breach)

Garante e contrasto al web scraping

- **Provvedimento 20/05/2024: Web scraping ed intelligenza artificiale generativa - nota informativa e possibili azioni di contrasto**

l'Autorità ha ritenuto necessario fornire a quanti pubblicano online dati personali in qualità di titolari del trattamento talune prime indicazioni sull'esigenza di compiere alcune valutazioni in ordine all'esigenza di adottare accorgimenti idonei a impedire o, almeno, ostacolare il web scraping.

Al riguardo **precisazioni anche da parte di ANAC**, con parere del 7/2/2025: «Web scraping ed intelligenza artificiale generativa. Richiesta di parere sulle misure da introdurre per prevenire il web scraping dei dati personali nella sezione "Amministrazione Trasparente"» : contrasto a web scraping non può portare a limitare l'accesso alla sezione «Amministrazione trasparente» dei siti web delle pp.aa., in contrasto con obblighi trasparenza d.lgs. 33/2013