UNIVERSITÀ
DEL SALENTO

"Linee guida privacy sul Processo decisionale automatizzato e profilazione" in compliance al Regolamento UE 679/2016

La realizzazione del documento è stata curata da:

- *Dott.ssa Giuseppina CAMPANILE*
- *Dott.ssa Alessandra CARITÀ*
- *Avv. Maria Ida Anna GIANNELLI*
- *Ing. Tiziana MONTANARO*

SOMMARIO

INTRODUZIONE

Il presente documento è stato redatto al fine di fornire una guida operativa di Ateneo in tema di profilazione e processo decisionale automatizzato in applicazione delle disposizioni introdotte dalla normativa europea in materia di protezione dati personali, ed in particolare dagli articoli 4 e 22 del Regolamento europeo n.2016/679 (GDPR).

Nella redazione delle presenti Linee Guida si è tenuto conto del:

- "*Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*" -GDPR;
- Decreto Legislativo 10 agosto 2018 n, 101 "*Disposizioni per l'adeguamento della Normativa Nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)*";
- Decreto legislativo 30 giugno 2003, numero 196, recante il "*Codice in materia di protezione dei dati personali*", come modificato con la L. 27 dicembre 2019, n. 160, con il D.L. 14 giugno 2019, n. 53, con il D.M. 15 marzo 2019 e con il Decreto di adeguamento al GDPR (Decreto Legislativo 10 agosto 2018, n. 101);
- Decreto legislativo 7 marzo 2005, n. 82 "*Codice dell'Amministrazione Digitale (CAD)*" come modificato da ultimo con D.L. 30 dicembre 2019, n. 162;
- Linee Guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del Regolamento 2016/679 adottate il 3 ottobre 2017, come modificate il 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione Dati – WP 251;
- Linee guida sulla trasparenza ai sensi del Regolamento 2016/679 adottate il 29 novembre 2017, come modificate l'11 aprile 2018 dal Gruppo di Lavoro articolo 29 per la protezione Dati WP 260;
- Manuale sulla sicurezza nel trattamento dei dati personali adottato da European Union Agency for Network and Information Security (ENISA) nel dicembre 2017;
- Consiglio d'Europa - Raccomandazione CM/Rec(2010)13 del Comitato dei Ministri agli Stati Membri sulla protezione delle persone fisiche con riguardo al trattamento automatizzato di dati personali nel contesto di attività di profilazione (Adottata dal Comitato dei Ministri il 23 novembre 2010 in occasione del 1099mo incontro dei Rappresentanti dei Ministri;

- Consiglio d'Europa - Raccomandazione CM/REC (2018)x del Comitato dei Ministri agli Stati membri sugli orientamenti per promuovere, proteggere e adempiere i diritti dei minori nell'ambiente digitale (progetto riveduto, 25 luglio 2017).

Il presente documento è suscettibile di integrazioni, modifiche e correttivi alla luce dell'evoluzione della normativa di riferimento

1. DEFINIZIONI

1.1. PROFILAZIONE

Per profilazione si intende, ai sensi e per gli effetti dell'art. 4, comma 4, del Regolamento europeo n.2016/679 (GDPR) "*una qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*".

La profilazione richiede che:

- la raccolta dei dati e la loro successiva elaborazione debba essere automatizzata;
- oggetto dell'elaborazione debbano essere i dati personali;
- l'obiettivo finale debba essere quello di valutare aspetti personali relativi a una persona fisica.

La profilazione è quindi un processo decisionale automatizzato finalizzato alla raccolta di informazioni personali degli individui per suddividerli in gruppi o categorie a seconda del loro comportamento o delle loro caratteristiche. Il profilo dell'individuo così ottenuto potrà poi essere usato per prevedere o analizzare in modo automatizzato la persona e le sue preferenze.

1.2. PROCESSO DECISIONALE AUTOMATIZZATO

Il processo decisionale automatizzato è disciplinato dall'art. 22 del Regolamento EU/2016/679 che prevede, al comma 1, che "*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*."

Il processo decisionale automatizzato, quindi, è lo strumento che consente di assumere decisioni con mezzi tecnologici senza l'intervento o il coinvolgimento umano ("algoritmizzazione").

Le decisioni automatizzate possono essere basate su qualsiasi tipo di dati, ad esempio:

- dati forniti direttamente dall'interessato;
- dati osservati riguardo a una persona;
- dati derivati o desunti, come un profilo della persona che è già stato creato.

1.3. INTERAZIONI TRA PROFILAZIONE E PROCESSO DECISIONALE AUTOMATIZZATO

In generale, la profilazione consiste nella raccolta di informazioni su una persona (o un gruppo di persone) e nella valutazione delle loro caratteristiche o dei loro modelli di comportamento al fine di

includerli in una determinata categoria o gruppo, in particolare per analizzare e/o fare previsioni (ad es. sui loro comportamenti, sui loro interessi presenti e futuri etc)[1].

Esistono tre modalità d'uso della profilazione:

a. profilazione generale;
b. processo decisionale basato sulla profilazione;
c. decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produce
   effetti giuridici o incide in modo analogo significativamente sull'interessato.

Il processo decisionale automatizzato è il mezzo che consente di assumere decisioni senza il coinvolgimento di un essere umano che possa influenzare ed eventualmente cambiare il risultato attraverso la sua autorità o competenza.

Ne consegue che le decisioni automatizzate possono essere prese ricorrendo o meno alla profilazione.

Per contro la profilazione può essere svolta senza che vengano prese decisioni automatizzate[2].

Ma la decisione automatizzata e la profilazione non sono necessariamente attività separate. Se una decisione automatizzata può essere adottata senza aver creato un profilo dell'individuo, essa , in altri casi può trasformarsi in profilazione a seconda del modo in cui i dati vengono utilizzati[3].

2. DISPOSIZIONI SUL PROCESSO DECISIONALE AUTOMATIZZATO

2.1. INTRODUZIONE

Il processo decisionale automatizzato è un processo in cui la decisione viene assunta da un complesso di algoritmi[4] implementati da sistemi tecnologici senza che sia previsto un significativo intervento umano. Per intervento umano significativo si deve intendere quello in cui chi interviene può prendere una

---

[1] A riguardo le Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottate il 3 ottobre 2017, come modificate il 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione Dati – WP 251 chiariscono che l'articolo 4, punto 4, fa riferimento a "*qualsiasi forma di trattamento automatizzato*" e non al trattamento "*unicamente*" automatizzato (di cui all'articolo 22). Pertanto, la profilazione deve implicare una qualche forma di trattamento automatizzato, sebbene il coinvolgimento umano non comporti necessariamente l'esclusione dell'attività dalla definizione.

[2] A riguardo le Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottate il 3 ottobre 2017, come modificate il 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione Dati – WP 251 portano l'esempio dell'istituto bancario che prima di decidere se concedere o meno un prestito prende in considerazione il punteggio sull'affidabilità creditizia del mutuatario, associandolo a ulteriori interventi significativi svolti da esseri umani prima che venga adottata qualsiasi decisione relativa alla persona in questione.

[3] Sulla base delle Linee guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottate il 3 ottobre 2017, come modificate il 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione Dati – WP 251 ad esempio infliggere una multa per eccesso di velocità esclusivamente sulla base delle prove fornite dall'autovelox è un processo decisionale automatizzato che non implica necessariamente la profilazione. Tuttavia, la decisione di infliggere la multa sarebbe basata sulla profilazione se le abitudini di guida della persona fossero state monitorate nel tempo e, ad esempio, l'ammontare della multa fosse il risultato di una valutazione che coinvolge altri fattori quali l'eventuale recidiva di eccesso di velocità o l'eventuale recente violazione di altre disposizioni del codice della strada.

[4] Algoritmo: sequenza definita di passi elementari (istruzioni) che servono per risolvere un problema

decisione tale da modificare il risultato dell'algoritmo automatizzato anche alla luce di altre condizioni che non son state tenute in considerazione nel trattamento algoritmico.

Un esempio di processo automatizzato può essere considerato l'autovelox che fa scattare la multa a seguito del rilevamento della velocità di transito del veicolo da parte di un dispositivo elettronico che segnala il superamento di una soglia di velocità preimpostata.

Un altro esempio può essere la valutazione del rendimento lavorativo di un dipendente basato su un certo numero di parametri esempio: numero di task portati a termine nell'unità di tempo; numero di email inviate, numero di telefonate evase nell'unità di tempo etc..

In ambito universitario si può pensare al processo che consente gli scatti stipendiali alla luce di alcuni parametri rilevati o acquisiti senza che sia prevista la presenza di apposita commissione di valutazione.

Per sommi capi l'art. 22 del GDPR afferma **il divieto** di sottoporre le persone fisiche ad un trattamento di dati completamente automatizzato (senza l'intervento umano) quando le conseguenze di questo trattamento producano effetti giuridici sulla persona o effetti analogamente gravi.

Prevede la **presenza di eccezioni** alla regola, e, in presenza di tali eccezioni il titolare del trattamento deve **adottare misure adeguate** per tutelare i diritti, le libertà ed i legittimi interessi dell'interessato; ancora una volta, in linea con l'impianto normativo del GDPR si riconosce all'interessato il diritto di avere il controllo dei propri dati da cui il diritto ad essere informato sulla logica del trattamento automatizzato e sulle conseguenze dello stesso; il diritto di ottenere l'intervento umano e di contestare la decisione.

Inoltre, il titolare **è tenuto a svolgere una valutazione di impatto** sulla protezione dei dati che si rende utile anche a chiarire la natura e gravità dei rischi legati al trattamento nonché il tipo di garanzie che devono essere riconosciute.

2.2. ANALISI DI DETTAGLIO DELL'ARTICOLO

L'art. 22 del GDPR, "Processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione" afferma quanto segue:

"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."

Decisione basata unicamente sul trattamento automatizzato: il trattamento è esclusivamente automatizzato se il risultato della valutazione si raggiunge solo per applicazione di un algoritmo con sistemi tecnologici che, sulla base di dati in input, a seguito di opportuna elaborazione software producono dei dati in output (risultato).

La decisione produce effetti giuridici quando influisce su: libertà di associazione, libertà di voto, libertà di intraprendere azioni legali, cancellazione di un contratto, diritto ad usufruire di agevolazioni fiscali, prestazioni sociali, indennità di alloggio, rifiuto di cittadinanza, ammissione in un paese, etc..

Anche se gli effetti non sono di natura giuridica ma sono ugualmente gravi da incidere sulla vita di una persona ***la decisione incide in modo analogo significativamente sulla sua persona quando***:

- incide in maniera significativa sulle circostanze, sul comportamento o sulle scelte dell'interessato;
- ha un impatto prolungato o permanente sull'interessato; o
- nel caso più estremo, porta all'esclusione o alla discriminazione di persone.

Il considerando 71 elenca due esempi esplicativi:

- rifiuto automatico di una domanda di credito online
- pratiche di assunzione elettronica senza interventi umani

Le *Linee Guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai fini del regolamento 2016/679 adottate il 3 ottobre 2017, come modificate il 6 febbraio 2018 dal Gruppo di lavoro articolo 29 per la protezione Dati – WP 251* (d'ora innanzi LG WP 251) aggiungono altri esempi:

- decisioni che influenzano le circostanze finanziarie di una persona, come la sua ammissibilità al credito;
- decisioni che influenzano l'accesso di una persona ai servizi sanitari;
- decisioni che negano a una persona un'opportunità di impiego o pongono tale persona in una posizione di notevole svantaggio;
- decisioni che influenzano l'accesso di una persona all'istruzione, ad esempio le ammissioni universitarie.

In tutti i casi in cui si possono avere effetti significativi, o sono in gioco effetti giuridici sulla persona è necessario prevedere un processo umano in grado di controllare, validare, confermare o smentire la valutazione automatizzata alla quale quindi non si può ricorrere in maniera esclusiva[5].

[5] Sentenza 13 settembre 2019, n. 10964 del T.A.R. Lazio che accoglie il ricorso di un docente ed annulla un'ordinanza del Ministero dell'Istruzione, dell'Università e della Ricerca, Ufficio Scolastico Regionale per la Puglia in quanto ritiene che sia "dirimente in punto di diritto l'argomento secondo cui è mancata nella fattispecie una vera e propria attività amministrativa, essendosi demandato ad un impersonale algoritmo lo svolgimento dell'intera procedura di assegnazione dei docenti alle sedi disponibili nell'organico dell'autonomia della scuola"; sentenza commentata da https://www.altalex.com/documents/news/2019/10/31/algoritmo-puo-sostituire-attivita-uomo-in-procedura-amministrativa

2.3. ECCEZIONI AL DIVIETO DI TRATTAMENTO AUTOMATIZZATO ESCLUSIVO

Esistono delle eccezioni per le quali il ricorso ad una esclusiva valutazione automatizzata può legittimamente incidere sui diritti della persona anche senza intervento umano:

1. quando sia necessaria per concludere o eseguire un contratto tra interessato e titolare del trattamento;
2. quando sia autorizzata dal diritto dell'Unione o dello stato membro;
3. quando vi sia il consenso esplicito dell'interessato.

In questi casi, ad esclusione del caso 2, il titolare del trattamento deve adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato: il **diritto di ottenere l'intervento umano** da parte del titolare del trattamento e il **diritto di esprimere la propria opinione e di contestare la decisione**.

2.4. PROCESSO DECISIONALE INTERAMENTE AUTOMATIZZATO E CATEGORIE DI DATI PARTICOLARI

Il processo decisionale automatizzato che comporta l'uso di categorie particolari di dati personali è consentito soltanto se sono soddisfatte le seguenti condizioni cumulative (articolo 22, paragrafo 4):

- esiste un'eccezione applicabile in virtù dell'articolo 22, paragrafo 2;
- si applicano la lettera a) o g) dell'articolo 9, paragrafo 2:
  - a) "*vi è un consenso esplicito dell'interessato*" o
  - g) "*il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;*"

In questi casi il titolare deve mettere in atto misure di garanzia adeguate per proteggere i diritti e le libertà dell'interessato. A tale scopo lo svolgimento di una valutazione di impatto renderà chiaro al titolare la natura delle misure di garanzia in relazione ai rischi che la valutazione avrà evidenziato.

2.5. OBBLIGHI IN MATERIA DI TRASPARENZA E DIRITTO DI ACCESSO.

Per ogni trattamento che prevede un processo decisionale esclusivamente automatizzato è necessario:

1. comunicare all'interessato che sarà svolta tale tipo di attività
2. fornire informazioni significative sulla logica utilizzata
3. spiegare l'importanza e le conseguenze previste da tale trattamento

Questo in adempimento di quanto previsto nel GDPR in: art. 13 par. 2 lettera f), art. 14 par. 2 lettera g) e considerando 61 in cui si evidenziano l'importanza di informare l'interessato in merito all'esistenza di un trattamento automatizzato e le sue conseguenze.

Nel rispettare tale "diritto all'informazione" si contempera contestualmente il diritto dell'interessato ad esprimere la propria opinione e contestare la decisione secondo quanto previsto dall'art. 22 par. 3.

In particolare, quando il titolare è una Pubblica Amministrazione che intende adottare una decisione che può avere effetti avversi su di una persona, la Pubblica Amministrazione ha l'obbligo di sentirla prima di agire e di consentirle l'accesso ai suoi archivi e documenti, e, infine, ha l'obbligo di fornire le ragioni della propria decisione.

L'informazione dell'esistenza di un trattamento automatizzato, non è sufficiente per consentire alla persona l'esercizio del diritto di opporsi, ma è altresì necessario conoscere la logica che viene applicata (calcoli, misurazioni, valutazioni, condizioni) e i dati sui quali l'algoritmo stesso opera. È importante fornire "informazioni significative" nel senso che esse siano sufficienti a cogliere i meccanismi che sono alla base della decisione. Non sempre è necessario giungere alla pubblicazione dell'algoritmo utilizzato, ma è importante spiegare quali dati siano acquisiti in input, se trattasi di dati prelevati da altre fonti ed il livello di aggiornamento degli stessi e contestualmente è utile esplicitare, anche in forma grafica, i passi adottati per giungere alla decisione.

In alcuni casi tuttavia la pubblicazione dell'algoritmo può essere prevista a seguito di accesso agli atti allo scopo di tutelare il principio di trasparenza dell'azione amministrativa anche in linea con quanto richiesto dall'art. 15 par.1 lettera h[6].

Il titolare del trattamento, inoltre, deve fornire informazioni complete ed esplicative delle conseguenze del trattamento decisionale automatizzato ricorrendo anche ad esempi concreti e reali di possibili effetti.

Per esempio, è consigliato il ricorso a grafici e tecniche visive in generale per meglio raccontare e descrivere gli effetti delle decisioni o per illustrare quello che è accaduto nel passato in casi simili.

In alcuni casi si può prevedere il ricorso a meccanismi che consentono all'interessato di verificare il proprio profilo o collocazione all'interno di una decisione automatizzata.

Allo stesso tempo si possono fornire agli interessati metodi e strumenti per aggiornare i dati presenti nel proprio profilo.

2.6. MISURE DI GARANZIA

L'art. 22 per i casi contemplati nel paragrafo 2 in cui si applichino decisioni automatizzate relativamente a:

[6] Si veda sentenza T.A.R. Lazio Sez. III bis, 14 febbraio 2017, n. 3769, e le considerazioni su "L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà di Andrea Simoncini BioLaw Journal – Rivista di BioDiritto, n. 1/2019

- esecuzione di un contratto
- presenza di consenso esplicito

prevede che l'interessato possa chiedere:

- un intervento umano
- esprimere il proprio punto di vista e contestare una decisione

L'intervento umano richiesto deve poter:

- valutare i dati pertinenti in modo approfondito
- considerare ulteriori dati forniti dall'interessato

L'interessato, inoltre, in base al considerando 71 ha il diritto di ottenere una spiegazione della decisione conseguita.

Da queste misure di garanzia ne discende che è sempre necessario salvaguardare il principio di trasparenza del trattamento con lo scopo di fornire all'interessato tutti gli strumenti necessari alla propria difesa e salvaguardia dei propri diritti.

Il titolare del trattamento deve porre estrema attenzione ad aspetti quali:

- natura e pertinenza dei dati rispetto al processo decisionale in corso; un set errato di dati di partenza non può far altro che alterare i risultati derivanti dall'applicazione del processo automatizzato;
- processo logico che è alla base della sequenza di operazioni algoritmiche che portano alla decisione
- controlli regolari di garanzia della qualità dei sistemi per assicurare che le persone siano trattate in maniera equa e non siano discriminate sulla base di categorie particolari di dati personali o in altro modo;
- verifica degli algoritmi – testare gli algoritmi utilizzati e sviluppati dai sistemi di apprendimento automatico per dimostrare che stanno effettivamente funzionando come previsto e non producono risultati discriminatori, errati o ingiustificati;
- laddove il processo decisionale basato sulla profilazione abbia un impatto elevato sulle persone fisiche prevedere un audit di terzi che certifica il buon funzionamento dell'algoritmo o del sistema automatico.
- per gli algoritmi di terzi, ottenimento di garanzie contrattuali che sono stati effettuati audit e test e che l'algoritmo è conforme alle norme concordate;
- misure specifiche per la minimizzazione dei dati al fine di prevedere periodi di conservazione chiari per i profili e per tutti i dati personali utilizzati durante la creazione o l'applicazione dei profili;

- utilizzo di tecniche di anonimizzazione o pseudonimizzazione nel contesto della profilazione;
- modi per consentire all'interessato di esprimere il proprio punto di vista e contestare la decisione;
- meccanismo per l'intervento umano in determinati casi, ad esempio fornendo un collegamento a una procedura di ricorso nel momento in cui la decisione automatizzata viene trasmessa all'interessato, con termini concordati per il riesame e la designazione di un punto di contatto per qualsiasi domanda.
- categorie di dati che sono state o saranno utilizzate nella profilazione o nel processo decisionale;
- motivi per i quali tali categorie sono considerate pertinenti;
- modalità di creazione del profilo utilizzato nel processo decisionale automatizzato, ivi comprese le statistiche utilizzate nell'analisi;
- motivi per i quali tale profilo è pertinente per il processo decisionale automatizzato;
- modalità di utilizzo del profilo ai fini di una decisione riguardante l'interessato.

Il titolare del trattamento può altresì valutare opzioni quali:

- meccanismi di certificazione per i trattamenti;
- codici di condotta per la verifica dei processi che comportano apprendimento automatico;

Il titolare inoltre deve rendere chiaro all'interessato il suo diritto ad opporsi.

In sintesi possiamo riconoscere i principi che devono essere tutelati come segue:

1. il principio di non esclusività: si concretizza nel divieto di applicare decisioni derivate esclusivamente dall'applicazione di un processo decisionale automatizzato.
2. il principio di conoscibilità: si concretizza in una serie di azioni che il titolare del trattamento deve intraprendere per garantire la chiarezza delle decisioni intraprese.
3. il principio di non discriminazione: si concretizza nell'assicurare che l'algoritmo implementato e la natura dei dati considerati non comportino effetti discriminatori per alcune categorie di persone.

3. I PROCESSI DI PROFILAZIONE E I MINORI

Anche in ambito universitario, seppur in maniera meno diffusa rispetto al settore privato, può accadere di utilizzare processi automatizzati per l'acquisizione ed il trattamento dei dati di minori (come ad esempio per tutte quelle iniziative del c.d. "Marketing Universitario che si vanno sempre più diffondendosi per orientare ed informare i potenziali nuovi studenti delle Scuole superiori sulle opportunità e le offerte formative delle Università.

3.1.GDPR E MINORI, GESTIRE CONSENSO E PRIVACY

Per garantire maggiore protezione dei dati dei minori sono stati introdotti obblighi supplementari in relazione ai servizi della cosiddetta società dell'informazione e garantire la privacy dei ragazzi sui social e raggiungere così la necessaria compliance in ambito GDPR e minori, anche alla luce del D.lgs. 101 entrato in vigore il 19 settembre 2018.

Ogni ente deve valutare il tipo di pubblico che fornisce dati personali alla sua organizzazione e nel caso in cui si tratti di minorenni, deve attenersi a quanto specificato all'articolo 8 del GDPR.

In merito all'offerta diretta di servizi della società dell'informazione ai minori, l'art. 8, paragrafo 1, GDPR stabilisce che, laddove la base giuridica è il consenso dell'interessato quest'ultimo è validamente prestato qualora il minore abbia almeno 16 anni. Per età inferiori ai 16 anni il trattamento è lecito soltanto se e nella misura in cui il consenso è prestato o autorizzato dal titolare della responsabilità genitoriale, salva la possibilità degli Stati membri di derogare il limite fino a 13 anni. Di conseguenza, mediante adozione di apposita normativa nazionale, ciascuno Stato membro può prevedere un limite di età di 15, 14 o 13 anni.

Il titolare del trattamento dovrà tenere presente tale deroga in caso fornisse un servizio transfrontaliero in quanto non sarà possibile riferirsi semplicemente a quanto stabilito nello stato membro sede del suo stabilimento principale.

Con particolare riferimento alla normativa italiana, l'art. 2-quinquies del D.lgs. 101/2018 stabilisce che il limite di età per il consenso valido non potrà essere inferiore ai 14 anni.

A tanti è apparsa una scelta opportuna in quanto va ad uniformarsi con quanto stabilito per i consensi relativi ad altre discipline (vedi legge n. 184 del 1983 sull'adozione, legge n. 71 del 2017 sul cyberbullismo).

Ulteriore specificazione si trova nel par. 3 dell'art. 8 GDPR che stabilisce che le norme relative ai requisiti di autorizzazione genitoriale nei confronti dei minori non pregiudicano "*le disposizioni generali del diritto dei contratti degli Stati membri, quali le norme sulla validità, la formazione o l'efficacia di un contratto rispetto a un minore*". Di conseguenza, i requisiti per la validità del consenso all'uso dei dati relativi a minori rientrano in un quadro giuridico da considerarsi distinto dal diritto contrattuale nazionale.

Pertanto, i due regimi giuridici possono essere applicati simultaneamente ma tanto non significa che siano coincidenti.

3.2.LA RETE E I MINORI: PERCHÉ RICHIEDONO MAGGIORI TUTELE

Le ragioni di una tutela privilegiata nei confronti dei minori sono esplicate chiaramente dallo stesso legislatore comunitario nel Considerando 38 del GDPR ove è previsto che "*I minori meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei*

rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali. Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo dei dati personali dei minori a fini di marketing o di creazione di profili di personalità o di utente e la raccolta di dati personali relativi ai minori all'atto dell'utilizzo di servizi forniti direttamente a un minore. […]".

È opportuno premettere che l'art. 8 GDPR non riguarda qualunque trattamento online di dati che si riferiscano ai minori, né qualunque servizio della società dell'informazione al quale i minori possano accedere, bensì si applica **solo ai servizi oggetto di offerta diretta e il cui legittimo trattamento sia basato sul consenso informato dell'interessato.**

Quindi, a titolo esemplificativo, se un minore acquista online suonerie per smartphone la raccolta dei dati (nome, cognome, indirizzo e-mail, dettagli di pagamento) sarà necessaria all'esecuzione di un contratto e pertanto il trattamento dei dati sarà lecito ai sensi dell'art. 6, par. 1, lettera b, GDPR.

Se, invece, il titolare intende utilizzare l'indirizzo e-mail del minore anche per l'invio di newsletter, sarà necessario raccogliere il suo consenso in quanto il trattamento dei dati personali per finalità di marketing non rientra nell'ambito del contratto.

Tanto è valido, come pure previsto dal Gruppo ex art. 29 nelle Linee guida sul consenso aggiornate al 10 aprile 2018, ad esclusione del caso in cui "*un prestatore di servizi della società dell'informazione chiarisce ai potenziali utenti che il servizio è offerto esclusivamente a persone aventi almeno 18 anni, e ciò non è smentito da altri elementi (come il contenuto del sito o piani di marketing)"*. In tale circostanza il servizio non sarà ritenuto fornito direttamente a un minore e l'articolo 8 GDPR non si applicherà.

Il legislatore europeo ha previsto che i minori abbiano maggiori tutele perché sono particolarmente vulnerabili nell'ambiente online e più facilmente influenzabili dalla pubblicità comportamentale. Diversi studi hanno rilevato che le prassi di marketing attraverso i social media, i giochi online e le applicazioni mobile hanno un impatto evidente sul loro comportamento (a tal proposito, vedi qui o qui). Nei giochi online, ad esempio, la profilazione può servire per individuare i giocatori più propensi a spendere o per fornire annunci personalizzati a cui non corrisponde una maturità da parte del minore nel riconoscere la ragione commerciale di una pratica di marketing.

Tuttavia il minore ha diritto a frequentare la rete e pertanto la protezione rafforzata si deve coordinare con la ricerca continua di "*delicati bilanciamenti tra libertà di espressione, pensiero, associazione, e partecipazione dei minori alla vita di relazione e alla costruzione della comunità in cui vivono*".

Un punto che merita di essere segnalato è che ai sensi del considerando 38, il consenso di un genitore o del tutore non è richiesto nel contesto di servizi di prevenzione o consulenza offerti direttamente al minore.

3.3. CONSENSO DEL MINORE DI 16 ANNI: LA SCELTA ITALIANA

I trattamenti di profilazione in ambito Universitario che coinvolgono i minori (ad esempio per le attività di c.d. Marketing Universitario per orientare ed informare i potenziali nuovi studenti di Scuole superiori sulle opportunità le offerte formative) sono prevalentemente orientati a minori che hanno già compiuto i 16 anni di età e, pertanto, a minori che hanno già raggiunto la cosiddetta età del "consenso digitale".

Come anticipato, l'art. 2-quinquies della normativa italiana ha stabilito che "*In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale*".

Pertanto, come nel caso dei processi Universitari orientati a studenti delle Scuole superiori, se il minore afferma di aver raggiunto l'età del consenso digitale, il titolare del trattamento dovrà compiere ogni ragionevole sforzo per verificare la veridicità della dichiarazione in quanto se un minore presta il consenso senza avere l'età sufficiente il trattamento dei dati sarà illecito.

A titolo esemplificativo, in Italia il titolare che voglia assicurarsi che i clienti minorenni ma comunque con età maggiore dei 14 anni si abbonino ai servizi automatizzati in cui è prevista l'acquisizione ed il trattamento di dati personali dovrà:

1. effettuare controlli appropriati per verificarne la veridicità dell'età;
2. acquisire dal minore il consenso al trattamento dei dati personali;

4. VALUTAZIONE DI IMPATTO SUL TRATTAMENTO (DPIA)

I processi automatizzati di profilazione possono comportare dei rischi elevati per i diritti e le libertà delle persone fisiche (art. 35 par. 1). Il Regolamento chiarisce che ciò può verificarsi, in particolare, con l'utilizzo di nuove tecnologie.

Se la valutazione preliminare del rischio condotta su determinati trattamenti di profilazione, mostra effettivamente che i trattamenti in esame comportano un rischio elevato, il titolare è tenuto a condurre una valutazione di impatto sulla protezione dei dati prima di procedere al trattamento. Il Regolamento prevede che una DPIA debba essere condotta, in ogni caso, in presenza di decisioni automatizzate basate su trattamenti automatizzati/profilazioni, trattamenti su larga scala di dati sensibili o monitoraggio su larga scala di aree accessibili al pubblico (art. 35 par. 3).

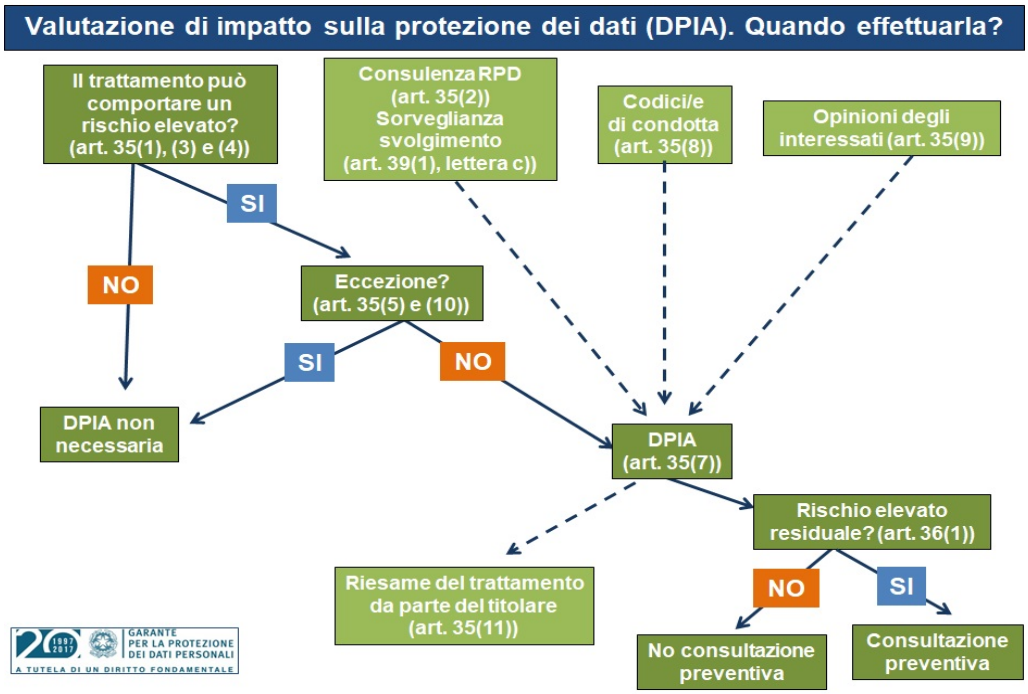
A titolo esemplificativo, alcuni trattamenti dei dati in ambito Universitario che potrebbero essere suscettibili di una valutazione DPIA in quanto svolgono attività di profilazione basata sull'utilizzo di processi automatizzati e nuove tecnologie, sono:

- Utilizzo di cookies tecnici e di profilazione proprie e di terze parti per la navigazione sul Portale e sui siti di Ateneo.
- Marketing Universitario:
- Questionari ed analisi statistiche i cui dati vengono acquisiti attraverso strumenti informatici:

Qui di seguito vengono illustrati i tratti salienti dei un processo di valutazione di impatto che può applicato ad alcuni dei trattamenti sopra richiamati.

IL PROCESSO DPIA

Il WP29 ha fornito linee guida che hanno schematizzato efficacemente i principi base della DPIA:



Il processo di DPIA ha inizio quando nasce l'idea di un nuovo trattamento e prima che questo sia implementato. Il processo deve essere riattivato quando ci sono variazioni significative del trattamento o delle sue modalità che possono mettere a rischio i diritti o le libertà fondamentali degli interessati.

Si può sintetizzare che le fasi di processo da osservare per realizzare una DPIA sono le seguenti modalità, più specificatamente dettagliate nel corso dei paragrafi che seguono:

-Valutare la necessità di adottare e condurre un'attività di DPIA;

-Valutare la conformità al GDPR e al principio di liceità;

-Descrizione del trattamento;

-Valutare il rischio;

-Gestione del rischio;

-Piano di azione

4.1. FASE 1 - VALUTARE LA NECESSITÀ DI CONDURRE UN'ATTIVITÀ DI DPIA

La fase 1 ha come obiettivo la necessità di stabilire se rispetto ad una determinata attività ricorra o meno la necessità di effettuare una Valutazione di Impatto, anche alla luce di quanto stabilito dal Garante per la Protezione dei dati personali.

Si tratta di effettuare una analisi del contesto e, come indicato nel flusso di processo, di condurre una prima analisi di contesto che consenta di identificare quali rischi possono manifestarsi nell'esecuzione di un trattamento o quali cause possono renderlo insicuro.

4.2. FASE 2 – VALUTARE LA CONFORMITÀ DEL TRATTAMENTO AL GDPR

In questa fase si procede ad un'analisi della liceità, della necessità e della proporzionalità del trattamento rispetto alle finalità, con lo scopo di rendere espliciti gli scopi di impiego dei dati perseguiti con il trattamento e le ragioni delle modalità adottate e gli interessi legittimi del Titolare. Le misure previste per conformarsi al GDPR (v. art. 35, paragrafo 7, lettera d) - considerando 90) e, nello specifico, anche al principio di liceità (art. 6) sono valutate attraverso i seguenti tre step:

A. Misure che contribuiscono alla proporzionalità e necessità del trattamento
B. Misure che contribuiscono ai diritti delle persone interessate
C. Liceità.

A. MISURE CHE CONTRIBUISCONO ALLA PROPORZIONALITÀ E NECESSITÀ DEL TRATTAMENTO

La proporzionalità e la necessità sono valutate rispetto all'art. 35 par. 7 lett. b) del GDPR. Nell'allegato delle linee guida WP29[7] - Criteri per un accettabile DPIA, sono fornite alcune tabelle utili a valutare la proporzionalità e necessità del trattamento.

B. MISURE CHE CONTRIBUISCONO AI DIRITTI DELLE PERSONE INTERESSATE

In questa fase è necessario definire i processi privacy (informative, consenso, opposizione al trattamento, accesso alle informazioni, correzione, cancellazione, ecc) idonei a garantire l'esercizio dei diritti.

C. LICEITÀ

La valutazione della liceità si fonda sull'art. 6 del GDPR.

4.3. FASE 3 - DESCRIZIONE DEL TRATTAMENTO

Si tratta di descrivere il ciclo di vita dell'informazione, in termini di raccolta, archiviazione, utilizzo e cancellazione.

Tale fase ha lo scopo di evidenziare quale informazione viene usata, per fare cosa e chi può accedervi. La descrizione dei flussi è fondamentale: solo una precisa comprensione dell'impiego dei dati consente di evidenziare i rischi ai quali si sono esposti.

La comprensione del ciclo di vita delle informazioni può avvenire ricorrendo alle metodologie formulate dalla ISO, che propone il seguente *workflow diagram*, relativo al trattamento di dati personali.

La Natura/Tipologia dei Dati Personali trattati è fondamentale per determinare la valutazione degli impatti potenziali per i diritti e le libertà delle persone in caso di definizione del rischio per accesso illegittimo, modifica indesiderata e perdita o indisponibilità dei dati personali.

Definiti i dati e il contesto coinvolto nel trattamento è possibile descrivere i flussi dei dati personali. Si suggerisce di utilizzare la forma grafica dei flow chart, che si presta a valutazioni d'insieme.

Tabella di esempio di categorie di interessati nell'ambito Universitario:

Categorie di interessati	**Risposta si/no**
Dipendenti	
Docenti	
Assegnisti	
Dottorandi	
Studenti	
Aspiranti collaboratori	
Studenti 150 ore	
Fornitori	
Clienti	
Collaboratori esterni	
Minori	
Altri soggetti da identificare nel caso di contratti di ricerca.	
Stakeholder (partecipanti ai corsi ecc.)	

Tabella di esempio di check list per l'identificazione dei dati personali trattati

Dati personali trattati		
Natura del dato trattato	Tipologia	Si/no
Dati Comuni	Anagrafici	
	Foto	
	video	
Dati Salute	Stato di salute	
	Sorveglianza sanitaria	
	Dati diagnostici	
Dati genetici	Dati genetici	
Dati biometrici	Firma grafometrica	

Dati particolari	Retribuzione	
	Giudizi di idoneità a mansioni specifiche	
	Esposizione a particolari rischi	
Dati giudiziari	Provvedimenti giudiziari	
	Sentenze di condanna	

L'identificazione dei dati personali trattati ha un ruolo centrale per fissare la valutazione degli impatti potenziali per i diritti e le libertà delle persone per le ipotesi di accesso illegittimo, modifica indesiderata e perdita o indisponibilità dei dati personali.

Occorre anche rilevare gli strumenti che sono usati per il trattamento dei dati personali. Nella tabella si propone un esempio di quelli che possono essere gli asset coinvolti in un trattamento di dati personali tenuto conto delle norme ISO e del WP art. 29.

4.4. FASE 4 – VALUTAZIONE DEI RISCHI

In questa fase vanno identificati quali potenziali minacce possono riguardare gli interessati. Il processo di valutazione dei rischi deve tener conto di tutte le entità coinvolte. Possiamo individuare minacce legate ad eventi:

- di contesto
- degli strumenti
- al comportamento umano.

L'analisi dei rischi richiede la corretta identificazione delle minacce che possono aver successo sui dati coinvolti nel trattamento.

La valutazione dei rischi stabilisce il valore delle attività di informazione, identifica le minacce applicabili e le vulnerabilità che esistono (o possono esistere), identifica i controlli esistenti e il loro effetto sul rischio identificato, determina le potenziali conseguenze.

Si possono prendere in considerazione le classi di rischio in relazione all'effetto della minaccia sulle caratteristiche del dato personale. **Le minacce** che possono insidiare le tre caratteristiche fondamentali dei dati personali: **la Riservatezza (R); Integrità (I); Disponibilità (D).**

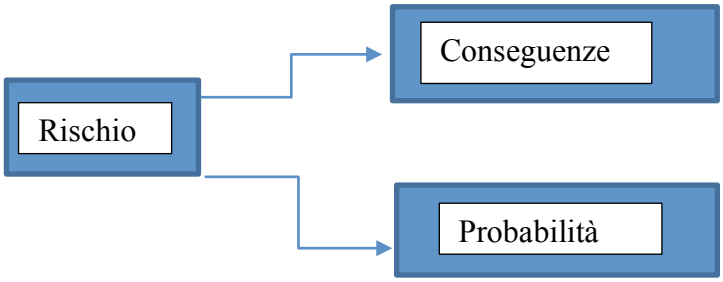
Definizione	**Tipologia di violazione**	**Effetti**
Riservatezza (R)	accesso illegittimo	divulgazione/accesso non autorizzato
Integrità (I)	modifica indesiderata	modifica
Disponibilità (D)	scomparsa dei dati (compresa l'indisponibilità momentanea dei dati)	distruzione/ perdita

4.5.FASE 5 – ANALISI DEL RISCHIO

È la fase destinata a identificare le azioni da intraprendere per contrastare i rischi, tenendo conto che la DPIA ha come obiettivo la riduzione del rischio o di portare il rischio ad un livello accettabile.

Per rischio possiamo intendere la realizzazione di potenziali conseguenze negative e/o non desiderate di un evento. Possiamo definire il Rischio come la combinazione della probabilità (P) e delle conseguenze (impatto) (C) del verificarsi di un particolare evento pericoloso.

La quantificazione dei rischi può quindi essere espressa adottando una funzione del tipo: **R=f (C,P), dove R rappresenta il rischio, C la gravità delle conseguenze e P la probabilità o la frequenza con cui si verificano le conseguenze.**



Risulta conveniente concentrare l'attenzione su possibili scenari di impatto, considerando le potenziali ricadute negative sui diritti e le libertà delle persone i cui dati personali sono trattati. Nella tabella si indicano quelli che sono gli scenari di impatto più rilevanti che poi devono essere calati nel contesto specifico di dove si esegue la DPIA.

Scenario di Impatto	Descrizione
Danno Reputazionale (DR)	Trattamenti di dati personali invasivi della privacy o violazione di dati personali (c.d. «data breach») comportano la delegittimazione da parte degli stakeholder, degli interessati e compromettono la reputazione dell'ente.
Violazioni di Norme di legge (VN)	Trattamenti di dati personali effettuati in modo illecito o viola- zione di dati personali (c.d. «data breach») comportano sanzioni civili/amministrative/penali o il pagamento di penali contrattuali.
Richieste di Risarcimento (RR)	Trattamenti di dati personali effettuati in modo illecito o di violazione di dati personali (c.d. «data breach») comportano richieste di risarcimento da parte degli interessati.

Secondo tale approccio la valutazione sia dell'IMPATTO che della PROBABILITA' di verificarsi dell'evento dannoso sono sviluppate tramite una metodologia qualitativa usando le sotto elencate definizioni:

Livello di Probabilità di successo della minaccia			
1	2	3	4
Trascurabile	**Limitato**	**Significativo**	**Massimo**
Trascurabile: l'esecuzione di una minaccia sfruttando le proprietà delle risorse di supporto non sembra possibile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei archiviati in una stanza protetta da un lettore di badge e un codice di accesso).	Limitato: l'esecuzione di una minaccia sfruttando le proprietà delle risorse di supporto sembra essere difficile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei archiviati in una stanza protetta da un lettore di badge).	Significativo: l'esecuzione di una minaccia sfruttando le proprietà delle risorse di supporto sembra essere possibile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei conservati negli uffici a cui non è possibile accedere senza aver prima effettuato il check-in alla reception).	Massimo: Eseguire una minaccia sfruttando le proprietà delle risorse di supporto sembra essere estremamente facile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei conservati in una lobby).

È in questa Fase che si decide se i livelli di rischio residuo risultano accettabili o richiedono un intervento. Le possibili modalità di gestione dei Rischi sono tradizionalmente quattro:

- **ACCETTARE:** decidere di accettare il rischio, a fronte di una valutazione costi/benefici;
- **RIDURRE:** Mitigare il rischio, ovvero ridurre il rischio ad un livello accettabile per il business, attraverso l'adozione di contromisure sostenibili;
- **TRASFERIRE:** trasferire il rischio ad altre parti (ad es. fornitori, outsourcer, società di assicurazione, cliente, ecc.);
- **RIMUOVERE:** evitare il rischio, rinunciando, ad esempio, ad effettuare il trattamento in esame.

Qualora il rischio residuo sia ritenuto elevato, il titolare del trattamento, prima di procedere al trattamento, consulterà l'autorità di controllo (la *c.d.* Consultazione preventiva, art. 36, paragrafo 1).

4.6. FASE 6 – IL PIANO DI AZIONE

Il piano di azione, che costituisce chiaramente un sostegno all'accountability, consente di definire un piano condiviso delle misure da adottare, delle responsabilità di esecuzione e di verifica, di assunzione da parte del titolare, della consapevolezza del Rischio residuo.

Si tratta di rilevare le misure idonee per ridurre probabilità e impatto. I controlli che il Titolare deve valutare per mitigare i rischi sul trattamento possono riguardare le misure descritte di seguito.

MISURE E CONTROLLI DI TIPO ORGANIZZATIVO

Tali misure sono a loro volta raggruppabili in:

- **Organizzazione e governance:** specifici ruoli e responsabilità all'interno dell'organizzazione, controlli interni di supervisione, definizione dei ruoli per la gestione dei progetti, regole di interazione e le rispettive responsabilità in caso di contitolarità di un trattamento.

- **Processi: procedure e policy interne,** modelli di gestione dei rischi, gestione degli incidenti, delle modifiche e delle notifiche alle Autorità, contratti per proteggere le informazioni trattate in ambiti esternalizzati, accordi che rendano evidente quali informazioni debbano essere condivise, come e con chi.
- **Formazione e consapevolezza:** formazione adeguata del personale e consapevolezza dei potenziali rischi, selezione degli incaricati in base a qualifiche e competenze dimostrabili, guide operative per il personale su come usare i nuovi sistemi e su come condividere i dati quando necessario, materiale informativo per gli utenti, misure che consentano agli interessati di accedere alle proprie informazioni e al tempo stesso che rendano gli interessati consapevoli di come sono protette le proprie informazioni, di prevedere canali con cui gli utenti possano contattare l'organizzazione in caso di necessità di assistenza e con cui le organizzazioni possano rispondere alle richieste di accesso da parte degli interessati.

MISURE E CONTROLLI DI TIPO TECNOLOGICO

Si tratta ad esempio di misure di:

- **Anonimizzazione:** rimozione o mascheratura delle informazioni personali quando non necessarie
- **Pseudonimizzazione:** sostituzione dei riferimenti personali con identificatori finti e garanzia che le informazioni aggiuntive per l'attribuzione dei dati personali ad uno specifico Interessato siano conservate in metadati separati (Considerando 28)
- **Cifratura dei dati,** dei messaggi o degli archivi: soluzioni atte a rendere incomprensibili i dati acceduti tranne ai soli autorizzati che possiedono la chiave di decifratura.

MISURE E CONTROLLI SUI DATI E SUGLI ARCHIVI

Si tratta ad esempio di misure di **misure e controlli di sicurezza fisica**, come, ad esempio sui supporti cartacei, sugli accessi fisici, sulla sicurezza degli impianti, dell'hardware e dei macchinari, protezione da fonti di rischio non umane ecc.