STORYLINE DEL CORSO
PERSONALE DELL'AMMINISTRAZIONE CENTRALE E PERIFERICA DEL MIUR

APPROFONDIMENTI IN TEMA DI SICUREZZA E PRIVACY

Le novità in tema di sicurezza e trattamento dei dati personali alla luce del GDPR e del Codice della privacy (così come novellato dal D.Lgs. 101/2018).

APRILE 2019

Sommario

STORYLINE DEL CORSO
Corso dedicato al Personale dell'Amministrazione Centrale e periferica del MIUR

1 MODULO 1
GDPR: UNA PANORAMICA D'INSIEME

1.1 IL GDPR E LE NORME SULLA GESTIONE DEL RISCHIO

1.1.1 PREMESSA

Il Regolamento (UE) 2016/679[1] del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (indicato anche con l'acronimo GDPR, o RGPD) entra in vigore il 27 aprile 2016 e diviene pienamente applicabile in tutti gli Stati membri dell'Unione Europea dal 25 maggio 2018. Il GDPR, infatti, non richiede un'apposita norma di recepimento da parte degli Stati membri poiché - contrariamente a quanto accade con le direttive europee - il regolamento[2] è direttamente applicabile (*self-executing*).

Il Legislatore europeo ha scelto quindi un approccio diverso rispetto alla previgente disciplina in materia di trattamento di dati personali - contenuta, appunto, nella Direttiva 1995/46/CE (abrogata dal GDPR) in quanto ha ritenuto che lo strumento regolamentare fosse quello più idoneo a garantire l'applicazione omogenea in tutto il territorio dell'Unione Europea.

Con il GDPR si è voluto dare risposta a due esigenze fondamentali: da un lato quella di creare una normativa adeguata alle innovazioni tecnologiche e sociali che sono intervenute successivamente ai tempi per i quali era stata pensata la disciplina della Direttiva 95/46/CE e, dall'altro quella di garantire un adeguato ed elevato livello di protezione dei dati personali che fosse uniforme per tutta l'Unione europea. Pur essendo direttamente applicabile a tutti gli Stati membri, il GDPR rimette alla disciplina nazionale il compito di regolamentare alcuni aspetti specifici, come ad esempio la disciplina dell'accesso agli atti, quella del diritto del lavoro o, ancora, del rapporto tra informazione e privacy.

Il "vecchio" Codice in materia di protezione dei dati personali o Codice della Privacy - D.Lgs. 196/2003 - è stato recentemente oggetto di un'intensa attività di revisione al fine di adeguare l'ordinamento interno al GDPR, e per regolamentare gli aspetti per la cui regolamentazione il GDPR rinviava al Legislatore nazionale.

L'adeguamento è avvenuto con il D.Lgs. 10 agosto 2018 n. 101[3], entrato in vigore il 19 settembre dello stesso anno, ma per il completamento del quadro mancano ancora due importanti

[1] Il cui testo è reperibile nel sito della Gazzetta ufficiale dell'Unione europea al seguente link *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT* e anche nel sito del Garante Privacy al seguente link *https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597* (arricchito con i riferimenti ai Considerando del GDPR).

[2] I regolamenti sono atti giuridici definiti nell'articolo 288 del trattato sul funzionamento dell'Unione europea (TFUE). Sono di applicazione generale, vincolanti in tutti i loro elementi e direttamente applicabili in tutti i paesi dell'Unione europea (UE) in base al secondo comma del medesimo art. 288 TFUE.

[3] La delega al Governo italiano è contenuta nell'art. 13 della L. 163/2017. Il testo del D.Lgs. 101/2018 è reperibile sul sito della Gazzetta Ufficiale al seguente link *http://www.gazzettaufficiale.it/eli/id/2018/09/04/18G00129/sg*. Il

provvedimenti (uno del Garante e l'altro del Ministero della Giustizia) che dovranno dettare regole ulteriori rispettivamente per i trattamenti di dati genetici, biometrici e relativi alla salute, e per i dati relativi a condanne penali e reati.

Nel *corpus* normativo del GDPR si possono individuare due principi cardine: quello della c.d. *accountability* (tradotto nella versione italiana del GDPR con il termine di "responsabilizzazione") e quello relativo alla sicurezza dei dati personali (mediante l'adozione di adeguate misure tecniche e organizzative).

Il primo di questi due principi (contenuto nel secondo comma dell'art. 5 del GDPR[4]) prevede che il titolare del trattamento debba assicurare ed essere in grado di dimostrare di aver rispettato i principi applicabili al trattamento dei dati personali. Allo stesso modo, spetterà al titolare del trattamento dei dati personali valutare i rischi incombenti sui trattamenti e individuare le misure tecniche e organizzative adeguate al fine di escludere (o, quantomeno, attenuare) tali rischi. La corretta gestione del rischio (termine che ricorre ben 81 volte nel testo normativo) è quindi uno degli elementi nodali della disciplina.

In secondo luogo, il GDPR, nell'occuparsi del tema della sicurezza del trattamento, prevede che il titolare e il responsabile del trattamento debbano adottare "misure tecniche e organizzative" adeguate. Nel GDPR non è più prevista un'elencazione puntuale delle misure di sicurezza (analogamente a quanto accadeva con le misure minime di sicurezza previste dall'All. B del Codice della Privacy italiano), ma ci si "limita" a offrire solamente un criterio per l'individuazione delle specifiche misure tecniche e organizzative da approntare, volta per volta, al trattamento.

Il GDPR, infatti, prescrive l'adozione di misure di sicurezza (tecniche e organizzative) che siano adeguate a fronteggiare (escludendolo o limitandolo al massimo) il rischio[5] incombente sui dati personali oggetto di ogni singolo trattamento posto in essere. Il GDPR ha l'obiettivo di tutelare i diritti e le libertà delle persone fisiche contro i rischi che possano derivare da un trattamento non corretto dei dati personali.

È proprio il riferimento all'aggettivo "adeguato" che, nel GDPR, segna il definitivo abbandono del concetto di sicurezza "minima" basato sulla prescrizione di una serie di precauzioni (spesso sterile o inefficace) per l'approdo a una soluzione in cui spetta al titolare o al responsabile del trattamento comprendere quali siano le misure adeguate - individuate in base a una serie di parametri di riferimento (quali dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche) - a proteggere i dati personali da essi sottoposti a trattamento.

L'attenzione del GDPR per le misure di sicurezza, oltretutto, si spinge oltre attraverso la previsione dell'introduzione di nuovi e specifici concetti, rispetto alla previgente disciplina, quali quelli della "*privacy by design*" e della "*privacy by default*". Con tali previsioni, infatti, si intende anticipare il momento di applicazione delle tutele sui dati personali. Attraverso le disposizioni sulla *privacy by*

Garante della Privacy ha pubblicato il testo consolidato del Codice della Privacy, disponibile su https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29.

[4] L'ultimo comma dell'art. 5 del GDPR testualmente recita: "*Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo* («*responsabilizzazione*»)".

[5] Il rischio, così come inteso dalla norma ISO 31000, è qualsiasi circostanza futura e incerta che sia potenzialmente in grado di ostacolare (in modo più o meno serio) il raggiungimento dell'obiettivo di un corretto trattamento dei dati personali.

design e *by default*, in sostanza, si introduce, per la prima volta, una modalità di protezione dei dati che assume un ruolo centrale sin dal momento della progettazione degli strumenti o delle modalità attraverso le quali i trattamenti saranno effettuati.

Pertanto, è necessario mettere in atto, sulla base di quanto previsto dall'art. 25, par. 1 del Regolamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento, misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie previste dal Regolamento, nonché a tutelare i diritti degli interessati. Inoltre, si devono porre in essere, sulla base di quanto previsto dall'art. 25, par. 2 del Regolamento, misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento nel rispetto del principio della minimizzazione del dato, assicurando la liceità del trattamento.

Le novità in materia di trattamento dei dati personali, per la Pubblica Amministrazione, sono significative e, di seguito verranno illustrate le altre innovazioni, gli istituti e le misure introdotte dal GDPR sulla protezione dei dati personali, con un'attenzione particolare alle misure di sicurezza e a uno degli obblighi più significativi e innovativi, vale a dire la notifica delle violazioni di dati personali (c.d. "*data breach*").

1.1.2 L'OGGETTO E LE FINALITÀ DEL REGOLAMENTO

L'art. 1 del Codice della Privacy, come modificato dal D.Lgs. 101/2018, prevede che il trattamento dei dati personali debba avvenire secondo le norme del GDPR e del Codice stesso, e nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.

L'oggetto, le finalità, l'ambito di applicazione e gli altri principi generali devono pertanto ricavarsi dalla normativa europea: partiamo quindi dall'esame di questi tre aspetti.

L'art. 1 del Regolamento delimita l'oggetto della disciplina nella protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali, e, contemporaneamente, nella finalità di assicurare la libera circolazione dei dati stessi.

È dunque chiaro, fin dal primo articolo, che la disciplina riguarda i dati relativi alle persone fisiche (e non quelli di soggetti differenti, quali persone giuridiche, enti o associazioni). Pertanto, i dati relativi a società, associazioni o enti in generale, non rappresentano dati personali soggetti alla tutela del GDPR[6].

L'impianto normativo ha una finalità specifica e chiara: proteggere i diritti e le libertà fondamentali delle persone fisiche, e, in particolare, il diritto alla protezione dei dati personali.

Questo significa che l'applicazione dei principi (anche in tema di misure di sicurezza, sia tecniche che organizzative) deve tendere proprio a evitare, per quanto possibile, che il non corretto trattamento di dati personali cagioni dei danni, sia materiali che immateriali, quali ad esempio - come chiariscono i "Considerando"[7] 74 e 85 - perdita del controllo dei dati personali, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della

[6] Per fare alcuni esempi pratici, l'indirizzo della sede, la partita IVA, il codice IBAN di una società (o di un'associazione), il codice meccanografico o numero di telefono di una Istituzione Scolastica o Università non sono dati personali ai sensi del GDPR.

[7] I "Considerando" sono contenuti nelle premesse delle norme dell'Unione europea, e il GDPR ne annovera ben 173. A differenza degli articoli, i Considerando non costituiscono norme cogenti, ma sono assai utili per comprendere e interpretare il significato delle disposizioni a cui si riferiscono.

pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica.

In altre parole, tutti i principi che andremo a esaminare non servono a garantire una protezione formale, ma a evitare, ad esempio, che un soggetto venga discriminato a seguito della illecita comunicazione o diffusione della sua appartenenza a un partito politico o sindacato, del suo orientamento sessuale o di una patologia che lo affligge, o che alcuni, a causa della indebita diffusione delle loro generalità complete, subiscano (o possano subire) il "furto" della propria identità.

1.1.3 L'AMBITO DI APPLICAZIONE

Abbiamo già visto che la disciplina si applica ai trattamenti di dati delle persone fisiche, non essendo "dati personali" quelli delle persone giuridiche. Dobbiamo però chiederci se il Regolamento si applichi a tutti i trattamenti di dati personali, o vi siano delle eccezioni.

In primo luogo, la disciplina si applica a tutti i trattamenti automatizzati di dati personali. Non bisogna però fare l'errore di pensare che i trattamenti "tradizionali" o cartacei non siano considerati dal GDPR. L'art. 2, infatti, precisa che il Regolamento si applica anche ai trattamenti non automatizzati di dati personali, purché siano "*contenuti in un archivio o destinati a figurarvi*".

Ne consegue, evidentemente, che tutti i trattamenti di dati personali, anche quelli meramente cartacei, che siano effettuati nell'ambito dell'attività del MIUR, sono soggetti (almeno potenzialmente) all'applicazione del Regolamento. Anche nel contesto di un'Amministrazione sempre più digitale, pertanto, non bisogna dimenticare che i documenti cartacei continuino a circolare e debbano essere trattati in modo corretto. Lo smarrimento o la sottrazione di un fascicolo cartaceo contenente dati personali rappresenterà (o potrà rappresentare), pertanto, una violazione di dati personali, tanto quanto la sottrazione dei medesimi dati contenuti in un archivio informatico.

Sono invece espressamente esclusi (come peraltro accadeva già in vigenza della Direttiva 95/46) i trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere "esclusivamente personale o domestico". Il Regolamento europeo, dunque, non si applica ai trattamenti di dati effettuati in un contesto meramente personale e non professionale, limitato alla sfera privata, come ad esempio la rubrica del telefono personale, o la corrispondenza privata. L'eccezione, naturalmente, non potrà mai trovare applicazione per i trattamenti effettuati dai dipendenti del MIUR nell'ambito delle proprie mansioni lavorative, in quanto non si tratterebbe - con tutta evidenza - di un'attività a carattere esclusivamente privato del dipendente.

Quanto previsto dal Regolamento non si applica poi ai trattamenti effettuati per fini di prevenzione, indagine, accertamento o perseguimento di reati o di esecuzione delle sanzioni penali. Questi trattamenti, prima inclusi nel Codice della Privacy, sono oggi disciplinati dalla Direttiva (UE) 2016/680[8], recepita in Italia con il D.Lgs. 51/2018, richiamato dall'articolo 2-*octies* del D.Lgs 101/2018 in relazione ai principi relativi al trattamento di dati relativi a condanne penali e reati. Il D.Lgs. 101/2018 va ad aggiungersi al Decreto Legislativo n. 51 del 2018, con il quale l'ordinamento italiano ha attuato la Direttiva 2016/680, relativa alla protezione delle persone fisiche con riguardo

[8] Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle Autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio - https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L0680.

al trattamento dei dati personali da parte delle Autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati, completando il recepimento del c.d. Pacchetto protezione dati dell'Unione europea.

L'eventuale richiesta, ad esempio, di dati o di documenti da parte della Polizia giudiziaria, o dell'Autorità giudiziaria, per finalità di indagine, o di prevenzione dei reati, o anche l'accesso a banche dati per le stesse ragioni, non seguirà, pertanto, le regole del GDPR, ma quelle del D.Lgs. di recepimento della Direttiva appena menzionata.

Il Legislatore nazionale ha poi ritenuto di sfruttare gli spazi di manovra lasciati dal GDPR (in particolare dall'art. 23) per introdurre delle limitazioni.

La disciplina dei diritti dell'interessato dal trattamento dei dati, è ora integralmente contenuta nel Regolamento, che consente agli Stati membri di limitare, in presenza di specifiche circostanze, l'esercizio dei diritti stessi. A tal fine provvedono i nuovi articoli 2-*decies* e 2-*undecies* del Codice che limitano l'esercizio dei diritti dell'interessato quando dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto ad alcuni specifici interessi (art. 2-*decies*) o alla salvaguardia e l'indipendenza della Magistratura (art. 2-*undecies*). La riforma differenzia il perimetro delle possibili limitazioni, che a salvaguardia dell'indipendenza della Magistratura possono essere più estese comprendendo anche il diritto all'informativa e alla comunicazione in caso di data breach.

L'art. 2-*duodecies*, in particolare, dispone, per questi trattamenti, che i diritti e gli obblighi, previsti dal GDPR agli artt. 12-22, e la comunicazione dei *data breach* dell'art. 34, non siano disciplinati dal Regolamento stesso, ma dalle norme speciali. Per fare un esempio pratico, dunque, l'accesso ai dati personali di un procedimento dinnanzi il tribunale civile non sarà regolato dall'art. 15 del GDPR, ma dalle corrispondenti norme del Codice di procedura civile in tema di accesso agli atti procedimentali e rilascio di copie.

Per quanto riguarda l'ambito territoriale di applicazione delle norme in esame, il GDPR non si applica soltanto al trattamento dei dati personali effettuato nel contesto delle attività di un titolare o di un responsabile stabilito nell'Unione europea (indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione stessa) ma si estende al trattamento dei dati personali di interessati che si trovino nell'Unione che sia effettuato da un soggetto non stabilito nell'Unione, quando le attività riguardino:

a) L'offerta di beni o la prestazione di servizi agli interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;

oppure

b) Il monitoraggio del loro comportamento nella misura in cui tale comportamento abbia luogo all'interno dell'Unione.

Vi è quindi un ambito di applicazione ben più vasto del mero territorio dell'Unione europea: le norme che stiamo esaminando si applicano, almeno in potenza, a tutti i trattamenti pur effettuati da soggetti non stabiliti nella UE, nel caso in cui riguardino cittadini dell'Unione e a condizione che gli stessi trattamenti consistano in un'offerta di beni e servizi a loro indirizzata, o che il loro comportamento sia oggetto di monitoraggio.

1.1.4 LE DIVERSE CATEGORIE DI DATI PERSONALI E LA TUTELA DIFFERENZIATA

Prima di affrontare le varie tipologie di dati, dobbiamo chiarire che cosa si intenda per "dato personale".

Secondo il GDPR, si considera dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)"[9]. La persona fisica si considera identificabile quando possa essere individuata, direttamente o indirettamente, con riferimento a dati identificativi, quali il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Quando invece non è possibile, neanche indirettamente, risalire a una persona fisica identificata o identificabile, si parla di "dati anonimi", come vedremo tra poco.

Il GDPR distingue nettamente tre categorie di dati personali. Questa distinzione era già presente nella precedente disciplina, ma adesso viene articolata in maniera parzialmente diversa. Si devono pertanto distinguere i dati "comuni", dalle "categorie particolari di dati" e dai dati relativi a condanne penali e reati.

È fondamentale individuare correttamente le categorie di dati che sono ricompresi in ogni trattamento: la natura dei dati, infatti, incide in maniera rilevante sui rischi che il trattamento può comportare, sulle misure che vanno adottate, e sulla disciplina complessiva del trattamento.

È intuitivo, infatti, comprendere come il processo di trattamento dei dati, ad esempio relativo ad un procedimento disciplinare, o all'attribuzione dei benefici di cui alla L. 104/1992, presenti rischi ben diversi rispetto ad altri casi, in cui vengono trattati soltanto dati comuni.

È quindi di capitale importanza la corretta compilazione (e l'aggiornamento, quando necessario) del Registro delle attività di trattamento di cui all'art. 30 del GDPR, di cui ci occuperemo più avanti, registro che deve contenere, tra l'altro, proprio l'indicazione delle categorie di dati, per ciascuna attività di trattamento.

I dati comuni sono individuati in negativo, in quanto sono tutti quei dati personali che non rientrano nelle "categorie particolari" o che non siano dati inerenti a condanne penali e reati.

Le "categorie particolari di dati" (che coincidono - seppur parzialmente - con i "vecchi" dati sensibili) sono rappresentate da: dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici (intesi a identificare in modo univoco la persona), e dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

L'art. 9 stabilisce un generale divieto di trattamento, temperato da alcune eccezioni, che esamineremo più avanti, quando andremo a occuparci della base legale necessaria per poter trattare i dati. La disciplina è completata, a livello italiano, dagli artt. 2-*sexies* e 2-*septies* del Codice Privacy, che esamineremo più avanti.

I dati giudiziari (art. 10 del GDPR e art. 2-*octies* del Codice Privacy), sebbene non rientrino tra le particolari categorie di dati, meritano particolare attenzione. Concernono i dati relativi alle condanne penali e ai reati o connesse a misure di sicurezza. Anche il loro regime è caratterizzato da importanti restrizioni, previste sia dal GDPR che dalla normativa nazionale, e che esamineremo più avanti.

[9] La definizione è analoga a quella già prevista nella normativa previgente.

1.1.5 DATI ANONIMI E PSEUDONIMI

È bene chiarire il concetto di "dati anonimi". Essi infatti non sono dati personali. Se il dato personale è quel dato riconducibile ad una persona fisica identificata o identificabile, il dato anonimo è quello che non consente tale identificazione.

Il dato anonimo nasce originariamente tale, oppure lo diventa in forza di un processo di oscuramento del dato personale "in chiaro". Si tratta, in questo caso, di un dato che era "personale" in origine e che è stato in seguito privato di tutti gli elementi capaci di ricondurlo ad una persona fisica determinata o determinabile.

I dati pseudonimi sono invece quei dati personali che non consentono l'identificazione di una persona fisica determinata senza l'utilizzo di informazioni aggiuntive. Condizione imprescindibile è che tali informazioni aggiuntive siano conservate separatamente e custodite con misure adeguate a evitare che vengano ricondotte a una persona specifica.

Per fare un esempio, si pensi a una banca dati in cui i dati identificativi dei soggetti sono sostituiti da una sigla alfanumerica. Il soggetto che elabora questi dati non sarà in grado di sapere a quali persone essi si riferiscano, in quanto la connessione tra le sigle e le persone è contenuta in altra banca dati, separata e distinta.

Il trattamento di dati pseudonimi è pur sempre un trattamento di dati personali, come è chiarito nel "Considerando" 28. La pseudonimizzazione può ridurre i rischi per gli interessati e aiutare i titolari e i responsabili del trattamento a rispettare i loro obblighi di protezione dati, ma ciò non esime dall'adottare altre misure a protezione.

Il GDPR annovera la pseudonimizzazione tra le tecniche più efficaci al fine di garantire la sicurezza dei dati, e ridurre i rischi. Essa sarà efficace a garantire la sicurezza dei dati solo se le misure tecniche saranno supportate da una corretta gestione dei sistemi.

Vi sono svariate norme del Regolamento che richiamano espressamente la pseudonimizzazione. Tra le altre, l'art. 25 la menziona tra le misure di sicurezza tecniche adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, e analoga indicazione è data dall'art. 32, in tema di sicurezza del trattamento.

1.1.6 BASI GIURIDICHE DEL TRATTAMENTO

Qualsiasi trattamento di dati personali - tra quelli, ovviamente, rientranti nell'ambito di applicazione materiale (art. 2) o territoriale (art. 3) del GDPR - deve avvenire in modo lecito, corretto e trasparente nei confronti dell'interessato. Il concetto di "liceità" richiamato dall'art. 5 del GDPR richiama il concetto di "base giuridica" del trattamento, ossia quell'elemento che giustifica e rende lecito, appunto, il trattamento dei dati personali. Affinché il trattamento di dati personali sia lecito esso pertanto deve fondarsi su di uno dei presupposti espressamente individuati nel Regolamento.

Il GDPR indica, all'art. 6, le basi giuridiche che rendono il trattamento lecito:

- ☑ La presenza del consenso dell'interessato a che i propri dati siano usati "*per una o più specifiche finalità*";
- ☑ La necessità di trattare i dati dell'interessato per dare esecuzione a un contratto o alle misure precontrattuali che siano adottate su richiesta dello stesso interessato;
- ☑ La necessità di trattare i dati personali al fine di adempiere a un obbligo legale al quale sia soggetto il titolare del trattamento;
- ☑ La necessità di effettuare il trattamento dei dati personali al fine di salvaguardare gli interessi vitali dell'interessato o di un'altra persona fisica;

- ☑ La necessità del trattamento dei dati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui sia investito il titolare del trattamento;
- ☑ La necessità di effettuare il trattamento 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)[10].

Nell'ambito delle attività del MIUR, la maggior parte dei trattamenti di dati personali (comuni) avranno come base legale l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ovvero l'adempimento di un obbligo legale.

L'art. 2-*ter* del Codice Privacy ha precisato che la base giuridica, per quanto concerne i compiti di interesse pubblico o connesso all'esercizio di pubblici poteri, debba essere costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.

Si tratta di una indicazione ben più rigida rispetto a quella precedente, risultante dagli artt. 18 e 19 del Codice della Privacy previgente. In precedenza, infatti, il trattamento di dati personali (comuni) poteva essere effettuato dai soggetti pubblici (esclusi gli enti pubblici economici) "soltanto per lo svolgimento delle funzioni istituzionali" (art. 18, comma 2), ma questo trattamento era consentito "anche in mancanza di una norma di legge o di regolamento che lo preveda espressamente" (art. 19, comma 1).

Il nuovo assetto, al contrario, impone necessariamente, quale imprescindibile condizione di liceità del trattamento, l'individuazione della norma di legge (o, nei casi previsti dalla legge, di regolamento), che attribuisca il compito di interesse pubblico, o l'esercizio di pubblici poteri.

La norma di legge (come chiarito dal Considerando 45 del GDPR) non deve essere specifica per ogni singolo trattamento, ma può essere la base per più trattamenti. Essa deve, tra l'altro, stabilire la finalità del trattamento. Inoltre, tale atto legislativo potrebbe precisare le condizioni generali del presente regolamento che presiedono alla liceità del trattamento dei dati personali, prevedere le specificazioni per stabilire il titolare del trattamento, il tipo di dati personali oggetto del trattamento, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto.

In altre parole, non basta più (per legittimare il trattamento di dati "comuni" da parte del MIUR o delle scuole) il generico richiamo allo svolgimento delle funzioni istituzionali, ma occorre la puntuale verifica della norma di legge che attribuisca all'ente il compito o il potere.

L'art. 2-*ter* disciplina poi (in maniera sostanzialmente analoga al precedente assetto) due modalità particolari di trattamento: la comunicazione[11] di dati personali e la loro diffusione[12].

---

[10] Il MIUR non si potrà avvalere di questa base giuridica, per i trattamenti effettuati quale Autorità pubblica nell'esecuzione dei propri compiti.

[11] Per comunicazione deve intendersi, ai sensi dell'art. 2-ter, comma 4 lett. a del Codice Privacy, il "dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione".

[12] Per "diffusione" ai sensi dell'art. 2-ter, comma 4, lett. b del Codice Privacy si intende "il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione".

La comunicazione presuppone una "fuoriuscita" del dato personale dalla sfera di controllo del titolare, in conseguenza della quale il dato stesso viene reso conoscibile (senza necessità che lo stesso venga trasferito) ad altri soggetti determinati (diversi dall'interessato, dai designati, dagli autorizzati o dai responsabili). Si pensi, ad esempio, alla comunicazione di dati tra il MIUR e un altro Ente pubblico, o tra una Scuola e un Ente locale. Si individuano tre ipotesi distinte di comunicazione:

1. La comunicazione tra titolari che trattino i dati nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è lecita se **prevista da norma di legge** (o, nei casi previsti dalla legge, di regolamento). Occorre dunque, anche in questo caso, una norma espressa che preveda la comunicazione stessa.
2. Se, invece, anche in **assenza di norma**, la comunicazione è comunque necessaria per lo svolgimento di compiti di interesse pubblico e di funzioni istituzionali, occorre attivare una procedura che prevede una sorta di silenzio-assenso: l'attività può essere iniziata se si effettua una comunicazione al Garante, e decorrono quarantacinque giorni, senza che quest'ultimo abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.
3. La comunicazione (sempre da parte di un soggetto che tratti i dati nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri) a un soggetto che intenda trattare i dati per **finalità diverse** è infine lecita soltanto se prevista da norma di legge o (nei casi previsti dalla legge) di regolamento.

La diffusione di dati presuppone il dare conoscenza dei dati personali a soggetti indeterminati in qualunque forma, anche mediante la loro messa a disposizione o consultazione. Tale diffusione da parte di un soggetto che li tratti nell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri è, invece, lecita (ai sensi dell'art. 2-*ter*, comma 3) soltanto se prevista da norma di legge o - nei casi previsti dalla legge - di regolamento. Questa disposizione è analoga a quanto previsto nel Considerando 154 del GDPR, il quale afferma che "*i dati personali contenuti in documenti conservati da un'autorità pubblica o da un organismo pubblico dovrebbero poter essere diffusi da detta autorità o organismo se la diffusione è prevista dal diritto dell'Unione o degli Stati membri cui l'autorità pubblica o l'organismo pubblico sono soggetti*".

Anche in questo caso non vi è alcuna sostanziale novità rispetto al passato: perché vengano diffusi dati personali da parte del MIUR (o delle scuole), occorre una base normativa specifica. In assenza di una norma *ad hoc*, è vietato diffondere dati personali (o si deve procedere alla loro irreversibile anonimizzazione).

In conclusione, è fondamentale, per ogni trattamento, individuare correttamente quale sia la fonte normativa che consenta al Ministero di trattare, comunicare o diffondere i dati personali: in questa operazione, è di grande aiuto una corretta compilazione del Registro delle attività di trattamento con riguardo alla individuazione della base giuridica di ogni attività di trattamento.

IN PARTICOLARE: IL CONSENSO

Il consenso, ex art. 4 par. 1, n. 11 del GDPR, è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato che esprime il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, al trattamento dei suoi dati. Si presuppone che il soggetto che conferisce il consenso abbia la capacità giuridica per farlo.

Come visto, il consenso è solo una delle basi giuridiche del trattamento. E dunque non è affatto richiesto quando esista un'altra condizione legittimante, quale ad esempio l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, ovvero l'obbligo di legge.

È pertanto errata la prassi che prevede la richiesta del consenso per queste tipologie di trattamento. Le pubbliche amministrazioni non dovevano, neanche prima del GDPR, domandare il consenso al trattamento dei dati personali, qualora il trattamento fosse connesso allo svolgimento delle funzioni istituzionali (art. 18 del "vecchio" Codice Privacy). Il Considerando 43, inoltre, afferma espressamente che il consenso non costituisce un valido fondamento giuridico per il trattamento dei dati personali, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento. Questo squilibrio è evidente soprattutto nelle ipotesi in cui il titolare del trattamento sia un'Autorità pubblica, in quanto tale circostanza rende improbabile che il consenso sia liberamente prestato.

Nell'ambito delle attività del MIUR, pertanto, il consenso, quale base legale, troverà un'applicazione decisamente marginale. L'art. 29 WP (Gruppo dell'articolo 29 per la tutela dei dati - Article 29 Working Party), nelle sue linee guida[13], ritiene che sia improprio ritenere che le Autorità pubbliche nello svolgimento delle proprie finalità istituzionali possano basarsi sul consenso per effettuare il trattamento dei dati personali, poiché quando il titolare del trattamento è un'Autorità pubblica sussiste un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. Nella maggior parte dei casi, infatti, l'interessato non dispone di alternative realistiche all'accettazione per poter usufruire di quel determinato servizio pubblico. Pertanto, nell'esercizio delle finalità istituzionali le pubbliche amministrazioni svolgono l'attività di trattamento facendo ricorso ad altre basi legittime per il trattamento. Comunque il consenso non è sempre escluso, ma può essere appropriato soltanto in quelle circostanze in cui è pacifico che sia assolutamente libero e laddove l'eventuale diniego non pregiudichi in alcun modo l'erogazione dei servizi. In particolare, si fa l'esempio della richiesta di consenso, da parte di una Scuola, per l'utilizzo delle fotografie degli studenti in una rivista studentesca. Il consenso sarà libero, qualora sia chiaro che agli studenti non vengano negati l'istruzione o altri servizi e che essi possano liberamente rifiutare senza subire pregiudizio.

LA BASE GIURIDICA PER IL TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI

Esaminiamo ora in quali casi si possano lecitamente trattare le categorie particolari di dati.

Come abbiamo visto in precedenza, infatti, vi è un generale divieto di trattare dati che rientrano nelle "categorie particolari", salva la presenza di specifiche eccezioni, che sono individuate nel comma 2 dell'art. 9 del Regolamento.

Tra le varie eccezioni, le più pertinenti rispetto ai trattamenti effettuati da un Ente come il MIUR sono le seguenti:

- ☑ Il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare 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 interno, o da un contratto collettivo ai sensi del diritto interno, e in presenza di garanzie appropriate;
- ☑ Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o interno. Il trattamento deve essere comunque proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure

[13] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051. Le linee guida sono disponibili anche in italiano.

appropriate e specifiche per tutelare i diritti fondamentali e gli interessi del soggetto i cui dati vengono trattati.

Il concetto di "interesse pubblico rilevante" è ulteriormente esplicitato nell'art. 2-*sexies,* comma II, del Codice Privacy, il quale dispone che il trattamento sia ammesso qualora sia previsto dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, da regolamento. Le disposizioni normative interne devono specificare i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dei soggetti interessati.

Il comma terzo dell'art. 2-*sexies* contiene un'elencazione di trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico che sono considerati appunto di "interesse pubblico rilevante". Tra questi possiamo menzionare l'accesso ai documenti amministrativi e l'accesso civico, i rapporti tra soggetti pubblici e gli enti del terzo settore, l'istruzione e formazione in ambito scolastico, professionale, superiore o universitario, la gestione dei rapporti di lavoro, e i trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica.

Il Garante dovrà inoltre, sulla base dell'art. 2-*septies* del Codice della Privacy, emanare un provvedimento (che verrà aggiornato con cadenza almeno biennale), che conterrà delle misure a garanzia per i trattamenti di dati genetici, biometrici e relativi alla salute. La stessa norma prevede anche che, nel rispetto degli obblighi di sicurezza, sia ammesso l'utilizzo dei dati biometrici per le procedure di accesso fisico e logico ai dati da parte dei soggetti autorizzati, ma sempre nel rispetto delle misure di garanzia individuate dal Garante.

Per sintetizzare, con riguardo ai trattamenti di dati biometrici (si pensi ai sistemi di autenticazione che si basano sull'impronta digitale), occorre che vi sia sempre un'idonea base legale, e che siano rispettate le misure di garanzia previste dall'art. 2-*septies* del Codice della Privacy.

LA BASE GIURIDICA PER IL TRATTAMENTO DI DATI RELATIVI A CONDANNE PENALI E REATI

Abbiamo già visto come, ai sensi dell'art. 10 del GDPR, il trattamento di dati personali relativi a condanne e reati, o alle connesse misure di sicurezza, debba avvenire soltanto sotto il controllo dell'Autorità pubblica oppure qualora il trattamento sia autorizzato dal diritto dell'Unione o dal diritto interno, e si prevedano garanzie appropriate per i diritti e le libertà degli interessati. Questa norma non si applica però ai trattamenti di dati personali effettuati ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, che sono regolati dalla Direttiva 2016/680/UE e dal D.Lgs. 51/2018.

L'art. 2-*octies* del Codice Privacy integra quanto disposto dall'art. 10, stabilendo che, in mancanza di disposizione di legge o di regolamento, i trattamenti di dati e le relative garanzie dovranno essere individuate in un decreto del Ministro della Giustizia, da adottarsi sentito il Garante.

Il terzo comma del medesimo articolo contiene poi un elenco di trattamenti, relativi a condanne penali, reati e connesse misure di sicurezza, che sono consentiti se autorizzati da norma di legge o, nei casi previsti dalla legge di Regolamento. In questa elencazione, ritroviamo alcuni tra i trattamenti che possono riguardare le attività del MIUR, tra cui:

- ☑ L'adempimento degli obblighi o l'esercizio dei diritti nell'ambito dei rapporti di lavoro;
- ☑ La verifica e l'accertamento dei requisiti di onorabilità, dei requisiti soggettivi e dei presupposti interdittivi;

- ☑ L'esercizio del diritto di accesso ai dati e documenti amministrativi;
- ☑ L'adempimento di obblighi previsti da disposizioni di legge in materia di comunicazioni e informazioni antimafia;
- ☑ L'accertamento del requisito di idoneità morale di coloro che intendono partecipare a gare d'appalto;
- ☑ L'attuazione della disciplina in materia di attribuzione del *rating* di legalità delle imprese;
- ☑ L'adempimento degli obblighi in tema di antiriciclaggio.

Si prevede, infine, che qualora il trattamento di dati giudiziari sia effettuato sotto il controllo dell'Autorità pubblica, debba essere applicato l'art. 2-*sexies* del Codice Privacy, che abbiamo esaminato prima, e che regola il trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante. Sembrerebbe quindi (ma la recentissima entrata in vigore della norma non consente delle conclusioni certe) che il trattamento di dati giudiziari effettuato sotto il controllo di un'Autorità pubblica sia sottoposto alle stesse regole applicabili alle categorie particolari di dati.

1.1.7 I SOGGETTI

Nel Regolamento europeo alcune figure soggettive fondamentali nell'ambito del trattamento dei dati personali: la comprensione dei diversi ruoli e funzioni (e la ripartizione dei compiti anche all'interno del Ministero) è imprescindibile al fine di costruire un organigramma coerente e funzionale al rispetto dei principi del Regolamento e dei diritti degli interessati. Più avanti esamineremo, in sintesi, le figure principali.

IL TITOLARE E IL CONTITOLARE

Il titolare del trattamento (Data Controller) è la persona fisica o giuridica, l'Autorità pubblica, il servizio o altro organismo che decide i mezzi e le finalità del trattamento. Il titolare è dunque l'Ente, e pertanto va individuato nel MIUR quale titolare unico. Le specifiche attività in capo al titolare possono essere espletate dalle varie Direzioni e Uffici del MIUR, nella sua articolazione centrale e periferica che include gli Uffici Scolastici Regionali (art. 8 del D.P.C.M. 11 febbraio 2014, n. 98). In particolare, il MIUR ha attribuito compiti e funzioni connessi al trattamento di dati personali a soggetti specifici, con la Direttiva n. 239 del 25 marzo 2019, ai sensi della previsione di cui all'art. 2-*quaterdecies* del D.Lgs.196/2003. L'art. 2-*quaterdecies*, infatti, prevede da un lato che il titolare possa 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 e, dall'altro che il titolare debba individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta.

Nell'organizzazione disegnata dalla Direttiva MIUR 239/2019, pertanto, si possono individuare tre differenti categorie di soggetti:

1) Soggetti mediante i quali il MIUR esercita le funzioni di titolare del trattamento;
2) Soggetti designati dal Titolare - a mezzo dei soggetti di cui al punto precedente - ai quali sono affidati specifici compiti e funzioni connessi al trattamento dei dati personali;
3) Soggetti autorizzati al trattamento dei dati personali tra i quali sono ricompresi:
   a. I Dirigenti degli Uffici dirigenziali generali e non generali;
   b. Il personale non dirigente in servizio e il Personale della Scuola comandato;

c. Soggetti esterni che prestano la loro attività in favore del MIUR.

In particolare, il MIUR, nella sua qualità di **titolare del trattamento**, esercita tali funzioni a mezzo del Capo di Gabinetto, dei Capi dei Dipartimenti, nonché dei Dirigenti preposti agli Uffici Scolastici Regionali. Tali soggetti, nell'ambito delle rispettive strutture, sono tenuti ad assicurare il rispetto degli obblighi e degli adempimenti in materia di protezione dei dati personali, tra i quali:

- ☑ Porre in essere le misure tecniche e organizzative adeguate previste dal GDPR;
- ☑ Fornire adeguate istruzioni agli autorizzati al trattamento;
- ☑ Aggiornare periodicamente il registro delle attività di trattamento;
- ☑ Notificare le violazioni dei dati personali al Garante per la protezione dei dati personali e, ove necessario, comunicarle agli interessati;
- ☑ Effettuare le valutazioni di impatto ove previsto;
- ☑ Autorizzare i soggetti esterni al trattamento dei dati personali.

I soggetti mediante i quali il MIUR esercita le funzioni di Titolare a livello di Amministrazione centrale, hanno facoltà di designare, quali soggetti attuatori degli adempimenti previsti dal Regolamento, i Dirigenti degli uffici di livello dirigenziale generale.

A livello di Amministrazione periferica, potranno essere designati, ove ritenuto necessario, i Dirigenti degli uffici di livello dirigenziale non generale.

La designazione deve avvenire per mezzo di un atto formale, con contestuale comunicazione di istruzioni specifiche e puntuali sulla base dei compiti affidati, con previsione dell'obbligo di tenere costantemente aggiornato il soggetto che esercita le funzioni di Titolare in relazione a tale attività. I soggetti Designati svolgono i compiti e le funzioni a essi delegate nell'ambito delle proprie competenze per i trattamenti connessi ai processi di cui sono responsabili.

Con riguardo agli autorizzati le istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo alla policy del Ministero in materia di sicurezza informatica.

I Dirigenti degli uffici di livello dirigenziale non generale sono individuati sulla base dell'ufficio a cui sono assegnati e, pertanto, sono direttamente autorizzati in base alla Direttiva n. 239/2019 al trattamento dei dati connessi allo svolgimento delle competenze amministrative dell'ufficio di

riferimento. Lo stesso vale per il personale non dirigente e il personale comandato/utilizzato della scuola con la possibilità di limitazioni formali nel caso in cui tale personale non tratti tutti i dati di competenza dell'ufficio di assegnazione. In questo caso l'atto che limita l'autorizzazione deve determinare con chiarezza l'ambito di trattamento a cui la singola persona fisica sia autorizzata.

I soggetti che esercitano le funzioni di Titolare del trattamento o i soggetti Designati devono, perciò, formalizzare per iscritto e notificare le suddette limitazioni individuando in modo specifico e chiaro l'ambito di trattamento che ogni soggetto è autorizzato a trattare.

Al fine di coordinare tutte le attività di tali diversi soggetti esercenti le funzioni del titolare del trattamento, e assicurare omogeneità e coerenza del trattamento dei dati personali, è previsto che il Capo Dipartimento per la programmazione e la gestione delle risorse umane, finanziarie e strumentali fornisca le indicazioni di carattere generale per la definizione delle policy in materia di trattamento dei dati personali nell'ambito del MIUR.

Ciascun soggetto che esercita le funzioni di Titolare nomina un *Referente per la privacy* per ciascuna Direzione generale o per la propria struttura di riferimento.

Il Referente agisce a supporto delle funzioni di coordinamento e funge quale punto di contatto con il Responsabile della protezione dei dati (DPO). I Capi dipartimento possono nominare un *Referente per la privacy* per ciascuna Direzione generale.

Gli Istituti Scolastici sono invece titolari distinti dal MIUR in quanto dotati di autonomia. Il percorso di conformità al GDPR del Ministero ha portato a concludere che Amministrazione Centrale e Istituti Scolastici hanno distinte competenze per Legge o Regolamento nel determinare finalità e mezzi del trattamento di dati personali (art. 4, n. 7 del Regolamento UE 679/2016).

La titolarità è uno *status* che deriva dal potere decisorio in ordine alle modalità e finalità del trattamento, e non ha bisogno di essere formalizzata in alcun modo.

Vi possono essere delle ipotesi in cui siano più soggetti a decidere congiuntamente i mezzi e le finalità del trattamento. In questo caso, regolato dall'art. 26 del GDPR, occorre procedere alla formalizzazione di un accordo interno tra i contitolari, che regoli i profili essenziali del trattamento di dati personali. Nell'accordo si può anche (è una facoltà e non un obbligo) individuare il "punto di contatto", vale a dire il soggetto a cui gli interessati possono fare riferimento per l'esercizio dei loro diritti.

Nell'ambito delle attività del MIUR vi sono vari esempi di contitolarità. Ad esempio, possono individuarsi due ipotesi di contitolarità tra il MIUR e gli Istituti Scolastici, con riguardo alla gestione dei contratti a tempo indeterminato e determinato del personale docente. I mezzi e le finalità di questi trattamenti (funzionali al perfezionamento dell'assunzione del personale docente, con riferimento agli aspetti relativi al trattamento giuridico ed economico, nonché alla verifica del possesso dei requisiti per l'assunzione) non sono infatti decisi esclusivamente dal MIUR o dall'Istituto Scolastico, e pertanto ci si trova in una situazione di contitolarità.

IL GRUPPO DI LAVORO INTERDIPARTIMENTALE PER LA PRIVACY

Si segnala che, in base alla summenzionata Direttiva MIUR n. 239/2019, si è prevista la costituzione di un "**Gruppo di lavoro interdipartimentale per la privacy**" che è presieduto dal Capo Dipartimento per la Programmazione e la Gestione delle Risorse Umane, finanziarie e strumentali ed è composto dal DPO, da un Dirigente per ogni Dipartimento e per gli Uffici di diretta collaborazione, nonché da uno o più "Referenti per la privacy". Questo soggetto svolge le funzioni di coordinamento e raccordo tra le diverse strutture e il DPO.

IL RESPONSABILE DEL TRATTAMENTO

Il responsabile del trattamento (*Data Processor*) è la persona fisica o giuridica che tratta i dati per conto del titolare. Il Responsabile, nell'ambito della sistematica del GDPR, è sempre un soggetto esterno rispetto all'organizzazione del titolare, contrariamente a quanto accadeva nella vigenza dell'art. 29 del Codice Privacy. Il titolare deve scegliere esclusivamente dei responsabili che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, affinché il trattamento soddisfi i requisiti del regolamento e garantisca la tutela dei diritti dell'interessato. Nell'ambito del MIUR - sulla scorta di quanto previsto dalla Direttiva n. 239 del 25 marzo 2019 - il Responsabile del trattamento tratta i dati personali secondo le istruzioni ricevute dal soggetto che esercita le funzioni del Titolare del trattamento e assicura che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

Per fare alcuni esempi, si pensi al fornitore di un servizio di posta elettronica, o al soggetto esterno a cui è affidata l'elaborazione e gestione di una graduatoria, o al fornitore di servizi *cloud*: tutti questi soggetti, in quanto trattano dati per conto del titolare, sono da individuarsi come "responsabili".

Il rapporto tra titolare e responsabile deve essere regolato, secondo quanto prevede l'art. 28 del GDPR, da un "*contratto o altro atto giuridico*", che sia vincolante, e che individui con precisione l'oggetto del trattamento, la sua durata, la natura, le finalità, il tipo di dati personali, nonché gli obblighi e i diritti del titolare. Tale contratto deve essere sottoscritto, secondo quanto previsto dall'art. 7 dalla Direttiva n. 239 del 25 marzo 2019, dal soggetto che esercita le funzioni del Titolare, salvo che sia affidato a un soggetto Designato.

Occorre pertanto provvedere a stipulare idonei accordi ovvero, laddove l'attività di trattamento sia acquisita mediante evidenza pubblica, a integrare i bandi e i capitolati per includervi quanto richiesto dall'art. 28 stesso.

I DESIGNATI E GLI AUTORIZZATI

Nel previgente impianto del Codice Privacy, l'art. 29 individuava i c.d. "responsabili interni"[14].

Ai responsabili (figura facoltativa e rimessa alla discrezionalità del titolare) potevano essere affidati dei compiti, che andavano analiticamente descritti. Normalmente ai responsabili (interni) venivano affidati compiti di supervisione e controllo dei trattamenti di dati personali per le aree di loro competenza, compresa la nomina degli "incaricati". Questi soggetti oggi vengono, per lo più, indicati con il termine "designati".

L'art. 30 regolava invece la figura degli "incaricati", le persone fisiche che procedevano materialmente al trattamento di dati personali, e che dovevano operare sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite. Questi soggetti, invece, sono oggi per lo più indicati con il termine "autorizzati".

Il GDPR, in coerenza con il principio di responsabilizzazione, non individua specifiche disposizioni, lasciando al titolare l'onere di regolamentare, con proprie misure organizzative, l'organigramma relativo al trattamento di dati personali, e limitandosi a prevedere (artt. 29 e 32) che chiunque abbia accesso ai dati personali, sotto l'autorità del titolare o del responsabile, debba essere debitamente istruito. Le misure organizzative in questione sono previste, nell'ambito delle attività del MIUR, dalla già richiamata Direttiva n. 239 del 25 marzo 2019.

[14] Abbiamo visto sopra che, sulla base del GDPR, il "responsabile" è soltanto il soggetto esterno che tratta dati per conto del titolare.

Il D.Lgs. 101/2018, introducendo nel Codice Privacy l'art. 2-*quaterdecies*, ha provveduto a individuare in maggiore dettaglio le attribuzioni di funzioni e compiti in materia di trattamento di dati personali.

I "soggetti designati"[15], previsti dal primo comma dell'art. 2-*quaterdecies*, sono le persone fisiche a cui il titolare o il responsabile attribuiscono specifici compiti e funzioni connessi al trattamento. Questi compiti e funzioni, nel rispetto del principio di responsabilizzazione, devono essere esplicitamente indicati, delimitando in tal modo l'ambito del trattamento. Questa figura è dunque, come anticipato, simile al "vecchio" responsabile interno. Potranno quindi essere attribuiti al designato, ad esempio, i compiti legati alla conclusione dei contratti con i responsabili esterni, alla supervisione e controllo del rispetto dei principi in materia di trattamento, per le aree o i servizi di competenza, o la nomina degli "autorizzati" al trattamento.

Nell'ambito del MIUR, i soggetti che esercitano le funzioni di titolare del trattamento possono affidare specifici compiti e funzioni, connessi al trattamento dei dati personali, a Dirigenti che da essi dipendono. Questi soggetti, che potremmo definire "Designati" al trattamento svolgono i compiti e le funzioni loro assegnati seguendo le istruzioni ricevute e in forza di un atto di designazione espressa.

I compiti e funzioni che possono essere assegnati ai Designati sono delineati nelle Linee guida sui soggetti del processo di gestione della privacy del Ministero, di cui alla Direttiva del Ministro del 25 marzo 2019, n. 239, dell'aprile 2019, e possono consistere nel:

a) Porre in essere misure tecniche e organizzative adeguate per garantire che il trattamento dei dati personali sia effettuato conformemente alle disposizioni del Regolamento;
b) Adottare soluzioni di *privacy by design* e *by default*;
c) Tenere costantemente aggiornato il Registro delle attività di trattamento;
d) Predisporre le informative relative al trattamento dei dati personali nel rispetto degli artt. 13 e 14 del Regolamento;
e) Fornire ai soggetti autorizzati a compiere operazioni di trattamento istruzioni specifiche e puntuali per il corretto trattamento dei dati;
f) Predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
g) Provvedere, anche tramite gli autorizzati, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;
h) Disporre l'adozione dei provvedimenti imposti dal Garante;
i) Collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
j) Individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali autorizzati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
k) Garantire al Responsabile del Computer Emergency Response Team (CERT) del MIUR o dell'Unità di presidio regionale i necessari permessi di accesso ai dati e ai sistemi per l'esercizio dei compiti assegnati nell'ambito della gestione degli incidenti di sicurezza;
l) Effettuare la preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

[15] Questa la dizione dell'art. 2-quaterdecies Codice Privacy.

m) Consultare il Garante, nei casi previsti dall'art. 36 del Regolamento, quando la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio elevato;
n) Richiedere obbligatoriamente nelle richieste di sviluppo di software e di piattaforme l'applicazione della policy in materia di sicurezza di sviluppo delle applicazioni;
o) Designare i Responsabili esterni del trattamento e gestire le segnalazioni dei Dirigenti degli uffici di livello dirigenziale non generale in relazione a eventuali inadempimenti dei suddetti Responsabili;
p) Sottoscrivere gli atti di consultazione preventiva al Garante;
q) Autorizzare i soggetti esterni che prestano la loro attività in favore della rispettiva struttura, dando loro specifiche istruzioni in relazione alle attività di trattamento dati assegnate.

Il secondo comma dell'art. 2-*quaterdecies*, ricollegandosi agli artt. 29 e 32 del GDPR, prevede che il titolare (o il responsabile) debbano individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la loro autorità diretta. Si tratta, appunto dei "soggetti autorizzati", figura che appare accostabile, come già anticipato, alla vecchia definizione di "incaricato al trattamento". Occorre pertanto prevedere che chiunque tratti dati personali sotto l'autorità diretta del titolare riceva specifiche istruzioni, accompagnate da idonea formazione.

Nell'ambito delle organizzazioni complesse, pertanto, occorre individuare i soggetti designati, a cui attribuire specifici compiti e funzioni, e provvedere a fornire idonee e dettagliate istruzioni a tutti coloro che trattano i dati sotto l'autorità del titolare stesso.

In base alla già richiamata Direttiva MIUR n. 239 del 25 marzo 2019, sono individuati, quali autorizzati al trattamento dei dati personali:

a) I Dirigenti degli uffici dirigenziali generali e non generali, in relazione alle competenze attribuite o comunque esercitate presso gli Uffici cui sono preposti secondo l'organizzazione del MIUR;
b) Il personale non dirigente in servizio nei limiti delle competenze attribuite all'ufficio o struttura di appartenenza;
c) Il personale della Scuola comandato nei limiti delle competenze attribuite all'ufficio o struttura di appartenenza;
d) I soggetti esterni che prestano la loro attività in favore del MIUR.

I soggetti di cui alla lett. d) devono essere espressamente autorizzati dal soggetto che esercita le funzioni del Titolare del trattamento. I soggetti di cui alla lett. a), invece, hanno l'obbligo di assicurare che il personale assegnato ai rispettivi uffici abbia adeguata conoscenza delle modalità di trattamento.

Abbiamo già visto che chiunque abbia accesso ai dati personali, sotto l'autorità del titolare o del responsabile, debba essere preliminarmente autorizzato e debitamente istruito. L'autorizzazione e le istruzioni, per ciascun soggetto o tipologia di soggetti (siano essi designati al trattamento o **autorizzati** al trattamento) sono, in genere, contemplate nello stesso atto.

Per quanto riguarda gli autorizzati, le già menzionate Linee Guida del MIUR di aprile 2019 prevedono che essi siano tenuti a conformare i trattamenti a loro assegnati alla normativa in materia di protezione dei dati personali e alle istruzioni ricevute, e che, in linea generale, siano tenuti a:

☑ Trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;

☑ Verificare la legittimità e correttezza dei trattamenti, valutando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Le istruzioni possono essere diversificate, disciplinando eventuali aspetti di dettaglio in relazione alle specificità dei singoli trattamenti, e devono comunque contenere un espresso richiamo alla policy del Ministero in materia di sicurezza informatica.

L'INTERESSATO

L'interessato è la persona fisica a cui si riferiscono i dati personali oggetto di trattamento. Si ribadisce che "interessato" possa essere solo e soltanto la persona fisica. Rientreranno pertanto in questa categoria i professionisti o gli imprenditori individuali, ma non, ad esempio, le società, le Scuole o le Università, le istituzioni AFAM.

L'interessato può esercitare i diritti previsti dagli articoli da 15 a 22 del GDPR. Tra questi vanno menzionati il diritto di poter accedere ai propri dati, e alle informazioni relative alle modalità di trattamento (compresa l'esistenza di eventuali procedimenti decisionali automatizzati), il diritto di rettifica, il diritto di cancellazione, il diritto di limitazione e quello di opposizione al trattamento. Un discorso più approfondito meritano il diritto alla portabilità e il diritto a non essere sottoposti a un procedimento decisionale automatizzato.

L'art. 20 introduce, nel caso di un trattamento automatizzato basato sul consenso o sul contratto, il diritto alla portabilità del dato, vale a dire il diritto di poter richiedere al titolare del trattamento i dati che riguardano l'interessato, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasferirli ad altro titolare in maniera automatica (se possibile). Questo innovativo diritto, modellato sulla "portabilità" del numero di telefono o del mutuo, va sottolineato che non è però applicabile ai trattamenti necessari per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare.

Riveste particolare interesse il diritto previsto dall'art. 22, il quale prevede che l'interessato possa 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. Anche questo diritto subisce però delle eccezioni, laddove il trattamento sia necessario per l'esecuzione di un contratto, sia autorizzato dal diritto dell'Unione o dal diritto interno, e si prevedano adeguate garanzie, o vi sia il consenso esplicito dell'interessato stesso.

Il titolare deve dare risposta alle richieste al massimo entro un mese, ai sensi dell'art. 12 del GDPR, ma il termine è prorogabile, previo motivato avviso all'interessato, di altri due mesi. Occorre quindi prevedere specifiche procedure (come è usuale fare in tema di accesso documentale e di accesso generalizzato) per regolamentare l'esercizio dei diritti dell'interessato, al fine di essere in grado di rispondere entro il termine previsto. Ma, ancora prima delle procedure, occorre, in applicazione del principio di *privacy by design*, prevedere che i sistemi informativi siano configurati in modo tale da consentire in maniera agevole l'esercizio dei diritti stessi.

Il novellato Codice della Privacy prevede che tali diritti possono essere limitati qualora dal loro esercizio possa derivare un pregiudizio effettivo e concreto a determinati interessi individuati espressamente dalla normativa. Nell'ambito delle pubbliche amministrazioni, quali il MIUR, le ipotesi di limitazione possono essere circoscritte all'art. 2-*undecies* comma 1, lett. f), ossia nel caso in cui l'esercizio del diritto possa recare pregiudizio alla riservatezza dell'identità del dipendente che segnala, ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in

ragione del proprio ufficio. La confidenzialità del c.d. "*whistleblower*" è infatti garantita mediante la sottrazione della sua segnalazione sia all'accesso documentale, che all'accesso ai dati personali ai sensi dell'art. 15 del GDPR.

LA FIGURA E I COMPITI DEL DATA PROTECTION OFFICER

Il GDPR, nell'ottica della responsabilizzazione, introduce la figura del Data Protection Officer (DPO) o Responsabile per la Protezione dei Dati (RPD), disciplinata agli art. 37, 38 e 39 del GDPR e dall'art. 2-*sexiesdecies* del novellato D.Lgs. 196/2003.

La nomina è obbligatoria per le pubbliche amministrazioni[16]. Il DPO - che può essere una figura sia interna che esterna (con apposito contratto di servizi) - è designato, secondo quanto prevede l'art. 37, in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti che gli sono assegnati sulla base del GDPR.

Il MIUR ha nominato il proprio Responsabile della Protezione dei Dati con atto di designazione Prot. n. 0000282 - 16/04/2018[17], precisando che i compiti del Responsabile nominato attengono all'insieme dei trattamenti di dati effettuati dal Ministero dell'Istruzione, dell'Università e della Ricerca. I dati di contatto sono disponibili (oltre che nelle informative) anche nella sezione amministrazione trasparente del sito, alla voce "Altri Contenuti"[18].

I compiti del DPO sono elencati all'art. 39 del GDPR, e, precisamente:

- ☑ Offrire consulenza a titolare, responsabile e dipendenti;
- ☑ Fornire il parere (se richiesto) sulla valutazione d'impatto ex art. 35 del GDPR;
- ☑ Sorvegliare sul rispetto della disciplina sulla protezione dati e sulle politiche del titolare in materia di protezione dei dati personali, compresa la sensibilizzazione e la formazione;
- ☑ Cooperare con l'Autorità Garante, e fungere da punto di contatto.

Nello svolgimento di tutte queste attività il DPO deve considerare debitamente i rischi connessi alle attività di trattamento.

Le funzioni di consulenza e di sorveglianza del DPO (funzioni che devono essere conosciute da tutti i dipendenti) sono fondamentali, nell'ottica della corretta individuazione e gestione dei rischi per i diritti e le libertà fondamentali.

Il Responsabile della Protezione dei Dati deve essere tempestivamente coinvolto in tutte le questioni riguardanti il trattamento di dati personali. Laddove ad esempio il MIUR debba intraprendere, magari in forza di una nuova disposizione di legge, o per effetto di una nuova articolazione delle competenze, un nuovo trattamento di dati personali, o vengano significativamente modificate le modalità o le finalità di un trattamento preesistente, sarà opportuno coinvolgere fin dal principio il DPO, per ricevere consulenza e tenere nel dovuto conto i profili di protezione dei dati personali.

---

[16] La norma europea esenta da questo obbligo le Autorità giurisdizionali nell'esercizio delle loro funzioni. Tuttavia, il Codice della Privacy, all'art. 2-sexiesdecies, ha previsto esattamente l'opposto, sfruttando l'ambito di discrezionalità concesso al Legislatore nazionale.

[17] http://www.miur.gov.it/documents/20182/0/DM+282+del+16-04-2018+Responsabile+Protezione+Dati+personali.pdf/d3c1223c-4e1f-44fe-8f41-c82990411a1a.

[18] http://www.miur.gov.it/altri-contenuti-protezione-dei-dati-personali.

Una funzione importante svolta dal DPO è quella legata al contatto con gli interessati, i quali possono interpellarlo per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti. Per questa ragione, come già sottolineato, i dati di contatto del DPO del MIUR sono indicati nelle informative e nel sito.

La figura del DPO è circondata da specifiche cautele: egli infatti non deve svolgere altri compiti e funzioni che ingenerino conflitto d'interessi, è autonomo, non può ricevere direttive o istruzioni, non può essere rimosso per l'adempimento dei propri compiti, e riferisce direttamente al vertice gerarchico.

1.1.8 IL REGISTRO DEL TRATTAMENTO

Il Registro delle attività di trattamento (art. 30 del GDPR) è, come abbiamo già avuto modo più volte di notare, uno strumento funzionale al principio di *accountability* ed è fondamentale per la valutazione del rischio.

L'art. 30 stabilisce il contenuto minimo, che, per il registro del titolare, contempla le seguenti informazioni: le finalità del trattamento, la descrizione delle categorie di interessati e delle categorie di dati personali, le categorie di destinatari a cui i dati sono stati o saranno comunicati, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, i termini ultimi previsti per la cancellazione delle diverse categorie di dati e, infine, una descrizione generale delle misure di sicurezza adottate.

Deve essere compilato in forma scritta, anche elettronica, dal titolare e dal responsabile. La sua redazione, compilazione e aggiornamento è certamente obbligatoria per le pubbliche amministrazioni.

Il già menzionato DM n. 239 del 25 marzo 2019, all'art. 9, prevede che la tenuta e l'aggiornamento del Registro delle attività di trattamento spetti ai soggetti che esercitano le funzioni del Titolare, in relazione ai loro ambiti di competenza.

Il Garante per la protezione dei dati personali ha, di recente, reso disponibili delle chiare e concise "FAQ" (domande ricorrenti) sulla compilazione e gestione del Registro[19].

1.1.9 LA DPIA (DATA PROTECTION IMPACT ASSESSMENT)

La DPIA (o valutazione d'impatto sulla protezione dei dati, prevista all'art. 35 del GDPR) consiste[20] in un processo finalizzato a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali. La DPIA non deve essere, tuttavia, attuata in relazione a qualsiasi trattamento di dati personali ma è obbligatoria, per il titolare, quando il trattamento rappresenti un rischio elevato per i diritti e le libertà delle persone fisiche.

Può ravvisarsi un "rischio elevato" nei casi in cui vi sia un monitoraggio sistematico dei comportamenti degli interessati svolto in maniera automatizzata (ad esempio la profilazione) da cui derivano effetti giuridici, o nei casi in cui siano trattati dati personali di un gran numero di soggetti interessati e siano trattate categorie particolari di dati o dati giudiziari (i trattamenti su larga scala), o anche nei casi in cui vi sia una combinazione di questi e altri fattori.

---

19 https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

20 Come indicato nelle Linee guida dell'art. 29 WP.

L'art. 29 WP (Gruppo dell'articolo 29 per la tutela dei dati - Article 29 Working Party) individua nelle linee guida le ipotesi obbligatorie, tra le quali vi sono: i trattamenti inerenti ai dati relativi a soggetti vulnerabili come minori, anziani, soggetti con patologie psichiatriche, etc.; il monitoraggio sistematico e su larga scala di una zona accessibile al pubblico, ad esempio con la videosorveglianza (ipotesi peraltro prevista espressamente anche dall'art. 35 del GDPR); la combinazione o il raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale, come avviene, ad esempio, anche con i Big Data.

In presenza di uno o più di tali fattori, pertanto, la valutazione d'impatto deve essere effettuata dal titolare del trattamento prima di dare inizio al trattamento stesso e tale DPIA dovrà contemplare i contenuti minimi previsti dall'art. 35 del GDPR.

Vista la sua utilità, il Gruppo ex art. 29 suggerisce di adottare la DPIA anche al di fuori delle ipotesi previste come obbligatorie, consentendo al titolare del trattamento di conoscere in maniera approfondita le tipologie di trattamento al fine di evitare incidenti futuri.

L'11 ottobre 2018 il Garante Privacy ha emanato un provvedimento[21] sulla DPIA nel cui Allegato 1 sono elencate le tipologie di trattamento soggette necessariamente a valutazione d'impatto. Il *focus* del Garante è concentrato sui trattamenti effettuati su larga scala o in maniera sistematica, con tecnologie innovative (ad esempio l'IoT o l'intelligenza artificiale) ma anche con videosorveglianza, sui trattamenti che riguardino categorie particolari di dati o dati giudiziari. Non solo. L'attenzione è rivolta, oltre che ai dati relativi alla salute, alla condizione personale o familiare, anche a quelli che riguardano il rendimento professionale, l'affidabilità e il comportamento, gli interessi personali, l'ubicazione o gli spostamenti dell'interessato.

Il Garante, inoltre, ha suggerito per la valutazione di impatto l'utilizzo del software PIA[22] elaborato dalla CNIL (l'Autorità Garante francese), tradotto completamente in italiano, in quanto rappresenta un valido supporto alla realizzazione di una valutazione d'impatto.

1.1.10 LE DISPOSIZIONI TRANSITORIE DEL D.LGS. 101/2018

Come abbiamo visto nella premessa, il Legislatore italiano è intervenuto con il D.Lgs. 101/2018, entrato in vigore il 19 settembre del 2018, per armonizzare la disciplina italiana e regolamentare gli aspetti rimessi all'ordinamento nazionale dal Regolamento europeo. Le norme rilevanti del decreto di armonizzazione e le novità sono illustrate nelle relative parti del presente corso. Il decreto contiene, inoltre, alcune disposizioni transitorie e di coordinamento: esaminiamo brevemente quelle più rilevanti. Gli artt. 20 e 21 regolano la disciplina transitoria dei codici di deontologia e buona condotta e delle autorizzazioni generali emanate dal Garante, mentre l'art. 22 contiene delle importanti disposizioni di coordinamento. In particolare, si prevede che:

- ☑ Le disposizioni dell'ordinamento nazionale si debbano interpretare e applicare alla luce della disciplina dell'Unione europea in materia di protezione dei dati personali e debbano anche assicurare la libera circolazione dei dati personali tra gli Stati membri;

[21] Il provvedimento e il relativo allegato sono reperibili al seguente link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9058979.

[22] Del software PIA è disponibile anche la versione italiana e può essere scaricato al seguente indirizzo web https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil.

- ☑ Le espressioni "dati sensibili" e "dati giudiziari", ovunque ricorrano, si intendono riferite, rispettivamente, alle "categorie particolari" di dati di cui all'articolo 9 del GDPR, e ai dati relativi a condanne penali e reati di cui all'articolo 10;
- ☑ I trattamenti già in corso, svolti per l'esecuzione di un compito di interesse pubblico e che possano presentare rischi elevati, in ordine ai quali il Garante potrà emanare delle misure a garanzia ai sensi dell'art. 2-*quinquiesdecies* del Codice Privacy, possono proseguire qualora avvengano in base a espresse disposizioni di legge o regolamento o atti amministrativi generali, o nel caso in cui siano stati sottoposti a verifica preliminare o autorizzazione del Garante;
- ☑ I provvedimenti del Garante continuano ad applicarsi, in quanto compatibili;
- ☑ I rinvii (contenuti in norme di legge e di regolamento) alle disposizioni del Codice Privacy, abrogate dal D.Lgs. 101/2018, si intendono riferiti alle corrispondenti disposizioni del GDPR e del D.Lgs. 101/2018, in quanto compatibili;
- ☑ Le disposizioni previgenti del Codice Privacy, relative al trattamento di dati genetici, biometrici o relativi alla salute, continuano a trovare applicazione, in quanto compatibili con il GDPR, sino all'adozione delle misure di garanzia che dovranno essere emanate sulla base dell'articolo 2-*septies* del Codice Privacy novellato.

La fase transitoria è quindi particolarmente complessa, dovendosi analizzare, caso per caso, quale sia il regime dei singoli trattamenti (soprattutto per i trattamenti relativi allo stato di salute, e per quelli riguardanti dati biometrici), in base alla vecchia e alla nuova normativa: importanti indicazioni potranno certamente venire dai primi provvedimenti del Garante in materia.

1.2 AMMINISTRAZIONE, GDPR E TRASPARENZA (aspetti applicativi)

1.2.1 IL DELICATO BILANCIAMENTO TRA PRIVACY E TRASPARENZA, ALLA LUCE DEL NOVELLATO CODICE DELLA PRIVACY

Il rapporto tra privacy e trasparenza nella Pubblica Amministrazione si regge su un delicato equilibrio. La regola generale è che le pubbliche amministrazioni possono diffondere dati personali solo se ciò è ammesso da una specifica disposizione di legge o, nei casi previsti dalla legge, di regolamento. D'altra parte, le stesse sono onerate di veri e propri obblighi di pubblicazione, in ossequio al principio della trasparenza nella Pubblica Amministrazione. Certo è che, nell'adempiere agli obblighi di pubblicazione, la Pubblica Amministrazione deve rispettare i principi in materia di protezione dei dati personali, secondo quanto ricordato anche nelle Linee guida del Garante Privacy del 2014, tutt'ora attuali nonostante la base normativa sia stata significativamente modificata[23].

Il Codice della Privacy, come modificato dal D.Lgs. 101/2018, ha sostanzialmente confermato l'assetto normativo precedente. L'art. 2-*ter*, comma 3, infatti, prevede che la diffusione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, sia ammessa soltanto quando prevista da legge, o, nei casi previsti dalla legge, da regolamento, mentre l'art. 2-*septies*, comma 8, stabilisce un generale divieto di diffusione dei dati genetici, biometrici e relativi allo stato di salute.

[23] Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati - https://www.garanteprivacy.it/en/home/docweb/-/docweb-display/docweb/3134436.

Per sintetizzare, le pubbliche amministrazioni possono diffondere dati solo laddove vi sia una norma di legge (o nei casi previsti dalla legge, di regolamento) che imponga tale diffusione, mentre non possono mai diffondere dati idonei a rivelare lo stato di salute.

Ma, anche laddove vi sia una norma espressa, occorre sempre valutare quali dati personali siano pertinenti e adeguati rispetto alle finalità, evitando accuratamente di effettuare pubblicazioni che non rispettino il principio di minimizzazione di cui all'art. 5, comma 1, lett. c del GDPR, o che vengano mantenute sul sito dell'Amministrazione per un tempo più lungo di quanto previsto dalla norma che impone la pubblicazione stessa.

1.2.2 PRIVACY E PUBBLICAZIONI OBBLIGATORIE: L'ART. 7-BIS DEL D.LGS. 33/2013

Il D.Lgs. 33/2013, noto anche come Decreto Trasparenza, impone alle pubbliche amministrazioni e ai soggetti tenuti al rispetto della normativa sulla trasparenza una serie di obblighi di pubblicazione di informazioni, dati e documenti sui propri siti istituzionali, e prevede, in caso di omesso adempimento, la possibilità in capo a chiunque sia interessato di presentare istanza di accesso civico per ottenere la pubblicazione dei dati, informazioni e documenti. Lo scopo del Decreto è la trasparenza (intesa come "accessibilità totale dei dati e delle informazioni") e la conoscibilità per i cittadini dell'organizzazione e delle attività delle pubbliche amministrazioni, anche al fine di contrastare la corruzione all'interno della Pubblica Amministrazione stessa, nel rispetto della disciplina in materia di protezione dei dati personali.

L'art. 7-*bis*, rubricato Riutilizzo dei dati pubblicati, al comma IV prevede che: "*nei casi in cui norme di legge o di regolamento prevedano la pubblicazione di atti o documenti, le pubbliche amministrazioni provvedono a rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari*[24]*, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione*".

L'art. 7-*bis* regola dunque, i rapporti tra la normativa in materia di protezione dei dati personali, stabilendo una serie di regole, coerenti anche con le modifiche apportate al Codice Privacy, già sintetizzate:

- ☑ Si possono diffondere dati personali solo se vi è un espresso obbligo di legge;
- ☑ Anche in caso di obbligo, non si possono diffondere i dati non pertinenti, o, nel caso di dati giudiziari o rientranti nelle categorie particolari, non indispensabili rispetto alle finalità della pubblicazione;
- ☑ È sempre vietato diffondere dati inerenti allo stato di salute e la vita sessuale.

IN PARTICOLARE: LA CORRETTA PUBBLICAZIONE DEI CURRICULUM VITAE

Il D.Lgs. 33/2013 prevede all'art. 15 l'obbligo di pubblicazione per le pubbliche amministrazioni dei curricula professionali concernenti i titolari di incarichi di collaborazione o consulenza, nei limiti dei dati pertinenti alle finalità di trasparenza perseguite e da effettuarsi entro tre mesi dal conferimento dell'incarico e per i tre anni successivi alla cessazione dell'incarico. In base alle indicazioni del Garante è consentita la pubblicazione dei soli dati personali la cui diffusione sia realmente necessaria e proporzionata alla finalità di trasparenza perseguita nel caso concreto. Bisogna pertanto provvedere all'oscuramento delle informazioni che risultano eccedenti o non pertinenti rispetto alla finalità di trasparenza.

[24] Il richiamo ai dati sensibili va inteso ora riferito alle "categorie particolari di dati" ex art. 9 GDPR, mentre per i dati giudiziari si deve fare riferimento ai dati relativi alle condanne penali e reati ex art. 10 GDPR.

Sono pertinenti dati relativi ai titoli di studio e professionali o relativi alle esperienze lavorative, le conoscenze linguistiche o informatiche, la partecipazione a seminari, convegni o le pubblicazioni. Viceversa, sono dati eccedenti il codice fiscale, l'indirizzo o il recapito telefonico personale. Di questi ultimi non è consentita la pubblicazione e il titolare è tenuto ad attenta verifica del contenuto del curriculum.

1.2.3 PUBBLICAZIONE DEI "DATI ULTERIORI" E ANONIMIZZAZIONE

Abbiamo visto in precedenza come si possano diffondere dati personali solo laddove vi sia una base normativa adeguata.

Il D.Lgs. 33/2013 regola espressamente la possibilità di pubblicare "dati ulteriori", vale a dire dati per i quali non sussista un obbligo di pubblicazione. In questo caso, l'art. 7-*bis*, comma III prevede che dati, informazioni e documenti possano essere pubblicati soltanto "*procedendo alla indicazione in forma anonima dei dati personali eventualmente presenti*". I dati dunque devono essere correttamente anonimizzati, in modo che non sia assolutamente possibile risalire agli interessati a cui i dati originariamente si riferivano. La regola contenuta nella norma appena esaminata ha portata generale, e non è limitata soltanto ai dati pubblicati nella sezione "amministrazione trasparente".

1.2.4 PRIVACY E ACCESSO GENERALIZZATO (O FOIA)

L'accesso generalizzato, definito anche FOIA (*Freedom of Information Act*), è una nuova figura, disciplinata dall'art. 5 comma II del D.Lgs. 33/2013 ed entrato in vigore il 23 dicembre 2016, e, in coerenza con il nuovo concetto di trasparenza come "accessibilità totale", consiste nel diritto di chiunque di accedere ai dati e documenti detenuti dalle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico.

Questo diritto, naturalmente, è soggetto a limitazioni, al fine di bilanciarlo con altri interessi. Queste limitazioni sono contenute nell'art. 5-*bis*, che prevede delle esclusioni assolute (contenute al comma III) e delle esclusioni relative (al comma II).

Ci limiteremo a esaminare quelle rilevanti in ordine al rapporto tra trasparenza e privacy, sottolineando come il Codice della Privacy, all'art. 59, comma 1-*bis* (introdotto dal D.Lgs. 101/2018) chiarisce che i presupposti, le modalità e i limiti per l'esercizio del diritto di accesso civico restino disciplinati proprio dal D.Lgs. 33/2013.

Occupandoci prima delle esclusioni assolute rilevanti in tema di trattamento di dati personali, dobbiamo menzionare i dati inerenti allo stato di salute e alla vita sessuale, nonché i dati da cui possa inferirsi un disagio economico e sociale: essi rientrano tra i dati per i quali vige un divieto assoluto di ostensione a seguito di accesso generalizzato.

L'art. 5-*bis* del D.Lgs. 33/2013, al secondo comma, lett. a) prevede invece un'esclusione relativa, che stabilisce come l'accesso generalizzato possa essere rifiutato se il diniego è necessario per evitare un pregiudizio concreto alla protezione dei dati personali. Si consideri, inoltre, che qualora l'istanza di accesso generalizzato venga negata o differita a causa di un presunto "pregiudizio concreto" alla protezione dei dati personali, nell'eventuale fase di riesame del provvedimento, di fronte al Responsabile della Prevenzione della Corruzione e della Trasparenza - RPCT (ai sensi dell'art. 5, comma 7, del D.Lgs. 33/2013) quest'ultimo dovrà, prima di assumere le proprie decisioni in merito al riesame, contattare il Garante per la protezione dei dati personali il quale dovrà rispondere entro

dieci giorni. Occorre quindi trovare un bilanciamento tra la trasparenza come accessibilità totale e la tutela dei dati personali, sulla base del GDPR e del novellato Codice della Privacy.

Delle prime indicazioni possono ricavarsi dalla Determinazione n. 1309 del 28/12/2016 dell'ANAC[25], nella quale si afferma che "*con riferimento alle istanze di accesso generalizzato aventi a oggetto dati e documenti relativi a (o contenenti) dati personali, l'ente destinatario dell'istanza deve valutare, nel fornire riscontro motivato a richieste di accesso generalizzato, se la conoscenza da parte di chiunque del dato personale richiesto arreca (o possa arrecare) un pregiudizio concreto alla protezione dei dati personali, in conformità alla disciplina legislativa in materia. La ritenuta sussistenza di tale pregiudizio comporta il rigetto dell'istanza, a meno che non si consideri di poterla accogliere, oscurando i dati personali eventualmente presenti e le altre informazioni che possono consentire l'identificazione, anche indiretta, del soggetto interessato*".

Nella stessa determinazione, sono poi individuati una serie di criteri che le pubbliche amministrazioni devono tenere presenti, ai fini della valutazione del pregiudizio concreto. Utili indicazioni possono ricavarsi anche dai plurimi pareri che il Garante Privacy ha emanato in tema di istanze di accesso generalizzato, disponibili sul sito dell'Autorità, nella sezione "provvedimenti".

1.2.5 ACCESSO DOCUMENTALE (L. 241/90) E TRATTAMENTO DEI DATI PERSONALI

In precedenza abbiamo trattato il nuovo istituto dell'accesso generalizzato. Non dobbiamo però dimenticarci dell'accesso agli atti "ordinario", vale a dire dell'accesso documentale ex artt. 22 e ss. della L. 241/1990. L'art. 86 del GDPR consente la comunicazione di dati personali contenuti in documenti ufficiali, conformemente al diritto dell'Unione (o al diritto interno), "al fine di conciliare l'accesso del pubblico ai documenti ufficiali e il diritto alla protezione dei dati personali".

La norma rilevante è il già citato art. 59 del D.Lgs. 196/2003, la quale ci dice che, (fatti salvi i dati inerenti allo stato di salute e alla vita sessuale) i presupposti, le modalità, i limiti per l'esercizio del diritto di accesso a documenti amministrativi contenenti dati personali - e la relativa tutela giurisdizionale - continuano a essere disciplinati dalla L. 241/1990 e dalle altre disposizioni in materia, anche per ciò che concerne le categorie particolari di dati e i dati inerenti alle condanne penali e reati, nonché le operazioni di trattamento eseguibili.

Se invece l'accesso (documentale) riguarda dati inerenti allo stato di salute ovvero la vita o l'orientamento sessuale (o dati genetici, ma è improbabile che il MIUR tratti questa categoria di dati personali), l'art. 60, con formulazione analoga a quella già vigente, impone di applicare il criterio del bilanciamento di interessi. Il trattamento è infatti consentito soltanto se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso sia di rango almeno pari ai diritti dell'interessato, ovvero consista in un diritto della personalità o in un altro diritto o libertà fondamentale.

Anche con riguardo ai trattamenti relativi alle istanze di accesso, troveranno comunque applicazione i principi generali del GDPR, e in particolare il principio di minimizzazione: i dati personali dovranno pertanto essere sempre "*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*".

[25] http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6666.

2 MODULO 2
LA SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI

2.1 SICUREZZA INFORMATICA NEL TRATTAMENTO DEI DATI PERSONALI

2.1.1 DALLE MISURE DI SICUREZZA MINIME E IDONEE ALLE MISURE ADEGUATE TECNICHE E ORGANIZZATIVE

Per quanto riguarda le misure di "sicurezza dei dati e dei sistemi", il "vecchio" Codice della Privacy (prima delle modifiche di armonizzazione al GDPR, entrate in vigore il 19 settembre 2018) prevedeva un generalizzato "obbligo di sicurezza" al cui interno venivano individuate da un lato le c.d. "misure minime" e, dall'altro, le c.d. "misure idonee". L'obbligo generalizzato di sicurezza, previsto all'art. 31, era finalizzato a "*ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito*".

Le misure minime di sicurezza - individuate, come abbiamo visto, "nel quadro dei più generali obblighi di sicurezza" - erano definite e catalogate nell'Allegato B del Codice stesso. Tali misure riguardavano tutti i trattamenti di dati personali effettuati con o senza l'ausilio di strumenti elettronici (artt. 34 e 35 del previgente Codice[26]) e la loro mancata adozione integrava il reato (contravvenzionale) previsto dall'art. 169[27], punito con l'arresto sino a due anni.

Le c.d. "misure idonee", invece, si individuavano - in via residuale - in tutte le altre misure di sicurezza ulteriori rispetto a quelle minime e che non erano, perciò, elencate o espressamente definite. Le misure idonee erano, pertanto, tutte quelle che potevano essere individuate (oltre alle misure minime) al fine di "ridurre al minimo i rischi". Il Codice (come avviene anche con il GDPR), infatti, era ben consapevole del fatto che un rischio non possa mai essere eliminato completamente. Per questo motivo anche il Codice (come il GDPR), sulla scorta delle indicazioni previste dalla ISO 31000 sulla gestione del rischio, prevedeva un obiettivo lasciando al singolo la facoltà di individuare le modalità attraverso cui raggiungerlo: garantire confidenzialità, integrità e disponibilità dei dati personali oggetto di trattamento. Si noti, inoltre, che il mancato rispetto delle misure "idonee" non poteva dar luogo a una sanzione penale ma, ciò nonostante, poteva essere fonte di responsabilità in sede civile (ad esempio nei procedimenti per risarcimento del danno derivante da trattamento dei dati personali).

Con il GDPR si abbandona la tradizionale ripartizione tra misure minime e misure idonee per concentrarsi sulle "misure tecniche e organizzative" adeguate al trattamento. Ed è proprio il titolare (o il responsabile del trattamento) a dover comprendere - sulla base di alcuni parametri indicati nell'art. 32 del GDPR - quali siano le misure tecniche e organizzative da adottarsi. Con il principio della accountability (o "responsabilizzazione"), previsto al par. 2 dell'art. 5, infatti, il titolare è (deve

[26] L'art. 34 prevedeva le seguenti misure minime, obbligatorie, per le ipotesi di trattamento di dati personali effettuato con strumenti elettronici: a) autenticazione e politiche di gestione delle credenziali; b) sistema di autorizzazione; c) aggiornamento periodico dell'ambito del trattamento consentito ai singoli interessati; d) protezione degli strumenti informatici, previsione di sistemi antivirus o anti-intrusione; e) copie di backup; f) sistemi di cifratura per trattamenti di dati relativi a stato di salute o vita sessuale effettuati da organismi sanitari.
L'art. 35, invece, con riferimento ai trattamenti effettuati senza l'ausilio di strumenti elettronici prevedeva, oltre all'aggiornamento periodico dell'ambito del trattamento consentito ai singoli interessati (previsto anche per i trattamenti effettuati con strumenti elettronici), l'adozione di misure di custodia di atti e documenti e di previsione di un sistema di conservazione in archivi protetti.

[27] Il reato in questione puniva con l'arresto sino a due anni chiunque, essendovi tenuto, omettesse di adottare le misure minime previste dall'articolo 33.

essere) oltre che competente a trattare i dati personali "in maniera da garantire un'adeguata sicurezza", anche in grado di comprovarlo.

Nel GDPR non troviamo, quindi, alcuna indicazione sulle misure specifiche da approntare ma unicamente i criteri per individuare delle misure tecniche ma anche organizzative che siano adeguate al singolo caso. In base al principio di responsabilizzazione, quindi, non potranno aversi soluzioni "preconfezionate"[28] di sicurezza tecnica e organizzativa "adeguata" ma dovranno sempre adottarsi soluzioni "su misura" (che devono essere individuate dal titolare).

Le misure di sicurezza previste dal GDPR, si è detto, sono "tecniche e organizzative". Ciò significa che oltre agli aspetti tecnici l'art. 32, oggi, ricomprende anche le misure che il titolare deve individuare (sempre in base al principio di responsabilizzazione) sul versante organizzativo. In quest'ambito, quindi, rientrano le decisioni circa l'organizzazione interna del titolare[29], la corretta individuazione dei responsabili esterni, la idonea individuazione della figura del Data Protection Officer e così via.

L'art. 32 del GDPR, quindi, prevede che il titolare e il Responsabile del trattamento mettano in atto "misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio". Come nella previgente disciplina, anche nel GDPR l'obiettivo fondamentale è ridurre il rischio che incombe sui dati personali. Ma come possono, titolare e responsabile del trattamento, comprendere quando le misure di sicurezza sono adeguate al rischio? Devono tenere in considerazione una serie di elementi previsti, sempre, dall'art. 32:

- ☑ Stato dell'arte in tema di misure di sicurezza;
- ☑ Costi per l'attuazione delle misure;
- ☑ Natura, oggetto, contesto e finalità del trattamento;
- ☑ Livello del rischio incombente su diritti e libertà delle persone fisiche.

Con riferimento al "livello di rischio" occorre considerare che il rischio è inteso come un qualcosa di incerto e indefinito che si frappone al raggiungimento dell'obiettivo (che in questo caso è la tutela dei diritti e delle libertà delle persone fisiche). E il rischio può essere "ponderato" tenendo in considerazione da un lato la probabilità di verificazione del rischio e dall'altra l'impatto, il danno che il rischio creerebbe una volta concretizzatosi.

Si noti, inoltre, che quando il GDPR sembra fare un'elencazione delle misure di sicurezza, lo fa a fini esemplificativi e non tassativi o esaustivi[30]. Il Legislatore europeo suggerisce, inoltre, che l'adesione

[28] È per questo motivo che, ad esempio, l'Art.29 WP ha precisato che "non esistono alternative valide alle soluzioni 'su misura'. Un approccio uguale per tutti avrebbe il solo effetto di costringere i responsabili del trattamento all'interno di strutture inadatte e si rivelerebbe quindi fallimentare" (Art. 29WP, Parere 3/2010 - WP 173).

[29] Il GDPR infatti non disciplina più quelli che sono le modalità organizzative interne, se non nei limiti indicati all'art. 29. Sul punto si veda *supra* il capitolo 7.3.

[30] Il comma 1 dell'art. 32 del GDPR, infatti elenca le misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (a. la pseudonimizzazione e la cifratura dei dati personali; b. la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c. la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d. una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento) ma lo fa premettendo "tra le altre, se del caso". Con "tra le altre" comprendiamo che le misure elencate al comma 1 non sono certo esaustive di tutte le misure che il titolare potrebbe dover applicare. Con "se del caso", l'art. 32, sta precisando che non è detto che una o più misure indicate nell'articolo in esame possano essere necessarie nell'ambito delle specifiche attività di trattamento attuate dal titolare.

da parte del titolare o del responsabile del trattamento a un codice di condotta o a un meccanismo di certificazione possa rappresentare un buon elemento per dimostrare la conformità del trattamento a quanto prescritto in materia di sicurezza. Al momento attuale, però, non vi è alcuna certificazione o codice di condotta che sia stato approvato dal Garante.

Il titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) La pseudonimizzazione e la cifratura dei dati personali;
b) La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
Ad esempio, l'adozione da parte del titolare o responsabile del trattamento di soluzioni modellate sui principi di *privacy by design* e *by default* è considerata, dal GDPR, una misura efficace per garantire che i prodotti o i servizi utilizzati dal titolare, nell'ambito del trattamento, siano in grado di offrire un'adeguata protezione dei dati personali trattati e, al contempo, un buon livello di mitigazione del rischio.

2.1.2 TECNICHE PER ASSICURARE SU BASE PERMANENTE LA RISERVATEZZA, L'INTEGRITÀ, LA DISPONIBILITÀ E LA RESILIENZA DEI SISTEMI E DEI SERVIZI DI TRATTAMENTO

Abbiamo visto che l'art. 32 del GDPR individua tra le misure tecniche e organizzative che - se del caso - titolare e responsabile del trattamento debbano applicare anche quelle in grado di "*assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*".

Il riferimento corre, con tutta evidenza, alla triade "confidenzialità, integrità e disponibilità". Una volta che i dati personali siano mantenuti confidenziali (ossia nessun soggetto che non sia legittimato possa entrare in contatto con essi), integri (ossia nessun soggetto non legittimato possa modificarli) e disponibili (ossia che il titolare o il responsabile ne conservino la disponibilità per il soddisfacimento dei fini previsti per il trattamento specifico) potrà dirsi che il trattamento è rispettoso dei principi di cui all'art. 5 del GDPR. Si tratta di principi espressamente richiamati dal Considerando 49 del GDPR nel punto in cui si definisce la sicurezza delle reti e dell'informazione come "*la capacità di una rete o di un sistema d'informazione di resistere a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche*".

Il concetto, infine, di "resilienza dei sistemi e dei servizi di trattamento" fa riferimento a quella capacità di un sistema o di un servizio di adeguarsi agli eventi imprevisti o anomali (potenzialmente dannosi) prevenendoli o, successivamente, ripristinando una condizione di normalità. Si tratta, in sostanza, di una capacità di attutire in modo "elastico" i rischi o i danni imprevisti.

Il riferimento, invece, al fatto che riservatezza, integrità, disponibilità e resilienza siano assicurati "su base permanente" chiarisce che la "sicurezza" non sia un concetto statico ma debba essere affrontato nella sua dimensione "dinamica". Per garantire, su base permanente, un elevato livello di sicurezza sui dati personali trattati dall'Amministrazione è, pertanto, necessario monitorare costantemente l'efficacia e l'efficienza delle misure di prevenzione del rischio informatico e aggiornarle o implementarle ove necessario.

Fra le tecniche in grado di assicurare tale risultato, vanno ricomprese anche quelle relative all'adozione di sistemi e servizi per il trattamento dei dati personali che siano modellati sui principi di *privacy by design* e *privacy by default*. Si tratta di sistemi che assicurano la protezione dei dati fin dalla progettazione e per impostazione predefinita.

Importante è anche il rispetto del principio di minimizzazione dei dati (richiamato dall'art. 5 del GDPR) e l'uso di tecniche di pseudonimizzazione o di cifratura in grado di minimizzare l'uso dei dati personali, a seconda del tipo di attività da attuare volta per volta, al fine di ridurre l'area di potenziale attacco e, quindi, da ridurre l'impatto che il rischio avrebbe sui dati trattati dall'Amministrazione.

2.1.3 LE MMS-PA (MISURE MINIME DI SICUREZZA PER LA PUBBLICA AMMINISTRAZIONE) DELLA CIRCOLARE AGID 2/2017

Si è già fatto cenno alle "Misure Minime di Sicurezza per la P.A." previste dall'AgID nella Circolare 2/2017, che rappresentano un punto di riferimento per la predisposizione e il monitoraggio della sicurezza informatica nelle amministrazioni. La finalità principale è quella di indicare alle stesse le misure minime di sicurezza ICT da adottare al fine di contrastare le minacce più frequenti e comuni cui sono soggetti i sistemi informativi. Non si tratta, ovviamente, delle "misure minime" già previste dall'Allegato B) del previgente Codice della Privacy anche se vi sono certamente rilevanti punti di contatto. Le MMS-PA non sono (ovviamente) collegate al Regolamento, ma ciò non toglie che anche il loro rispetto rappresenti un utile alleato nell'adeguamento richiesto dall'art. 32 del GDPR.

Le misure indicate spaziano dalla gestione dei dispositivi hardware a quelli software, con particolare attenzione al profilo dell'autorizzazione e autenticazione, anche con riguardo ai dispositivi mobili (laptop, server e workstation). Le misure riguardano inoltre la gestione del capitale umano che passa attraverso un controllo dei privilegi attribuiti a ogni utente in qualità di amministratore (ad esempio registrando ogni accesso effettuato, limitando i privilegi solo a coloro i quali abbiano competenze adeguate, evitando credenziali di autenticazione deboli, etc.).

Fondamentale è ritenuto il monitoraggio costante delle informazioni al fine dell'individuazione delle vulnerabilità e prevenzione degli attacchi informatici anche in un'ottica di resilienza informatica.

La circolare AgID indica le procedure e gli strumenti necessari a garantire il ripristino delle informazioni critiche in caso di necessità (ossia a seguito di incidente informatico). Tra esse ricordiamo la necessità di fare le copie di sicurezza delle informazioni strettamente necessarie al completo ripristino del sistema. A sua volta la riservatezza delle informazioni contenute nelle copie di sicurezza dovrà essere protetta con idonee misure fisiche ovvero mediante cifratura.

La circolare contiene anche un modulo di implementazione delle misure minime che ha lo scopo di aiutare le amministrazioni a valutare il livello di copertura prodotto dalle misure già adottate, delle procedure intraprese e delle verifiche poste in essere. Il modulo doveva poi essere firmato digitalmente dal responsabile e marcato temporalmente entro il 31 dicembre 2017. Il documento dovrà essere inviato al CERT-PA in caso di incidente informatico unitamente alla segnalazione e alla descrizione dell'incidente stesso.

2.2 IL DATA BREACH

2.2.1 CONFIDENZIALITÀ, INTEGRITÀ E DISPONIBILITÀ: LE SFACCETTATURE DELLA SICUREZZA

La violazione dei dati personali è definita dall'art. 4 comma 12 del GDPR come "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*". Si tratta, per l'appunto, di una violazione di sicurezza.

L'art. 29 WP (Gruppo dell'articolo 29 per la tutela dei dati - Article 29 Working Party), nelle proprie linee guida sulle violazioni di dati personali[31], distingue tre categorie, basandosi sui principi di sicurezza delle informazioni:

- ☑ Violazioni della confidenzialità: si verifica ad esempio quando un errore del sistema consente anche a terzi non autorizzati di accedere ai dati personali;
- ☑ Violazioni dell'integrità: consiste in una accidentale o non autorizzata alterazione dei dati;
- ☑ Violazione della disponibilità: si riscontra ad esempio quando l'azione di un ransomware (un software malevolo che opera cifrando i dati dei sistemi, per richiedere poi un riscatto) provochi la perdita dell'accesso o la distruzione dei dati personali.

Naturalmente, una violazione può rientrare in più categorie contemporaneamente. Si pensi all'azione di chi si introduce indebitamente nel sistema, prenda visione di dati personali e li alteri, comportando una violazione sia di confidenzialità che di integrità. O al caso in cui venga smarrito un supporto che contiene dati personali e non se ne abbia una copia (violazione di confidenzialità e di disponibilità).

2.2.2 SICUREZZA INFORMATICA E POSSIBILITÀ DI PREVEDERE LE POSSIBILI VIOLAZIONI

Il GDPR, in coerenza al principio di responsabilizzazione e di sicurezza, impone l'adozione di un sistema di misure tecniche e organizzative adeguate a prevenire (anche) le violazioni di dati personali.

Le misure di sicurezza, che abbiamo già esaminato, dovranno anche comprendere i sistemi di rilevazione delle violazioni, e dovranno essere organicamente collegate alle misure organizzative di gestione delle violazioni stesse, che si dovranno rendere conoscibili anche ai soggetti esterni all'Ente (si pensi ad esempio ai responsabili ex art. 28 GDPR e alle società che effettuano la manutenzione dei sistemi informatici).

Nella gestione delle violazioni, al di là dei profili formali, occorre sempre avere particolare cura nell'adozione di idonee misure per porre rimedio alle violazioni stesse. La minimizzazione dei possibili danni è, infatti, uno degli adempimenti centrali in capo al titolare.

2.2.3 DOCUMENTAZIONE DEL DATA BREACH: IL REGISTRO DELLE VIOLAZIONI

Sempre nell'ottica del rispetto del principio di responsabilizzazione, è indispensabile dotarsi di procedure specifiche per la gestione delle violazioni di dati personali, che individuino i soggetti coinvolti, e gli snodi principali, fino ad arrivare all'eventuale notificazione al Garante, o alla comunicazione agli interessati. In questo contesto è fondamentale la istituzione a livello di Amministrazione centrale di un Registro delle violazioni del Ministero. Esso deve essere aggiornato sia in caso di asseverazione del data breach sia in caso di falso positivo.

---

[31] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

Il GDPR all'art. 33, comma V, impone di documentare qualsiasi violazione (con l'indicazione delle circostanze, delle conseguenze e dei successivi provvedimenti adottati).

2.2.4 NOTIFICA ALL'AUTORITÀ DI CONTROLLO

Il GDPR prevede l'obbligo per tutti i titolari di provvedere alla notificazione delle violazioni di dati personali (il c.d. data breach), all'Autorità di controllo nazionale, ossia il Garante per la protezione dei dati personali.

La notifica al Garante deve essere effettuata entro 72 ore decorrenti non dall'evento, ma dalla scoperta dello stesso da parte del titolare, e senza ingiustificato ritardo. Il termine, quindi, parte dal momento in cui il titolare maturi la ragionevole certezza che un incidente di sicurezza abbia compromesso dei dati personali. Qualora la notifica non sia tempestiva occorrerà motivare le cause del ritardo.

La notifica è sempre obbligatoria, salvo che sia improbabile che sussista un rischio per i diritti e le libertà delle persone fisiche. Si impone, quindi, una pur sommaria valutazione del rischio. Ad esempio, si potrà ritenere tale "improbabilità" quando l'incidente riguardi dati già pubblici (si pensi ai dati pubblicati in amministrazione trasparente), oppure quando si tratti di una indisponibilità transitoria che non incida in maniera significativa (come può accadere per un blocco temporaneo di uno o più sistemi informatici).

L'art. 33 comma 3 del GDPR indica il contenuto minimo della notifica:

- ☑ La descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- ☑ Il nome e i dati di contatto del Responsabile della Protezione dei Dati o di altro soggetto presso cui ottenere più informazioni;
- ☑ La descrizione delle probabili conseguenze delle violazioni dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e per attenuare i possibili effetti negativi.

2.2.5 IPOTESI DI COMUNICAZIONE AGLI INTERESSATI

L'art. 34 del GDPR impone l'obbligo per il titolare, accanto alla notifica al Garante, di comunicare agli interessati la violazione di dati personali, laddove questa possa provocare un rischio elevato per i diritti e le libertà delle persone fisiche. La comunicazione all'interessato può essere anche richiesta dal Garante nell'ipotesi in cui si ravvisi un rischio elevato per i dati personali.

La comunicazione dovrà essere effettuata il prima possibile, e comunque senza ingiustificato ritardo, utilizzando un linguaggio semplice e chiaro per descrivere i contenuti indicati dall'art. 33 del GDPR.

La comunicazione non è necessaria, secondo quanto previsto dall'art. 34, comma 3, quando:

- ☑ Il titolare ha adoperato tutte le misure tecniche e organizzative adeguate di protezione relativamente ai dati oggetto di violazione, in particolar modo quelle che rendono i dati incomprensibili (come la cifratura);
- ☑ Il titolare abbia successivamente adottato tutte le misure necessarie per scongiurare un rischio elevato;
- ☑ La comunicazione al singolo interessato richiede degli sforzi sproporzionati; in tale caso occorre comunque procedere con comunicazioni pubbliche o similari.

2.2.6 IL RIPRISTINO DEI DATI IN CASO DI INCIDENTE

Uno degli aspetti fondamentali della disciplina in materia di sicurezza e privacy è la capacità del Ministero di garantire su base permanente la tutela dei dati personali, nelle sue diverse forme di riservatezza, integrità, disponibilità e resilienza. Per realizzare tale obiettivo è necessario che sia previsto un sistema che renda possibile il ripristino delle informazioni in caso di incidente, come abbiamo già avuto modo di sottolineare sia quando abbiamo affrontato l'obbligo di sicurezza, sia in tema di MMS-PA.

2.2.7 LA SEGNALAZIONE DEL DATA BREACH AI SENSI DELLA CIRCOLARE 2/2017 DELL'AGID

Come già visto in precedenza, la Circolare AgID n. 2/2017[32], rubricato "Misure minime di sicurezza ICT per le pubbliche amministrazioni", prescrive alle P.A. (a tutte le Amministrazioni di cui all'art. 2, comma 2, del D.Lgs. 82/2005) di comunicare le violazioni di sicurezza anche al CERT-PA[33].

L'art. 4 della Circolare 2/2017 dell'AgID prevede che il modulo di implementazione sia firmato digitalmente con marcatura temporale[34]. Dopo la sottoscrizione il modulo di implementazione delle MMS-PA "*deve essere conservato e, in caso di incidente informatico, trasmesso al CERT-PA insieme con la segnalazione dell'incidente stesso*".

[32] http://www.gazzettaufficiale.it/eli/id/2017/05/05/17A03060/sg.

[33] https://www.agid.gov.it/it/sicurezza/cert-pa.

[34] Il modulo deve essere sottoscritto digitalmente dal soggetto di cui all'art. 3 e dal responsabile legale della struttura.

3 APPROFONDIMENTI OPERATIVI - PRINCIPALI RISCHI (E ACCORGIMENTI) IN MATERIA DI SICUREZZA INFORMATICA

3.1 IL MALWARE: RANSOMWARE IN PARTICOLARE

I **malware** rappresentano uno dei maggiori pericoli per i sistemi informatici attraverso i quali siano trattati dei dati personali. Con il termine malware ci si riferisce a un'ampia categoria di software creati appositamente per danneggiare o alterare i sistemi informatici-bersaglio (spesso si fa impropriamente riferimento ai malware con il termine "virus informatico"). Il malware può colpire differenti tipologie di bersaglio (computer, dispositivi mobili, tablet, etc.) e può avere differenti finalità (danneggiamento, alterazione o introduzione abusiva nei sistemi informatici, estorsione di denaro etc.).

Rientra nell'ampia categoria dei malware anche la sottocategoria dei **ransomware**, ossia quei software malevoli che, una volta introdottisi all'interno del sistema operativo-bersaglio e averne alterato in qualche modo il funzionamento o l'accessibilità ai documenti in esso contenuti, richiedono un riscatto in denaro (solitamente in valuta virtuale come, ad esempio, bitcoin) in cambio delle credenziali per ripristinare il corretto funzionamento del dispositivo o l'accessibilità ai file. In genere i ransomware rendono inaccessibili i file mediante l'uso della cifratura.

Prevenire il contagio da ransomware[35] può non essere semplice, soprattutto se il contagio avvenga per il tramite di un dispositivo connesso a una rete locale in cui non tutti gli utenti siano adeguatamente formati sui rischi informatici ai quali sono continuamente esposti.

Sarà necessario dotare i sistemi informatici con i quali siano trattati dati personali di un sistema antivirus da tenere costantemente aggiornato. Potrà inoltre utilizzarsi un approccio di tipo "*endpoint security*" in cui, il sistema integrato di protezione sia in grado di identificare comportamenti anomali all'interno del sistema informatico da proteggere e blocchi quelle attività causate, magari, da un malware non ancora conosciuto e che, quindi, un semplice antivirus tradizionale non sarebbe in grado di individuare.

3.2 DISPOSITIVI BYOD E SICUREZZA INFORMATICA

BYOD è l'acronimo di "*Bring Your Own Device*", con il quale si fa riferimento a una politica in base alla quale le aziende private o gli enti pubblici consentono ai dipendenti o agli utenti di utilizzare i propri dispositivi personali (computer, tablet, smartphone, etc.) anche in ambito lavorativo accedendo, di conseguenza, a informazioni o dati dell'Ente o dell'azienda. I BYOD se da un lato consentono all'Ente un risparmio di spesa nell'acquisto di dispositivi "aziendali" da fornire ai dipendenti, dall'altro rappresentano una fonte di rischio in considerazione della impossibilità per l'Ente o l'azienda di controllare le vulnerabilità di cui siano affetti o gli eventuali malware di cui siano portatori.

I BYOD, inoltre, sono uno strumento ritenuto utile, per le finalità didattiche, anche dal Piano Nazionale Scuola Digitale (PNSD) nel punto in cui si fa riferimento al "Piano di azione n. 6 - Linee guida per politiche attive di BYOD (Bring Your Own Device)". Si fa riferimento alle linee guida che il MIUR svilupperà in collaborazione con AgID e Garante per la protezione dei dati personali per

[35] Si può notare che le email di phishing che veicolano i ransomware (ma il malware in genere) possono essere confezionate in modo molto accurato in modo da convincere, ad esempio, il destinatario che cliccando sul link contenuto all'interno dell'email potrà verificarsi lo stato di consegna di un pacco o si potrà scaricare una fattura per una prestazione ricevuta o altro.

finalità, ad esempio, di compilazione del registro elettronico o di partecipazione alle attività progettuali tra studenti e docenti. Nell'ambito di queste politiche occorre porre particolare attenzione al profilo della sicurezza informatica posto che i dispositivi personali possono essere veicolo di differenti tipologie di attacchi ai sistemi dell'Amministrazione e degli altri utenti connessi alla rete della medesima.

3.3 IL SOCIAL ENGINEERING

Con il termine "*social engineering*" (o ingegneria sociale) si fa riferimento a una serie di attività (spesso finalizzate a un attacco ai sistemi informatici) che hanno quale obiettivo non tanto il sistema informatico quanto l'utilizzatore del medesimo sistema. L'attaccante che volesse, in ipotesi, attaccare i sistemi informatici di un Istituto Scolastico potrebbe ottenere informazioni utili ad accedere a un sistema informatico pur rispettoso dello stato dell'arte della sicurezza informatica in tema di protezione. Tuttavia, la debolezza, nel sistema, potrebbe risiedere proprio nel dipendente dell'Ente pubblico che possa essere tratto in inganno al fine di consegnare credenziali di accesso o possa essere utilizzato quale veicolo della stessa infezione.

Per questo motivo si ritiene che l'unica difesa contro questo genere di attacco sia una formazione costante dei dipendenti sui profili di sicurezza informatica e sulle tipologie di attacco basate su tecniche di *social engineering*.

3.4 PHISHING

Si è già accennato ai profili di "insicurezza" legati alle email di phishing che, oltre a rappresentare un rischio per le risorse economiche dell'Amministrazione o dei singoli dipendenti, potrebbe essere un veicolo di malware con comprensibili contraccolpi sui sistemi informatici-bersaglio.

Per phishing, in genere, si fa riferimento a una tecnica di attacco "a strascico" (ossia un attacco non mirato ma eseguito inviando contemporaneamente a numerosi destinatari la medesima comunicazione) basata su email confezionate in modo da indurre il destinatario a cliccare sugli allegati o a seguire i link eventualmente contenuti.

3.5 RETI WI-FI

Anche le reti Wi-Fi possono essere veicolo di attacco o di infezione dei dispositivi connessi a quella medesima rete. In particolare, esistono delle tecniche di attacco che consistono nel simulare una rete Wi-Fi dell'Ente pubblico in modo da dirottare o captare i contenuti degli ignari "navigatori" che non si accorgono di non essere connessi alla rete "dell'Ente" ma a una rete Wi-Fi creata appositamente con finalità malevole.

3.6 VULNERABILITÀ ED AGGIORNAMENTO DEI SISTEMI

Con riferimento alle misure di sicurezza che ciascun titolare o responsabile del trattamento dovrebbe adottare è essenziale ribadire che il GDPR non ne individua alcuna ma impone a tali soggetti di compiere una valutazione approfondita dei rischi e, conseguentemente, di apprestare le "difese" adeguate che siano necessarie a rendere il rischio accettabile. Per questo motivo non esistono più cataloghi normativi o regolamentari di misure di sicurezza da adottare, posto che ciascun soggetto obbligato dovrà individuare le misure in base a numerosi parametri. Esistono, tuttavia, delle misure che sono ritenute utili a priori. Una di queste è quella che impone un aggiornamento costante del software a disposizione.

È importante comprendere, inoltre, che le politiche di sicurezza su qualsiasi sistema informatico non possono mai ritenersi un "punto d'arrivo" posto che vengono continuamente individuate le vulnerabilità di dispositivi, sistemi operativi o software e che queste possono essere sfruttate dagli attaccanti. Non si potrà mai, pertanto, avere una situazione di "sicurezza assoluta" dal punto di vista informatico ma si dovrà costantemente lavorare per garantire l'aggiornamento dei sistemi e delle misure di protezione (siano essi hardware o software come firewall, sistemi antintrusione, antivirus, etc.). L'aggiornamento dei sistemi operativi è essenziale e deve essere costantemente monitorato.

Occorre, tuttavia, considerare che in un sistema informatico complesso in cui operino differenti tipologie di dispositivi, differenti tipologie di sistemi operativi e software, e in cui si intersechino le attività di tali differenti sistemi è ben possibile - e anzi non è infrequente - che a un aggiornamento di uno di tali sistemi possa conseguire la mancanza di interoperabilità o di funzionamento di altri sistemi collegati. Questo problema è determinato proprio dal fatto che non sempre i sistemi sono interoperabili e compatibili tra di loro e, ad esempio, un software gestionale dell'Amministrazione, una volta aggiornati i sistemi operativi sui quali questo software viene utilizzato, potrebbe smettere di funzionare perché non riconosce l'ambiente in cui si trova a operare.

Al fine di evitare questo tipo di problemi è necessario affidare la gestione e l'aggiornamento dei sistemi istituzionali a soggetti effettivamente competenti. Ricordiamo, inoltre, che scegliere soggetti esterni realmente competenti alla gestione o aggiornamento dei dati (anche personali) in essi contenuti può essere rilevante in sede di scelta del Responsabile esterno del trattamento (ai sensi dell'art. 28 del GDPR). I trattamenti automatici svolti dagli Uffici MIUR e dalle Istituzioni Scolastiche, effettuati con gli strumenti e le procedure previsti dal SIDI, sono svolti nella cornice di politiche e misure di sicurezza specifiche, definite nei contratti di gestione in outsourcing vigenti, costantemente implementate e aggiornate a seguito di attività di monitoraggio e *tuning*. Le misure elencate di seguito fanno riferimento a *best practices* che possono eventualmente integrare quanto già in essere, anche nell'ambito di trattamenti con strumenti informatici effettuati al di fuori del SIDI.

3.7 I SISTEMI DI BACKUP

Già il "vecchio" Codice della Privacy individuava nelle misure di backup una tecnica necessaria a prevenire le perdite accidentali o connesse ad attacchi mirati ai sistemi informatici e ai dati in essi contenuti. Il backup consiste nella creazione di copie (integrali o incrementali) del contenuto dei dispositivi di memorizzazione al fine di consentire un pressoché immediato ripristino dei dati nel caso di una loro cancellazione accidentale o dovuta a un attacco (ad esempio un attacco a mezzo ransomware). È importante che siano assicurate efficaci politiche di conservazione dei dati e, in particolare, che siano adottati idonei sistemi di backup e di conservazione delle copie di sicurezza.

3.8 LA CIFRATURA

Attraverso le tecniche di cifratura (che si basano su differenti algoritmi) è possibile garantire una inaccessibilità alle informazioni a soggetti non in grado di eseguire l'inverso procedimento di decifratura. Esistono vari algoritmi di cifratura che si differenziano tra loro essenzialmente per essere basati su algoritmi a chiave simmetrica o, al contrario, su algoritmi a chiave asimmetrica. Nella prima tipologia il medesimo algoritmo è utilizzato sia per cifrare (o criptare) che per decifrare (o decriptare) i contenuti. Nella seconda tipologia, invece, una chiave (pubblica o privata) è usata per la cifratura e l'altra (privata o pubblica) è usata, per decifrare i contenuti.

Nella seconda tipologia rientrano, ad esempio, i sistemi di cifratura basati sull'uso della firma digitale. Qualora il mittente intenda inviare telematicamente, anche avvalendosi di un sistema "non sicuro" di comunicazione (quale, ad esempio, l'email) un documento in modo da assicurarsi che solo l'effettivo destinatario possa accedere al contenuto potrà utilizzare il software di gestione della firma digitale per cifrare il documento. Tale software chiederà al mittente di ricercare la chiave pubblica della relativa firma digitale del destinatario al fine di criptare il documento. Una volta criptato potrà essere allegato e inviato al destinatario il quale, utilizzando la chiave privata della firma digitale, potrà decriptare il documento cifrato con la relativa chiave pubblica.

Allo stesso modo un soggetto potrebbe voler inserire un documento all'interno di un dispositivo portatile (come, ad esempio, una pennina USB) ed essere sicuro che, dovendosi spostare dal posto A (ad esempio dal luogo di lavoro) al posto B (ad esempio la propria abitazione), qualora dovesse smarrire la pennina USB nessuno possa accedere ai contenuti del documento memorizzato sulla medesima pennina USB. Per far ciò potrà utilizzare la chiave pubblica della propria firma digitale per cifrare il documento mentre si trova nel posto A e, poi, una volta giunto nel posto B, decifrare il documento utilizzando la chiave privata della propria firma digitale.

Si noti che il GDPR fa spesso riferimento alla cifratura come uno dei possibili strumenti per assicurare l'esistenza di garanzie adeguate nella protezione dei dati (ad esempio si veda l'art. 6, par. 4, lett. e, oppure, ancora, l'art. 32, par. 1, o l'art. 34, par. 3, lett. a). Inoltre, il Considerando 83, in modo ancor più esplicito, prevede che "*per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura*".

3.9 LA DISMISSIONE DELL'HARDWARE E LA CANCELLAZIONE DEI DATI

Ulteriore profilo da considerare in caso di dismissione di sistemi di memorizzazione delle informazioni è quello relativo alla cancellazione sicura dei dispositivi. È noto, infatti, che la semplice cancellazione dei file mediante ricorso al "cestino" del sistema operativo non è in grado di eliminare realmente dal supporto di memorizzazione le informazioni in esso contenute. Poiché una dismissione non corretta di sistemi di memorizzazione (quali memorie USB, hard disk delle postazioni lavorative, smartphone, etc.) può integrare un'ipotesi di *data breach*, allora sarà necessario ricorrere, prima della dismissione dell'hardware in questione, a sistemi di cancellazione sicura dei dati (*wiping*).

3.10 LE POLICY SULLA SICUREZZA INFORMATICA

È possibile aumentare il livello di consapevolezza dei rischi, in capo a tutti i dipendenti dell'Ente, attraverso un documento contenente le politiche sulla sicurezza informatica stabilite dall'Ente stesso, previa verifica delle aree, dispositivi e strumenti esposti a rischio informatico. Una volta individuate le aree a rischio - con la collaborazione di personale altamente specializzato nel tema della sicurezza informatica - sarà possibile descrivere, all'interno di tale documento, le misure da adottarsi al fine di prevenire qualsiasi incidente informatico, nonché quelle di contenimento dell'impatto dell'incidente informatico una volta verificatosi.

Le policy sulla sicurezza, che devono essere distribuite e rese note a tutta l'Amministrazione, possono rappresentare, infatti, un'occasione per definire in modo chiaro le istruzioni per i dipendenti che abbiano ricevuto, per l'adempimento della propria prestazione lavorativa, strumenti informatici (quali computer, tablet, smartphone), esposti ai rischi informatici più diffusi.

4 ABBREVIAZIONI

- ☑ **AgID** (Agenzia per l'Italia Digitale) www.agid.gov.it
- ☑ **Article 29 WP** Il Gruppo di lavoro istituito dall'art. 29 della direttiva 95/46 (organismo consultivo e indipendente, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, Garante europeo e da un rappresentante della Commissione) e che con il GDPR viene trasformato nel Comitato Europeo per la Protezione dei Dati - EDPB (artt. 68 e ss.)
- ☑ **BYOD** (Bring Your Own Device) Si tratta di tutti quei dispositivi elettronici personali (che possono essere, ad esempio, USBPEN, computer, tablet, smartphone, etc.) nella titolarità di chi sia stato autorizzato a impiegarli anche sul posto di lavoro
- ☑ **CAD** (Codice dell'Amministrazione Digitale) D.Lgs. 82/2005
- ☑ **CERT-PA** (Computer Emergency Response Team Pubblica Amministrazione) è una struttura che opera all'interno dell'AgID ed è preposta al trattamento degli incidenti di sicurezza informatica relativi ai sistemi informativi delle pubbliche amministrazioni
- ☑ **CSIRT** (Computer Security Incident Response Team)
- ☑ **DPO** (Data Protection Officer) vd. anche RDP
- ☑ **DPIA** (Data Protection Impact Assessment) valutazione d'impatto sulla protezione dei dati - art. 35 GDPR
- ☑ **GDPR** (Regolamento Generale sulla protezione dei dati personali) Reg. UE 2016/679
- ☑ **ICT** (Information and Communication Technology) Tecnologie dell'Informazione e della Comunicazione
- ☑ **IoT** (Internet of Things - Internet delle Cose) Oggetti connessi alla rete Internet che, attraverso la comunicazione o la diffusione di dati acquisiti dall'ambiente circostante o attraverso la ricezione di comandi particolari, possono offrire servizi ulteriori
- ☑ **MMS-PA** (Misure Minime di sicurezza per la Pubblica Amministrazione) Descritte dalla Circolare n. 2/2017 dell'AgID
- ☑ **NIS** (Network and Information Security)
- ☑ **PA** (Pubblica Amministrazione)
- ☑ **RPCT** (Responsabile della Prevenzione della Corruzione e della Trasparenza)
- ☑ **RPD** (Responsabile della Protezione dei Dati - vd. DPO)
- ☑ **WP** (Working Party) vd. anche Article 29 WP (Gruppo dell'articolo 29 per la tutela dei dati).

5 LINKOGRAFIA

- ☑ http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679&from=EN (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)
- ☑ http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig= (Codice in materia di protezione dei dati personali - DECRETO LEGISLATIVO 30 giugno 2003, n. 196)
- ☑ www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2018-08-10;101!vig= (Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 - D.Lgs. 10 agosto 2018, n. 101)
- ☑ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 (Guidelines on Data Protection Officers ('DPOs'))
- ☑ http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 (Personal data breach notification under Regulation 2016/679 (wp250rev.01))
- ☑ http://194.242.234.211/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati (Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679)
- ☑ http://garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali (Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali - Garante Privacy)
- ☑ http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7322110 (Nuove FAQ sul Responsabile della Protezione dei dati (RPD) in ambito pubblico (in aggiunta a quelle adottate dal Gruppo Art. 29))
- ☑ http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3134436 (Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati)
- ☑ http://www.anticorruzione.it/portal/public/classic/AttivitaAutorita/AttiDellAutorita/_Atto?ca=6666 (Linee guida recanti indicazioni operative ai fini della definizione delle esclusioni e dei limiti all'accesso civico di cui all'art. 5 co. 2 del d.lgs. 33/2013)

6 MATERIALI DI APPROFONDIMENTO

- ☑ Il GDPR (nella sua versione rettificata del maggio 2018)
- ☑ Il nuovo Codice della Privacy, così come modificato dal D.Lgs. 101/2018
- ☑ Il D.Lgs. 101/2018, con particolare attenzione alle norme ulteriori rispetto a quelle di aggiornamento del D.Lgs. 196/2003
- ☑ La valutazione d'impatto del Garante della Privacy - Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018
- ☑ Le linee guida dell'Art.29 WP (attualmente Comitato europeo per la protezione dei dati personali)
  - ❖ Linee guida Art29WP sul consenso
  - ❖ Linee guida Art29WP sul DPO
  - ❖ Linee guida Art29WP sulla trasparenza
  - ❖ Linee guida Art29WP sulla notifica dei data breach
  - ❖ Linee guida Art29WP sulle decisioni automatizzate
  - ❖ Linee guida Art29WP sull'applicazione e la previsione delle sanzioni amministrative pecuniarie
  - ❖ Linee guida Art29WP sulla portabilità dei dati
  - ❖ Allegato alle linee guida sulla portabilità dei dati
  - ❖ Linee guida Art29WP sulla DPIA
  - ❖ Linee guida Art29WP per l'individuazione dell'autorità di controllo capofila
  - ❖ Linee guida del EDPB 4/2018 relative all'accreditamento degli organismi di certificazione ai sensi dell'articolo 43 del GDPR
  - ❖ Linee guida EDPB 2/2018 sulle deroghe di cui all'articolo 49 del GDPR
- ☑ La Circolare 2/2017 dell'AgID
- ☑ Le linee guida per la predisposizione dell'informativa sul trattamento dei dati ai sensi degli artt. 13 e 14 Regolamento UE 679/2016 (Dicembre 2018)
- ☑ Le linee guida sui soggetti del processo di gestione della privacy del Ministero - Direttiva del Ministro del 25 marzo 2019, n. 239 (Aprile 2019).