STORYLINE DEL CORSO - PERSONALE ATA

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 ATA

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 "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, con il D.Lgs. 10 agosto 2018 n. 101[3] (entrato in vigore il 19 settembre), al fine di adeguare l'ordinamento interno al GDPR, e per regolamentare gli aspetti per la cui regolamentazione il GDPR rinviava al Legislatore nazionale.

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.

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"

[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 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*»)".

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.

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'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 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.

[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.

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".

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.

1.1.3 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".

Per il GDPR è dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato)"[6]. 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.

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.

1.1.4 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.

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

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.

1.1.5 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)[7].

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

Nell'ambito delle attività degli Istituti Scolastici, 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.

Il nuovo assetto impone 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[8] di dati personali e la loro diffusione[9].

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.

[8] 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".

[9] 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".

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.

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.

Nell'ambito delle attività delle Istituzioni Scolastiche, 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[10], 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 che possa 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

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

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

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.

1.1.6 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 dell'Ente) 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 mentre, come approfondiremo tra breve, gli Istituti Scolastici sono titolari autonomi.

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).

Gli Istituti Scolastici, come abbiamo anticipato, 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.

Ne consegue che ciascun Istituto Scolastico è da intendersi quale titolare dei trattamenti per i quali decide modalità e finalità. Si pensi, ad esempio, ai trattamenti di dati effettuati mediante il registro elettronico, o alle pubblicazioni sul sito della Scuola, o all'eventuale pagina che la Scuola attivasse sui social network (ad esempio Facebook).

Bisogna evitare l'errore di ritenere che il titolare del trattamento sia il legale rappresentante dell'Ente (e dunque, per gli Istituti Scolastici, il Dirigente Scolastico): è l'Ente stesso, nel suo complesso, e non il legale rappresentante, ad essere il titolare. Il Dirigente scolastico si porrà come soggetto che esercita le funzioni di titolare.

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 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.

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* (ad esempio il registro elettronico): 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.

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"[11].

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.

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"[12], 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.

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.

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

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

Il singolo Istituto Scolastico, quindi, nell'ambito della sua autonomia organizzativa, potrà individuare - ai sensi dell'art. 2-*quaterdecies* del D.Lgs. 196/2003 così come modificato dal D.Lgs. 101/2018 - la soluzione più idonea a gestire, dal punto di vista organizzativo interno, la tutela dei dati personali di cui l'Istituto stesso sia titolare. In questa sua qualità, pertanto, l'Istituto Scolastico, a mezzo del Dirigente Scolastico, adotta gli opportuni provvedimenti relativi all'ambito tecnico e organizzativo. Il Dirigente Scolastico potrà, pertanto, decidere di individuare uno o più designati al trattamento dei dati personali, oltre a dover individuare specificamente i soggetti autorizzati al trattamento dei dati personali di cui l'Istituto Scolastico sia titolare, fornendo a questi ultimi idonee e specifiche istruzioni sul trattamento dei dati personali.

Abbiamo, infatti, 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 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.

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.

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[13]. 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[14], 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"[15].

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.

Il Responsabile della Protezione dei Dati deve essere tempestivamente coinvolto in tutte le questioni riguardanti il trattamento di 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.

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.

1.1.7 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

[13] 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.

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

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

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 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[16].

1.2 AMMINISTRAZIONE, GDPR E TRASPARENZA (aspetti applicativi)

1.2.1 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*[17]*, 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

[16] https://www.garanteprivacy.it/home/faq/registro-delle-attivita-di-trattamento.

[17] 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.

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.

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.

1.2.2 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[18], 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*

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

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".

1.2.3 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 l'Istituto Scolastico 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*".

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[19]) e la loro mancata adozione integrava il reato (contravvenzionale) previsto dall'art. 169[20], 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.

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

[19] 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.

[20] 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.

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"[21] 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[22], 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.

2.1.2 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.

[21] 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).

[22] 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.

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[23], 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.

2.2.2 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 di un Registro delle violazioni.

[23] 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).

2.2.3 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.

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 attenuarne i possibili effetti negativi.

2.2.4 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.

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

Come già visto in precedenza, la Circolare AgID n. 2/2017[24], 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[25].

L'art. 4 della Circolare 2/2017 dell'AgID prevede che il modulo di implementazione, una volta firmato digitalmente con marcatura temporale[26]. 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*".

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

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

[26] 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[27] 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

[27] 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 de-cifratura. 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 APPROFONDIMENTI OPERATIVI PER LA SCUOLA

4.1 TRATTAMENTO DI DATI RELATIVI A STUDENTI: LA PUBBLICAZIONE DEGLI ESITI DI ESAMI E SCRUTINI

La norma di riferimento per quanto riguarda la pubblicazione degli esiti di esami e scrutini è quella di cui all'art. 96 del D.Lgs. 196/03 così come modificata dal D.Lgs. 101/2018.

L'art. 96 prevede che "*al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonché le istituzioni di alta formazione artistica e coreutica e le università statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalità*".

La norma in questione, inoltre, fa salva la previsione di cui allo statuto delle studentesse e degli studenti della Scuola secondaria secondo il quale "la comunità scolastica promuove la solidarietà tra i suoi componenti e tutela il diritto dello studente alla riservatezza" (DPR 249/98).

Più rilevante è l'ultimo comma dell'art. 2 che non prevede alcuna modifica alla disciplina attualmente in vigore "in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'Istituto e di rilascio di diplomi e certificati". Per questo aspetto rappresenta, pertanto, ancora un valido supporto il Vademecum pubblicato dal Garante per la protezione dei dati personali "La Scuola a prova di privacy".

4.2 LE INFORMAZIONI (INFORMATIVA PER IL TRATTAMENTO DEI DATI PERSONALI) DA FORNIRE NELLA PAGINA SOCIAL DELLA SCUOLA

Recentemente la Corte di Giustizia UE (nella causa C-210/16 con sentenza del 5 giugno 2018 - Wirtschaftsakademie Schleswig-Holstein) ha stabilito che Facebook e l'amministratore di una "fanpage" (la c.d. "pagina Facebook") si trovino, con riferimento alla pubblicazione dei contenuti nella suddetta pagina, in rapporto di contitolarità. Per tale motivo è necessario che l'Istituto Scolastico inserisca, nella pagina social della Scuola, un'informativa ai sensi dell'art. 13 del GDPR.

4.3 LA SICUREZZA INFORMATICA E I REGISTRI ELETTRONICI

I registri elettronici, come qualsiasi altro software, sono esposti - soprattutto quando connessi alla rete Internet (o anche in una LAN - *Local Area Network*) - ai medesimi rischi ai quali sono comunemente esposti tutti gli altri sistemi informatici della Scuola. Considerando che esistono, allo stato, diversi tipi di registro elettronico, non si possono offrire risorse tecniche circa la sicurezza di tali strumenti. Le regole basilari della sicurezza informatica, comunque, rappresentano una buona base di partenza per ridurre i rischi legati, appunto, all'utilizzo del registro elettronico.

Qualora, inoltre, la gestione del registro elettronico si basi su un sistema di memorizzazione in cloud, si dovrà valutare attentamente il contenuto dell'accordo tra Istituto Scolastico e fornitore del servizio del registro elettronico, dato che quest'ultimo deve essere individuato quale "responsabile del trattamento" ex art. 28 GDPR, e deve fornire idonee garanzie.

5 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).

6 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)

7 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).