DIDATTICA A DISTANZA E PROTEZIONE DEI DATI,
INDICAZIONI MINITERIALI CON IMPRECISIONI

approfondimento a cura di Giambattista Rosato – esperto giuridico e DPO

In questo momento di emergenza nazionale da Coronavirus, le scuole italiane avrebbero bisogno di indicazioni operative concrete che possano aiutarle nel pianificare le nuove attività di didattica a distanza nel rispetto della normativa sulla protezione dei dati, ma il Ministero dell'Istruzione con la nota esplicativa fornisce delle indicazioni superficiali e anche errate in alcuni passaggi.

Gli **errori** e la **superficialità** che caratterizzano le indicazioni del Ministro dell'Istruzione in tema di protezione dei dati personali suonano come una **beffa** per gli istituti scolastici, in prima linea per garantire, anche a distanza e con i pochi mezzi a disposizione, la **continuità didattica**.

In questo periodo di emergenza da Coronavirus, in cui studenti, famiglie e docenti si trovano catapultati gioco forza nella didattica a distanza, non bisogna infatti sottovalutare le problematiche legate (anche) alla protezione dei dati personali dei ragazzi, per la maggior parte minorenni, e alla sicurezza dei sistemi informativi e dei dati trattati dalle scuole.

Per questo motivo, è essenziale che le Scuole con il proprio **Responsabile per la protezione dei dati** ("DPO") devono costruire un percorso di formazione a distanza che possa tutelare i diritti degli studenti, ***tout court***.

Il Ministero dell'Istruzione sembra essere consapevole di queste tematiche e dell'importanza del rispetto della normativa per la protezione dei dati personali, anche in un momento del genere. In una recente nota, indicante alcune istruzioni operative per la didattica a distanza, il Ministero dell'Istruzione ha quindi inteso riportare anche alcune indicazioni proprio in merito alla privacy.

Per quanto ogni autorevole indicazione in tal senso sia sempre ben accetta, ritengo modestamente che il Ministero dell'Istruzione avrebbe potuto fare un lavoro migliore, data la complessità della materia ed i diritti in gioco.

Consenso: sì o no?

Per prima cosa il Ministero dell'Istruzione ci tiene a precisare che: "*[…] le istituzioni scolastiche non devono* ***richiedere il consenso*** *per effettuare il trattamento dei dati personali (già rilasciato al momento dell'iscrizione) connessi allo svolgimento del loro compito istituzionale, quale la didattica, sia pure in modalità "virtuale" e non nell'ambiente fisico della classe*."

Questa precisazione purtroppo è fuori luogo e parzialmente incorretta. È vero che le istituzioni scolastiche non sono tenute a richiedere il consenso agli studenti prima di effettuare il trattamento dei dati personali per ragioni di didattica; ***ma è assolutamente errato affermare che questi avrebbero dovuto rilasciarlo al momento dell'iscrizione***. La condizione di liceità, cioè il fondamento giuridico che rende lecito un trattamento di dati personali, in questo caso non è il consenso. A seconda delle diverse fasi e finalità del trattamento, la corretta base giuridica deve essere individuata tra:

i) esecuzione del contratto;

ii) adempiere ad un obbligo legale (es. rendicontazione verso un Ente);

iii) esecuzione di un compito di interesse pubblico.

Anche nel caso in cui sia necessario trattare categorie particolari di dati personali (come informazioni relative allo stato di salute o convinzioni religiose), non è necessario chiedere il consenso. Questo

perché il trattamento di questi dati, è legittimato direttamente dalla legge, che prescrive la predisposizione di piani educativi individualizzati (PEI) come previsto dalla legge n. 104/92, L. n. 328/2000 e D.Lgs. n. 66/2017.

In sostanza**, il consenso nel contesto scolastico è marginale e rilevante solo per attività facoltative e accessorie**, come possono essere comunicazioni promozionali o la diffusione di fotografie o video sul web, salvo alcune esigenze ampiamente documentate nel PTOF.

La *gaffe* del Ministero dell'Istruzione potrebbe portare ad interpretazioni distorte che potrebbero costare molto alle scuole in termini di efficienza.

Acquisire il consenso significa caricare il sistema di un onere burocratico non indifferente. Il consenso deve essere documentato e conservato in modo tale da dimostrarne l'acquisizione. In altre parole: copie cartacee e/o elettroniche di documenti che dovranno essere conservati per tutta la durata del rapporto con lo studente e anche oltre. Tutto questo, senza considerare che il consenso dovrebbe essere liberamente prestato, per specifiche finalità e liberamente revocabile dallo studente. Queste caratteristiche intrinseche del consenso chiaramente non potrebbero sussistere qualora la Scuola decidesse di acquisire un consenso unitario per il trattamento dei dati nel contesto della didattica, che comprende al suo interno numerose finalità, anche molto spesso eterogenee tra loro.

La speranza è che i DPO delle scuole siano in grado di interpretare la normativa correttamente, senza tener conto dell'evidente *gaffe* del Ministero dell'Istruzione.

Trasparenza, liceità, correttezza

Il Ministero dell'Istruzione esprime alcuni concetti importanti: "*Le istituzioni scolastiche sono invece tenute, qualora non lo abbiano già fatto, ad* ***informare gli interessati del trattamento*** *secondo quanto previsto dagli artt. 13 e 14 del Regolamento UE 2016/679 e a garantire che i dati personali siano trattati in modo lecito, corretto e trasparente, che siano raccolti per finalità determinate, esplicite e legittime, che siano trattati in modo non incompatibile con tali finalità […]*"

I principi espressi dal Ministero dell'Istruzione sono direttamente mutuati dal Reg. UE 2016/679 (**GDPR**), che prescrive l'obbligo di rispettare i principi applicabili al trattamento di dati personali. La capacità di rispettare questi principi dovrà essere evidentemente traslata anche alle **attività di didattica a distanza**, che dovranno essere organizzate tenendo conto dei requisiti del GDPR. A tal proposito è giusto ricordare che sarà probabilmente necessario aggiornare **le informative per studenti, famiglie e docenti**, comunicando tutte le informazioni necessarie sulle nuove attività di trattamento di dati personali che saranno realizzate. Allo stesso modo sarà necessario riportare le nuove attività nel **Registro delle attività di trattamento**, così da semplificare l'esame analitico delle singole attività.

Divieto di profilazione, diffusione e comunicazione … siamo sicuri?

Il Ministero dell'Istruzione prosegue poi: *"[…] evitando qualsiasi forma di profilazione, nonché di diffusione e comunicazione dei dati personali raccolti a tal fine, che essi siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per cui sono trattati […]*"

A ben vedere, la prima parte di questo passaggio sembra **inopportuna**. Il Ministero dell'Istruzione sembrerebbe vietare qualsiasi forma di profilazione, senza giustificarne le motivazioni.

La profilazione è descritta nel GDPR come "*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali*

relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica".

Benché sia un trattamento evidentemente invasivo e che spesso comporta diversi rischi per le persone, è **ingiustificato vietarne l'esecuzione *tout court***. La profilazione in ambito scolastico non trova ancora molto spazio, ma è indubbiamente uno strumento che può portare grandi vantaggi agli istituti scolastici. Attraverso la correlazione tra diverse categorie di informazioni è possibile ottenere informazioni utili e utilizzabili per **anticipare bisogni degli studenti** e, in generale, compiere scelte informate.

Certamente, profilare soggetti vulnerabili come gli studenti può essere fatto soltanto dopo la valutazione del rischio e valutazione d'impatto, garantendo un **adeguato livello di sicurezza** e tutela dei diritti degli studenti. Vietare la profilazione in questo senso, peraltro senza alcuna contestualizzazione in merito alla didattica a distanza, sembra semplicemente irragionevole.

Allo stesso modo il Ministero dell'Istruzione **sembrerebbe vietare qualsiasi diffusione o comunicazione di dati** – anche qui senza contestualizzare e senza tenere in considerazione che la comunicazione di dati a diversi soggetti coinvolti è quasi sempre necessaria. D'altronde, c'è un motivo se il nome completo del GDPR è Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Che senso ha vietare la comunicazione dei dati?

Sicurezza dei dati e rischi

Il Ministero dell'Istruzione afferma che i dati dovranno essere "[…] trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali".

Gli istituti scolastici sono tenuti a garantire un'adeguata sicurezza dei dati trattati, che in breve significa rispettare le principali buone prassi e raccomandazioni in materia di cyber sicurezza, oltre che adottare un vero e proprio sistema di gestione dei rischi cyber, che nel contesto della didattica a distanza e lavoro agile/smart working aumentano esponenzialmente. Subire un incidente informatico (e conseguente violazione di dati personali) in un momento del genere potrebbe significare il blocco totale di tutte le attività, con gravissime ed evidenti conseguenze per tutti (scuola, docenti, famiglie e studenti).

Purtroppo, da questo punto di vista la situazione italiana, specie nelle scuole è drammatica. Nelle scuole non sono presenti persone competenti in materia di cybersicurezza e le scuole spesso a distanza di alcuni anni non risultano adeguate alle **Misure minime di sicurezza ICT,** ai sensi dell'art. 14-bis del **Codice dell'Amministrazione Digitale** (CAD). Benché tali misure minime debbano ritenersi cogenti.

I responsabili del trattamento

Il Ministero dell'Istruzione prosegue poi parlando dei fornitori di servizi necessari per realizzare le attività di didattica a distanza, ricordando alle scuole che sono tenuti "a stipulare contratti o atti di

individuazione del responsabile del trattamento ai sensi dell'articolo 28 del Regolamento, che per conto delle stesse tratta i dati personali necessari per l'attivazione della modalità didattica a distanza".

L'indicazione, corretta, manca di un passaggio preliminare. Le scuole, così come chiunque decida di affidare una o più attività di trattamento a soggetti terzi esterni (qualificati come Responsabili del trattamento) sono tenuti, prima di tutto, a valutare le garanzie che questi offrono per soddisfare i requisiti del GDPR. L'art. 28 del Regolamento è chiarissimo. **L'affidamento incauto a fornitori non in grado di prestare garanzie adeguate può comportare responsabilità diretta** per *culpa in eligendo*, anche in solido con il fornitore.

Obbligo di valutazione d'impatto?

Il Ministero dell'Istruzione conclude ricordando alle scuole che sono tenuti "a sottoporre i trattamenti dei dati personali coinvolti a valutazione di impatto ai sensi dell'articolo 35 del Regolamento".

La **valutazione d'impatto** è un processo inteso 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, valutando detti rischi e determinando le misure per affrontarli. In pratica, è il momento *clou* del sistema di gestione per la protezione dei dati.

La valutazione d'impatto, in alcuni casi, è obbligatoria. In particolare, il Regolamento europeo prescrive che sia obbligatorio sottoporre un trattamento a valutazione d'impatto quando questo può presentare un rischio elevato per diritti e libertà delle persone. Oltre a questo, deve ricordarsi il recente provvedimento dell'Autorità Garante (Provv. n. 467/2018) in cui sono indicate alcune attività di trattamento che per loro natura presentano un rischio elevato per le persone, e pertanto devono essere obbligatoriamente sottoposte a valutazione d'impatto. Fra i trattamenti elencati nel citato provvedimento troviamo i "Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)".

Il provvedimento indica le categorie di soggetti vulnerabili. Tale elencazione non deve ritenersi tassativa ed esaustiva, poiché a titolo esemplificativo anche i dipendenti rientrano nella nozione di soggetti vulnerabili.

Con un approccio sistemico diverso, l'obbligo di valutazione d'impatto, così come affermato dalla circolare del Ministero dell'Istruzione, potrebbe essere fuori luogo, per due ordini di motivi.

Primo, il Regolamento europeo prevede che la valutazione d'impatto debba essere effettuata sulla base di una valutazione del rischio, tenendo conto del contesto concreto. Allo stesso modo il provvedimento 467/2018 del Garante si basa su una valutazione "aprioristica" che dovrebbe comunque essere contestualizzata. Per agevolare la valutazione del rischio il **Comitato europeo per la protezione dei dati** ha predisposto delle linee guida in materia di valutazione d'impatto, indicando nove indicatori di rischio. In presenza di almeno due di questi indicatori di rischio, deve ritenersi obbligatorio sottoporre il trattamento a valutazione d'impatto.

Il motivo è semplice: la valutazione d'impatto è un processo complesso che può richiedere un notevole investimento di risorse, e che pertanto non può essere reso obbligatorio a prescindere dal contesto concreto.

Secondariamente, l'art. 28 del Regolamento prevede che l'Autorità di controllo (il Garante) redige un elenco delle tipologie di trattamenti soggetti al requisito di valutazione d'impatto. Tale elenco è

sottoposto alla valutazione del Comitato Europeo, per assicurarne la compatibilità con il GDPR e l'uniformità, nel rispetto del principio di coerenza.

Il Ministero dell'Istruzione potrebbe quindi non essere competente a disporre l'obbligo di sottoporre specifiche attività di trattamento a valutazione d'impatto.

Conclusioni

In conclusione, le indicazioni operative del MIUR risultano superficiali e anche errate in alcuni passaggi, di fatto poco più che una clausola di stile.

È evidente che qualsiasi indicazione da parte del Ministero riveste particolare importanza, ed è un vero peccato sprecare queste occasioni con note non adeguate ad affrontare i rischi a cui sia le scuole che gli studenti sono soggetti in questo particolare momento storico.