“Gli errori” relativi alla privacy nella nota Miur sulla didattica a distanza

orizzontescuola.it/gli-errori-relativi-alla-privacy-nella-nota-miur-sulla-didattica-a-distanza/

March 19, 2020

contributo di Avv. Graziano Garrisi, avv. Rossella Lozito, dott.ssa Chiara Delaini * – L’ultima nota del Ministero dell’Istruzione, la nr. 388 del 17 marzo 2020, fornisce le prime indicazioni operative per la didattica a distanza, con la quale tutte le scuole si stanno misurando, a causa dell’emergenza sanitaria che ha colpito il nostro Paese.

La nota, in particolare, si propone di offrire e chiarire alcuni aspetti di natura operativa in relazione agli strumenti adottati dalle istituzioni scolastiche per consentire ai vari operatori coinvolti nella didattica di continuare a lavorare in modalità virtuale.

Com’è noto, la contingenza delle circostanze ha imposto l’adozione di strumenti di didattica a distanza (a ben vedere non del tutto innovativi visto che molte scuole già li utilizzavano per lo svolgimento del normale percorso didattico) che, da un lato, devono garantire la continuità del diritto all’istruzione in un momento così delicato (in caso contrario si potrebbe configurare anche interruzione di pubblico servizio) e, dall’altro, assicurare la conformità alla normativa vigente, per quanto possibile.

Chiariamo subito che l’atto di cui discutiamo è una “nota” ministeriale, operativa in ambito di didattica a distanza. Formalmente non qualificata come “circolare”, pur avendone tutti i contenuti. Se “nota” di certo è solo indicativa, può essere disattesa dagli uffici cui si rivolge, possibilmente con un’adeguata motivazione.

Anche se volessimo definirla “circolare” non muta di fatto la conclusione.

Una circolare ministeriale può avere varie funzioni. La “circolare” (?) di cui discutiamo può essere definita organizzativa, per taluni aspetti anche interpretativa, in ogni caso di certo non può produrre effetti al di fuori dell’Amministrazione emanante e, come da insegnamento delle sentenze Cass. SSUU n. 23031/2007 e Consiglio di Stato n. 7521/2010, può comunque essere disattesa dagli uffici della stessa Amministrazione con un’adeguata motivazione. Ad una circolare non può quindi essere riconosciuta alcuna efficacia normativa esterna rispetto all’Amministrazione emanante e non può essere annoverata fra gli atti generali di imposizione in quanto essa non può né contenere disposizioni derogative di norme di legge, né essere considerata al pari di una norma regolamentare vera e propria.

Questione consenso

In relazione alla questione privacy, la nota in esame chiarisce subito (semmai ce ne fosse bisogno) che le scuole non hanno bisogno di raccogliere il consenso dei genitori o degli alunni maggiorenni per fornire i servizi di didattica a distanza.

Questa è senz'altro uno dei compiti istituzionali della scuola e la modalità diversa di esplicazione – virtuale e non in presenza- non ne inficia la natura.

Fin qui, nulla quaestio, salvo poi specificare (tra parentesi) che il consenso le scuole lo avrebbero dovuto raccogliere a inizio anno scolastico.
Su tale aspetto, occorre ricordare che il 99% delle attività di trattamento delle pubbliche amministrazioni non ha e non può avere come "base giuridica" il consenso, bensì l'esecuzione di compiti di intesse pubblico, l'adempimento a obblighi di legge (come specifica dall'art. 2-ter del D.Lgs. 196/2003 – Codice Privacy) e, semmai vi fosse un trattamento di categorie particolati di dati, i "motivi di interesse pubblico rilevante" (che ne caso specifico è il diritto all'istruzione – art. 2 sexies, comma 2lett. bb del D.Lgs. 196/2003 – Codice Privacy).

A supportare questa osservazione c'è non solo la norma, ed in particolare l'articolo 6 del regolamento UE 2016/679, declinato dai citati articoli del D.Lgs. 196/03 sugli aspetti Italiani, ma anche il considerando 43, che ne illustra la ratio, e l'autorevole linea guida sul consenso pubblicata dal Comitato Europeo per la Protezione dei Dati che recita: "Il considerando 43 indica chiaramente che è improbabile che le autorità pubbliche possano basarsi sul consenso per effettuare il trattamento, poiché quando il titolare del trattamento è un'autorità pubblica sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. In molti di questi casi è inoltre evidente che l'interessato non dispone di alternative realistiche all'accettazione (dei termini) del trattamento. Il Gruppo di lavoro ritiene che esistano altre basi legittime, in linea di principio più appropriate, per il trattamento da parte delle autorità pubbliche".

Riteniamo quindi pacifico che nessuna delle attività svolte dalla scuola nell'esercizio dei suoi compiti istituzionali di interesse pubblico possano in alcun modo essere assoggettate a consenso, contrariamente a quanto indicato dal MIUR nella nota.

Questione atti di nomina a responsabile esterno

Le criticità del contenuto della nota si manifestano soprattutto subito dopo, quando il MIUR, con una sintesi sin troppo veloce e fuorviante, ricorda alle scuole gli obblighi del GDPR, in tre punti.

Sul primo non ci dilunghiamo in quanto, seppur non perfetto, riprende i principi generali in materia, quali la liceità, la correttezza, la trasparenza e la sicurezza del trattamento.

Già il secondo punto lascia perplessi: la necessità di "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".

In altre parole, secondo il Ministero dell'Istruzione, tutti i fornitori delle piattaforme o degli strumenti utilizzati dai docenti per la didattica a distanza devono essere nominati, con atto formale, responsabili esterni del trattamento.

Ma non si è detto, nelle precedenti comunicazioni istituzionali e nella stessa Nota di cui discutiamo, che alle scuole è lasciata la più ampia libertà nella scelta degli strumenti da utilizzare?

Ricordiamo che nell'emergenza, e in assenza di indicazioni univoche, le scuole sono ricorse a una serie di soluzioni per garantire il diritto allo studio dei ragazzi, da quelle più "professionali" come Microsoft 365 o GSuite For Education, a piattaforme generalmente utilizzate per scopi personali come Whatsapp, Telegram, finanche strumenti opensource come Jitsi.

Il MIUR ci sta dicendo che dobbiamo trasmettere a Facebook (proprietario del servizio Whatsapp), Google o Skype un atto formale firmato digitalmente dal Dirigente Scolastico di nomina a responsabile del trattamento? E in quale lingua, inglese?

Ed in virtù di quale vincolo i suddetti soggetti dovrebbero assoggettare i loro servizi, sistematicamente e tipicamente rivolti ai singoli individui e quindi erogati in qualità di titolari del trattamento, alle disposizioni di un ente pubblico italiano?

E' vero anche che molte software house che forniscono già alle scuole gli applicativi di contabilità, personale o Registro elettronico si sono attrezzate, implementando i loro servizi e mettendo a disposizione alcune piattaforme per la didattica a distanza. In questo caso può essere ragionevole (in quanto gli stessi fornitori degli applicativi agiscono già in qualità di responsabili del trattamento per l'archiviazione dei dati degli alunni sui loro server) estendere il relativo atto di nomina anche a questa nuova attività di trattamento; sempre che, ovviamente, i servizi siano erogati in tal senso e sotto il controllo dell'Istituto Scolastico. Se invece sono integrati con altre piattaforme web i cui fruitori sono le singole persone fisiche, come sopra, anche le piattaforme integrate agiranno come soggetti indipendenti e la scuola potrà solo rendere debita informativa agli utilizzatori.

Questione valutazione di impatto

Infine, il punto tre: le scuole sono tenute a "sottoporre i trattamenti dei dati personali coinvolti a valutazione di impatto ai sensi dell'articolo 35 del regolamento [Reg. UE 679/2016]" (c.d. DPIA- Data Protection Impact Assessment)

L'articolo citato del Regolamento europeo dispone che il titolare, prima di avviare un trattamento che – "allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità – può presentare un rischio elevato per i diritti e le libertà delle persone fisiche", operi una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

In altre parole, l'obbligo di effettuare una DPIA è conseguente alla presenza di un rischio elevato per i diritti e le libertà delle persone (che in questo caso sono gli studenti ed i docenti), che i trattamenti specificati possano comportare.

Il GDPR elenca i casi nei quali è necessario procedere alla DPIA, ovvero:
• trattamenti che comportino una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
• trattamenti, su larga scala, di categorie particolari di dati personali (come i dati relativi alla salute, all'orientamento sessuale, all'appartenenza religiosa ecc) di dati relativi a condanne penali e a reati;
• trattamenti che operino la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
Il Garante per la Protezione dei Dati italiano, con provvedimento n. 467 del 1 ottobre 2018, ha meglio specificato tutti i trattamenti che debbono essere sottoposti a DPIA, ovvero:
• valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";
• automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato;
• che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app;
• su larga scala di dati aventi carattere estremamente personale, ovvero dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti);
• effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si pensi all'utilizzo di dispositivi che geolocalizzano il dipendente per distribuire delle consegne);
• non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo), ma solo su "LARGA SCALA" come precisato dall'Autorità Garante nei suoi chiarimenti interpretativi forniti al provvedimento citato;
• effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il Wi-Fi tracking)

ogniqualvolta ricorra anche almeno un altro dei nove criteri individuati dal WP29 nel provvedimento n. 248/2017;
• che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;
• di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);
• di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse;
• sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento,
• sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
Dall'elenco sopra indicato si evince come alcun trattamento rientri nell'obbligo per le scuole di effettuare una valutazione d'impatto sulla protezione dati in quanto:
• non può applicarsi il concetto di larga scala a una scuola che opera su un territorio limitato;
• le piattaforme utilizzate non si basano su nuove tecnologie innovative (quali l'IoT, i sistemi di intelligenza artificiale, l'utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale, monitoraggi effettuati da dispositivi wearable, tracciamenti di prossimità come ad es. il Wi-Fi tracking, etc.);
• attraverso la FaD e la DaD non si realizza alcun trattamento di categorie particolari di dati.

Da ultimo, ma non da meno, è importante ricordare che il rischio dipende dalle attività effettuate: se quindi gli istituti scolastici, effettuando la valutazione del rischio, che comunque è obbligatoria per legge, stabiliscono misure di comportamento e di protezione adeguate a proteggere gli studenti (ed in particolare i minori) dai rischi di utilizzo dei dati personali che transitano nei sistemi di DAD e FAD, il rischio elevato non si configura in alcun modo.

Dunque, vi sono almeno tre considerazioni da fare in ordine alla nota MIUR, circa la necessità di sottoporre a DPIA il trattamento connesso alla didattica a distanza.

La prima: in quale, tra l'esaustivo elenco di trattamenti "rischiosi" fornito dal Garante, rientrerebbe la didattica a distanza?

La seconda: perché il Ministero non aveva mai, prima d'ora, indicato tale necessità, pur essendo, la didattica a distanza, in uso in numerose scuole da diverso tempo (pensiamo a quelle che l'hanno attivata per i ragazzi costretti a casa o a ricoveri ospedalieri di lungo termine)?

La terza: come potrebbe un Dirigente scolastico farsi carico di effettuare una valutazione d'impatto sulla protezione dei dati (che, si ricorda, è preliminare all'inizio del trattamento) visto che la didattica a distanza è già iniziata in molte scuola già da una settimana?

Conclusioni

Ad opinione di chi scrive, sembra che il Ministero non abbia compreso a fondo la ratio della normativa europea in materia di protezione dei dati e, probabilmente, nemmeno le modalità di messa a disposizione e utilizzo degli strumenti DAD/FAD in relazione ad essa.

Vero è che una nota non è vincolante, dunque non può imporre obblighi in capo alle scuole, e non può di certo regolamentare aspetti ultronei che sono in realtà già disciplinati da fonti legislative di rango superiore (gerarchia delle fonti).

Tuttavia, soprattutto in questo momento di grande incertezza generale, non può ulteriormente aggravare di dubbi e perplessità i DS e DSGA.

Il nostro invito è quello di valutare con attenzione l'applicazione della suddetta nota per quanto concerne gli aspetti privacy citati e auspichiamo un intervento chiarificatore dell'Autorità Garante, al fine di indicare al MIUR la giusta via nell'applicazione delle norme di settore, tale da non disorientare ulteriormente DS e DSGA, già messi a dura prova in questo periodo emergenziale.

***Avv. Graziano Garrisi**
LiquidLaw s.r.l. – Azienda spinoff di UniSalento
Privacy Consultant e DPO
Responsabile Gruppo di ricerca «Privacy e Data Protection»
dell'Osservatorio Mediterraneo sulla Cultura Digitale – MODiCT di
UniSalento
Cultore della materia in Informatica giuridica – UniSalento

avv. Rossella Lozito
LiquidLaw s.r.l. – Azienda spinoff di UniSalento
DPO e consulente in tema di Amministrazione digitale

dott.ssa Chiara Delaini
Consulente di direzione ed esperto certificato in materia di protezione
dei dati personali
DPO e formatrice in tema privacy