LEX FOR SCHOOL

VALERIO DE FEO

# DIDATTICA A DISTANZA, VALUTAZIONE D'IMPATTO E UTILIZZO DEL REGISTRO ELETTRONICO

## … IN ATTESA CHE INTERVENGA IL GARANTE DELLA PRIVACY

Aggiornato al 31 marzo 2020

GRUPPO SPAGGIARI PARMA

**1ª edizione marzo 2020**


Via F. Bernini, 22A - 43126 Parma
Tel. 05212992
E-mail: info@spaggiari.eu
www.spaggiari.eu



La realizzazione di un libro comporta per l'Autore e il Gruppo Spaggiari Parma S.p.A. un attento lavoro di revisione e controllo sulle informazioni contenute nel testo, sull'iconografia e sul rapporto che intercorre tra testo e immagine. Nonostante il continuo miglioramento delle procedure di controllo è quasi impossibile pubblicare un libro del tutto privo di errori o refusi. Per questa ragione ringraziamo fin d'ora i lettori che li vorranno indicare al Gruppo, al seguente indirizzo:

Via Bernini, 22A - 43126 Parma
E-mail: info@spaggiari.eu

## INDICE

## 1. VALUTAZIONE DEI RISCHI E VALUTAZIONE D'IMPATTO

In relazione alla Nota Miur 388/2020 e all'indicazione ivi contenuta di eseguire una valutazione di impatto in relazione alle attività di didattica distanza, ci sentiamo di mettere in comune alcune riflessioni, in attesa di una auspicata presa di posizione del Garante della Protezione dei dati personali.

In relazione a tutti i trattamenti di dati personali effettuati dalle scuole, va evidenziato che le Istituzioni Scolastiche, da sole o con il loro DPO, devono obbligatoriamente eseguire una **valutazione dei rischi,** per analizzare quali sono i rischi per gli interessati (docenti, alunni, famiglie, ecc.) legati ai trattamenti effettuati.

La valutazione dei rischi serve per adottare, poi, le misure di sicurezza (antivirus, procedure di gestione password, controllo accessi, ecc.) che sono necessarie per proteggersi il più possibile dai rischi evidenziati.

Questo concetto di valutazione del rischio dovrebbe essere applicato anche in relazione alle piattaforme digitali usate dalle scuole, compreso il registro elettronico, utilizzato in vario modo dalle Istituzioni Scolastiche Italiane; si va da attività svolte al minimo indispensabile (voti e presenze) ad attività molto complesse e articolate.

Un elemento di complessità è però rappresentato dal fatto che, in relazione ad alcuni trattamenti, il GDPR ci dice che la semplice valutazione dei rischi non basta, serve qualcosa in più.

In particolare, l'art 35 del Regolamento UE 2016/679, evidenzia che "se un trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare **un rischio elevato per i diritti e le libertà delle persone fisiche**, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali."

In sostanza, di norma, si fa la valutazione dei rischi, ma al ricorrere delle condizioni indicate dall'art. 35 la valutazione dei rischi non basta più e serve un processo più approfondito e complesso che si chiama, appunto, valutazione d'impatto e serve a studiare l'impatto dei trattamenti sui diritti fondamentali delle persone. Come si fa la valutazione d'impatto? Il Gruppo Articolo 29 ha fornito le linee guida, sulla base delle quali sono stati prodotti anche dei software, si tratta di competenze che un DPO deve avere. È una attività di analisi e bilanciamento degli interessi non banale.

## 2. NOVE CRITERI PER LA VALUTAZIONE D'IMPATTO

Il Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, ha adottato anche alcune linee guida in materia, fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018.

**Queste linee guida hanno individuato i seguenti nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un "rischio elevato" e che dunque necessitano di valutazione d'impatto**:

1) valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "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";

2) processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone;

3) monitoraggio sistematico degli interessati;

4) dati sensibili o dati aventi carattere altamente personale;

5) trattamento di dati su larga scala;

6) creazione di corrispondenze o combinazione di insiemi di dati;

7) dati relativi a interessati vulnerabili;

8) uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;

9) quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto".

Il Gruppo Articolo 29 ha evidenziato che **al ricorrere di due o più dei predetti criteri** vi è l'indice di un trattamento che presenta un rischio elevato per i diritti e le libertà degli interessati e per il quale è quindi richiesta una valutazione d'impatto.

## 3. ATTIVITÀ SOGGETTE A VALUTAZIONE D'IMPATTO

**Il Garante privacy italiano** "allo scopo di specificarne ulteriormente il contenuto e a complemento dello stesso" documento del Gruppo Articolo 29, a sua volta con il Provvedimento n. 467 dell'11 ottobre 2018 **ha redatto un elenco di attività che, soggette al meccanismo di coerenza, andrebbero sottoposte a valutazione d'impatto. Vediamole.**

1.Trattamenti 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".

2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un con-

tratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).

3. Trattamenti 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, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

4. Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa riferimento, fra gli altri, ai 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).

5. Trattamenti 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.

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

7. Trattamenti 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 criteri individuati nel WP 248, rev. 01.

8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9. Trattamenti 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).

10. Trattamenti 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.

11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Questo complesso di indicazioni ci fa subito dire che non appare possibile affermare, come fa invece la Nota 388/2020, senza distinzione alcuna, che tutte le Istituzioni Scolastiche devono fare la valutazione d'impatto in merito alle attività di didattica a distanza. Peraltro, questa posizione non è stata, fino ad oggi, espressa nemmeno dal Garante della privacy, che non sarebbe male se si pronunciasse sul tema. **Al contrario, bisogna di volta in volta capire, sulla base delle attività svolte dalla scuola, se si rientra nei casi presenti negli elenchi appena riportati.**

Peraltro, sul sito del Garante della privacy è apparso il seguente chiarimento interpretativo in relazione ad alcuni punti dell'elenco che abbiamo appena presentato.

*Chiarimento interpretativo: Si evidenzia come le espressioni trattamenti "sistematici" e "non occasionali" indicate nell'Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione di impatto di cui ai punti 6, 11 e 12 sono riconducibili al criterio della "larga scala" così come espressamente illustrato al quinto criterio del WP 248 (pag. 11):*

*"5. trattamento di dati su larga scala: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:*

*a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;*

*b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;*

*c. la durata, ovvero la persistenza, dell'attività di trattamento;*

*d. la portata geografica dell'attività di trattamento;"*

Anche in relazione ai trattamenti di dati di minori, quindi, deve esserci comunque una situazione di vulnerabilità e il trattamento deve essere su larga scala.

Quindi, si ribadisce che sul punto non sono immaginabili automatismi, ma una valutazione seria da fare di volta in volta con il DPO, con cui scegliere se fare una più semplice valutazione dei rischi o una più complessa valutazione d'impatto, in relazione alla concreta presenza di un rischio elevato per i diritti e le libertà degli interessati coinvolti.

Si coglie l'occasione di ribadire, in relazione alla nota MIUR 388/2020, che non è immaginabile nessun automatismo o nessuna semplificazione nemmeno in

ordine alla nomina a responsabile del trattamento (richiamata come necessaria dalla Nota) che, al contrario, in molti casi non andrà fatta, data l'occasionalità dell'uso di certe piattaforme.

Ricordiamo che le finalità del trattamento della didattica a distanza sono le stesse della didattica in classe. È chiaro che in momenti di emergenza, si fa molta fatica a coordinare le iniziative della didattica a distanza dei docenti, che spesso scelgono autonomamente le piattaforme da utilizzare, senza il supporto del Dirigente o del DPO.

In questi casi, il criterio che guida nell'uso di piattaforme esterne è quello di usare meno dati personali possibili e di non lasciare dati personali conservati su queste piattaforme (discorso a parte va fatto per il registro elettronico, ovviamente, dato che ha un'altra funzione); quindi meno dati possibili e per il minor tempo necessario.

In sostanza, bisognerebbe andare a vedere di volta in volta di che servizio si tratta, chi tratta i dati, come, per quali finalità, le modalità e i tempi di conservazione dei dati, con quali misure di sicurezza, analizzando informativa e privacy policy. Operazioni molto difficili in momenti di emergenza, ma su cui comunque bisogna prestare attenzione (per questo, in questa fase, più si utilizzano piattaforme conosciute e meglio è). L'elemento della conservazione dei dati è molto importante. Ad esempio, se piattaforme di videoconferenza non fanno conservazione di dati o la fanno al minimo indispensabile, in linea teorica non dovrebbero rappresentare rischi particolari.

## 4. REGISTRO ELETTRONICO

Un'ultima considerazione sul tema registro elettronico.

Come tutti sappiamo, il registro elettronico è la piattaforma più in uso nelle scuole ed è quella più "controllata" dai DPO e più normata nell'utilizzo, nel senso che le scuole nominano le ditte esterne responsabili del trattamento e danno indicazioni sull'uso dei registri ai propri dipendenti.

Vista la presenza del Codice dell'Amministrazione Digitale (CAD) D.Lgs. 82 del 7 marzo 2005 che impone alle Pubbliche Amministrazioni di formare gli originali dei propri documenti con mezzi informatici, considerata la presenza di tante altre norme che vanno nel senso della dematerializzazione, valutato anche il Piano Triennale dell'AgID, non si capisce perché girino ancora "leggende metropolitane" sul famoso mancato piano di dematerializzazione che condizionerebbe la legittimità dell'uso del registro.

La norma istitutiva del registro elettronico è stata scritta dai tecnici del MIUR su iniziativa del Ministro Profumo e inviata al Governo per essere inserita poi nel D.L. n. 95/2012 contenente "Disposizioni urgenti per la razionalizzazione della spesa pubblica", convertito dalla Legge n. 135/2012.

Questa è storia.

Quando il MIUR o il Governo sono tornati sul tema, mai si è parlato di dipendenza del registro elettronico rispetto a un piano di dematerializzazione.

Si pensi alla Nota MIUR del 3 ottobre 2012, prot. AOOODPPR Reg. Uff. 1682/U con cui si invitano le scuole ad adottare il registro elettronico o al documento "Strategia per la crescita digitale 2014-2020" della Presidenza del Consiglio dei ministri o al "Piano Nazionale Scuola Digitale" che a pag. 65 parla di obbligo del registro previsto dal D.L. n. 95 del 2012, senza condizionamenti.

Proviamo, ora, a leggere il comma 27 e il comma 31 dell'articolo 7 del D.L. n. 95/2012. Il comma 27 recita:

"Il Ministero dell'istruzione, dell'università e della ricerca predispone entro 60 giorni dalla data di entrata in vigore della legge di conversione del presente decreto un Piano per la dematerializzazione delle procedure amministrative in materia di istruzione, università e ricerca e dei rapporti con le comunità dei docenti, del personale, studenti e famiglie."

Il comma 31 recita:

"A decorrere dall'anno scolastico 2012-2013 le Istituzioni Scolastiche e i docenti adottano registri on line e inviano le comunicazioni agli alunni e alle famiglie in formato elettronico."

Ora, il dato letterale non ci dice che i due commi dipendono l'uno dall'altro.

Peraltro, se l'adozione del registro dipendesse dal piano di dematerializzazione, in base al testo del comma 27, che parla di "procedure amministrative", tutti gli applicativi digitali usati dalle scuole per le pratiche amministrative non potrebbero essere usati perché manca il piano di dematerializzazione. Il ragionamento ci sembra che non regga.

Al riguardo, si ritiene di non essere d'accordo con quanto recentemente dichiarato da Antonello Soro, Presidente del Garante per la protezione dei dati personali, che il 20 marzo 2020, intervenendo alla trasmissione Zapping a RadioRai 1, ha di nuovo accreditato la tesi, in relazione al registro elettronico, del necessario intervento governativo che è mancato in questi anni.

Con questo non si vuole dire che l'uso del registro elettronico non ponga problemi o questioni in merito alla protezione dei dati personali. Il punto è che il Garante per la protezione dei dati personali potrebbe intervenire autonomamente sul tema, con un Provvedimento che contenesse tutte le indicazioni che si reputino necessarie, senza aspettare alcun piano di dematerializzazione o un intervento del Governo.

## 5. AGGIORNAMENTO DEL 31/03/2020

Come evidenziato dal titolo, questa monografia è stata scritta in attesa dell'intervento del Garante della protezione dei dati personali.

Il Garante, il 30 marzo, ha pubblicato un primo intervento di commento sul tema della didattica a distanza. Il documento è consultabile sia all'interno della banca dati di LexForSchool: bit.ly/BancadatiLFS

sia, direttamente, sul sito del Garante: bit.ly/GaranteprivacyFAD

Pur rimandando alla lettura integrale del provvedimento, riportiamo qui alcune indicazioni del Garante, che sono in linea con quanto scritto nella monografia.

Le scuole e le università che utilizzano sistemi di didattica a distanza non devono richiedere il consenso al trattamento dei dati di docenti, alunni, studenti, genitori, poiché il trattamento è riconducibile alle funzioni istituzionalmente assegnate a scuole e atenei.

Non è necessaria la valutazione di impatto, prevista dal Regolamento europeo per i casi di rischi elevati, se il trattamento dei dati effettuato dalle istituzioni scolastiche e universitarie, per quanto relativo a minorenni e a lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti.

Un conto è il registro elettronico, un conto sono piattaforme che eroghino servizi più complessi anche non rivolti esclusivamente alla didattica, in relazione alle quali si dovranno attivare i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare (evitando, ad esempio, geolocalizzazione e social login). Le istituzioni scolastiche e universitarie dovranno assicurarsi che i dati trattati per loro conto siano utilizzati solo per la didattica a distanza.

Il trattamento di dati svolto dalle piattaforme per conto della scuola o dell'università dovrà limitarsi a quanto strettamente necessario alla fornitura dei servizi richiesti ai fini della didattica on line e non per ulteriori finalità proprie del fornitore. I gestori delle piattaforme non potranno condizionare la fruizione di questi servizi alla sottoscrizione di un contratto o alla prestazione del consenso (da parte dello studente o dei genitori) al trattamento dei dati per la fornitura di ulteriori servizi on line, non collegati all'attività didattica.

Per garantire la trasparenza e la correttezza del trattamento, le istituzioni scolastiche e universitarie devono informare gli interessati (alunni, studenti, genitori e docenti), con un linguaggio comprensibile anche ai minori, riguardo, in particolare, alle caratteristiche essenziali del trattamento che viene effettuato.

Relativamente ai docenti, scuole e università, nel rispetto della disciplina sui controlli a distanza, dovranno trattare solo i dati strettamente necessari e comunque senza effettuare indagini sulla sfera privata.

# *Adesione all'offerta*

LEX FOR SCHOOL

▲ Istituzione Scolastica

▲ Avente sede / residente nel Comune di

▲ Codice Fiscale / Partita IVA ▲ CIG

▲ Telefono ▲ e-mail

▲ Referente / ruolo ▲ e-mail

☐ **CANTEMGIU/01** **Abbonamento 12 mesi**

***Canale di supporto giuridico dedicato ai professionisti della Scuola*** ***€ 399,00 i.i.***

▲ Data ▲ Timbro e Firma

## INFORMATIVA PRIVACY AI SENSI DELL'ART.13 REGOLAMENTO (UE) 2016/679 "GDPR"

SPAGGIARI in qualità di Titolare del trattamento dei dati personali, la informa che i dati conferiti mediante la redazione del "Modulo d'Ordine" saranno trattati con l'unico fine di gestire le operazioni di vendita e gli adempimenti ad essa connessi, nonché quelli di natura amministrativa, contabile e fiscale richiesti dalla legge applicabile. Qualora richiedesse assistenza post-vendita per acquisti o effettuasse qualsiasi altra richiesta a Spaggiari, i dati personali da Lei comunicati saranno trattati esclusivamente per dare seguito alle Sue richieste. In qualità di interessato Lei potrà, alle condizioni previste dal GDPR, esercitare i diritti sanciti dagli articoli da 15 a 21 del GDPR contattando il Titolare tramite la Funzione Compliance all'indirizzo e-mail: privacy@spaggiari.eu.