La gestione del dato personale negli ambienti e negli strumenti di analisi dell'apprendimento

Claudia BELLINI, Annamaria DE SANTIS, Katia SANNICANDRO, Tommaso MINERVA

Università di Modena e Reggio Emilia, Reggio Emilia (RE)

Abstract

In seguito dell'entrata in vigore del regolamento europeo e del D. Lgs. 101 del 2018 (che ha armonizzato il D. Lgs. 196 del 2003) e dopo i provvedimenti e i pareri del Garante italiano della privacy, il quadro normativo sulla gestione del dato personale si è necessariamente evoluto rispetto al passato.

Tali mutamenti impongono una nuova attenzione all'utilizzo dei dati personali nei contesti di apprendimento, sia per l'attività di analisi sui dati personali, aggregati grazie ai Learning Management System, sia per la semplice gestione quotidiana delle informazioni degli utenti nel rispetto del diritto alla trasparenza.

L'evoluzione tecnologica permette infatti di trattare e conservare una grande quantità di dati personali e di sviluppare ricerche nel campo dell'educazione proprio intorno ad essi: i nuovi software utilizzati negli istituti di formazione, le piattaforme online e gli strumenti in cloud ruotano intorno al dato personale.

Obiettivo del presente lavoro è approfondire il legame tra privacy ed educazione a partire dalla normativa di settore fino a proporre soluzioni tecniche per una corretta gestione del dato personale durante il lavoro svolto dagli attori accademici, particolarmente nel campo dell'e-Learning.

Keywords: e-Learning, Gestione del Dato, Strumenti di Apprendimento, Responsabilizzazione, GDPR

Introduzione

Con l'evoluzione tecnologica il settore dell'educazione ha subito un consistente cambiamento negli strumenti e nelle pratiche affrontando il passaggio cruciale dal cartaceo all'elettronico in ogni ambito. Gli strumenti di apprendimento, utilizzati in uno spazio online, da fisici diventano digitali (lezioni videoregistrate invece che in presenza, documenti, prove di valutazione in rete invece che su carta). Il dato personale degli attori accademici diventa fluido e accessibile a chiunque attraverso la conoscenza di una password che permette di accedere al sistema. Questo consente la velocizzazione dei processi e, allo stesso tempo, espone i soggetti interessati a nuovi rischi di violazione del diritto alla riservatezza.

Da parte sua, anche il settore della privacy ha subito un'evoluzione rispetto al passato, quando i principali elementi di attenzione e, quindi, di protezione erano il consenso informato e l'anonimizzazione. Con la proliferazione delle informazioni personali condivise in ogni momento attraverso i supporti digitali si è resa necessaria l'introduzione di nuove norme e nuovi strumenti; infatti, consenso e anonimato risultano oggi largamente insufficienti (Barocas & Nissebaum, 2014).

È sulla sfida posta dal trattamento dei big data che il settore educativo e del diritto alla riservatezza convergono come mai prima d'ora. Come affermato anche da Hoel and Chan (2015) "More and more of the forces that create global change are driven by data, and based on new practices of sharing data, e.g., mobile devices, social media, big data, sensors, and location-based services […] These services are also exploited in education" (p.2).

Oggi, la produzione continua di contenuti didattici erogati online e l'invio degli stessi verso un numero potenzialmente infinito di studenti permette la veloce e massiva aggregazione di dati, perlopiù facilmente scaricabili e condivisibili con chiunque ne sia interessato. Questi, inoltre, sono diventati una risorsa digitale per l'apprendimento tanto quanto i contenuti stessi e sono oggetto di dibattito sulla privacy, particolarmente sulle questioni legate all'etica dell'utilizzo.

Altro aspetto riguarda la tutela di chi produce, cioè i proprietari dei contenuti erogati online (più spesso i docenti). La governance accademica deve fornire loro tutela della privacy e del diritto d'autore nel lancio in rete di materiali originali che chiunque, una volta online, può utilizzare e ricondividere.

Non da ultimo c'è poi il lavoro quotidiano di management da parte di progettisti e tecnici di piattaforma caratterizzato dalla molteplicità di problematiche quali, ad esempio, la conservazione dei dati, la diffusione senza controllo dei contenuti, la protezione dell'immagine, la valutazione degli apprendimenti, la formazione del personale, etc.

Da questa sintesi di scenario appare evidente che è nell'e-Learning che si percepisce con forza la necessità di conoscere e comprendere le regole riguardanti la gestione del dato e la protezione del diritto alla riservatezza.

A livello normativo l'argomento è stato enfatizzato dall'entrata in vigore del General Data Protection Regulation (GDPR), il Regolamento europeo generale sulla protezione dei dati personali, emanato con lo scopo di uniformare tutte le legislazioni nazionali e adeguarle alle nuove necessità dettate dall'evolversi del contesto tecnologico. Questa è la prima importante evoluzione rispetto al passato, caratterizzato da normative frammentate e non uniformi tra i Paesi membri (per l'Italia, la D. Lgs. 196/2003).

Alla luce di questi mutamenti, nel presente lavoro vengono allineati i principi di natura giuridica e i requisiti organizzativi e tecnici inerenti alla gestione del dato personale, con particolare riguardo agli strumenti di apprendimento online. Fornendo delle indicazioni pratiche per gli attori coinvolti (docenti e personale tecnico di piattaforma in particolare) si mira ad aumentare la consapevolezza di tali requisiti sia per chi si affaccia per la prima volta all'argomento, sia per chi se ne occupa da anni, magari lavorando più per prassi che per norma.

La letteratura suggerisce che la *condivisione* del dato, anche in ambito educativo, dev'essere affrontata attraverso tre livelli d'indagine: legale, organizzativo e tecnico-semantico (Cooper & Hoel, 2015; Hoel & Chan, 2015). Pertanto, in linea con gli autori, proponiamo il medesimo ordine di approfondimento tematico sulla gestione del dato ponendo specifica attenzione al nesso con gli strumenti di apprendimento online, essenziali per le attuali pratiche educative.

1. Aspetti legali: l'evoluzione della normativa

Al fine di comprendere nel contesto italiano le evoluzioni che legano il settore del diritto alla riservatezza nella gestione del dato e l'ambito educativo occorre approfondire il passaggio dal D. Lgs. 196/2003 al GDPR nei suoi cambiamenti cardine. Uno dei più rilevanti è l'introduzione del principio di "responsabilizzazione" o *accountability* per il quale, dall'art. 5 par. 2 del GDPR, il titolare del trattamento è competente per il rispetto dei principi sanciti dal regolamento stesso e deve essere sempre in grado di comprovarlo. Ciò significa che è necessario trattare in modo lecito i dati personali degli interessati e poter documentare l'attività in ogni momento per non incorrere nelle sanzioni previste dal Regolamento. La responsabilizzazione del titolare è la grande rivoluzione rispetto al Codice della Privacy che prevedeva, invece, un elenco di 29 misure minime di sicurezza, contenute nell'Allegato B, uguali per tutti i soggetti titolari a prescindere dalla dimensione e complessità del caso. Nella quotidianità ciò comporta che mentre prima era sufficiente rispettare le disposizioni normative per dirsi adeguatamente protetti, oggi non ci sono punti o livelli da raggiungere. Occorre, dunque, un percorso di valutazione continua che consenta al titolare di determinare in autonomia le misure di sicurezza ritenute idonee per proteggere i propri dati personali. Questo percorso di responsabilizzazione investe chiaramente anche tutti gli altri attori coinvolti nel trattamento dei dati.

Nel caso dell'università, dunque, a prescindere dalla titolarità che resta dell'Ateneo, ogni docente, tecnico e persona incaricata al trattamento deve trattare i dati in base alle indicazioni del titolare e nel rispetto delle disposizioni normative. Considerando il campo specifico dell'e-Learning, sappiamo che ogniqualvolta un utente si interfaccia con la piattaforma, sia esso docente o discente, cede in vario modo i suoi dati personali attraverso molteplici azioni: iscrivendosi, caricando un corso, inviando richieste, gestendo i materiali, seguendo un corso e, quindi, fornendo i suoi dati di accesso e fruizione. I principi da rispettare per una corretta gestione di questi, contenuti nell'articolo 5 del GDPR, sono:

1) *Liceità, correttezza e trasparenza*: i dati devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
2) *Limitazione delle finalità*: i dati devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
3) *Minimizzazione dei dati*: i dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
4) *Esattezza e aggiornamento*: devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
5) *Limitazione della conservazione*: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.
6) *Integrità e riservatezza*: i dati devono 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.

Nella Tabella 1 viene mostrato come tali principi influenzino il lavoro degli attori interessati nel processo di gestione del dato e quali criticità possono emergere nel percorso verso la compliance privacy.

L'accountability si accompagna, inoltre, ai principi di "*privacy by design*" e "*privacy by default*" (art. 25, GDPR), peraltro già citati dagli autori della letteratura di settore come il modello che prevede l'introduzione delle corrette impostazioni a tutela del dato personale già durante la progettazione degli strumenti di analisi dell'apprendimento, in un approccio centrato sull'utente (studente) (Pardo & Siemens, 2014; Hoel & Chan 2015; Drachsler & Geller, 2016). Rispetto al D. Lgs. 196/2003 la privacy oggi deve essere pensata, e quindi rispettata, sin dalla fase di progettazione di qualunque strumento che utilizzi dati personali, che sia amministrativo o di ricerca scientifica.

1.1 Le figure di controllo

In base ai suddetti principi appare dunque essenziale, anche per l'università, definire chiaramente la propria privacy governance. Le figure previste dal GDPR sono:

7) il *Titolare*, colui che decide le modalità, le finalità e le misure di sicurezza del trattamento;
8) i *Responsabili del trattamento*, cioè tutti coloro i quali entrano in contatto con i dati del titolare e sono da esso designati tramite contratto; gli incaricati autorizzati dal titolare a trattare i dati personali;
9) il *Data Protection Officer* (DPO), nuova figura che affianca e consiglia il titolare.

Quest'ultimo merita menzione a parte dato che le autorità pubbliche sono obbligate alla nomina. Il DPO è una figura specializzata che informa e offre consulenza al titolare in merito agli obblighi derivanti dal GDPR; sorveglia l'osservanza del nuovo regolamento, compresa l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale; fornisce pareri in merito alla valutazione d'impatto; coopera con l'autorità di controllo; funge da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

L'individuazione di tali figure riveste un ruolo di massima importanza, particolarmente ai fini della sicurezza nella filiera del dato: il flusso dei dati personali, quando si ha ben chiara la privacy governance, è sicuramente più protetto poiché il titolare saprà sempre chi può maneggiare il dato e cosa può farne.

Infine vi è l'interessato, cioè la persona fisica a cui i dati personali si riferiscono. Tutto l'impianto normativo descritto mira proprio a tutelare questa figura dai rischi dei trattamenti effettuati sui suoi dati. L'interessato, infatti, rimane sempre in possesso dei suoi dati anche quando consegnati a un ente/ azienda: egli è il proprietario del dato e può accedervi, riprenderli, cancellarli liberamente.

Nel contesto dell'e-Learning il titolare è l'università o l'ente che gestisce la piattaforma; i responsabili esterni possono essere le software house che gestiscono la struttura informatica o le società che erogano servizi in cloud; gli interessati sono i docenti, gli utenti, gli studenti; gli incaricati, sono i tecnici di piattaforma e gli Instructional Designer che, sulla base di un'autorizzazione da parte del titolare, trattano operativamente i dati degli interessati (studenti).

1.2 Il data breach

Altra rilevante differenza rispetto al D. Lgs. 196/2003 è l'introduzione della comunicazione del *data breach*. Con tale termine, introdotto con Provvedimento del Garante per la Protezione dei Dati Personali, si intende qualunque violazione, anche accidentale, del dato personale. Un attacco informatico, la distruzione di documenti, una perdita di strumenti informatici contenenti dati personali; tutti questi casi sono qualificabili come data breach. In passato non era predisposto alcun obbligo di notifica delle eventuali violazioni dei dati personali.

Considerando la mole di dati che l'università gestisce, tratta e conserva, oggi è facile comprendere la gravità delle conseguenze di un eventuale attacco al sistema, furto o perdita di informazioni personali dei soggetti interessati.

2. Aspetti tecnici e organizzativi: la gestione del dato

Come titolari di una considerevole mole di dati personali l'università e, in generale, gli istituti di formazione, hanno l'obbligo di predisporre, attraverso un percorso di valutazione, le loro politiche e procedure interne (Cooper & Hoel, p. 35) e, nello specifico, adeguarsi tempestivamente al GDPR, perseguendo il principio di accountability. Il Titolare, da parte sua, mette in atto misure tecniche e organizzative adeguate e volte ad attuare in modo efficace i principi di protezione dei dati al fine della tutela dei diritti degli interessati, cercando di prevenire e non di correggere.

Non è semplice delineare delle informazioni di supporto alla gestione del dato prendendo in considerazione un sistema di e-Learning, data la vastità della casistica in cui gli attori possono incorrere nella quotidianità. Innanzitutto, bisogna considerare i principi e le azioni da intraprendere per una piena compliance con essi. Come suddetto, per il principio di accountability, ogni attore sarà in qualche modo responsabile dei trattati e delle azioni da intraprendere per evitare un eventuale data breach.

Pertanto, in linea con la necessità di una costante e continua valutazione del proprio lavoro rispetto alle necessità dettate dalla privacy, viene proposto in Tabella 1 un primo prodotto d'indagine tecnica di gestione del dato.

Le criticità elencate sono solo un esempio conseguente ad attività di gestione del dato personale; la casistica, ovviamente, può essere molto più vasta. Tuttavia, la sintesi proposta nella tabella mira a correlare principi e azioni degli interessati al fine di fornire un esempio che possa fungere da guida per gli attori accademici. Ogni università dovrebbe avere già individuato il DPO per occuparsi di tali questioni. Tuttavia, come mostrano i dati raccolti dalla CRUI (http://bit.ly/gdpr-crui) ad oggi solo 23 Atenei su 70 indagati ha effettuato la nomina. Pertanto, un primo strumento di orientamento sulla tematica può essere utile, in special modo per i docenti che, inoltre, meritano un ulteriore approfondimento per via delle attività legate alla ricerca. Oggi, l'utilizzo delle informazioni sull'apprendimento degli studenti è oggetto di un settore di ricerca in forte espansione, cioè quello dei Learning Analytics. I primi risultati d'indagine suggeriscono che i sistemi predittivi basati sui dati possano realmente migliorare l'apprendimento degli studenti, se utilizzati per progettare a monte insegnamenti situati e significativi. Tali questioni pongono il docente oltre i tecnicismi trattati nel presente lavoro e aprono altri scenari di ricerca.

Principi	Come rispettarle	Soggetti interessati	Criticità
Liceità, correttezza e trasparenza	Fornire agli interessati un'informativa chiara e comprensibile in cui sono indicate tutte le finalità perseguite e, se necessario, predisporre la raccolta del consenso	- Titolare: per la predisposizione del documento - Tecnici di piattaforma: devono garantirne la fruizione da parte degli interessati - Docente: devono attenersi, alle finalità indicate nell' informativa predisposta	- Mancata raccolta del consenso - Trattamenti eccessivi da parte dei docenti, ad esempio invio di dati a soggetti non autorizzati per ragioni di ricerca
Limitazione delle finalità	Evitare di trattare i dati personali per finalità non espressamente indicate nell'informativa	- Docente: in caso di trattamenti eccedenti rispetto alle finalità indicate (invio a soggetti terzi, ricerche che comportano trasferimento di dati, etc) occorre comunicare prima dell'operazione tale nuova finalità agli interessati	- Trattamento illecito dei dati con possibilità di data breach
Minimizzazione dei dati	Perseguire la pertinenza rispetto alle finalità: occorre richiedere e trattare solo i dati strettamente necessari all'utilizzo	- Titolare: decide quali dati trattare e predispone i moduli di raccolta per evitare dati eccedenti - Docente: non devono raccogliere dati non espressamente indicati dal titolare. Nel caso, devono fornire un'informativa e ottenere, eventualmente, il consenso da parte diretta dell'interessato	- Trattamento illecito di dati personali
Esattezza e aggiornamento	Aggiornare i dati e verificarne la correttezza in maniera continua	- Titolare: deve predisporre la procedura per la gestione di eventuali richieste - Docente: deve inoltrare le eventuali richieste ricevute al PTA che dovrà occuparsi della richiesta	- Trattamento di dati non esatti potrebbe comportare possibili illeciti, con conseguenze anche gravi per gli interessati: es. invio di comunicazioni importanti presso indirizzi vecchi
Limitazione della conservazione	Conservare i dati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati	- Titolare: predispone i tempi di conservazione e le procedure di cancellazione sicura dei dati personali	- Più dati vengono conservati e trattati maggiore sarà l'esposizione ad eventuali rischi di perdita del dato stesso
Integrità e riservatezza	Garantire un'adeguata protezione dei dati, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentale	- Titolare: attraverso un percorso di valutazione e adeguamento deve applicare le misure di sicurezza ritenute adeguate - Docente: deve rispettare le misure e le procedure adottate dal titolare	- Non rispettare o non applicare misure adeguate aumenta considerevolmente il rischio di violazione dei dati personali

Tabella 1 – Indicazioni tecniche sulla gestione del dato.

Conclusioni

Lo scopo dello studio condotto è quello di approfondire la tematica della gestione del dato personale come strumento per un uso corretto di questo durante le analisi sul comportamento degli studenti attraverso la piattaforma online, al fine di raggiungere un sistema predittivo per la progettazione dei corsi e il miglioramento del processo di apprendimento in tale ambiente. L'approccio è esplorativo e non ha pretese di esaustività, data la dinamicità e complessità dell'argomento ancora in fase emergente.

Tuttavia, è importante specificare che la gestione del dato personale si configura ormai come fondamentale attività di supporto, utile a produrre le suddette analisi raggiungendo la compliance privacy, al fine di non incorrere in atti illeciti, nel rispetto soprattutto degli studenti che "prestano" i propri dati a docenti ricercatori.

Nel caso di studi sui dati dell'apprendimento, magari invasivi sul comportamento degli utenti, essi dovrebbero innanzitutto essere posti nella condizione di porre domande sui dati, quali ad esempio: quali dati vengono utilizzati? Come ha fatto il sistema a raccogliere i dati sulle mie attività? Chi ha dato il permesso di utilizzare i miei dati? Per quanto tempo i dati sono disponibili per l'analisi, ecc.

Gli scenari futuri di ricerca, pertanto, sono focalizzati all'approfondimento delle questioni etiche rispetto all'argomento e alla creazione di un set di domande utili ai ricercatori per comprendere il limite delle proprie attività e condurre analisi qualificate, al fine di sollecitare il feedback dei principali interessati prima di iniziare un nuovo ciclo di progettazione.

Tali domande, in passato, non avrebbero avuto nemmeno ragione di esistere, ma oggi divengono la base di principi come la responsabilità e la trasparenza, fondamentali per assicurare la qualità di un sistema di istruzione.

Riferimenti bibliografici

Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications of the ACM*, 57(11), 31-33.

Cooper, A., & Hoel, T. (2015). *Data sharing requirements and roadmap*. Public Deliverable D, 7. Retrived from http://www.laceproject.eu/deliverables/d7-2-data-sharing-roadmap.pdf

General Data Protection Regulation, (2016). Retrived from https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32016R0679

Drachsler, H. & Greller, W. (2016). Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics. In *Proceedings of the sixth International Conference on Learning Analytics & knowledge* (pp. 89-98). ACM.

Hoel, T., & Chen, W. (2015). Privacy in learning analytics-implications for system architecture. In *Proceedings of the 11th International Conference on Knowledge Management*. Osaka: ICKM.

Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology*, 45(3), 438-450.