ATTUALITÀ

Smart teaching e smart learning in sicurezza

di **Redazione** · 17 aprile 2020, 00:01

*Considerazioni a cura del prof. Fulvio Oscar Benussi, di Aidr – italian digital revolution

Il prolungarsi della necessità del distanziamento sociale e il conseguente rinvio della riapertura delle scuole, implica la necessità di doversi occupare di CyberSecurity e di tutela della privacy delle piattaforme di didattica a distanza (1). Dopo un'analisi delle criticità delle piattaforme auspichiamo un intervento chiarificatore del Ministro.

Lo sforzo di alunni e studenti, delle loro famiglie, di docenti e dirigenti scolastici e più in generale dell'Amministrazione scolastica, di mantenere la continuità del servizio educativo mediante la didattica a distanza è encomiabile, ma i recenti fatti di cronaca suggeriscono di considerare con grande attenzione tutta la questione.

Il 9 aprile si è verificato un attacco hacker alla piattaforma didattica Axios (La Repubblica https://www.repubblica.it/cronaca/2020/04/09/news/axios_hacker-253550285/?ref=RHPPLF-BH-I253495487-C8-P4-S2.5-T1) mentre nei giorni precedenti si erano verificati attacchi di hacker ad altre piattaforme didattiche. Con gli attacchi veniva introdotto materiale violento e pornografico durante le lezioni e alcuni istituti hanno dovuto interrompere per alcuni giorni le lezioni a distanza.

Chiediamoci allora cosa avrebbe potuto fare la scuola per arginare questi problemi

La piattaforma didattica Axios ha subito un attacco hacker di tipo DDoS che provoca un enorme numero di accessi fraudolenti. Qualcosa di analogo a un tale tipo di attacco (2) lo hanno subito quelle scuole che, senza rivolgersi a piattaforme free, offerte dal mercato, hanno cercato di veicolare la loro didattica a distanza optando invece per soluzioni offerte dai provider di altri servizi digitali scolastici, ad esempio dai registri elettronici, e che hanno visto il proprio sistema "sedersi" e non riuscire a gestire l'enorme mole di traffico digitale generato.

Questo tipo di difficoltà è stata sperimentata anche oltralpe dai nostri vicini francesi che, per dare continuità alle attività scolastiche, hanno utilizzato, su tutto il territorio nazionale e per ogni tipo

di scuola, la piattaforma CNED chiamata “La mia classe a casa”. La scelta del Ministero francese di utilizzare questo sistema, tuttavia, ha incontrato alcune difficoltà. A causa delle troppo numerose connessioni contemporanee, l’accesso al sito è stato saturato ed è andato in blocco più volte.

In Italia, a parte le citate esperienze tentate in alcune scuole, si è scelto di non affidarsi a una piattaforma istituzionale nazionale, peraltro non disponibile, e che sarebbe stata da creare ad hoc.

Alla luce dell’esito della scelta effettuata dai francesi possiamo dire di essere stati più lungimiranti.

Ma ogni scelta che rinuncia a percorrere una strada porta come conseguenza che bisogna optare per l’altra alternativa, e il MIUR ha scelto di suggerire ai docenti l’utilizzo di piattaforme free offerte dal mercato.

Smart teaching e smart learning con piattaforme free

Nello svolgere attività didattiche a distanza con riferimento alla tutela della privacy di alunni e studenti bisogna considerare:

Le caratteristiche della postazione di lavoro dell’insegnante che la eroga (rif. Regolamento GDPR (3));
La formazione ad hoc e l’incarico per i singoli insegnanti;
le indicazioni presenti nel Provvedimento “Didattica a distanza: prime indicazioni (4)” del Garante per la protezione dei dati personali del 26 marzo 2020.
La postazione di lavoro dell’insegnante dovrà essere idonea a garantire che siano state previste le “misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento” (Rif. art. 28 comma 4 del Regolamento GDPR). Per non correre rischi di data breach (5), ciò dovrebbe comportare a nostro parere, che il computer utilizzato per la didattica a distanza debba essere protetto da antivirus e da Firewall. Inoltre il PC non dovrebbe essere utilizzato dall’insegnante anche per proprie attività personali come posta elettronica, account nei social network, ecc. che potrebbero favorire l’intrusione di malware, spyware, ecc. Inoltre, anche se sarebbe la soluzione ideale, non è possibile ipotizzare che: “La postazione di lavoro sia messa a disposizione, installata e collaudata a cura e a spese delle Istituzioni scolastiche ed educative, sulle quali andrebbero a gravare i costi di manutenzione e di gestione dei sistemi di supporto per i lavoratori”. Eppure queste sono le condizioni previste contrattualmente per il telelavoro del personale scolastico (ART.139 – disciplina del telelavoro CCNL Scuola 2006-2009) e anche se il telelavoro non era normato per gli insegnanti ai tempi della firma del CCNL la nuova situazione, a nostro avviso, permette l’analogia.

Tutte le condizioni sopra elencate sono evidentemente impossibili nelle attuali condizioni emergenziali.

Riteniamo però che sarebbe utile liberare il personale scolastico dalle responsabilità conseguenti ad eventuali violazione dei dati personali degli studenti dovuti al fatto che i docenti operino con Computer personali che, in molti casi, non hanno le caratteristiche sopra indicate come necessarie.

Auspichiamo in tal senso un intervento del Ministero che possa fare chiarezza a riguardo.

Per svolgere la didattica a distanza i docenti dovrebbero avere seguito un apposito corso di formazione (6) sulla normativa inerente la privacy (7) ed avere ricevuto dai rispettivi dirigenti scolastici una specifica lettera di incarico contenete le istruzioni specifiche per il trattamento dati personali area IT.

Vista le grandi novità connesse alla situazione attuale e l'urgenza di garantire continuità all'attività educativa, ci sembrano presenti difficoltà oggettive nell'attuazione puntuale di quanto sopra segnalato.

Le indicazioni presenti nel Provvedimento "Didattica a distanza: prime indicazioni" del Garante per la protezione dei dati personali del 26 marzo 2020 sono il riferimento sulla base del quale abbiamo analizzato le varie piattaforme di DAD utilizzabili.

"I dati personali dei minori, del resto, "meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali" (cons. 38 del Regolamento)".

Siamo partiti da questa considerazione del Garante nel procedere alla verifica delle piattaforme DAD che abbiamo analizzato.

Indicazioni sulla procedura seguita per analizzare le piattaforme DAD

Segnaliamo che le indicazioni che ora illustreremo possono essere seguite anche da quei docenti che volessero verificare la rispondenza alle norme sulla privacy di piattaforme DAD che stanno utilizzando, o si apprestano ad utilizzare.

Innanzitutto per la verifica bisogna leggere i disclaimer nella sezione – Privacy – della piattaforma. Segnaliamo che, per accertarsi di avere letto l'informativa sulla privacy nella sua interezza, non bisogna accontentarsi di riepiloghi e riassunti, ma bisogna recuperare la versione completa.

Spesso le piattaforme offrono l'accesso alla versione integrale solo mediante l'utilizzo di pulsanti e link attivabili con un click.

Va segnalato che quando il disclaimer della privacy è scritto per più servizi offerti o riguarda sia utenti del servizio che dipendenti dell'azienda risulta estremamente difficile capire quali specifiche possano riguardare gli altri e quali riguardano studenti o professori.

Il secondo passo è leggere l'informativa completa sui cookies per verificare quali informazioni raccolgono.

Il terzo passaggio è confrontare quanto dichiarato dal fornitore della piattaforma DAD con quanto previsto nel Provvedimento "Didattica a distanza: prime indicazioni" del Garante per la protezione dei dati personali al fine di evitarne l'utilizzo, per svolgere la DAD, nel caso la piattaforma considerata non soddisfi le indicazioni del Garante.

Analizzando numerose piattaforme DAD (8) abbiamo individuato alcune criticità.

Relativamente ai problemi legati alla profilazione, Il Garante afferma: "Laddove, invece, si ritenga necessario ricorrere a piattaforme più complesse e "generaliste", che non eroghino servizi rivolti esclusivamente alla didattica, si dovranno attivare, di default, i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare, sia in fase di attivazione dei servizi, sia durante l'utilizzo degli stessi da parte di docenti e studenti (evitando, ad esempio, il ricorso a dati sulla geolocalizzazione, ovvero a sistemi di social login che, coinvolgendo soggetti terzi, comportano maggiori rischi e responsabilità)."

Relativamente al dato relativo alla geolocalizzazione dell'utente tale dato può essere individuato anche acquisendo l'indirizzo IP (9) o l'indirizzo MAC (10).

Per la profilazione dell'utente (lo studente) il Garante afferma: "Tale specifica protezione dovrebbe, in particolare, riguardare l'utilizzo di tali dati a fini di marketing o di profilazione e, in senso lato, la relativa raccolta nell'ambito della fornitura di servizi ai minori stessi"

A riguardo, in alcune piattaforme DAD analizzate, abbiamo trovato indicazioni non proprio tranquillizzanti, ad esempio:

"Faremo anche sforzi ragionevoli per garantire che non utilizziamo i nostri prodotti per raccogliere informazioni quando visiti siti Web offerti da società diverse dalla nostra"
"la disattivazione dei Cookies tecnici indicati [...] potrebbe impedire la corretta navigazione sul Sito e/o limitarne la fruibilità (11)"
Per approfondire riteniamo anche utile segnalare in nota alcuni articoli (12) che hanno

evidenziato criticità di piattaforme DAD che gli insegnanti hanno usato e che in molti casi continuano ancora ad utilizzare.

Della piattaforma ZOOM Jules Polonetsky, amministratore delegato del Future of Privacy Forum, afferma “che i termini di servizio di Zoom includono alcune clausole che potrebbero invadere la privacy degli utenti. Per cui, come per tutti i prodotti, gli utenti dovrebbero fare attenzione ad utilizzare Zoom senza essere consapevoli di alcuni problemi di privacy che lo riguardano. Sempre Polonetsky afferma che la politica standard di Zoom sulla privacy consente di condividere i dati per il marketing mirato. E alcuni dei termini standard dell’azienda non sono coerenti con lo statunitense Family Educational Rights and Privacy Act, o FERPA, oltre ad altre norme in materia di protezione dei dati personali (possiamo indicare il GDPR) (13).”.

Segnaliamo anche l’attacco di phishing alla piattaforma Webex (14) di Cisco, per le indicazioni sulle cautele da avere e di cui rendere consci gli studenti circa i rischi legati a mail fraudolente che possono essere loro recapitate. E’, infatti, importante tutelare la classe virtuale da eventuali attacchi hacking effettuati da chi, conquistando la fiducia del destinatario con mail fraudolente, riesce ad ottenere le credenziali per accedervi e svolgere poi azioni di disturbo o peggio (15).

Conclusioni

L’intervento del Garante per la protezione dei dati personali sulle caratteristiche specifiche che le piattaforme di DAD devono garantire relativamente alla tutela della privacy dei minori (alunni e studenti) ha evidenziato in modo esplicito che esiste un problema privacy.

E’ evidente che le competenze multidisciplinari (16) necessarie per accertare se una piattaforma DAD garantisce il giusto livello di privacy non possono essere possedute e quindi pretese dai singoli insegnanti né dai singoli Dirigenti scolastici.

In particolare risulta improbabile che, per tali piattaforme DAD, gli insegnanti e i Dirigenti scolastici siano in grado, senza rischiare di sbagliare, di “attivare, di default, i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare, sia in fase di attivazione dei servizi, sia durante l’utilizzo degli stessi da parte di docenti e studenti” come richiesto dal Garante della privacy.

Per questo auspichiamo un intervento del Ministro che possa fare chiarezza sulla questione e permettere al personale della scuola di potere continuare le sue attività di didattica a distanza con la necessaria serenità

**Il prof. Fulvio Oscar Benussi, socio AIDR è docente di scuola secondaria di secondo grado, formatore e pubblicista. Esperto di innovazione didattica ha tenuto numerosi speech in Università italiane ed estere. Vari suoi contributi, molti redatti in collaborazione con Annamaria Poli ricercatrice dell'Università degli studi di Milano Bicocca, sono stati pubblicati in riviste scientifiche dell'ambito universitario.*

Note

1. Didattica a distanza, nel seguito DAD
2. Si tratta del tipo di attacco che recentemente si è ipotizzato abbia colpito il sito INPS
3. Per "Regolamento GDPR" intendiamo il REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016. https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=it
4. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9300784
5. Per data breach, in italiano violazione dei dati personali, si intende 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.
6. Vedere art. 32 comma 4 del GDPR
7. I dati relativi alla privacy degli studenti possono ad esempio essere la lista dei loro indirizzi mail.
8. Abbiamo analizzato varie piattaforme tra le quali anche quelle segnalate al link: https://www.istruzione.it/coronavirus/didattica-a-distanza.html
9. "[...] Tenendo con di tutto ciò, l'unica cosa che a noi "comuni mortali" è concessa fare è quella di localizzare un indirizzo IP ottenendo info generiche relative alla zona in cui è presente la centralina a cui fa capo la connessione di riferimento. Esistono infatti degli appositi strumenti adibiti allo scopo anche se, è bene tenerlo a mente, non permettono di conoscere via, numero civico e magari anche numero di telefono e nome e cognome di una persona. Ciò però non toglie il fatto che possano rivelarsi interessanti." Da: https://www.aranzulla.it/trovare-nome-e-indirizzo-di-casa-a-partire-da-un-indirizzo-ip-bufala-966.html Servizio di geolocalizzazione a partire dall'indirizzo IP https://it.geoipview.com/
10. "[...] Sebbene il MAC Address sia modificabile via software, trattasi di un dato che viene trasmesso quasi sempre in chiaro da parte dei vari dispositivi di rete. Dagli States, un'indagine ricorda come i telefoni Android annotino regolarmente gli indirizzi MAC dei dispositivi wireless rilevati nelle vicinanze trasmettendoli sui server di Google. Un'analoga prassi viene utilizzata da Apple, Microsoft e da Skyhook Wireless con l'intento di "mappare" la posizione geografica dei router e degli access point dislocati sull'intero globo terrestre." Tratto da: https://www.ilsoftware.it/articoli.asp?tag=Dammi-il-tuo-MAC-address-e-ti-diro-dove-ti-trovi_7476

11. Ricordiamo che il Garante afferma: “Laddove, invece, si ritenga necessario ricorrere a piattaforme più complesse e “generaliste”, che non eroghino servizi rivolti esclusivamente alla didattica, si dovranno attivare, di default, i soli servizi strettamente necessari alla formazione, configurandoli in modo da minimizzare i dati personali da trattare, sia in fase di attivazione dei servizi, sia durante l’utilizzo degli stessi da parte di docenti e studenti [...]”
12 Relativamente a ZOOM https://www.ilsole24ore.com/art/non-solo-privacy-zoom-bufera-elon-musk-vieta-l-utilizzo-dipendenti-AD2whdH?utm_medium=FBSole24Ore&utm_source=Facebook#Echobox=1585842151&refresh_ce=1
Vedere anche: https://www.wired.it/internet/web/2020/03/31/zoom-privacy-facebook/?refresh_ce=
13. L. Mischitelli, Zoom e Houseparty: tutti i problemi privacy e security delle app di videoconferenza più usate, https://www.agendadigitale.eu/sicurezza/privacy/zoom-e-houseparty-tutti-i-problemi-privacy-e-security-delle-app-di-videoconferenza-piu-usate/
14. Vedere: https://threatpost.com/cisco-critical-update-phishing-webex/154585/
15. Vedere: https://www.corriere.it/scuola/secondaria/20_aprile_01/coronavirus-lezioni-distanza-chi-fa-bullo-commette-reato-pagano-genitori-bbc54664-734c-11ea-bc49-338bb9c7b205.shtml e anche: https://iltirreno.gelocal.it/pisa/cronaca/2020/04/02/news/scuola-lezioni-a-distanza-interrotte-con-video-porno-o-violenti-1.38669535?refresh_ce
16. Per svolgere l’attività considerata sono necessarie competenze giuridiche, informatiche e linguistiche (spesso i disclaimer sono scritti in lingua inglese).

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2020/04/17/smart-teaching-e-smart-learning-in-sicurezza/

© 2026 Istituzioni24