RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318 • n. 1/2025 • DOI 10.32091/RIID0215 • articolo sottoposto a peer review • pubblicato in anteprima il 2 apr. 2025

Paola D'Abbrunzo

Regolamento generale sulla protezione dei dati e cybersecurity nelle pubbliche amministrazioni: le nuove sfide, le opportunità e best practices delle istituzioni scolastiche, nel contesto delle risorse del PNRR

Il lavoro si propone di fornire un'analisi dell'intersezione tra il Regolamento generale sulla protezione dei dati personali (GDPR), e la cybersecurity nelle pubbliche amministrazioni. In particolare, il focus del contributo sarà incentrato sulle istituzioni scolastiche e sull'effettivo grado di applicazione della normativa in materia di trattamento dei dati, nel contesto post-pandemico di digitalizzazione e utilizzo di strumenti cloud, mettendo in luce le criticità quotidiane che le scuole vivono e le soluzioni auspicabili per trovare il giusto bilanciamento tra spinte digitali ed esigenza di tutelare tutti i diritti fondamentali in materia di privacy e riservatezza. La trattazione fornirà una prima valutazione sul come e quanto le iniziative e le risorse del PNRR, che mirano a rafforzare i servizi di gestione della minaccia cyber per la protezione dell'ecosistema digitale nazionale, impattino sull'opera di ammodernamento e aggiornamento delle infrastrutture digitali e di sicurezza informatica delle istituzioni scolastiche.

GDPR – Privacy – Istituzioni scolastiche – PNRR – Cybersecurity

General Data Protection Regulation and Cybersecurity in public administrations: the new challenges, opportunities and best practices of educational institutions, in the context of the PNRR resources

The work aims to provide an analysis of the intersection between the General Data Protection Regulation (GDPR), and cybersecurity in public administrations. In particular, the focus of the contribution will be on educational institutions and the actual degree of application of the data processing regulations, in the post-pandemic context of digitalization and use of cloud tools, highlighting the daily critical issues that schools experience and the desirable solutions to find the right balance between digital pressures and the need to protect all fundamental rights in terms of privacy and confidentiality. The discussion will provide an initial assessment of how and to what extent the initiatives and resources of the National Recovery and Resilience Plan, which aim to strengthen cyber threat management services for the protection of the national digital ecosystem, impact the modernization and updating interventions of digital infrastructures and cybersecurity of educational institutions.

GDPR – Privacy – Educational institutions – NRRP – Cybersecurity

L'Autrice, laureata in Giurisprudenza e specializzata in professioni legali, è dipendente del Ministero dell'Istruzione e del Merito, in qualità di Direttore dei servizi generali e amministrativi

Sommario: 1. Premessa: definizione del dato personale e suo trattamento, in particolare nel contesto delle istituzioni scolastiche. – 2. Le specificità del trattamento dei dati nelle scuole. La base giuridica, il ruolo del titolare e del responsabile del trattamento, le norme più rilevanti del GDPR in materia. – 3. Il ruolo fondamentale della formazione continua degli stakeholder per la corretta applicabilità del Regolamento. – 4. Gli attacchi cyber nelle istituzioni scolastiche: il "phishing" e "pharming". Gli strumenti per garantire la sicurezza informatica e l'apporto, sul punto, delle risorse del PNRR. Osservazioni conclusive.

1. Premessa: definizione del dato personale e suo trattamento, in particolare nel contesto delle istituzioni scolastiche

Stando alla sua definizione, il dato personale[1] rappresenta "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)" e il suo "trattamento"[2] è inteso come qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione[3].

Il tema del trattamento del dato è particolarmente caldo, se si considera il contesto scolastico, posto che la maggior parte dei dati personali che ne costituiscono il database riguarda dati di minorenni e dati sensibili. Si pensi, ad esempio, a tutti i dati raccolti, nelle e dalle scuole, con riferimento agli alunni diversamente abili, per i quali, la loro gestione comporta il trattamento di documentazione medica, diagnosi, referti, decreti di invalidità. O anche ai dati giudiziari che possono essere oggetto di trattamento relativamente agli studenti, dati che rilevino le origini razziali ed etniche (possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri e in alcuni casi possono desumersi anche dai nominativi o dai dati anagrafici degli alunni) oppure le convinzioni religiose (per garantire la libertà di culto e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento). Siamo più che mai di fronte, quindi, al trattamento di dati sensibili e sensibilissimi[4], per i quali le scuole sono tenute a procedere solo nel rispetto e per quanto strettamente necessario al raggiungimento delle "finalità di istruzione e formazione".

In tale contesto, naturalmente, non va dimenticato che, insieme a tanti dati personali degli alunni, dati sensibili e, al limite, giudiziari, possono dover entrare in gioco anche nell'ambito dei rapporti di lavoro gestiti dagli enti scolastici con dirigenti, docenti e personale ATA. Il singolo istituto scolastico, sotto questo profilo, è, infatti, un ordinario datore di lavoro[5] che tratta i dati dei dipendenti per la gestione del rapporto lavorativo, nel rispetto

1. Per uno sguardo d'insieme, v. Belisario–Riccio–Scorza 2022.
2. Si veda D'Orazio–Finocchiaro–Pollicino–Resta 2021.
3. Cfr. artt. 4 e 7 del GDPR 2016/679.
4. Così Pizzetti 2021.
5. Sul punto, Pisani–Proia–Topo 2022.

delle norme che regolano tutte le sue fasi, dall'assunzione fino alla cessazione.

L'ambiente "scuola", dunque, è particolarmente complesso, sotto il profilo del trattamento dei dati personali e della tutela della privacy ed è questo il motivo per cui la sua regolamentazione è risultata spesso frastagliata e stratificata. Da questo punto di vista, la scelta del legislatore, di operare su un impianto normativo già esistente, innestando su di esso i nuovi obiettivi imposti dal GDPR, è risultata problematica: al netto di un innegabile miglioramento in termini di conoscibilità, circolazione, trattamento dei dati personali, ciò che si è ottenuto emendando il vecchio d.lgs. 196/2003 e il successivo d.lgs. 10 agosto 2018, n. 101, è, a parere di chi scrive, una eccessiva sovrapposizione tra gli istituti, incertezza sugli obblighi, indeterminatezza dei limiti.

2. Le specificità del trattamento dei dati nelle scuole. La base giuridica, il ruolo del titolare e del responsabile del trattamento, le norme più rilevanti del GDPR in materia

Proprio per questi motivi, e, data l'esigenza della protezione dei dati personali e della privacy[6], che nelle scuole è particolarmente rilevante, l'autorità di controllo, il Garante della privacy[7], nel 2023, ha sentito la necessità di aggiornare (alla luce del Regolamento UE 2016/679) e ampliare i contenuti già presenti nel vademecum del 2016, redigendo e pubblicando il nuovo vademecum 2023 dal titolo "La scuola a prova di privacy".

La revisione che viene richiesta dal GDPR, chiaramente richiamata nel vademecum, comincia dal novero dei soggetti coinvolti nel trattamento dei dati, dal momento che, al di là delle assonanze terminologiche, risultano profondamente incisi i ruoli e le responsabilità attribuiti a ciascuno di essi.

Alla luce di ciò, all'interno dell'organigramma dell'istituto scolastico, ogni scuola è tenuta così ad individuare le figure indicate dal GDPR e dal novellato Codice Privacy e che si possono così elencare:

- titolare del trattamento
- responsabili (esterni) del trattamento
- eventuali sub-responsabili
- responsabile della protezione dei dati

Il primo equivoco che va chiarito, per quanto possa suonare scontato agli esperti della materia, è che il titolare del trattamento, ossia il soggetto che determina le finalità e i mezzi del trattamento dei dati personali[8], sarà sempre l'istituto scolastico nel suo complesso e non già la persona fisica posta alla sua direzione, il cui ruolo sarà quello di dare esecuzione alle determinazioni del titolare. Nel nuovo quadro regolamentare, il titolare del trattamento è chiamato ad assicurare, attraverso scelte proprie, l'obiettivo del massimo grado di protezione dei dati trattati, facendosi guidare dal principio di accountability, o principio di responsabilizzazione, che, nella realtà dei fatti, si tradurrà, ad esempio, nell'accurata selezione dei soggetti cui affidare servizi e forniture. È proprio in relazione all'adeguatezza delle misure che si individua uno dei primi cambi di rotta rispetto alla normativa previgente. Il Codice Privacy, infatti, all'articolo 33 e nell'Allegato B, faceva riferimento ad una serie di misure minime – che tutti i titolari erano tenuti ad adottare – volte ad assicurare un livello basilare di protezione dei dati. Il legislatore europeo, invece, ben conscio dell'evoluzione e del progresso tecnologico ha spazzato via il requisito di misure "minime" prevedendo che i titolari adottino misure adeguate alla protezione dei dati in linea con la realtà in continuo mutamento. Conformemente a tale impostazione e in aderenza a tale inversione di tendenza, l'articolo 27, comma 1, lett. d), del d. lgs. n. 101/2018 ha abrogato proprio l'Allegato B del Codice Privacy.

Il legislatore nazionale, al novellato articolo 2 del d.lgs. 196/2003, ha, poi, previsto che, nell'ambito dell'organigramma organizzativo dell'istituto, specifici compiti e funzioni connessi al trattamento di dati personali siano demandati ad un ufficio o singolo dipendente, che però deve essere particolarmente qualificato e deve essere individuato con apposito atto di nomina. Quest'ultimo, può essere incaricato a coadiuvare la tenuta del registro delle

6. V. Relazione illustrativa riguardante "Disposizioni per l'adeguamento del Regolamento 2016/679 UE relativo alla protezione dei dati personali delle persone fisiche nonché alla loro libera circolazione, abrogazione della direttiva 95/46/CE", XVIII LEG - Schema di D.Lgs.
7. Sul ruolo del Garante, v. tra gli altri Busia–Ferola 2017.
8. Garante per la protezione dei dati personali 1997.

attività di trattamento[9], a coordinare l'attività di aggiornamento delle informative da rendere agli interessati[10] e a valutare i soggetti da nominare responsabili del trattamento[11].

Passando al responsabile del trattamento dei dati[12], questo è la persona fisica o giuridica, distinta dal titolare, che elabora dati per conto di quest'ultimo, sotto il suo controllo.

Requisito per la nomina è che il responsabile presenti garanzie sufficienti per mettere in atto opportune misure tecniche a tutela dei diritti degli interessati. Questa carica, che nelle scuole è svolta da un soggetto esterno, deve essere disciplinata da un contratto o da un atto giuridico, nel quale devono essere indicati i limiti e le istruzioni in merito al trattamento dei dati.

Una figura completamente nuova è, invece, quella del responsabile della protezione dei dati (RPD o, secondo l'acronimo inglese DPO – *Data Protection Officer*), la cui nomina è obbligatoria per tutte le autorità e gli organismi pubblici, dunque, anche per gli istituti scolastici pubblici: l'art. 37, par. 1, lett. a) del Regolamento prevede espressamente che "il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali". La medesima obbligatorietà non vale anche per gli istituti privati, sebbene appaia preferibile che anche tali soggetti vi procedano, tenuto conto delle specificità dei dati trattati, dei soggetti interessati (per lo più minori) e dei rischi connessi con le attività di trattamento[13].

A differenza del responsabile del trattamento, il responsabile della protezione dei dati può essere un soggetto sia interno che esterno all'istituto. Nel primo caso, la nomina andrà formalizzata con un atto di designazione e dovrà farsi particolare attenzione alla sussistenza, anche solo potenziale, di un conflitto d'interessi[14]. Qualora si opti per un soggetto esterno, l'istituto procederà invece a stipulare un contratto di servizio con la persona – fisica o giuridica – aggiudicataria della procedura selettiva, nella quale saranno indicati i requisiti di partecipazione, la durata e le caratteristiche di esecuzione della prestazione, anche in applicazione delle disposizioni del Codice dei contratti pubblici, d.lgs 36/2023. In ogni caso, sia esso interno o esterno, a seguito della nomina del responsabile del trattamento, e di qualsiasi variazione, i suoi dati di contatto dovranno essere comunicati, dal titolare al Garante, mediante la procedura telematica disponibile sul sito[15]. Questa disposizione mira a garantire che le autorità di controllo possano contattare il responsabile della protezione dei dati in modo facile e diretto[16].

Le funzioni "ibride" del responsabile riguardano soprattutto attività di consulenza, da fornire al titolare del trattamento, passando per la cura della formazione del personale, fino a sorvegliare l'osservanza della normativa, fornendo, quando richiesto, un parere in merito alle valutazioni d'impatto. Sul punto, si deve precisare che l'onere di assicurare il rispetto della normativa e la conformità delle

9. Cfr. GDPR 2016/679, art. 30.
10. *Ivi*, artt. 13 e 14.
11. *Ivi*, art. 28.
12. *Ivi*, artt. 28 e 29.
13. Così il Gruppo dei Garanti Ue (WP 29) approvava il 13 dicembre 2016 tre documenti con indicazioni e raccomandazioni su importanti novità del Regolamento 2016/679 sulla protezione dei dati; in particolare le Linee guida sul DPO specificano i requisiti soggettivi e oggettivi di questa figura, la cui designazione sarà obbligatoria per tutti i soggetti pubblici e per alcuni soggetti privati sulla base di criteri che il Gruppo ha chiarito nel documento. Nel documento vengono illustrate (anche attraverso esempi concreti) le competenze professionali e le garanzie di indipendenza e inamovibilità di cui il DPO deve godere nello svolgimento delle proprie attività di indirizzo e controllo all'interno dell'organizzazione del titolare.
14. Cfr. art. 38 del GDPR 2016/679.
15. V. sito del Garante per la protezione dei dati personali.
16. Per una visione d'insieme, v. Gruppo Articolo 29 2017-a, punto 2.6, in particolare, l'art. 37, par. 7 del Regolamento (UE) 2016/679 e l'art. 28, c. 4 del d.lgs. 18 maggio 2018, n. 51.

operazioni di trattamento al GDPR ricade comunque sempre sul titolare poiché il responsabile della protezione dei dati non risponde personalmente in caso di inosservanza del GDPR.

Quanto alla valutazione d'impatto, l'esecuzione di un DPIA (*Data Protection Impact Assessment*) è obbligatoria soltanto se è probabile che il trattamento "provochi un elevato rischio per i diritti e le libertà delle persone fisiche"[17]. Ciò è particolarmente rilevante quando viene introdotta una nuova tecnologia di elaborazione dati, specie se sensibili. Per questo motivo, nelle scuole, specie a seguito delle riforme imposte dal PNRR, che stanno comportando una vera e propria rivoluzione digitale con la migrazione al cloud di tutti gli applicativi gestionali e di lavoro[18], sembrerebbe assolutamente necessaria, almeno da questo momento in poi, la realizzazione del DPIA. Invero, ad oggi, tale pratica non è osservata in tutti gli istituti scolastici e sono pochi quelli in cui il titolare del trattamento (unico responsabile della valutazione d'impatto) procede alla o alle valutazioni per descrivere la necessità, la proporzionalità e i relativi rischi connessi al trattamento dei dati. Una DPIA, infatti, può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi. Sembra, però, che sul DPIA vi sia ancora un certo margine di discrezionalità in capo al titolare del trattamento nelle istituzioni scolastiche, anche perché le Linee guida[19] non contengono indicazioni specifiche su questo punto, a conferma che il loro contenuto e il loro obiettivo è essenzialmente procedurale. Eppure, il ricorso al DPIA dovrà iniziare ad essere costante, se ci si vuole allineare al contesto del GDPR, che, appunto, ribadisce la centralità del titolare in ordine alla valutazione dei trattamenti e alle misure da adottare per assicurare la loro compliance con le regole di protezione dei dati personali. In sostanza, la valutazione di rischio deve iniziare ad essere inteso come un processo e flusso costante e come una fase comunque necessaria per ogni trattamento e prima che il trattamento stesso inizi.

L'elasticità della interpretazione delle disposizioni sulla valutazione del rischio è, dunque, compensata dalla continua sottolineatura, peraltro supportata sia dall'art. 24, paragrafo 1, che dall'art. 35, paragrafo 11 del Regolamento, che, sia l'analisi dei rischi che il DPIA, inteso come individuazione delle misure necessarie, devono essere concepite come un processo costante e, continuamente, in rinnovamento. Una conferma, dunque, che il GDPR contiene una normativa molto elastica e, per questo, adattabile a ogni innovazione tecnologica che comporti appunto il trattamento di dati personali.

3. Il ruolo fondamentale della formazione continua degli stakeholder per la corretta applicabilità del Regolamento

Questo continuo "work in progress" che l'applicazione corretta del GDPR impone o imporrà alle scuole, è strettamente collegata a quell'attività di formazione del personale, a cui si faceva prima riferimento, e che il DPO dovrebbe curare. Arriviamo così, ad un punto nevralgico e dolente della trattazione. La formazione del personale rappresenta un altro importante milestone del PNRR. Le ultime due misure del PNRR, che stanno in questo momento interessando le scuole, introdotte, in Italia, con il d.m. 65/2023 e d.m. 66/2023 puntano, esclusivamente, all'aggiornamento e alla formazione del personale. Mentre il primo decreto, però, mira a formare i docenti delle scuole sulle discipline STEM e sul multilinguismo, il d.m. 66/2023 è la vera opportunità per le scuole per formare il proprio personale, specie quello che lavora nelle segreterie scolastiche, che ha a che fare tutti i giorni con

17. Cfr. art. 35, par. 1 del GDPR 2016/679 in base al quale "Quando un tipo di 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. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".
18. V. Missione 1, Componente 1, investimento 1.2 del PNRR "Abilitazione al Cloud per le PA Locali - Scuole".
19. Cfr. Gruppo di lavoro Articolo 29 2017, *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 4 aprile 2017.

tematiche quali la trasparenza e la sezione "amministrazione trasparente" dei siti web, il trattamento dei dati, la conservazione e l'archiviazione dei documenti, il rapporto con i dati sensibili degli alunni minori.

L'obiettivo è quello di sviluppare competenze digitali in linea con i quadri di riferimento europei DigComp 2.2 e DigCompEdu. La formazione, però, non potrà essere adeguata se non si considera che, allo stato attuale, il livello di preparazione delle segreterie scolastiche è basso o medio/basso e difficilmente performante rispetto ai nuovi adempimenti delle "scuole digitali". Si rileva, infatti, ancora molta superficialità nel trattamento dei dati personali, poca dimestichezza nel reperire in maniera corretta le informative, addirittura poca propensione dei titolari, ovvero degli istituti, a tener costantemente aggiornate le stesse, nel rispetto degli articoli 13 e 14 GDPR[20].

Partendo da tali considerazioni, sarebbe interessante monitorare, nel breve e medio periodo, come e se le scuole redigeranno informative non eccessivamente strutturate che potrebbero veder compromesso il requisito della chiarezza e della semplicità optando, invece, per una pluralità di informative ritagliate sulla categoria di interessati cui saranno dirette (alunni/famiglie da un lato, dipendenti dall'altro, fornitori etc.). La categoria degli interessati, ricordiamolo, nell'ambito degli istituti scolastici, è costituita perlopiù da soggetti minorenni che, dunque, non possono rilasciare alcun valido consenso al trattamento dei dati fino al compimento del diciottesimo anno di età[21]. Qualora, invece, lo studente dovesse raggiungere la maggiore età nel corso del ciclo scolastico sarà necessario acquisire il consenso direttamente dall'interessato e non dai genitori o dai soggetti che ne hanno precedentemente esercitato la responsabilità genitoriale.

Non è da sottovalutare, su questo punto specifico, il contesto socio-economico in cui la scuola opera. Contesti complessivamente più disagiati, scuole site in aree a rischio in termini di dispersione scolastica, aree periferiche, riscontrano sicuramente una maggiore difficoltà di reperimento delle informative da parte delle famiglie, a dimostrazione del fatto che, in generale, il trattamento dei dati può essere connesso ad aspetti socio/economici/culturali. Spesso risulta problematico far comprendere la base giuridica del trattamento, ovvero che il trattamento dei dati, nell'ambito della scuola, è strettamente necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, e che avviene solo in virtù di una norma di legge o, se ammesso dalla legge, di regolamento (art. 2 *ter* d.lgs. 101/2018) e per le categorie particolari di dati, indicati dall'art. 9 del GDPR, per motivi di interesse pubblico rilevante (art. 2 *sexies* d.lgs. 101/2018).

Un altro importante adempimento a cui spesso non viene data la giusta attenzione è la tenuta del registro delle attività di trattamento, secondo quanto previsto dall'art. 30 par. 1 del GDPR. Si tratta di un documento di censimento e analisi contenente le principali informazioni relative alle operazioni di trattamento effettuate, che si configura come una "fotografia" sullo stato attuale dei trattamenti posti in essere. Esso deve avere forma scritta, anche elettronica e deve essere sempre mantenuto aggiornato.

Per le istituzioni scolastiche, il Miur, con nota n. 877 del 3 agosto 2018, ha trasmesso uno schema di registro delle attività di trattamento, corredato da una guida operativa, per la compilazione dei campi individuati, ma anche per questo strumento, la sua utilizzazione è molto scarsa[22].

Sul grado di attuazione del GDPR, nelle istituzioni scolastiche, pertanto, si può concludere che

20. Sul punto, v. Garante per la protezione dei dati personali 2023-b: in particolare, parte II - L'attività svolta dal Garante - Punto 4. Il Garante e le amministrazioni pubbliche – Paragrafo 4.3. La protezione dei dati personali in ambito scolastico e universitario, p. 39.
21. Il legislatore nazionale, all'art. 2 *quinquies* del Codice Privacy, ha previsto che "Il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione" fattispecie che, allo stato, non sembra poter interessare il mondo della scuola.
22. Cfr. Garante per la protezione dei dati personali 2023-b e quanto evidenziato al sito Internet del GPDP, nella sezione dedicata alla Scuola.

la vera sfida sarà quella di rivedere l'organizzazione delle attività nel suo complesso, non semplicemente in termini formali – attraverso un adeguamento documentale – quanto, piuttosto, a realizzare una rivoluzione culturale all'interno di molte prassi[23]. E tale spinta può essere fornita, oggi, solo dal PNRR.

4. Gli attacchi cyber nelle istituzioni scolastiche: il "phishing" e "pharming". Gli strumenti per garantire la sicurezza informatica e l'apporto, sul punto, delle risorse del PNRR. Osservazioni conclusive

Ancora solo grazie alle risorse del PNRR, si potrà effettivamente parlare di implementazione dei sistemi e degli strumenti di prevenzione contro i cyber attacchi. In questo senso, la conoscenza di buone pratiche al fine di incrementare la sicurezza informatica è fondamentale per tutti, non solo per i lavoratori e i dipendenti della pubblica amministrazione a cui vengono rivolti gli sforzi maggiori. A maggior ragione, l'attenzione deve essere indirizzata a coloro che sono nella fase iniziale del loro corso di vita e che sono a rischio di incorrere in fenomeni quali la pedopornografia online, l'adescamento in rete, il cyberbullismo, la sextortion, la dipendenza patologica da Internet, l'estorsione di informazioni personali, come appunto possono essere i minori.

Cybersecurity nel contesto scolastico significa quindi due cose: da un lato, significa educare e promuovere un'alfabetizzazione digitale critica per i bambini e i ragazzi e guidare i genitori nell'uso di Internet da parte dei figli a casa; dall'altro, significa potenziare le infrastrutture digitali già esistenti nelle scuole o prevederne delle nuove, ma con adeguata preparazione e formazione di chi queste infrastrutture le deve gestire ed utilizzare. Se la trasformazione digitale affonda le proprie radici nei dati, è necessario che questi siano al sicuro e, per ottenere un simile risultato, non basta l'apporto tecnologico, soprattutto se non è inserito in un contesto di cultura della difesa e della sicurezza nel senso più ampio del termine. Il traguardo è ambizioso ma necessario e lo Stato italiano lo sa bene, tanto che il governo dell'allora premier Mario Draghi già approvava il d.l. 82/2021 con il quale, tra le altre cose, si è avuta la nascita dell'Agenzia per la cybersicurezza nazionale (ACN), di fatto operativa a partire dal mese di settembre del 2021.

I fondi del PNRR stanziati per la cybersicurezza ammontano a 623 milioni di euro: orbene, la parte più consistente, 301 milioni di euro, è destinata al potenziamento della resistenza cyber della PA, proprio per aumentarne la capacità di risposta, quindi reattività e non proattività[24]. I soldi stanziati (tra PNRR e ulteriori fondi deliberati dal governo) offrono una lettura che in linea di massima non ammette repliche: l'Italia si sta dotando delle infrastrutture per aumentare la propria resilienza agli attacchi cyber. Nonostante ciò, proprio per ricollegarci al quadro generale che si è cercato di fornire in questo lavoro, ben si può affermare che la sicurezza non è garantita soltanto dall'hardware e dal software, ma ha bisogno anche che lavoratori, studenti e cittadini siano più istruiti e formati, in modo da diventare più attenti. La cybersecurity deve essere un processo "aziendale" al pari degli altri e una dote che caratterizza i lavoratori, al pari delle conoscenze specifiche e tecniche relative alle professioni che svolgono.

Nel caso specifico delle scuole, diversi report[25]dimostrano, infatti, il notevole aumento degli attacchi ransomware nel comparto didattico,

23. Soro 2016, p. 20 ss., secondo cui si deve muovere alla ricerca di nuove e più efficaci forme di tutela delle nostre libertà, nel convincimento che la protezione dei dati personali rappresenta "la chiave attraverso cui è possibile ricercare il più alto punto di equilibrio tra uomo e tecnica".

24. Sul punto, v. Dipartimento per la trasformazione digitale 2022 e il programma di investimenti dell'Agenzia per la cybersicurezza nazionale, *Un programma di investimenti cybersecurity per un Paese ancora più sicuro*.

25. Cfr. Sophos 2022, Report dettagliato di studio annuale che ha coinvolto un totale di 730 professionisti IT dell'ambito didattico, che lavorano in aziende di medie dimensioni (100-5.000 dipendenti) distribuite fra 31 Paesi. Lo studio riporta la percentuale degli attacchi ransomware, i costi di ripristino e i livelli di copertura delle assicurazioni informatiche nel settore didattico. A causa dell'ampia varietà delle organizzazioni che operano nell'ambito didattico, il report fornisce dati separati per la scuola primaria o secondaria (fino a 18 anni) e per gli istituti universitari e parauniversitari (a partire dai 18 anni).

in questi ultimi anni, in cui gli operatori diventano spesso vittime inconsapevoli delle azioni di "phishing" e "pharming". Per phishing si intende quel tipo di attacco che consiste nell'inviare email malevole scritte appositamente con lo scopo di spingere gli utenti a rivelare informazioni bancarie, credenziali di accesso o altri dati sensibili; ciò avviene soprattutto quando le email sono "ben confezionate" e facilmente attribuibili a persone conosciute. Il termine pharming deriva invece dall'unione di "phishing" e "farming", e consiste in una metodologia in grado di dirottare il traffico internet verso server o siti gestiti dalla cybercriminalità, quindi non leciti, in modo da reperire tutte le informazioni e i dati personali ritenuti necessari ed "appetibili", perché essendo suscettibili di patrimonializzazione[26], e quindi di valutazione economica, ben si prestano alla loro commercializzazione indisciplinata, che pericolosamente, può diventare mercificazione.

Orbene, contrastare il phishing e il pharming non è facile, e tali fenomeni devono essere considerati come oggetto di formazione specifica e costante nel tempo. Su questi temi di cybersecurity, i programmi di sensibilizzazione del personale non possono avere un'efficacia permanente e devono essere ripetuti e aggiornati nel tempo (almeno una volta l'anno, meglio ancora semestralmente), se si considera l'alto grado di volatilità dei virus che, se reperiti e distrutti, vengono subito sostituiti da altri completamente nuovi.

Sarà importante e necessario, valutare, nel breve e medio periodo, quanti e quali scuole si adopereranno per includere la sicurezza informatica nell'offerta formativa degli alunni delle scuole primarie e secondarie, quante scuole prevedranno adeguati corsi di formazione per i dipendenti, quante faranno ricorso alla contrattualizzazione di un consulente esterno per gestire minacce e attacchi digitali.

Gli addetti ai lavori (AgID, Ministero per la Pubblica Amministrazione, Dipartimento per la Trasformazione Digitale) dovranno allora gettare le basi per l'elaborazione di uno studio, anche in un'ottica statistica, per rendicontare e dimostrare in che percentuale saranno effettivamente utilizzate nuove pratiche di miglioramento e prevenzione degli attacchi, quante applicheranno almeno le "misure minime" definite da AgID[27], l'Agenzia per l'Italia digitale, quanti dei soldi effettivamente stanziati verranno spesi per sviluppare competenze digitali in linea con i quadri di riferimento europei DigComp 2.2 e DigCompEdu e quanti per implementare le misure di Cybersecurity.

In fondo, sarò l'Unione europea a chiedercelo, nel momento in cui ci presenterà il conto per le risorse del PNRR concesse a favore dell'Italia.

Riferimenti bibliografici

AgID (2022), *Linee guida sull'accessibilità degli strumenti informatici dell'AgID*, 21 dicembre 2022

G. Alpa et al. (2021), *Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri*, in R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di), "Codice della privacy e data protection", Giuffrè, 2021

E. Belisario, G.M. Riccio, G. Scorza (a cura di) (2022), *GDPR e Normativa Privacy - Commentario*, IPSOA, 2022

F. Blefari, M. Paier, A.P. Paliotta (2023), *Educare alla sicurezza informatica: il ruolo delle scuole e del privato-sociale*, in "AgendaDigitale", 29 novembre 2023

L. Bolognini, E. Pelino (2024), *Codice della disciplina privacy*, Giuffrè, 2024

G. Busia, L. Ferola (2017), *Il Garante per la protezione dei dati personali. Le funzioni, i rapporti con le altre Istituzioni ed Autorità in Italia e in Europa*, in G. Busia, L. Liguori, O. Pollicino (a cura di), "Le nuove frontiere della privacy nelle tecnologie digitali", Aracne, 2017

26. Sentenza n. 2631/2021 del Consiglio di Stato.

27. Circolare n. 2 del 18 aprile 2017.

G. Carullo (2018), *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa,* Giappichelli, 2018

R. D'Orazio, G. Finocchiaro, O. Pollicino, G. Resta (a cura di) (2021), *Codice della privacy e data protection*, Giuffrè, 2021

Dipartimento per la trasformazione digitale (2022), *Cybersicurezza e resilienza per la trasformazione digitale della PA*, 2022

ENISA (2024), Implementing guidance. On Commission Implementing Regulation (EU) 2024/2690 of 17.10.2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures, October 2024

Garante per la protezione dei dati personali (2023-a), *La Scuola a prova di privacy*, 2023

Garante per la protezione dei dati personali (2023-b), *Relazione annuale 2023*

Garante per la protezione dei dati personali (1997), *Titolare, responsabile, incaricato - Precisazioni sulla figura del "titolare"*, doc. web n. 39785, 9 dicembre 1997

Gruppo di lavoro Articolo 29 (2017), *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*, 4 aprile 2017.

Gruppo di lavoro Articolo 29 (2017-a), *Linee guida sui responsabili della protezione dei dati (RPD)*, 2017

C. Pisani, G. Proia, A. Topo (a cura di) (2022), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Giuffrè, 2022

F. Pizzetti (a cura di) (2021), *Protezione dei dati personali in Italia tra GDPR e codice novellato*, Giappichelli, 2021

F. Pizzetti (2018), *Delega per il GDPR, i punti forti e deboli: un primo giudizio*, in "Agenda Digitale", 23 agosto 2018

Sophos (2022), *The State of Ransomware in Education 2022*, 21 luglio 2022

A. Soro (2016), *Liberi e connessi*, Codice, 2016