IL FATTORE UMANO E LA REGOLAZIONE DELLA CYBERSECURITY

Federica Camisa, Andrea Simoncini[1]

Sommario

Viviamo ormai da tempo in una realtà digitalizzata e costellata da molteplici attività dipendenti da sistemi tecnologici interconnessi. Una vera e propria transizione cibernetica, dunque, che da un lato offre prospettive di avanzamento e progresso, ma dall'altro espone gli utilizzatori a inedite minacce che permeano la sfera della sicurezza digitale e dei diritti fondamentali. La regolazione della cybersicurezza diviene elemento imprescindibile per mitigare l'incremento degli attacchi informatici potenzialmente dannosi per le infrastrutture e per i dati ivi contenuti. Per le stesse finalità e nonostante l'elevato tecnicismo che caratterizza la "sfera digitale", parimenti determinante risulta il fattore umano, ovvero il ruolo assunto dagli stessi utilizzatori.

Abstract

We live in a digitalised reality, where many activities depend on interconnected technological systems. A real cyber transition that offers the prospect of evolution and progress, but also exposes users to unprecedented threats in the field of digital security and fundamental rights. Therefore, cybersecurity regulation is imperative for containing potentially damaging cyber-attacks on infrastructures. For these same purposes, it is equally critical to consider the role that users play (i.e. the human factor).

Keywords: cyber attacks – cybersecurity – regulation – fundamental rights – human factor

1. Introduzione

Basta guardarsi intorno per realizzare che viviamo immersi in ambienti costantemente "connessi e intelligenti". Moltissime delle attività che svolgiamo, sia come singoli, sia come imprese o come pubbliche amministrazioni, dipendono sempre più da sistemi tecnologici tra loro interconnessi.

Con la rivoluzione cibernetica [1] e l'avanzamento delle nuove tecnologie digitali, è possibile realizzare in rete numerose e significative attività (accedere al Servizio

[1] Sebbene l'articolo sia il frutto di un lavoro comune, il paragrafo 1 è di Andrea Simoncini mentre i paragrafi 2, 3, 4 e 5 sono di Federica Camisa.

sanitario regionale, gestire il settore delle comunicazioni elettroniche, dell'energia, dei trasporti, ecc.).

Come tutte le innovazioni della tecnica, questi strumenti costituiscono contemporaneamente, da un lato, opportunità senza precedenti per il progresso e lo sviluppo della conoscenza, per il miglioramento culturale, sanitario ed economico; tuttavia, dall'altro lato, rappresentano un rischio e una potenziale minaccia, poiché attraverso essi possono realizzarsi inedite violazioni dei diritti [2].

Vivere in una realtà iperconnessa *(onlife* [3]*)* espone la società a una serie di nuove sfide legate al concetto di *sicurezza*, nonché a nuovi rischi di cui spesso non si ha percezione, né consapevolezza [4]. Si considerino, per esempio, le forme di sorveglianza di massa esercitabili mediante l'utilizzo delle tecnologie [5], come le c.d. tecniche di "profilazione" e i sistemi di videosorveglianza [6].
Oltre alle consuete dimensioni della sicurezza che attengono alla vita della persona – come il mantenimento dell'ordine pubblico, la sicurezza sul lavoro o la circolazione stradale – si affiancano, dunque, tutte le implicazioni suscitate dall'avvento del digitale, tra cui spicca la necessità di salvaguardare l'ambiente "virtuale" [7].

Nell'incessante progresso tecnologico, infatti, la rete e i servizi ivi offerti, divengono sempre più frequentemente bersaglio di attacchi informatici *(cyber attacks)*, i quali non solo possono causare malfunzionamenti e interruzioni dei servizi, ma possono altresì provocare preoccupanti fughe di dati personali. In questa prospettiva, emerge una stretta correlazione tra la salvaguardia delle infrastrutture e la tutela delle informazioni, richiamando in modo ineludibile la normativa relativa alla protezione dei dati personali, con particolare riferimento, a livello europeo, il *General Data Protection Regulation* (GDPR) [8].

Considerato il contesto in cui viviamo, caratterizzato da una crescente condivisione di dati personali e da sempre più frequenti violazioni della *cybersecurity*, l'Unione Europea, con il GDPR, ha manifestato un deciso impegno nella salvaguardia della privacy[2], o meglio, della protezione dei dati personali [9] e della sicurezza degli stessi [10]. La connessione tra il GDPR e la cybersicurezza richiede l'adozione di misure concrete volte all'implementazione di dispositivi sicuri e in grado di difendersi da possibili attacchi che potrebbero compromettere la riservatezza, integrità e disponibilità dei dati personali in essi contenuti [11]. In

[2] Il concetto di privacy affonda le sue radici in epoche piuttosto recenti. Una sua prima elaborazione giuridica può essere identificata solo verso la fine del diciannovesimo secolo. ® nel 1890, in occasione della pubblicazione dell'articolo *The Right to* Privacy di due giuristi statunitensi (D. Warren e L. D. Brandeis), che il concetto di privacy è riconosciuto come "il diritto ad essere lasciato solo". Da allora si osserva l'insorgere di una dimensione sociale della privacy. È risaputo come, a causa dell'incessante sviluppo tecnologico, la questione della tutela della sfera privata di ciascun individuo abbia assunto connotazioni completamente inedite, mettendo in crisi gli antichi schemi.
In altre parole, il diritto alla privacy ha subito un'evoluzione dalla sua concezione iniziale come diritto di essere lasciati soli al diritto di esercitare un controllo sulle informazioni riguardanti la sfera personale.

questo quadro emerge con chiarezza la necessità di mantenere un costante equilibrio tra le esigenze di protezione dati e di sicurezza, poiché sono due aspetti che, come abbiamo già detto, risultano strettamente interconnessi e reciprocamente dipendenti [12].
Posto che la sicurezza della rete diviene un elemento cardine che deve essere garantito nel mondo digitale [13], prima di interrogarci su come prevenire e reagire alle aggressioni perpetrate sul *web*, occorre chiarire cosa si intende con l'espressione «sicurezza»? Chi sono i soggetti che devono garantirla e in che modo è auspicabile farlo? Perché è importante discutere di un «diritto costituzionale ibrido» [14][3]?

Negli anni, la riflessione su queste domande ha assunto la consistenza di una vera e propria disciplina, quella della *cybersecurity* [15], intesa come «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche»[4].

È opportuno ora contestualizzare e delineare i confini entro cui sarà sviluppato il contributo per fornire sin dal principio una panoramica generale dei temi che saranno trattati.

Nei successivi paragrafi verrà approfondito il concetto di cybersicurezza e segnalata la sua centralità nelle dinamiche quotidiane. Un *focus* particolare sarà riservato all'esame di un caso paradigmatico: l'attacco informatico alla Regione Lazio. In tale occasione, verranno spiegate brevemente le dinamiche di tale aggressione per poi evidenziare le implicazioni e le conseguenze in termini di sicurezza delle infrastrutture e protezione dei dati personali.

Saranno poi dedicati alcuni paragrafi a una rapida analisi del quadro normativo, partendo inizialmente dalla legislazione vigente a livello europeo; per poi successivamente soffermarsi sul piano nazionale.

Una specifica riflessione sarà riservata al ruolo assunto dal fattore umano nel campo della sicurezza informatica al fine di comprendere come le dinamiche comportamentali e decisionali di ciascun utente possano incidere sulle vulnerabilità di un sistema informatico e possano, finanche, determinare il successo di un attacco informatico.

In conclusione sarà offerta una sintesi delle principali argomentazioni avanzate nel contributo, proponendo considerazioni critiche e sollecitazioni riguardo alla necessità di adottare un approccio che favorisca una maggiore pedagogia digitale e promuova buone pratiche nel cyberspazio.

[3] Con il termine «diritto costituzionale ibrido» l'autore, Andrea Simoncini, esprime la necessità di dover recepire i valori del diritto costituzionale sin nella fase di progettazione degli strumenti informatici.
[4] In questi termini si esprime l'art. Art. 2, punto 1) del Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cybersicurezza e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013.

2. La (cyber)sicurezza come esigenza quotidiana. Il caso dell'attacco informatico alla Regione Lazio

Come abbiamo visto, la capillare diffusione delle tecnologie e il loro sempre crescente impiego nelle più disparate attività quotidiane, nell'ambito di una società dell'informazione, incrementano il rischio di essere esposti, anche indirettamente, a nuove minacce che hanno come bersaglio le strutture informatiche.

I dati che emergono dal rapporto Clusit 2023 rilevano nel periodo dal 2018 al 2022 una crescita preoccupante degli attacchi informatici a livello globale pari al 60%[5]. Queste forme di attacchi, i c.d. *cyber attacks*[6], sono realizzati da soggetti malintenzionati che, attraverso azioni illegali compiute sovente nel c.d. *dark* web [16][7], sfruttano malignamente le vulnerabilità dei sistemi informatici con l'obiettivo di arrecare danni, causare l'interruzione di servizi, rubare i dati o chiedere riscatti (*ransomware*).

Un esempio di attacco informatico è quello che nell'agosto 2021, in piena emergenza pandemica da Covid-19, ha visto coinvolta la Regione Lazio.

L'aggressione cibernetica è stata perpetrata ai danni del centro di elaborazione dati (CED) e ha avuto una particolare risonanza soprattutto perché ha colpito anche le piattaforme adibite alla prenotazione dei vaccini contro il Covid-19. Seppure vi siano differenti ricostruzioni della vicenda, il dato certo è che sia stato utilizzato un *malware,* in particolare un *ransomware,* ossia un programma informatico dannoso che infetta il dispositivo e impedisce l'accesso a tutti o ad alcuni dei suoi contenuti per poi chiedere un riscatto per rimuovere tale limitazione.

Nel caso di specie, il *ransomware* avrebbe colpito un dispositivo, connesso al *server* di erogazione dei servizi di gestione e organizzazione delle attività di interesse regionale, di un dipendente che lavorava in *smartworking*. Questo attacco avrebbe causato una interruzione dei servizi del sistema sanitario regionale.

Le conseguenze spesso gravi derivanti da queste tipologie di attacchi informatici – che frequentemente si manifestano sotto forma di danni alle infrastrutture e di fughe di dati – confermano la rilevanza della disciplina sulla *cybersecurity* e, non

[5] Per un'analisi più approfondita è possibile consultare il report al seguente indirizzo: https://clusit.it/wp-content/uploads/area_stampa/2023/Anteprima_Rapporto_Clusit_2023.pdf (ultimo accesso novembre 2023).

[6] Si veda la definizione fornita dall'Enciclopedia Treccani https://www.treccani.it/vocabolario/cyberattacco_%28Neologismi%29/#:~:text=s.%20m.%20Attacco%20terroristico%20condotto%20con%20mezzi%20tecnologici%2C%20attraverso%20Internet (ultimo accesso novembre 2023).

[7] L'autore, Stefano Pietropaoli, per *dark web* intende quello spazio in cui «è possibile mettere in vendita le proprie prestazioni di qualsiasi natura esse siano, insieme ad altri oggetti e, purtroppo, persone». Questo termine, aggiunge l'autore, «va tenuto distinto dal deep web che pur non essendo indicizzato è perfettamente lecito».

limitandosi a colpire una singola entità o un singolo Stato membro ma diffondendosi in pochi minuti tra organizzazioni, settori e diversi Stati membri, è indispensabile la previsione di misure di prevenzione e contrasto che tengano in considerazione la dimensione transfrontaliera particolarmente marcata della materia.

Dinanzi all'evidenza di situazioni sociali in cui l'uso di determinati strumenti può recare danno alla vita o al patrimonio dei consociati, la reazione è stata quella, da un lato, di moltiplicare gli sforzi nella ricerca scientifica per aggiornare e migliorare i sistemi tecnici, in modo da "immunizzarli" il più possibile da questi attacchi malevoli o dall'uso criminoso che se ne può fare. Dall'altro lato, la risposta delle organizzazioni sociali e politiche è stata quella di proporre norme volte a vietare o disincentivare l'impiego illecito dei dispositivi tecnologici.

Nel paragrafo che segue proporremo una sintesi della disciplina normativa in materia di *cybersecurity,* dapprima a livello europeo e poi a livello nazionale [17], per infine soffermarci sul ruolo assunto in queste vicende da quello che definiamo il "fattore umano".

3. La reazione del legislatore

La preminente necessità di individuare una normativa specifica in materia di *cybersecurity* è stata chiara sin dalle fasi iniziali dello sviluppo della rete *internet*, quando si è compreso che gli attacchi informatici avrebbero inevitabilmente impattato sulle informazioni, sui dati e sui servizi offerti, determinando conseguentemente effetti diretti e, potenzialmente, di portata catastrofica sul tessuto sociale e sulle libertà sancite a livello costituzionale. La sicurezza informatica diviene dunque un fattore essenziale oltre che per la corretta operatività ed efficienza delle infrastrutture pubbliche e private, anche per garantire un sicuro esercizio dei diritti fondamentali [18], compresi i diritti alla riservatezza e alla protezione dei dati personali nonché la libertà di espressione e di informazione.

La natura globale delle minacce cibernetiche richiede una cooperazione internazionale e un'armonizzazione delle norme e delle pratiche di sicurezza informatica tra i Paesi. In questa prospettiva, il legislatore e le istituzioni pubbliche hanno reagito alla impellente esigenza di contrastare l'uso distorto e criminoso delle tecniche offerte dalla tecnologia, attraverso l'introduzione di disposizioni normative e regolamentazioni che mirano ad assicurare un ambiente digitale sicuro.

L'Unione europea, pioniera in questo ambito, si è occupata di analizzare approfonditamente le vulnerabilità, le minacce e il rischio associato agli *asset* informatici, al fine di salvaguardarli da potenziali attacchi suscettibili di cagionare danni di notevole entità [19].

La legislazione nazionale degli Stati membri in materia di *cybersecurity* è stata adottata seguendo l'impulso del legislatore eurounitario. E infatti, al quadro normativo europeo delineato nel corso degli anni, si sono affiancate le disposizioni dei legislatori nazionali [20].

3.1. L'ordinamento UE

L'Unione europea, come precedentemente affermato, ha posto le fondamenta normative della *cybersecurity*, le cui previsioni costituiscono oggi il cuore della strategia eurounitaria in tale ambito.

Nonostante le prime regolamentazioni sulla sicurezza informatica risalgano agli anni '90, il primo intervento che ha portato all'istituzione di un'apposita agenzia, l'*European Union Agency for Cybersecurity* (ENISA), è avvenuto nel 2004[8], in risposta alla necessità di riunire in capo ad un unico attore la responsabilità di contribuire alla politica informatica dell'UE, di migliorare l'affidabilità dei prodotti e dei servizi, nonché di delineare una strategia di sicurezza comune tra gli Stati membri. Nel corso del tempo, si è assistito a un progressivo consolidamento del ruolo riconosciuto all'ENISA accompagnato da un notevole accrescimento delle sue competenze[9].

Tra le iniziative di maggiore rilevanza figura la Direttiva NIS (*Network And Information Security*)[10], adottata nel 2016 e attuata in Italia solamente nel 2018, che rappresenta il primo esempio di normativa "orizzontale" e, quindi, il primo tentativo di armonizzazione dei livelli di sicurezza dei sistemi informatici [21]. Sostanzialmente gli scopi perseguiti sono quelli di migliorare le capacità *cyber* degli Stati membri, rafforzare la cooperazione e promuovere una cultura di prevenzione degli incidenti e di gestione del rischio.

Con lo strumento giuridico della direttiva, l'Unione ha voluto garantire, mediante la previsione di obblighi di risultato che stabiliscono standard minimi, un livello omogeneo di sicurezza delle infrastrutture sull'intero territorio europeo. In particolare, la Direttiva NIS ha identificato, attraverso una classificazione, i soggetti destinatari della disciplina. Questi ultimi si articolano in due categorie specifiche: gli "operatori economici di servizi essenziali" (art. 5) e i "fornitori di servizi digitali" (FSD), ciascuno dei quali è soggetto a precisi obblighi volti all'implementazione di adeguate misure tecniche e organizzative adeguate, atte a prevenire gli incidenti informatici (art. 14 e ss.).

L'indiscussa rilevanza strategica della disciplina sulla *cybersecurity*, insieme alla crescente necessità di incrementare i livelli di sicurezza e di delineare un quadro armonizzato atto a coordinare le iniziative in questo contesto, hanno stimolato il legislatore europeo a intervenire, nel 2019, mediante lo strumento giuridico del regolamento, per assicurare la diretta applicabilità delle disposizioni su tutto il

[8] Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione e che attribuisce alla stessa il compito di contribuire ad assicurare un elevato livello di sicurezza delle reti nonché a promuovere una cultura in materia a vantaggio dei cittadini, dei consumatori, delle imprese e delle organizzazioni del settore pubblico nell'Unione europea, contribuendo in tal modo al buon funzionamento del mercato interno.

[9] Il ruolo dell'ENISA è stato rafforzato prima con il Regolamento (UE) n. 526/2013, poi con il Regolamento UE 2019/881 (c.d. Cybersecurity Act).

[10] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

territorio europeo. L'entrata in vigore dell'EU Cybersecurity Act (o Cyber Act)[11] ha non solo definito una cornice normativa europea più coincisa rispetto al passato, ma ha altresì prefissato l'ambizioso obiettivo di instaurare un mercato unico digitale più sicuro attraverso l'introduzione di un sistema europeo di certificazione dei prodotti e dei servizi. In questa prospettiva, il Cyber Act ha rafforzato il ruolo dell'ENISA, conferendole la funzione fondamentale di coordinamento attivo al fine di garantire un elevato e omogeneo livello di sicurezza informatica all'interno dell'Unione Europea.

La declinazione di principi comuni e di regole di policy sulla *cybersecurity* per favorire una risposta comune alle crisi determinate da diversi livelli di *cyber* resilienza tra gli Stati membri, ha trovato un primo vero momento di concretizzazione all'interno della Direttiva NIS 2 [12] e della proposta di Regolamento Cyber Resilience Act (CRA) [22], dalle quali emerge un approccio maggiormente proattivo rispetto al passato. Nel dicembre 2020 la Commissione europea ha proposto la NIS 2 [23], entrata in vigore a gennaio 2023, che mira a sostituire la precedente NIS del 2016, ritenuta ormai non più adeguata alle crescenti e mutevoli minacce cibernetiche. Con questa nuova disciplina è stato operato un ampliamento dell'ambito di applicazione degli obblighi e degli *standard* di sicurezza informatica, ora estesi a una porzione più ampia dell'economia, al fine di fornire una copertura completa dei settori e dei servizi ritenuti di vitale importanza per le principali attività sociali ed economiche nel mercato interno. Questa nuova Direttiva, orientata alla creazione di un quadro normativo più nitido rispetto al passato e alla promozione di una definizione più efficace degli aspetti operativi, assegna, mediante un approccio *top down* e di *hard rule*, specifici obblighi di gestione e segnalazione dei rischi di cybersicurezza (artt. da 17 a 23) e obblighi in materia di condivisione delle informazioni (artt. 26 e 27) a tutti gli operatori del settore. I soggetti destinatari di tali obblighi sono distinti tra "soggetti essenziali" e "soggetti importanti", a seconda del settore in cui esercitano la propria attività. A titolo esemplificativo, i primi sono coloro che nei settori dell'energia, trasporti, bancario e sanitario (ecc.)[13], mentre i secondi sono coloro che operano nei settori dei servizi postali, gestione rifiuti, fabbricazione, produzione e distribuzione (ecc.)[14]. La *ratio* di tale

[11] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il Regolamento (UE) n. 526/2013 («Regolamento sulla cibersicurezza»), che disciplina e rafforza il ruolo dell'ENISA riconoscendole la funzione fondamentale di coordinamento attivo al fine di garantire un elevato e omogeneo livello di sicurezza informatica all'interno dell'Unione. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32019R0881 (ultimo accesso novembre 2023).

[12] Direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la Direttiva (UE) 2016/1148. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32022L2555 (ultimo accesso novembre 2023).

[13] Allegato I della Proposta di Direttiva NIS 2.

[14] Allegato II della Proposta di Direttiva NIS 2.

categorizzazione risiede nell'intenzione di evitare di sottoporre indifferentemente tutti gli operatori all'interno di un unico quadro di obblighi e doveri, proponendo invece un regime differenziato[15] che tenga conto del rischio che certi settori, proprio in virtù dell'attività svolta, potrebbero subire conseguenze più gravi in caso di violazioni della sicurezza. È proprio da questo ragionamento che nasce l'approccio di una regolazione del rischio.

La Direttiva NIS 2 manifesta chiaramente una duplice volontà del legislatore che, da un lato, interviene con una disciplina più chiara e uniforme identificando esplicitamente gli obblighi applicabili a tutti i destinatari e, dall'altro, riserva loro una sfera di autonomia. In particolare, gli operatori del settore beneficeranno del vantaggio di poter individuare, sulla base delle loro attività svolte e della conoscenza dei rischi ad esse connessi, gli ambiti prioritari su cui intervenire per colmare le lacune di sicurezza e ridurre le vulnerabilità a cui rimarrebbero altrimenti esposti. Questo processo li indurrà a adottare misure tecniche proporzionate e adeguate, nonché ad assumere una maggiore responsabilità in considerazione del regime di vigilanza a cui sono assoggettati e delle corrispondenti misure sanzionatorie.

Al fine di salvaguardare i consumatori e le imprese anche da prodotti digitali caratterizzati da livelli di sicurezza inadeguati e insufficienti, la Commissione europea, come già anticipato, ha fatto nuovamente ricorso allo strumento del Regolamento presentando il 15 settembre 2022, il Cyber Resilience Act (c.d. CRA)[16]. Con questa proposta, il legislatore europeo ha delineato un quadro dettagliato di obblighi e requisiti orizzontali di cybersicurezza, ai quali i soggetti destinatari, ossia i produttori e i fornitori, sono tenuti a adeguarsi a seconda dei prodotti con elementi digitali che intendono introdurre nel mercato interno[17].

---

[15] Per ciò che concerne invece l'approccio regolamentare e, quindi, la scelta concreta delle misure di mitigazione del rischio – che la Direttiva NIS 2 lascia in mano ai soggetti regolati (modello *bottom-up* e *co-regulation*) – si distingue la previsione di intervenire *ex ante* ed *ex post* per i soggetti essenziali e, unicamente, *ex post* per i soggetti importanti. Conseguentemente sono previsti due differenti sistemi di supervisione da parte delle Autorità competenti, da un lato, uno più stringente e proattivo mentre, dall'altro lato, uno più leggero e reattivo. Ad esempio, la classificazione dei soggetti è significativa al fine di prescrivere quando debba intervenire la scelta, da parte dei soggetti regolati, in ordine alle misure da applicare – se in via preventiva o se in via successiva – e, inoltre, al fine di assoggettare i destinatari ad un regime di vigilanza più o meno stringente a seconda dell'attività svolta.

[16] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454 (ultimo accesso novembre 2023).

[17] Infatti, a differenza della Direttiva NIS 2, il CRA fissa regole orizzontali, direttamente applicabili agli Stati membri, sull'immissione e sull'utilizzo di sistemi e prodotti con elementi digitali nel mercato dell'Unione. Ciò avviene mediante un approccio proporzionato basato sul rischio che prevede, similmente a quanto previsto dalla NIS 2, requisiti essenziali di sicurezza informatica che i prodotti digitali devono possedere (Allegato I, sez. 1), requisiti di gestione della vulnerabilità che i produttori devono rispettare (Allegato I, sez. II) e informazioni e istruzioni minime che devono essere fornite agli utenti con riferimento ai prodotti immessi sul mercato (Allegato II).
L'oggetto della regolazione nel CRA, a differenza della NIS 2 (che individua regole e requisiti facendo riferimento ai settori in cui gli operatori svolgono le proprie attività), riguarda nello specifico i "prodotti

La distinzione degli obblighi e dei requisiti operata a monte dal legislatore, prende atto non solo della categoria generale dei settori in cui agiscono i destinatari, quanto piuttosto della specificità dei prodotti con elementi digitali introdotti nel mercato. Questo approccio mira a creare le condizioni per lo sviluppo di prodotti con elementi digitali sicuri sin dalle fasi iniziali del ciclo di vita del prodotto. In ragione di questo principio (della *security by design*) è richiesto agli operatori del settore di agire in modo preventivo (*ex ante*), eliminando, sin dalle prima fasi di progettazione e produzione dei prodotti con elementi digitali, le vulnerabilità e i pericoli ad essi associati.

La scelta della fonte regolamentare sottostà alla volontà politica di istituire nuove regole uniformi a livello europeo, finalizzate ad aumentare il grado di fiducia tra gli utenti e promuovere l'attrattiva dei prodotti con elementi digitali provenienti dall'UE. Questo approccio implica un potenziamento del principio di proporzionalità delle misure tecniche, poiché gli operatori del settore saranno tenuti a implementare, in base al livello di rischio associato ai loro prodotti e già individuato dalla normativa, misure tecniche proporzionate e adeguate. Ciò determinerà altresì un ampliamento del principio di *accountability* degli operatori, i quali, nel conformarsi ai requisiti stabiliti dal legislatore, assumeranno la responsabilità del proprio operato.

Anche i sistemi informatici aziendali si trovano in una crescente condizione di vulnerabilità nei confronti di possibili attacchi informatici. Per tale ragione, il 14 dicembre 2022, il Parlamento europeo ha approvato un ulteriore Regolamento, denominato Digital Operational Resilience Act (c.d. DORA)[18] che definisce un *framework* comune di resilienza operativa digitale per tutti gli operatori del settore finanziario vincolandoli al rispetto di una serie di requisiti di sicurezza informatica.

Sulla base di tali fondamenta, si è sviluppata successivamente la legislazione nazionale in materia di cybersicurezza.

---

con elementi digitali" che l'art. 3 definisce come "qualsiasi prodotto che preveda almeno una componente digitale e che, anche solo potenzialmente, si connetta a Internet". In particolare, l'Allegato III effettuata una classificazione dei c.d. "critical products with digital elements" sulla base di due classi di rischio: quelli definiti a rischio moderato che rientrano nella "Class I" (password, software di condivisione, sistemi non rientranti nell'alto rischio) e quelli definiti a rischio elevato che rientrano nella "Class II" (cripto processori, chiavi pubbliche, certificatori, mobile devices).
A seconda dei prodotti coinvolti nelle attività dei produttori, fornitori e distributori, essi devono rispettare obblighi e doveri diversificati: meno stringenti nel caso di prodotti a rischio moderato, poiché gli operatori sono assoggettati ad un regime di autocertificazione vincolata al rispetto di standard di trasparenza finalizzata a garantire la conformità di tali prodotti alle regole di sicurezza; più stringenti nel caso di prodotti a rischio elevato che, per essere immessi nel mercato, devono rispettare una serie di requisiti obbligatori orizzontali per garantire una maggiore affidabilità nonché seguire le procedure di valutazione della conformità affidate, diversamente dall'altra categoria, ad un ente esterno. Invece, per i prodotti digitali classificati come sistemi di IA, previsti dall'art. 15 dell'AI ACT, l'art. 8 del CRA prevede una presunzione di conformità ai requisiti di sicurezza informatica e, dunque, sono prodotti esentati dal rispetto dei requisiti sopra descritti.

[18] Regolamento (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario. Consultabile al seguente indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554 (ultimo accesso novembre 2023).

3.2. L'ordinamento nazionale

L'Italia, sulla base del quadro normativo previsto dall'Unione europea, si è dotata di una cospicua normativa volta a disciplinare il settore della cybersicurezza.

In evidente ritardo rispetto agli altri Paesi, nel 2013 è stata formulata una prima architettura della sicurezza cibernetica nazionale mediante il DPCM del 24 gennaio 2013 (c.d. Decreto Monti)[19]. Il DPCM ha delineato «l'architettura istituzionale deputata alla sicurezza nazionale […] con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionale» assegnando a questo scopo compiti spesso strettamente complementari a vari attori istituzionali (Presidente del Consiglio dei ministri, Comitato Interministeriale per la Sicurezza della Repubblica, Dipartimento delle Informazioni per la Sicurezza, Nucleo per la Sicurezza Cibernetica) rendendo perciò indispensabile l'instaurarsi di numerose interazioni reciproche tra gli stessi.

Il panorama normativo nazionale ha poi subito modifiche nel 2017 con l'emanazione di un nuovo DPCM (c.d. Decreto Gentiloni)[20], che ha delineato i nuovi assetti organizzativi dell'architettura nazionale di *cybersecurity* e ha introdotto una Strategia nazionale in materia mediante l'adozione del nuovo Piano Nazionale[21], che aggiorna i provvedimenti del dicembre 2013.

Per il primo intervento di rango primario, invece, si è dovuto attendere il 2018, con l'emanazione del d.lgs. 65/2018 (c.d. d.lgs. NIS)[22]. Con questo atto l'Italia, in recepimento della Direttiva NIS, ha rafforzato il proprio quadro normativo in materia di *cybersecurity* attraverso l'istituzione del Perimetro di sicurezza nazionale cibernetica, oltre l'adozione di una Strategia nazionale di sicurezza cibernetica da parte del Presidente del Consiglio dei ministri[23].

---

[19] Decreto del Presidente del Consiglio dei ministri, 24 gennaio 2013, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale, attraverso il quale è stata delineata una prima architettura della materia fondata su due distinti documenti: il "Quadro strategico nazionale per la sicurezza dello spazio cibernetico" e il "Piano nazionale per la protezione cibernetica e la sicurezza informatica". Consultabile al seguente indirizzo: https://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg (ultimo accesso novembre 2023).

[20] Decreto del Presidente del Consiglio dei ministri, 17 febbraio 2017, Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali. Consultabile al seguente indirizzo: https://www.gazzettaufficiale.it/eli/id/2017/04/13/17A02655/sg (ultimo accesso novembre 2023).

[21] È stata comunicata sulla Gazzetta ufficiale n. 125 del 31 maggio 2017 l'adozione del nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica. Consultabile al seguente indirizzo: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf (ultimo accesso novembre 2023).

[22] Convertito con modificazioni dalla legge 4 agosto 2021, n. 109.

[23] Questa Strategia è orientata alla definizione di misure che riguardano la preparazione, risposta e recupero dei servizi a seguito di incidenti informatici. Essa comprende la formulazione di un piano di valutazione dei rischi informatici e l'implementazione di programmi volti a fornire formazione e sensibilizzazione nel campo della sicurezza informatica. Parallelamente, è previsto un piano complessivo di valutazione dei rischi che include anche l'ambito della ricerca e dello sviluppo nel contesto della cybersicurezza.

Al d.lgs. NIS ha fatto seguito il d.l. 21 settembre 2019, n. 105[24] che ha definito il Perimetro di sicurezza nazionale cibernetica [24] al fine di garantire un elevato livello di sicurezza delle reti, dei sistemi e dei servizi informatici delle amministrazioni pubbliche nonché degli enti e degli operatori sia pubblici che privati.

Sul piano del diritto, pertanto, si riscontra una continua evoluzione della cornice normativa, a cui si aggiungono il d.l. 14 giugno 2021, n. 82[25] e alcuni specifici commi della l. n. 197/2022[26].

Il d.l. 14 giugno 2021, n. 82 mira a rafforzare le misure a tutela della sicurezza mediante l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN), il Comitato interministeriale per la cybersicurezza (CIC) e il Nucleo per la cybersicurezza, al quale è conferito il ruolo di coadiuvare il Presidente del Consiglio dei ministri in materia di prevenzione di eventuali crisi o attacchi *cyber.* L'ACN assume la responsabilità di tutelare la sicurezza nazionale, inclusa quella nello spazio cibernetico, e dispone di funzioni di coordinamento tra le altre Autorità competenti nel settore e di predisposizione della Strategia nazionale di cybersicurezza. Al CIC sono attribuite funzioni di sorveglianza sull'attuazione della suddetta Strategia e di supporto alle politiche della Presidenza del Consiglio dei ministri nell'ambito del Perimetro di sicurezza. Infine, al Nucleo per la cybersicurezza è conferito il ruolo di coadiuvare il Presidente del Consiglio dei ministri nella prevenzione di eventuali crisi o attacchi *cyber.*
I commi da 899 a 902 della legge n. 197/2022 danno attuazione alla Strategia nazionale di cybersicurezza, formalmente adottata mediante DPCM in data 17 maggio 2022, e rendono effettivo il relativo piano di implementazione istituendo nel bilancio del Ministero dell'Economia e delle Finanze specifici Fondi.

Nella prospettiva di garantire infrastrutture tecnologiche adeguate alle sfide emergenti dalla digitalizzazione, la cybersicurezza assume un ruolo fondamentale anche all'interno del Piano Nazionale di Ripresa e Resilienza (PNRR)[27], specie nella Missione 1 incentrata sulla "Digitalizzazione, innovazione, competitività, cultura e turismo"[28]. La *cybersecurity*, infatti, costituisce, di fatto, la

[24] Convertito con modificazioni dalla legge 18 novembre 2019, n. 133.
[25] Convertito con modificazioni dalla legge 4 agosto 2021, n. 109. Il testo della legge è consultabile al seguente indirizzo: https://www.gazzettaufficiale.it/eli/id/2021/08/04/21G00122/SG (ultimo accesso novembre 2023).
[26] Legge 29 dicembre 2022, n. 197, Bilancio di previsione dello Stato per l'anno finanziario 2023 e bilancio pluriennale per il triennio 2023-2025, commi da 899 a 902. Al fine di implementare la Strategia nazionale di cybersicurezza, formalmente adottata mediante decreto del Presidente del Consiglio dei ministri in data 17 maggio 2022, e per concretizzare il relativo piano di implementazione, sono stati istituiti nel bilancio specifici Fondi.
[27] Trasmesso alla Commissione europea il 30 aprile 2021.
[28] Le iniziative in corso e quelle attuate comprendono l'investimento specifico sulla cibersicurezza (M1C1), la M1C1-5 per l'istituzione dell'Agenzia per la cybersicurezza nazionale e l'adozione del relativo regolamento (MITD).
Le attuali iniziative e quelle già attutate comprendono un investimento specifico in cybersecurity (M1C1, investimento 1.5). Inoltre, sono in corso di attuazione interventi quali la transizione verso l'ambiente cloud, l'integrazione di servizi digitali come pagoPA, le attività rivolte alla cibersicurezza e quelle volte allo sviluppo delle competenze digitali (M1C1, investimenti 1.1, 1.2, 1.7).

prima delle sei missioni delineate nel PNRR e ad essa sono pertanto destinate ingenti risorse finanziarie. Per il perseguimento degli obiettivi di digitalizzazione, il PNRR destina un importo pari a 40,29 miliardi di euro, corrispondenti a circa il 21,05% dell'importo totale del Piano. In particolare, nella sezione "Digitalizzazione, innovazione e sicurezza nella PA", è previsto un investimento specifico dedicato alla cybersicurezza pari a 623 milioni di euro, con cui viene sottolineata la necessità di incrementare le capacità *cyber* nazionali anzitutto attraverso la piena attuazione della disciplina in materia di Perimetro di sicurezza nazionale cibernetica. Questi finanziamenti sono indirizzati a quattro aree di intervento: al rafforzamento delle capacità di prevenzione dagli attacchi informatici e della gestione degli allarmi, allo sviluppo di più avanzate capacità tecniche di valutazione per un'erogazione dei servizi sempre più sicura, nonché all'aumento del personale dedicato alla prevenzione e all'indagine del crimine informatico.
Dal quadro normativo nazionale richiamato, emerge una progressiva tendenza dell'ordinamento italiano verso un approccio sempre più incisivo in materia di cybersicurezza, in linea con la cornice eurounitaria.

Data la complessità intrinseca del panorama offerto dalla *cybersecurity* si rivela essenziale, in punto di attuazione che i legislatori – prima europeo e poi nazionale – intervengano attraverso forme di regolazione efficaci ma soprattutto flessibili, in grado cioè di adattarsi ai rapidi progressi tecnologici. Tuttavia, la continua proliferazione di norme rischia di generare un quadro normativo intricato e variegato che, oltre a non facilitare una lettura unitaria degli obblighi e dei doveri, determina una disparità di livelli di cyber-resilienza tra gli Stati membri.

In tale scenario, l'elaborazione della Strategia europea dovrebbe favorire e promuovere, nel tentativo di stabilire principi e regole comuni e condivise, un maggior coordinamento tra gli Stati membri e garantire così un funzionamento più efficiente del mercato attraverso la creazione di un *framework* di cybersicurezza coerente e uniforme.

4. Il ruolo del fattore umano

In conclusione occorrerà ricondurre l'attenzione al "fattore umano".

Non vi sarà mai un sistema tecnico così perfetto o una regolazione talmente efficace da poter sostituire la responsabilità umana nell'uso della tecnologia.

Invero, nel settore della *cybersecurity* alla centralità assunta dalla tecnologia deve necessariamente affiancarsi il ruolo del fattore umano. Occorre ricordare, infatti, che la questione della sicurezza informatica coinvolge anzitutto i comportamenti delle persone e, di conseguenza, richiede un adeguato livello di conoscenza e di consapevolezza che dovrebbe caratterizzare l'agire umano nel mondo digitale. Il primo elemento che ci espone a un possibile uso criminale delle tecnologie è proprio rappresentato dall'ignoranza spesso impieghiamo questi strumenti. La diffusa consuetudine nell'utilizzo dei sistemi informatici, infatti, non implica automaticamente la conoscenza dei rischi e delle vulnerabilità ad essi associati [25]. È proprio in ragione di questa scarsa consapevolezza dei rischi e della

conseguente fragilità nelle difese che l'utente finale rappresenta un appetibile punto di accesso per gli attacchi informatici. L'attacco alla Regione Lazio che abbiamo esaminato costituisce un esempio che mette in luce in maniera inequivocabile come i comportamenti umani rivestano un ruolo cruciale nel determinare l'esito di un'aggressione, specialmente laddove siano impiegate tecniche di *phishing* per inoculare *malwares* nei sistemi informatici. Dal caso appena citato emerge chiaramente che gli elementi che possono compromettere la sicurezza informatica di un sistema sono, da un lato, gli stessi strumenti informatici, i quali possono manifestare vulnerabilità connesse alla loro infrastruttura o al loro funzionamento, e, dall'altro, l'errato o inconsapevole uso umano di tali strumenti.

Il fattore umano spesso rappresenta addirittura l'elemento determinante del successo dell'attacco informatico. A titolo esemplificativo, si possono considerare i risultati emersi dallo studio condotto nel quadro del progetto europeo Dogana [26][29]. Questi dati indicano che solo nel 3% dei casi il successo degli attacchi informatici può essere attribuito a vulnerabilità di natura tecnica, mentre nel restante 97%, l'esito positivo non è tanto correlato a falle nei sistemi informatici, quanto piuttosto alla fragilità e all'ingenuità delle persone (*social engineering*[30]). Il motivo per cui gli utenti risultano spesso bersagli o mezzi attraverso i quali sferrare gli attacchi informatici può essere attribuito alla facilità con cui possono essere ingannati e indotti a compiere azioni che, in modo inconsapevole, agevolano il successo dell'aggressione. Questo rischio sarebbe notevolmente ridotto se ciascun fruitore sviluppasse una maggiore consapevolezza e una più acuta percezione delle minacce che quotidianamente è possibile incontrare in rete.

Alcune buone pratiche attraverso le quali potremmo contribuire personalmente alla sicurezza dei nostri dati e alla tutela del nostro supporto informatico potrebbero essere, per citarne alcune: l'impiego di procedure di autenticazione robuste, l'implementazione di codici di accesso complessi, la configurazione di parametri di autorizzazione restrittivi, l'adozione di un sistema di *backup* e l'installazione di *antivirus* e *firewall*.

La mancata adozione di precauzioni elementari può essere imputata alla combinazione di diversi fattori, fra i quali spicca l'insufficiente educazione digitale, ossia l'assenza di adeguate competenze digitali di base. Per mitigare l'incidenza del fattore umano sui rischi associati alla *cybersecurity* è quindi essenziale investire nella alfabetizzazione digitale e nella formazione delle persone. Per raggiungere tale obiettivo è indispensabile sottolineare e riconoscere che il dominio della sicurezza informatica non può essere esclusivamente ancorato

[29] L'autore, Pier Luca Montessoro, a pp. 791-794, durante l'analisi del ruolo fattore umano nella *cybersecurity*, cita lo studio svolto nell'ambito del progetto Dogana.
[30] Basti pensi agli attacchi realizzati attraverso la tecnica del *phishing* e al fenomeno crescente detto *man-in-the-mail*, trattasi di una sofisticata manovra di attacco informatico in cui un individuo si insinua fraudolentemente nei trasferimenti di dati tra due parti, acquisendo, in modo clandestino, le informazioni tra le due parti al fine di accedere a informazioni riservate della vittima.

all'ambito tecnico, vale a dire ai vincoli normativi, ma richiede altresì un'indispensabile assunzione di consapevolezza proattiva in merito ai rischi connessi all'uso degli strumenti informatici. Questa epifania non deve limitarsi alla mera adozione di pratiche elementari di precauzione digitale e buone consuetudini di sicurezza informatica, ma deve estendersi anche all'allocazione di risorse verso programmi e iniziative finalizzate a promuovere una maggiore sensibilizzazione verso la cybersicurezza e a fornire agli utenti una formazione adeguata su come affrontare le minacce riscontrabili online.

5. Conclusione: rispetto delle regole e maggiore pedagogia digitale

L'esponenziale utilizzo di strumenti informatici, l'incessante evoluzione digitale, la crescente interconnessione e l'innegabile aumento degli attacchi cibernetici hanno rappresentato e rappresentano il cuore del dibattito in materia di *cybersecurity*.

Come è stato osservato la regolazione di questo settore e la necessità di affrontare l'incidenza del fattore umano sono questioni complesse e sfidanti. Da un lato perché la natura mutevole della tecnologia richiede una regolazione flessibile e adattabile; dall'altro perché, nonostante la predisposizione di regole e i continui progressi tecnologici, le azioni umane spesso continuano a compromettere la sicurezza delle infrastrutture. Il dato su questo punto è, per certi versi, sconfortante. Secondo l'indice DESI (*Digital Economy and Society Index*)[31] del 2022, basato sui dati dell'anno 2021, l'Italia, con riferimento alle competenze digitali di base, si colloca al 25° posto su 27 Stati membri dell'UE.
Parallelamente alla necessità di un impianto normativo robusto diventa, dunque, indispensabile l'elaborazione di programmi di educazione e formazione digitale, poiché altrimenti nessuna regola, per quanto rigorosa, potrà mai garantire la sicurezza se gli utenti non raggiungono un sufficiente grado di consapevolezza delle minacce informatiche.

Bibliografia

[1] Wiener, N. (1948). Cybernetics or Control and Communication in the Animal and the Machine. Cambridge.

Simoncini, A. (2019). "L'algoritmo incostituzionale: intelligenza artificiale il futuro della libertà", in BioLawJournal, 1, pp. 63 ss.; Frosini, V. (1968). Cibernetica e diritto. Edizioni di Comunità.

[31] Il Digital Economy and Society Index è uno strumento utilizzato dall'Unione Europea per valutare e confrontare il grado di digitalizzazione dei paesi membri in vari settori, tra cui l'educazione digitale. Questo indice considera diversi parametri, tra cui la connettività, le competenze digitali, l'uso di internet e servizi pubblici digitali. Il testo del 2022 è consultabile al seguente indirizzo: https://digital-strategy.ec.europa.eu/it/policies/desi (ultimo accesso novembre 2023).

[2] Micklitz, H.W., Pollicino, O., Reichman, A., Simoncini, A., Sartor, G., De Gregorio, G. (2021). Constitutional Challenges in the Algorithmic Society. Cambridge University Press.

[3] Floridi, L. (2015). The onlife Manifesto: Being Human in a Hyperconnected Era. Springer.

[4] Simoncini, A. (2021). "L'uso delle tecnologie nella pandemia e le nuove diseguaglianze", in Violante, L. e Pajano, A. Biopolitica, pandemia e democrazia. Rule of law nella società digitale. Il Mulino, pp. 225 ss.

[5] Resta, G. (2015). "La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE", in Diritto dell'informazione e dell'informatica, 4-5, pp. 697 ss.

Ziccardi, G. (2015). Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica. Giuffrè.

Rodotà, S. (1982). "Tecnologie dell'informazione e frontiere del sistema socio-politico", in Pol. dir., pp. 28 ss.

Rodotà, S. (1973). Elaboratori elettronici e controllo sociale, Il Mulino.

[6] Ziccardi, G.; Perri, P. (2019). Tecnologia e diritto (vol. III). Sorveglianza, segreto, controllo, cybersecurity, crimini informatici, cyberterrorismo, guerra dell'informazione, odio online. Giuffrè.

Ziccardi, G. (2015) Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica. Raffaello Cortina.

[7] De Vergottini, G. (2019). "Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normatizzata", in Rivista AIC, 4, pp. 65 ss.

[8] Finocchiaro, G. (2012). Privacy e protezione dei dati personali. Zanichelli.

Busia, G.; Liguori, L.; Pollicino, O. (2016). Le nuove frontiere della privacy nella tecnologia digitale. Aracne.

Zeno-Zencovich, V. (2018). "Data protection in the Internet", in Annuario di diritto comparato e di studi legislativi, pp. 431 ss.

[9] Brandeis, L.; Warren, S. (1890). "The Right to Privacy", in Harvard Law Review, pp. 193 ss.

Rodotà, S. (1973). Elaboratori elettronici e controllo sociale, Bologna, pp. 78 ss.

Rodotà, S. (1982). "Tecnologie dell'informazione e frontiere del sistema socio-politico", in Pol. dir., pp. 28 ss.

[10] Porcedda, M.G. (2023). Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis, Oxford.

[11] Maurino, M. (2023). "Cybersecurity, sicurezza nazionale e trattamento dei dati personali", in Ursi, R., La sicurezza nel cyberspazio, Franco Angeli, pp. 169 ss.

[12] Orofino, M. (2022). "Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione", in MediaLaws, 2, pp. 82 ss.

Brighi, R. (2021). “Cybersecurity. Dimensione pubblica e privata della sicurezza dei dati”, in Casadei, T.; Pietropaoli, S., Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali, CEDAM, pp. 135 ss.

[13] Busia, G. (2020). “Cybersecurity: una sfida per tutti”, in A. Contaldo, D. Mula, Pisa, Cybersecurity Law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche, pp. IX-XVI.

[14] Simoncini, A. (2019). “L’algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà”, in BioLawJournal, pp. 87 ss.

[15] Bruno, B. (2020). “La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell’Unione Europea”, in Federalismi.it, 14, pp. 11 ss.

[16] Pietropaoli, S. (2022). Informatica criminale. Diritto e sicurezza nell’era digitale. Giappichelli.

[17] Longo, E.; (in corso di pubblicazione). “La sicurezza nel ciberspazio. La disciplina della cybersecurity nell’Unione europea e in Italia”.

Cassano, G.; Iaselli, M.; Spangher, G.; (2022). “Cybersecurity: contesto normativo di riferimento a livello nazionale ed europeo”, in Dir. internet, 4, pp. 637 ss.

Renzi, A. (2021). “La sicurezza cibernetica: lo stato dell’arte”, in Giorn. di dir. amm., 4, pp. 538 ss.

[18] De Gregorio, G.; Dunn, P.; (2022) “The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age”, in Common Market Law Review, pp. 473 ss.

[19] Maglio, M. (2017), “Cybersecurity e dati personali”, in Maglio, M.; Polini, M.; Tilli, N.; Manuale di diritto alla protezione dei dati personali, pp. 719 ss.

[20] Cencetti, C. (2014). “Cybersecurity: Unione europea e Italia. Prospettive a confronto”. Edizioni Nuova Cultura.

Contaldo, A.; Peluso, F. (2018). “Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS”. Pacini Editore.

[21] Salandri, L.; Contaldo, A. (2016) “La nuova disciplina giuridica cd. “orizzontale” della cybersicurezza per le infrastrutture in un’ottica di sviluppo dei sistemi”, in Rivista amministrativa della Repubblica Italiana, 11-12, pp. 567 ss.

[22] Chiara, P.G. (2023). “Il “Cyber Resilience Act”: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cybersicurezza per prodotti con elementi digitali”, in Riv. it. inf. dir., 1, pp. 143 ss.

[23] Bavetta, F. (2023). “Direttiva NIS 2: verso un innalzamento dei livelli di cybersicurezza a livello europeo”, in MediaLaws. Rivista di diritto dei media, 3, pp. 405 ss.

[24] Poletti, S. (2023). “La sicurezza cibernetica nazionale ed europea, alla luce della creazione del perimetro di sicurezza nazionale cibernetica”, in MediaLaw, Rivista di diritto dei media, 2, pp. 398 ss.

Mele, S. (2020). “Il Perimetro di Sicurezza Nazionale Cibernetica”, in Diritto di internet, 1, pp. 15 ss.

[25] Montessoro, P. L. (2019). “Cybersecurity: conoscenza e consapevolezza come prerequisiti per l’amministrazione digitale”, in Istituzioni del federalismo, 3, pp. 783 ss.

BIOGRAFIE

Andrea Simoncini è professore ordinario di Diritto costituzionale presso l’Università degli Studi di Firenze dove ha ricoperto anche il ruolo di Direttore del Dipartimento di Scienze giuridiche. I suoi principali interessi di ricerca spaziano dai temi legati al diritto costituzionale italiano ed europeo alle fonti del diritto, al rapporto tra tecnologia e diritti costituzionali, al diritto ambientale, i diritti sociali e le relazioni tra il diritto naturale e il diritto positivo. È membro del comitato scientifico della Fondazione Security and Rights in the Cyberspace (SERICS) nonché Principal Investigator del progetto Law and regulation for a better-safe Cyberspace (CYBERIGHTS).

E-mail: andrea.simoncini@unifi.it

Federica Camisa è dottoranda di ricerca in Diritto pubblico presso l’Università degli Studi di Firenze e abilitata all’esercizio della professione forense. Ha frequentato il Seminario di Studi e Ricerche Parlamentari “Silvano Tosi” a seguito del quale ha svolto uno *stage* presso la Presidenza del Consiglio dei ministri. Le sue ricerche sono principalmente rivolte all’analisi del rapporto tra diritto e nuove tecnologie ed è attualmente impegnata nello studio delle interconnessioni tra ambiente e tecnologia. Si interessa inoltre di cybersecurity, privacy e Metaverso.

E-mail: federica.camisa@unifi.it