

L'approccio alla Cybersecurity nello scenario normativo europeo

The EU's regulatory approach to Cybersecurity

Valentina Amenta[♦], Rosaria Deluca[♦]

♦ Consiglio Nazionale delle Ricerche, Istituto di Informatica e Telematica, Unità Aspetti Legali e Contenzioso del Registro. it

Sommario

L'utilizzo dei dispositivi connessi a internet è ormai divenuto il paradigma socio-culturale della società in cui stiamo vivendo. Tuttavia, se da un lato dobbiamo riconoscere a queste tecnologie il valore di costituire un valido strumento di ausilio per le aziende e per il cittadino, non possiamo sottovalutare il rischio di esposizione agli attacchi cyber dei sistemi informatici riguardo alla gestione dei propri dati. Con questo lavoro abbiamo voluto focalizzare l'attenzione sulla normativa europea in materia di cybersecurity per comprendere gli obiettivi che stanno alla base della risposta dell'Unione europea agli attacchi cyber che potrebbero compromettere la competitività e la fiducia dei cittadini, in un mercato in continua evoluzione. In particolare, abbiamo analizzato la Direttiva (UE) 2016/1148 (NIS), la Direttiva (UE) 2055/2022 (NIS 2) e il Regolamento UE 2019/881 (Cybersecurity Act), infine il Regolamento UE 2016/679 in materia di protezione dei dati personali (GDPR) poiché non possiamo escludere che le minacce alla sicurezza informatica possano comportare, come effetto, un trattamento illecito di dati personali, impattando negativamente sui diritti e le libertà delle persone. Completano lo scenario normativo alcune considerazioni in merito alla recente approvazione da parte del Parlamento europeo del Regolamento sull'Intelligenza Artificiale (Artificial Intelligence Act) e all'accordo provvisorio sulla proposta di regole comuni di cybersecurity per i produttori e gli sviluppatori di prodotti con elementi digitali (Cyber Resilience Act).

Abstract

The use of devices connected to the internet is the socio-cultural paradigm of our society. However, we cannot underestimate the risk of exposure to cyber-attacks on computer

systems regarding the management of the data of companies and citizens. In this work, we focus our attention on European legislation on cybersecurity. We aim to understand the objectives underlying the European Union's response to cyber-attacks, as they could compromise competitiveness and citizens' trust in a constantly evolving market. We analyzed Directive (EU) 2016/1148 (NIS), Directive (EU) 2022/2555 (NIS 2) and EU Regulation 2019/881 (Cybersecurity Act), finally EU Regulation 2016/679 about protection of personal data (GDPR) as we cannot exclude that threats to IT security may result in the illicit processing of personal data, negatively impacting people's rights and freedoms. The regulatory scenario is completed by some considerations regarding the recent approval by the European Parliament of the Regulation on Artificial Intelligence (Artificial Intelligence Act) and the provisional agreement on the proposal for common cybersecurity rules for producers and developers of products with digital elements (Cyber Resilience Act).

Keyword

cybersecurity, cyber attack, accountability.

1 - Introduzione

Negli ultimi anni, stiamo assistendo ad una rapida evoluzione delle moderne tecnologie che percorre trasversalmente ogni ambito della nostra vita quotidiana rivoluzionando ogni sistema e settore, sociale, economico e culturale. In questo nuovo contesto, amplificato dall'esplosione dell'utilizzo dell'intelligenza artificiale, gli attacchi cyber sono divenuti sempre più frequenti e sofisticati, costituendo una minaccia crescente per i cittadini e per le aziende informatiche di tutto il mondo. Di fronte alla complessità di questo fenomeno, è stata avvertita, a livello europeo, l'esigenza di cooperare per definire e armonizzare un quadro giuridico di regole per rafforzare la sicurezza informatica e fornire sostegno alle aziende e ai cittadini arricchendone le competenze e riducendone al tempo stesso il divario, affinché gli stessi possano beneficiare dei vantaggi della tecnologia e migliorare la competitività sul mercato. Tali regole dovranno quindi indirizzare e guidare le aziende nell'implementazione e nella gestione delle tecnologie in modo da renderle funzionali al contesto in cui si applicano.

D'altro canto, poiché l'efficienza di una tecnologia non può prescindere dall'utilizzo che ne viene fatto, anche le aziende dovranno impegnarsi per garantire che vengano applicate in maniera corretta.

2 – La Direttiva NIS

La direttiva NIS 2016/1148 (Security of Network and Information systems), entrata in vigore il 16 luglio 2016 [1], è stata il primo atto legislativo dell'Unione europea in materia di cybersecurity con l'obiettivo di accrescere la collaborazione transfrontaliera, armonizzare le competenze professionali e rafforzare il controllo dei settori critici. Più specificamente, la NIS rappresenta il primo tentativo di rafforzare il livello globale di cybersicurezza tra gli Stati membri e di determinare una base di garanzie destinate a sviluppare un ecosistema di fiducia soprattutto per quelle aziende che forniscono servizi essenziali per il mantenimento di attività sociali ed economiche fondamentali che dipendono dalla rete e dai sistemi informativi e per i quali un incidente informatico avrebbe effetti negativi rilevanti sulla comunità.

I settori che rientrano nell'ambito di applicazione della direttiva NIS riguardano l'energia, i trasporti, le banche, i mercati finanziari, la sanità, la fornitura e la distribuzione di acqua potabile, le infrastrutture digitali, i motori di ricerca, i servizi cloud e le piattaforme di commercio elettronico. Altresì, la direttiva NIS consente agli Stati membri di estendere l'ambito di applicazione delle proprie disposizioni anche a settori diversi da quelli elencati nella stessa.

Le strategie nazionali, che ogni Paese dell'Unione deve adottare per il conseguimento e il mantenimento di un livello elevato di sicurezza, disciplinano un quadro di governance per conseguire gli obiettivi e le priorità della strategia, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti; devono essere indicate le misure di preparazione, risposta e recupero scelte dagli Stati, inclusa la collaborazione tra settore pubblico e settore privato, ed i programmi di formazione, sensibilizzazione e istruzione relativi

alla strategia in materia di sicurezza delle reti e dei sistemi informativi¹. Inoltre, è necessario che gli Stati individuino piani di ricerca e sviluppo relativi alla strategia da adottare, che sia elaborato un piano di valutazione dei rischi, e che sia previsto un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale. A tali scopi, gli Stati membri possono richiedere l'assistenza dell'ENISA (Agenzia dell'Unione Europea per la Cybersecurity) nello sviluppo delle strategie nazionali in materia di sicurezza delle reti e dei sistemi informativi. In ambito europeo, il ruolo di ENISA è fondamentale perché la sua missione è proprio quella di migliorare la sicurezza informatica e delle reti di telecomunicazioni dell'Unione europea². Dal 2012, infatti, l'ENISA sostiene gli Stati nello sviluppo, nell'attuazione e nella valutazione delle loro strategie nazionali in materia di cybersicurezza.

Grazie al dettato della NIS, l'ENISA ha visto accresciuto il proprio ruolo di assistenza agli Stati membri e al Gruppo di cooperazione nei loro compiti. Difatti, questa, oltre ad aiutare i Paesi dell'Unione ad affrontare le questioni comuni di cybersicurezza e a concordare gli approcci e le procedure comuni da seguire, individua le buone pratiche negli Stati membri per quanto riguarda l'attuazione della direttiva NIS sviluppando modelli e strumenti atti allo scopo³.

3 – Il Cybersecurity Act

Il Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio del 17 aprile 2019, cosiddetto Cybersecurity Act, entrato in vigore il 27 giugno 2019 [2], è, in quanto tale, immediatamente esecutivo in tutti gli Stati membri senza necessità di interventi attuativi da parte dei legislatori nazionali; la normativa individua il sistema di certificazione europeo per la sicurezza informatica dei prodotti ICT e dei servizi digitali e garantisce il rafforzamento del

¹Direttiva NIS 2: la sicurezza delle infrastrutture critiche, tra normativa e buone prassi, Cristina Spagnoli, Cybersecurity360,5 aprile 2023. Link: <https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-la-sicurezza-delle-infrastrutture-critiche-tra-normativa-e-buone-prassi/>

² Link al sito ufficiale UE di ENISA: <https://www.enisa.europa.eu/>

³ Enisa: "Nasce il quadro europeo delle competenze di cybersecurity, ecco perché è importante", Fabio Di Franco, Agenda Digitale, 9 dicembre 2022. Link: <https://www.agendadigitale.eu/sicurezza/cybersicurezza-arriva-il-quadro-europeo-delle-competenze-ecco-perche-e-importante/>

ruolo di ENISA nella prevenzione dei cyber-attacchi, rafforzando la propria posizione. Questo regolamento costituisce una parte fondamentale della nuova strategia per la sicurezza cibernetica dell'Europa, e consente non solo di rafforzare la resilienza dell'Unione agli attacchi informatici, ma anche di creare un mercato economico unico in grado di garantire la cybersecurity in termini di prodotti, servizi e processi. In tale contesto, il riconoscimento reciproco, da parte degli Stati membri, delle certificazioni UE ha come principale obiettivo quello di aumentare il coordinamento, anche attraverso l'incremento di un uguale livello di consapevolezza in tutta l'area eurocomunitaria. In quest'ottica, dunque, il Cybersecurity Act si affianca alla Direttiva NIS.

A tale proposito riportiamo la definizione con la quale il Cybersecurity Act, all'art. 2, spiega il significato del termine "cybersicurezza" ovvero 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"*. Più precisamente consiste nell'insieme di tecnologie, processi e misure di protezione progettate per ridurre il rischio di attacchi informatici.

Anche in questo caso il ruolo dell'ENISA è quello di sostenere e collaborare attivamente con le istituzioni, gli organi e gli organismi dell'UE e con gli Stati membri, evitando la duplicazione delle attività e promuovendo le sinergie, avvalendosi anche dei contributi e della collaborazione del settore privato.

4 – La Direttiva NIS2

Vista la crescita esponenziale degli attacchi informatici avvenuti tra l'ultima parte del 2022 e la prima parte del 2023, si è reso necessario, aggiornare la normativa precedente nell'ottica di ampliare il campo di applicazione e preparare le aziende alle sfide attuali e future della sicurezza delle reti e dei sistemi informativi. Il 16 gennaio 2023 nasce quindi la Direttiva NIS2 e gli Stati UE avranno tempo fino al 17 ottobre 2024 per recepire le sue disposizioni con una normativa nazionale [3]. Tra i capisaldi della direttiva NIS2 possono essere ricordati la rideterminazione e l'ampliamento dei settori che si distinguono per le loro dimensioni, il loro impatto e il loro ambito, ovvero: infrastrutture digitali e digital provider; finanza; salute; reti idriche; energia; olio e gas; trasporti; pubblica amministrazione; reti e servizi per la

comunicazione elettronica pubblica; servizi postali; aerospazio; prodotti medicali, prodotti chimici, prodotti farmaceutici e dispositivi medicali; rifiuti; filiera agro-alimentare; data center e social network; il potenziamento degli organi e delle attività di supervisione a livello comunitario, con l'obiettivo di migliorare la collaborazione per contrastare la minaccia informatica globale grazie alla condivisione delle esperienze tra gli Stati membri.

I requisiti minimi previsti dalla normativa che i soggetti coinvolti devono garantire riguardano: analisi e valutazione dei rischi di sicurezza dei sistemi informativi, sia attraverso operazioni di identificazione rapida delle vulnerabilità per valutare il livello di esposizione al rischio (*vulnerability assessment*), sia attraverso test di simulazione di attacchi informatici (*penetration test*) che sfruttano proprio quelle stesse vulnerabilità per verificarne la robustezza; gestire gli incidenti di sicurezza informatici con un piano e un'attività di monitoraggio continuo e di *incident response*; dotarsi di un piano di continuità di business e gestione delle crisi; testare regolarmente la sicurezza dell'infrastruttura ICT e l'efficacia delle misure di gestione del rischio adottate; e infine, assicurare la sicurezza nel processo di acquisizione di un prodotto dal fornitore al cliente c.d. "*supply chain*"⁴ al fine di creare un clima di responsabilità condivisa nei confronti della gestione del rischio e dell'adozione delle necessarie misure di prevenzione e rimedio agli attacchi informatici per tutti gli attori coinvolti, controllando che i propri fornitori dispongano di adeguati requisiti in termini di sicurezza. Le infrastrutture critiche⁵ e i servizi essenziali importanti dovranno mantenere un

⁴ Significato di Supply chain da Wikipedia: a gestione della catena di distribuzione (supply chain management, SCM) riguarda diverse attività logistiche delle aziende, con l'obiettivo di controllare le prestazioni e migliorarne l'efficienza. Tra queste attività sono incluse la catalogazione sistematica dei prodotti e il coordinamento strategico dei vari membri della catena di distribuzione. Il supply chain management fornisce quindi un collegamento e si occupa di coordinare le attività di produzione, acquisto e logistica.

⁵ Significato di infrastrutture critiche dal sito del Ministero dell'interno: "Le infrastrutture critiche sono le risorse materiali, i servizi, i sistemi di tecnologia dell'informazione, le reti e i beni infrastrutturali che, se danneggiati o distrutti, causerebbero gravi ripercussioni alle funzioni cruciali della società, tra cui la catena di approvvigionamenti, la salute, la sicurezza e il benessere economico o sociale dello Stato e della popolazione".

Link:

registro delle vulnerabilità, cooperare con gli Stati europei alla gestione delle crisi informatiche; redigere una relazione annuale sullo stato della cybersecurity; creare e gestire un report di tutte le entità che forniscono servizi transfrontalieri come cloud computing, registrazioni di nomi a dominio e altro ancora; consentire le revisioni inter pares per gli Stati membri e mantenere aggiornate le loro strategie informatiche; istituire un gruppo di intervento per la cybersecurity in caso di incidente nonché di un'autorità competente per le reti e i sistemi informativi nazionali che cooperino tra tutti gli stati membri.⁶

5 – Cybersecurity e GDPR

Quando parliamo della rapida evoluzione tecnologica e della conseguente creazione di nuovi modelli di utilizzo delle “informazioni”, il pensiero ricade inevitabilmente sulle garanzie di sicurezza di eventuali dati personali a cui tali informazioni si riferiscono. Per approfondire questi aspetti, abbiamo dunque ritenuto opportuno analizzare il Regolamento europeo in materia di protezione dei dati personali Reg. (UE) 2016/679 (GDPR), vincolante per tutti gli stati membri e divenuto efficace a partire dal 25 maggio del 2018, lasciando così un periodo di due anni di tempo per adeguarsi alle novità legislative. Il GDPR ha sostituito i contenuti della direttiva sulla protezione dei dati (Direttiva 95/46/CE, 1995) e ha abrogato gli articoli del codice per la protezione dei dati personali (D.lgs. 196/2003) in Italia, ribadendo concetti già presenti nelle normative precedenti ma introducendo diverse novità incentrate sulla tutela dei diritti e delle libertà delle persone fisiche e di conseguenza sulla protezione dei dati personali che ad esse si riferiscono **[4]**.

https://www1.interno.gov.it/mininterno/export/sites/default/it/sezioni/sala_stamp/0867_2008_02_14_app_infrastrutture_critiche.html

⁶ “La Direttiva NIS2 avanza: come prepararsi in questi 9 mesi,” Maria Beatrice Versaci e Andrea Pauri, Cybersecurity360, 10 gennaio 2024. Link: <https://www.cybersecurity360.it/news/la-direttiva-nis2-avanza-come-prepararsi-in-questi-9-mesi/>

I suoi obiettivi riguardano la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all'interno dell'Unione europea, lo sviluppo del mercato unico digitale europeo e, infine, la risposta alle nuove sfide derivanti dalle nuove tecnologie digitali. Rimanendo in tema di sicurezza informatica la relazione fra GDPR e cybersecurity si manifesta attraverso due principi fondamentali: il principio di Accountability e il principio di Privacy by design e by default. Secondo il principio di Accountability, il titolare del trattamento⁷ deve determinare le finalità del trattamento e i mezzi dello stesso, mettendo in atto le misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è stato effettuato conformemente al GDPR. La garanzia e il rispetto del diritto alla riservatezza e alla protezione dei dati deve essere considerato valutato e attestato dal Titolare sin dalla progettazione di ogni processo e progetto e dei relativi supporti informatici tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche (Privacy by design). Il titolare del trattamento deve infine mettere in atto misure tecniche e organizzative adeguate a garantire che siano trattati per impostazione predefinita solo i dati personali necessari per ogni specifica finalità del trattamento [5].

Se poniamo a confronto GDPR e Direttiva NIS notiamo che quest'ultima, così come attuata nel nostro ordinamento dal D.lgs. 65/2018, non si prefigge direttamente il compito di assicurare la tutela dei dati personali, ma piuttosto quello di definire obblighi di adozione di specifiche misure di sicurezza volte a conseguire un livello elevato di sicurezza della rete e dei sistemi informativi in ambito nazionale, contribuendo ad incrementare il livello comune di sicurezza nell'Unione Europea. Tuttavia, sebbene GDPR e NIS siano due normative volte a tutelare differenti beni giuridici, esse potrebbero risultare, nella pratica, parzialmente sovrapponibili.

⁷ Titolare: è la persona fisica, l'autorità pubblica, l'impresa, l'ente pubblico o privato, l'associazione, ecc., che adotta le decisioni sugli scopi e sulle modalità del trattamento (articolo 4, paragrafo 1, punto 7), del Regolamento UE 2016/679).

Non è possibile escludere, infatti, che attacchi a sistemi c.d. “critici” possano comportare, come effetto, un trattamento illecito di dati personali, impattando negativamente sui diritti e le libertà degli utenti.

Uno scenario di questo tipo comporta, concretamente, l’esigenza da parte delle società coinvolte nei sopraccitati trattamenti, di rivedere, a livello di processo, le misure di sicurezza adottate, valutando l’opportunità di declinare la tutela del dato a seconda delle informazioni delle quali questo è portatore.

Oltre al GDPR, è opportuno evidenziare che nell’ambito della cybersecurity la gestione dei rischi è già stata affrontata attraverso la compliance agli standard internazionali ISO 27001, 31000, 22301⁸, che sanciscono le buone pratiche di sicurezza informatica per tutte le organizzazioni che vi aderiscono tra cui l’analisi, la verifica, la regolamentazione delle procedure, il monitoraggio, il miglioramento continuo dei sistemi di gestione per la sicurezza delle informazioni, e la più recente norma tecnica ISO/IEC 42001: 2023 “Information Technology Artificial Intelligence - Management System” (AIMS), creata al fine di supportare e responsabilizzare le aziende relativamente al contesto sulla base del quale dovrà essere predisposta l’analisi dei rischi anche in vista di eventuali controlli⁹.

Un settore molto importante che evidenzia la necessità di integrare la privacy e la cybersecurity, riguarda la condivisione delle minacce (la c.d. threat intelligence sharing). Con questa pratica le aziende e le pubbliche amministrazioni condividono le minacce informatiche e la vulnerabilità dei sistemi. Il Regolamento (UE) 2022/2554 (DORA: Digital Operation Resilience Act) [6] ad esempio, che si applica al settore finanziario, incoraggia le entità finanziarie a scambiarsi reciprocamente informazioni e analisi delle minacce informatiche.

⁸ Per approfondimenti: “Cyber Security e IT: linee guida, best practice e standards”, Alessio Pennasilico, Cybersecurity Act, 18 aprile 2018.

⁹ ISO/IEC 42001:2023, lo standard per il sistema di gestione dell’intelligenza artificiale: le finalità”, Monica Perego, Cybersecurity360, 4 gennaio 2024.

In questo modo, le stesse entità finanziarie possono sfruttare collettivamente, sia sul piano strategico che sul piano operativo, le conoscenze e le esperienze pratiche che hanno acquisito a livello individuale al fine di accrescere le proprie capacità di valutare e monitorare adeguatamente le minacce informatiche. Per realizzare questa importantissima finalità, le entità finanziarie devono dar vita a processi di condivisione dei dati che siano disciplinati in modo da garantire la riservatezza dell'attività economica e della protezione dei dati personali ai sensi del GDPR. Lo stesso principio di possibile scambio delle informazioni e di integrazione con il GDPR è ravvisabile anche nella NIS 2 che all'art. 121 riconosce lo scambio delle informazioni sulle minacce e vulnerabilità e le misure relative alla prevenzione, al rilevamento, all'individuazione, al contenimento e all'analisi degli incidenti e alla risposta agli stessi, evidenziando l'obbligo di fondare il trattamento sulle apposite basi giuridiche definite dal GDPR tra le quali vengono poste in evidenza l'interesse legittimo del titolare, l'obbligo legale, compito di interesse pubblico o connesso all'esercizio di pubblici poteri), ai sensi dell'art. 6 comma c), e). f).

A questo punto, come accennato nella parte introduttiva di questo lavoro, riteniamo opportuno ricordare che lo scorso 13 marzo il Parlamento europeo ha approvato "l'Artificial Intelligence Act" e che ad oggi attendiamo soltanto la pubblicazione nella Gazzetta Ufficiale. Si tratta della prima normativa europea che regolamenterà l'utilizzo dell'Intelligenza Artificiale (IA) attraverso regole chiare per i produttori che intendano immettere sul mercato sistemi basati sull'intelligenza artificiale e per tutelare gli utenti che li useranno e che obbligherà le aziende a prestare particolare attenzione al bilanciamento tra i benefici e i danni di queste nuove tecnologie in termini di trasparenza, equità e sostenibilità. Gli elementi principali dell'accordo provvisorio possono essere riassunti in norme sui modelli di IA di carattere generale ad alto impatto che possono causare rischi sistemici in futuro, nonché sui sistemi di IA ad alto rischio, un sistema di governance a livello dell'UE con funzioni di supervisione, ma anche di sviluppo di modelli e metodologie per la gestione dei rischi, ampliamento dell'elenco dei divieti con alcune eccezioni per le autorità che operano per contrastare la criminalità e obbligo per gli utilizzatori di sistemi di IA ad alto rischio di effettuare una valutazione d'impatto

ai sensi del GDPR prima di mettere in uso un sistema di IA e a forme di profilazione e meccanismi di decisione automatizzata sempre più sofisticati. L'accordo provvisorio prevede che questo nuovo regolamento diventi operativo dopo due anni dalla sua entrata in vigore salvo alcune eccezioni per disposizioni specifiche. [7]

Desideriamo infine ricordare che lo scorso 30 novembre il Parlamento e il Consiglio europeo hanno raggiunto un accordo provvisorio sulla proposta legislativa che prevede una serie di requisiti di cyber security per i prodotti digitali, prima della loro immissione sul mercato. "Il Cyber Resilience Act" [8]. Tale accordo mira a definire un ampio quadro normativo per la sicurezza informatica dei prodotti digitali connessi in rete ("Internet of Things") ed immessi sul mercato dell'Unione, prevedendo obblighi più stringenti in capo ai relativi produttori. Il pacchetto di regole riguarda principalmente: l'obbligo di effettuare le valutazioni dei rischi; il rilascio di dichiarazioni di conformità; la collaborazione con le autorità competenti; la trasparenza sulla sicurezza dei prodotti; la definizione di processi di gestione delle vulnerabilità; la gestione degli incidenti informatici. A tali obblighi si aggiunge quello della sensibilizzazione e formazione delle persone coinvolte, dai fabbricanti, agli esportatori, inclusi i commercianti. Verranno inoltre introdotti meccanismi di vigilanza del mercato ai fini dell'applicazione delle norme con il coinvolgimento dell'Enisa). Saranno inoltre previsti dei tempi necessari per risolvere le vulnerabilità dei prodotti immessi sul mercato e renderne quindi pubblica l'avvenuta risoluzione.

In questo contesto possiamo valutare come gli ambiti di intervento delle normative finora esaminate, siano diversi, ma tutte hanno origine da un'unica esigenza: una più forte consapevolezza, a livello europeo, circa l'importanza di mettere in atto una strategia efficace e precisa in tema di sicurezza e prevenzione.

6 – Conclusioni (sviluppi futuri)

L'era tecnologica che stiamo affrontando porta con sé vantaggi e opportunità, ma al tempo stesso rileva forti preoccupazioni perché le tecnologie se non adeguatamente gestite, possono diventare una grave minaccia per la sicurezza globale. Analizzando queste problematiche abbiamo appurato che per garantire lo sviluppo economico e la competitività globale le aziende devono garantire un rapporto di fiducia con i cittadini il più possibile trasparente, leale e corretto. Pertanto, sebbene non si possa evitare che la fiducia comporti di per sé l'accettazione di un rischio che non può essere mai nullo, questo deve essere valutato, calcolato e affrontato con professionalità, impegno e progettazione. Per accrescere la fiducia dei cittadini in un'economia sempre più digitale, è inoltre importante che le aziende cooperino tra loro mettendo a fattor comune la condivisione delle esperienze e delle professionalità. Il tutto all'interno di una cornice giuridica completa di norme, requisiti tecnici, standard e procedure il più possibile armonizzate, efficaci e cyber resilienti.

Quello che abbiamo imparato dall'esperienza degli ultimi anni riguardo alla tecnologia, è che quando si parla di questo argomento, guardare alla tematica da una prospettiva internazionale risulta imprescindibile. Di fronte alla velocità dello sviluppo tecnologico occorre una sempre più forte cooperazione tra gli Stati e una disciplina etico giuridica ed economica quanto più armonizzata e strutturata e caratterizzata da norme che contribuiscono alla realizzazione di uno spazio di sicurezza e benessere per i cittadini. Per far ciò è necessario rafforzare il sistema governance aziendale, far crescere l'occupazione e allineare le competenze in questo settore investendo nella sicurezza in modo appropriato. Non meno importante è la necessità di una svolta culturale riguardo a questo settore che coinvolga le diverse organizzazioni e che abbia come punti di forza la formazione, la responsabilizzazione dei vertici aziendali e la convergenza tra competenze informatiche e giuridiche in modo da consentire agli operatori del settore di parlare un linguaggio comune¹⁰.

¹⁰ Per approfondimenti: Report Cybersecurity & Privacy: gap e margini di convergenza, Federprivacy – 07 novembre 2023, Redazione Ipsos Quotidiano.

Bibliografia

[1] 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 (direttiva NIS).

Link: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016L1148>

[2] 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) 526/2013 (Cybersecurity Act).

Link: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019R0881&from=PT>

[3] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS2).

Link: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555&from=EN>

[4] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GDPR). Link: <https://www.garanteprivacy.it/il-testo-del-regolamento>

[5] Linee guida EDPB 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita (versione 2.0, 20 ottobre 2020).

Link: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_it.pdf

[6] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011 (regolamento DORA).

Link: <https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32022R2554>

[7] Accordo definitivo sulla proposta l'Artificial Intelligence Act.

Link: <https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf>

[8] Accordo provvisorio sulla proposta per il Cyber Resilience Act.

Link: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6168