Rivista elettronica di Diritto, Economia, Management

Inquadra il QR-CODE per il download degli altri numeri della Rivista

Numero 1 - 2025

NIS 2 e Cybersecurity

A cura di Sarah Ungaro

FONDATA E DIRETTA DA
DONATO A. LIMONE

CLIOEDU®

ISSN 2039-4926

La "Rivista elettronica di Diritto, Economia, Management" è un periodico totalmente digitale, accessibile e fruibile gratuitamente, che ha lo scopo di trattare le diverse tematiche giuridiche, economiche e manageriali con un approccio integrato e trasversale, di tipo comparato, in un contesto locale, nazionale, comunitario ed internazionale caratterizzato dalla società dell'informazione, dalla trasformazione digitale, dalla globalizzazione dei mercati, da processi innovativi di tipo manageriale ed organizzativo nei settori pubblico e privato.
La rivista ha anche la finalità di ospitare contributi di giovani studiosi per valorizzarne le attitudini alla ricerca e il loro contributo allo sviluppo delle scienze giuridiche, sociali, economiche e manageriali.

Direzione e redazione: Via Riccardo Grazioli Lante, 15 – 00195 Roma - *donato.limone@gmail.com*

Gli articoli pubblicati nella rivista sono sottoposti ad una procedura di valutazione anonima. Gli articoli sottoposti alla rivista vanno spediti alla sede della redazione e saranno dati in lettura ai referees dei relativi settori scientifico disciplinari.

Anno XV, n. 1/2025
ISSN 2039-4926
Autorizzazione del Tribunale civile di Roma N. 329/2010 del 5 agosto 2010
Editor ClioEdu
Roma - Lecce

Codice etico: *www.clioedu.it/rivistaelettronica#codice-etico*
Procedure di referaggio: *www.clioedu.it/rivistaelettronica#referaggio*
Elenco dei numeri pubblicati: *www.clioedu.it/rivistaelettronica*

Indice

N. 1 - 2025 - pp. 3-4

Editoriale

Questo numero è il primo del 2025, anno che sarà caratterizzato:

a) dalla *applicazione* di alcuni regolamenti UE in materia di digitale (approvati dal 2022 al 2024): (regolamento sulla IA, 2024; regolamento eIDAS, 2024; regolamento Data Act, 2023; regolamento Digital Service Act, 2022; il Digital Market Act, 2022; Il Digital Governance Act, 2022);
b) dalla *evoluzione/involuzione* di nuovi mercati del settore;
c) dalla evoluzione della integrazione, in particolare, dei processi di trasformazione digitale ed ecologico;
d) dal processo più ampio dell'*innovazione* (in tutti i settori) che dovrà inevitabilmente utilizzare un approccio sempre più sistemico (visioni; strategie; dati; mercati; politiche; tecnologie; cambiamenti sociali, culturali ed economici).

Nel 2025 si chiuderà il PNRR (salvo diverse decisioni): e faremo una rendicontazione dei risultati! E risponderemo a tante domande: abbiamo speso tanti soldi, con quale effetto? Abbiamo "solo" speso o abbiamo anche "investito" sul futuro e per il futuro?; quali risultati ed occasioni reali per i "giovani"? Abbiamo "solo" distribuito "risorse finanziarie" ad enti ed imprese per "accontentare tutti" oppure abbiamo iniziato ad operare con un po' di strategia per innovare? Abbiamo contribuito a cambiare la burocrazia pubblica: per renderla semplificata, trasparente, digitale, accessibile, sostenibile? Abbiamo perso una grande occasione come Paese e come Europa oppure abbiamo "seminato" su di un nuovo terreno dissodato a dovere?

La nostra Rivista seguirà questo processo di ***rendicontazione*** vera, concreta, critica, attraverso contributi scientifici, culturali, tecnici sempre con un approccio interdisciplinare (diritto, economia, management per l'innovazione digitale).

Ed iniziamo con questo numero a dare il nostro contributo con un fascicolo speciale dedicato a ***NIS 2 e Cybersecurity***: tema di grande attualità che richiede una riflessione attenta, seria, partecipata, trasparente. *La sicurezza digitale riguarda aspetti istituzionali, sociali, economici, politici, organizzativi, procedurali, documentali, informativi, tecnici.* La sicurezza digitale esprime la complessità di un cambiamento radicale globale molto significativo che richiede una politica ed una strategia pubblica capace di conoscere, valutare, determinare in modo "intelligente" questa transizione della nostra epoca. L'attuale livello politico ed istituzionale segue ancora strade tradizionali, non ha percepito la esigenza di cambiamento: opera per slogan, arriva in ritardo sulla trasformazione digitale, non ha il senso del futuro perché ha perso anche il senso del presente. Eppure abbiamo bisogno di una politica come guida, di un diritto che stimola l'innovazione e che non arrivi in ritardo

costringendo a cambiare secondo vecchi canoni e modelli regolatori superati. *Ormai le tecnologie, le innovazioni digitali e non solo, esprimono processi di trasformazione, di transizione, di cambiamento che seguono modelli e ritmi totalmente autonomi e maturi rispetto ai modelli usurati che sono alla base delle decisioni pubbliche in questi processi.* La sicurezza tecnologica riguarda allora persone, comunità, organizzazioni pubbliche e private, dati personali e non, sistemi sociali ed economici, sistemi culturali: dobbiamo affrontare questa "nuova dimensione" (non è solo un tema) nella logica dei sistemi complessi in continua dinamica e mutamento. Dobbiamo essere sempre più società "intelligenti", individui "intelligenti", sistemi di conoscenza "intelligenti".

Questo numero è stato progettato e curato dalla avvocata Sarah Ungaro con grande preparazione professionale e con passione. Il nostro grazie per questa sua curatela anche a nome del comitato scientifico e di redazione della Rivista. Il mio ringraziamento agli autori di questo volume.

La prefazione è di Agostino Ghiglia, componente dell'Autorità Garante per la protezione dei dati. L'articolo di Marco Biagini e Giorgia Zunino si occupa di difesa (*Cybersecurity, intelligenza artificiale, e difesa: riflessioni sulle normative europee e nazionali per un nuovo modello di regolamentazione nell'era dell'innovazione tecnologica accelerata)*. Su Data breach tra privacy e security il contributo di Andrea Lisi (*Data breach tra privacy e security: una proposta di sopravvivenza normativa, etica, logica e organizzativa in caso di violazioni nel trattamento dei dati)*. Sull'ACN interviene Stefano Marzocchi *(Il ruolo strategico dell'Agenzia per la cybersicurezza nazionale nella tutela integrata del dato)*. Su NIS2 ed eIDAS l'articolo di Giovanni Manca (*Il regolamento europeo 2024/1183 (eIDAS2) e l'impatto della Direttiva 2022/2555 (NIS2) sui servizi fiduciari)*. Di Cristian Catalano e Mario Angelelli un contributo su informatica attiva nella pubblica amministrazione *(Condivisione security teste per migliorare la difesa informatica attiva nella pubblica amministrazione*). Corrado Giustozzi interviene con un articolo di carattere generale (*Direttiva NIS2: genesi, attuazione, impatti)*. Sui servizi fiduciari in Italia l'articolo di Luigi Foglia *(La cibersicurezza per la fornitura di servizi fiduciari in Italia)*. Sul tema come applicare la NIS2 nelle imprese un contributo di Eleonora Faina e Carlo Didonè *(NIS2-Ready? L'applicazione della direttiva NIS2 nelle imprese italiane. Tempistiche e nodi da sciogliere)*. L'articolo di Sarah Ungaro chiude il volume (*Autenticità dei dati: l'altro pilastro fondamentale della cybersecurity)*.

Il Direttore della Rivista
Donato A. Limone

N. 1 - 2025 - pp. 5-8

Prefazione

Agostino Ghiglia

La recente Direttiva NIS 2 22022/2555 (Network and Information Security) è stata adottata dalla Commissione Europea per rafforzare il livello di sicurezza delle reti e dei sistemi informativi nell'Unione Europea, in un contesto di crescenti minacce e vulnerabilità cyber.

Essa rappresenta un passo significativo verso il rafforzamento della cybersecurity all'interno dell'Unione Europea. La NIS 2, che sostituirà la direttiva NIS (EU) 2016/1148, persegue l'obiettivo di una creazione di un framework di cybersicurezza europeo che armonizzi e superi le discrasie applicative fra stati membri della precedente direttiva.

L'obiettivo è rafforzare le misure di cybersecurity e ciò è possibile con l'integrazione tra le varie normative e linee guida europee in tema di protezione dati e privacy. La direttiva, infatti, si allinea con altre regolamentazioni sulla protezione dei dati come il GDPR e l'Atto sulla Resilienza Cibernetica, introducendo misure di supervisione e applicazione più rigorose.

Questo nuovo quadro normativo, sostituendo la precedente Direttiva UE 2016/1148, impone nuovi obblighi ai soggetti "essenziali" e "importanti", con l'obiettivo di creare una strategia comune di cybersicurezza nell'Unione Europea, introducendo significative novità come, ad esempio, un approccio multirischio e misure di sicurezza specifiche e l'inclusione settori critici come energia, trasporti, sanità e infrastrutture digitali, eliminando la distinzione tra operatori di servizi essenziali e fornitori di servizi digitali.

Poiché si tratta di una direttiva e non di un regolamento come il GDPR, è richiesto che tutti gli Stati Membri la recepiscano, entro il 17 ottobre 2024, sviluppando piani nazionali per la sicurezza e costituendo team specializzati per attuare la direttiva.

Le misure di gestione dei rischi di cybersecurity sono attentamente selezionate per essere adeguate e proporzionate, con l'obiettivo di affrontare in modo efficace i potenziali rischi per la sicurezza dei sistemi e delle reti informatiche.

I soggetti "essenziali" e "importanti" dovranno implementare tali misure, integrandole sia nelle loro attività quotidiane che nella fornitura dei servizi con l'obiettivo di prevenire o minimizzare gli impatti degli incidenti sulla sicurezza dei sistemi e delle reti.

Un elemento chiave introdotto dalla NIS 2 è l'approccio multirischio, che va oltre la difesa contro gli attacchi cyber tecnici, considerando anche rischi legati alle persone, agli eventi fisici e ambientali.

Questo tipo di approccio, molto simile a quello previsto nel Regolamento UE 679/2016 GDPR, richiede una valutazione completa dei rischi, una gestione efficace delle risorse umane e dei processi interni, nonché una stretta collaborazione e condivisione delle informazioni tra gli attori coinvolti.

La direttiva impone ai soggetti interessati di attuare specifiche misure di sicurezza, come: politiche di analisi dei rischi, gestione degli incidenti, continuità operativa e sicurezza della catena di approvvigionamento. È fondamentale che le aziende interessate sviluppino un *Incident Plan*, che includa procedure di notifica alle autorità competenti e definisca chiaramente i ruoli e le responsabilità del personale coinvolto nella gestione degli incidenti.

Adeguarsi alla NIS 2 non è solo una questione di conformità normativa, ma rappresenta un'opportunità per introdurre una cultura della cybersicurezza in azienda e migliorare il livello complessivo di sicurezza informatica. È essenziale che le aziende e soggetti interessati comincino fin da subito a predisporre un piano di adeguamento, implementando progressivamente misure di sicurezza misurabili e fornendo formazione al personale.

Uno degli aspetti più rilevanti della direttiva NIS 2 riguarda la gestione degli incidenti, ovvero gli eventi che possono compromettere la disponibilità, l'integrità, l'autenticità o la confidenzialità dei dati o dei servizi.

Si prevede infatti che i soggetti destinatari, tenuti ad adottare strumenti di analisi e gestione dei rischi, debbano segnalare alle autorità competenti gli incidenti che abbiano un impatto significativo o sostanziale sul funzionamento dei servizi essenziali o importanti. È previsto un processo di segnalazione dell'evento rilevante entro 24 ore (la norma definisce tale segnalazione preallarme), con successiva notifica dell'incidente entro 72 ore. La segnalazione degli incidenti ricalca sostanzialmente la procedura di notifica di una violazione dei dati personali (data breach ex art.33

GDPR).

Come previsto anche in materia di protezione dei dati personali, infatti, la direttiva stabilisce che questi soggetti debbano adottare misure per prevenire, rilevare, gestire e mitigare gli incidenti, nonché per ripristinare la normalità il prima possibile.

La gestione degli incidenti ha anche un'importante connessione con il Regolamento UE 2016/679 (GDPR), che disciplina la protezione dei dati personali nell'Unione Europea.

Il GDPR prevede infatti che i titolari del trattamento dei dati personali debbano notificare alle autorità di controllo le violazioni dei dati personali, ovvero gli incidenti che comportano una distruzione, una perdita, una modifica, una divulgazione o un accesso non autorizzato ai dati personali, entro 72 ore dalla loro scoperta.

Inoltre, il GDPR impone ai responsabili del trattamento dei dati personali di adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza appropriato al rischio.

È bene chiarire che, sebbene le norme abbiano scadenze simili in fatto di notifica, quello che cambia sono le metriche di misurazione della gravità dell'evento: nel caso della direttiva NIS 2 ci si focalizza sull'interruzione del pubblico servizio, mentre nel caso del GDPR l'attenzione viene posta sui potenziali rischi che l'evento potrebbe comportare per diritti e le libertà degli individui.

Può pertanto accadere che vi siano eventi rilevanti per il contesto data protection ma non cyber security (o viceversa): ad esempio, una errata pubblicazione di dati on line sul portale di un ente pubblico potrebbe comportare una rilevante violazione di dati personali ai sensi del GDPR, ma sicuramente non sarebbe oggetto di attenzione in ambito NIS 2.

Un altro tema è la procedura di notifica: trattandosi di autorità competenti diverse e differenti informazioni da notificare, si dovrà intervenire con modus operandi differenti, in cui potrebbero variare i soggetti operanti all'interno dell'organizzazione.

La convivenza di questi aspetti si preannuncia quindi piuttosto strutturata, per cui le organizzazioni dovranno predisporre idonee procedure operative per adempiere correttamente ai differenti obblighi di legge.

Uno degli aspetti più critici sarà garantire la coerenza tra le procedure di notifica previste dalle due normative. Le organizzazioni saranno tenute a seguire protocolli differenti in base alla natura dell'incidente (dati personali o altri tipi di dati

critici), ma il rischio di sovrapposizioni o di incertezze operative potrebbe rallentare la capacità di risposta in caso di attacchi.

Il Decreto legislativo 138/2024, che recepisce la Direttiva NIS 2 dell'Unione Europea, e la Legge 90/2024 hanno segnato una svolta importante nel panorama normativo italiano. Queste nuove disposizioni mirano a rafforzare la sicurezza dei dati e delle infrastrutture critiche, introducendo obblighi più stringenti per le organizzazioni che operano in settori essenziali, e stabilendo un quadro normativo più chiaro e coordinato in tema di gestione e prevenzione degli incidenti di sicurezza.

Queste nuove norme portano un importante rafforzamento delle misure di sicurezza richieste, ponendo particolare attenzione alla protezione dei dati, inclusi quelli personali, e al miglioramento delle capacità di risposta a eventuali incidenti di sicurezza, con particolare riguardo a settori strategici e a operatori di servizi essenziali. In questo contesto, il ruolo dell'Autorità Garante per la protezione dei dati personali emerge come centrale, non solo per l'attenzione alla protezione dei dati, ma anche per il coordinamento con le nuove normative in tema di sicurezza informatica.

Le novità introdotte dal D.lgs. 138/2024 e dalla Legge 90/2024 rappresentano un passo avanti significativo per il rafforzamento della sicurezza informatica in Italia, con un impatto diretto tanto sul settore pubblico quanto su quello privato. L'implementazione della Direttiva NIS 2 e delle nuove disposizioni sulla protezione dei dati richiede un approccio integrato e coordinato tra le varie autorità competenti e le organizzazioni coinvolte. In questo contesto, il Garante per la Protezione dei Dati Personali svolge un ruolo cruciale, soprattutto per garantire la coerenza delle normative con il GDPR e per promuovere una cultura della sicurezza che tuteli non solo i dati personali, ma anche le infrastrutture critiche su cui si basa la nostra società.

Dott. Agostino Ghiglia
Componente Autorità
Garante per la protezione dati personali

N. 1 - 2025 - pp. 9-25

Cybersecurity, intelligenza artificiale e Difesa: Riflessioni sulle normative europee e nazionali per un nuovo modello di regolamentazione nell'era dell'innovazione tecnologica accelerata

Marco Biagini, Giorgia Zunino

Abstract: L'interrelazione tra cybersecurity e intelligenza artificiale (IA) è oggi un elemento centrale anche nel panorama normativo internazionale, come contemplato dalla Direttiva Europea *Network and Information Systems* 2 (NIS 2) e dal Regolamento *EU Artificial Intelligence (AI) Act*, che stabiliscono i requisiti normativi per la cybersicurezza delle tecnologie digitali, promuovendo al contempo l'uso sicuro ed etico dell'IA. Dal punto di vista nazionale, l'interazione tra la Legge 90/2024 e il Disegno di Legge (DdL) sull'intelligenza artificiale dal quale è scaturita la Strategia Italiana per l'intelligenza artificiale è da considerarsi cruciale per affrontare le crescenti minacce cibernetiche. Ma è proprio così? Viviamo in un periodo di straordinaria accelerazione tecnologica e il rischio di obsolescenza e non aderenza dei regolamenti collegati è reale, soprattutto in settori particolarmente critici, come quello della Difesa.
Con le *regulatory sandbox*, previste all'art. 57 dell'*EU AI Act* e la cui implementazione presumibilmente potrà essere contemplata anche nella stesura del nuovo EU *Cyber Resilience Act*, viene fornito uno degli strumenti creati per realizzare un nuovo modello di regolamentazione detto "Regolamentazione Anticipata". Il *framework* proposto dalle *sandbox* permette di intercettare il "*sweet spot*" tra "*ability to control*" e "*knowledge of impact*" previsto da dal Dilemma di *Collingridge*, fornendo gli strumenti per una transizione più fluida verso l'adozione sicura su larga scala di nuove tecnologie, nella fattispecie legate all'uso della IA nella cybersecurity.
Una politica di implementazione ben definita delle strategie nazionali, anche attraverso la sperimentazione delle "*regulatory sandbox*", potrà rafforzare ulteriormente la posizione dell'Italia in ambito internazionale sia nella sicurezza cibernetica che nell'intelligenza artificiale, sfruttando le sinergie normative offerte dai due settori tecnologici, anche nell'ambito della Difesa.

The interrelationship between cybersecurity and artificial intelligence (AI) is now also a central element in the international regulatory landscape, as contemplated by the European Network and Information Systems Directive 2 (NIS 2) and the EU Ar-

tificial Intelligence (AI) Act Regulation, which establish regulatory requirements for cybersecurity of digital technologies while promoting the safe and ethical use of AI. From a national perspective, the interaction between Law 90/2024 and the Draft Law (DdL) on Artificial Intelligence from which the Italian Artificial Intelligence Strategy emerged is to be seen as crucial in addressing the growing cyber threats. But is this really the case? We live in a period of extraordinary technological acceleration, and the risk of obsolescence and non-adherence of related regulations is real, especially in particularly critical sectors, such as Defense.
With the regulatory sandboxes, provided for in Article 57 of the EU AI Act and the implementation of which can presumably also be contemplated in the drafting of the new EU Cyber Resilience Act, one of the tools created to realize a new regulatory model called "Anticipatory Regulation" is provided. The framework proposed by the sandboxes makes it possible to intercept the "sweet spot" between "ability to control" and "knowledge of impact" envisioned by Collingridge's Dilemma, providing the tools for a smoother transition to the safe large-scale adoption of new technologies, in this case related to the use of AI in cybersecurity.
A well-defined implementation policy of national strategies, including through the experimentation of "regulatory sandboxes," can further strengthen Italy's position in the international arena in both cybersecurity and artificial intelligence, taking advantage of the regulatory synergies offered by the two technology sectors, including in the Defense area.

Parole chiave: cybersecurity, intelligenza artificiale, sandbox, AI Act, NIS 2, Legge 90/2024, Difesa.

1. Introduzione

L'evoluzione del cyberspazio ha portato a dover intraprendere sfide di sicurezza sempre più complesse, passando da una comunità ristretta di esperti "eternauti" con un'etica condivisa, a un ambiente globale e accessibile esposto a minacce sempre più sofisticate perpetrate sia da singoli individui che da gruppi criminali e/o terroristici più o meno organizzati. Infatti, le nuove sfide nella cybersecurity sono anche rappresentate dall'utilizzo di sistemi basati su intelligenza artificiale (IA) generativa, come *Copilot* e *Strawberry*[1], che semplificano l'accesso all'elaborazione e sviluppo

[1] https://www.wired.it/article/openai-strawberry-intelligenza-artificiale/

di codice, che spesso si rivela estremamente vulnerabile, e di tools per la generazione di codici adattivi, cioè che permettono a un modello di IA di progredire da soli creando nuovi dati di addestramento. Questi strumenti progettati per assistere programmatori e utenti comuni, forniscono nuove superfici di attacco che potrebbero essere sfruttate da *hacker* esperti, e inoltre possono essere facilmente "manipolati" per costruire attacchi cibernetici anche da comuni malintenzionati. Tutto diviene più accessibile e facile, facile come esfiltrare i dati con una *prompt injection*.[2]
In questo scenario si evidenzia la stretta interrelazione tra la cybersecurity e l'IA, ove l'efficacia dei sistemi di cybersecurity può invece essere migliorata attraverso l'implementazione di modelli di IA. Un esempio è dato dall'implementazione di sistemi addestrati all'analisi predittiva e alla rilevazione di anomalie, che permettono di identificare e rispondere alle minacce informatiche con maggiore velocità e precisione.

La sinergia tra cybersecurity e IA è quindi cruciale per creare un ecosistema digitale più sicuro e resiliente, in cui le tecnologie IA possano essere utilizzate per migliorare la sicurezza cibernetica senza compromettere la sicurezza stessa. Questo richiede un approccio integrato che consideri sia le opportunità che le sfide poste dall'IA nella cybersecurity. Dal punto di vista normativo, l'Unione Europea (UE) con la direttiva *Network and Information Systems* 2 (NIS 2)[3] e il regolamento *Artificial Intelligence (AI) Act*[4] ha di fatto evidenziato detta dicotomia anche sul piano giuridico. Interdipendenza che traspare anche dall'impianto normativo nazionale che, con la legge 90/2024 e il Disegno di Legge (DdL) sull'IA, sembra recepire in modo ampio e pionieristico le disposizioni dell'Unione. Infatti, la Strategia Italiana per l'intelligenza artificiale 2024-2026 introduce un approccio integrato per lo sviluppo e l'adozione dell'IA[5] in Italia, fornendo un quadro regolamentare chiaro.

Un aspetto importante della strategia è l'introduzione delle "*regulatory sandbox*" per favorire lo sviluppo dell'IA sotto la supervisione di autorità di controllo[6]. Nell'attuale contesto di rapidissima evoluzione tecnologica, emerge l'urgenza di muoversi su due piani fondamentali per garantire sia innovazione che sicurezza.

---

[2] https://www.guerredirete.it/ai-come-ti-esfiltro-i-dati-con-una-prompt-injection/

[3] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 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 (Direttiva NIS).

[4] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[5] https://www.agendadigitale.eu/cultura-digitale/regulatory-sandbox-per-unia-innovativa-e-a-basso-rischio-benefici-e-limiti/

[6] https://www.dirittobancario.it/art/la-strategia-italiana-per-lintelligenza-artificiale-2024-2026/

Le norme rappresentano uno strumento insostituibile per indirizzare le priorità e fornire indicazioni chiare su quale futuro desideriamo costruire. Ma quale futuro intendiamo realizzare? Chi governa ha la responsabilità e il privilegio di contribuire attivamente a questo processo sfruttando gli strumenti disponibili, come l'AI Act, per creare un ambiente favorevole anche nella cybersecurity.

Alla luce dello sforzo normativo che la nazione sta affrontando, sulla scia del recepimento della normativa europea, oggi è lecito interrogarsi se questo impianto sia effettivamente all'altezza delle sfide e delle aspettative del presente e soprattutto se fornisca gli strumenti necessari a incrementare la difesa e la sicurezza nazionale, garantendo al contempo l'evoluzione della cornice normativa per il corretto uso di nuove e dirompenti tecnologie e per il contrasto alle nuove minacce.

2. Il panorama normativo europeo e nazionale a confronto

La Direttiva NIS 2 (UE 2022/2555), quale atto legislativo dell'Unione Europea, mira a rafforzare significativamente la cybersicurezza in tutti gli Stati membri[7], sostituisce e amplia la precedente Direttiva NIS del 2016, introducendo requisiti più stringenti per la gestione dei rischi informatici e la segnalazione degli incidenti[8]. La NIS 2 estende il suo campo di applicazione a un numero maggiore di settori critici, tra cui energia, trasporti, sanità e infrastrutture digitali, eliminando la distinzione tra operatori di servizi essenziali e fornitori di servizi digitali[9], introducendo due nuove categorie di soggetti, chiamati Soggetti Essenziali e Soggetti Importanti.

Gli Stati membri hanno recepito la Direttiva UE 2022/2555 nella loro legislazione nazionale entro il 17 ottobre 2024, con l'obiettivo di creare un *framework* di sicurezza cibernetica europeo armonizzato e più robusto e, sebbene la Direttiva ampli significativamente il suo campo di applicazione includendo nuovi settori critici e strategici, tuttavia non si estende direttamente al campo di applicazione militare e della Difesa in senso stretto. Nonostante ciò, i principi e le strategie adottate nella NIS 2 possono essere applicati anche al settore della Difesa, in particolare per quanto riguarda la gestione del rischio e la sicurezza informatica, introducendo requisiti di sicurezza cibernetica più stringenti e ampliando il suo ambito di applicazione. Inoltre, ponendo l'accento sulla necessità di garantire l'interoperabilità e la connet-

[7] https://www.nis-2-directive.com

[8] https://www.trendmicro.com/it_it/compliance/NIS 2-direttiva.html

[9] https://www.federprivacy.org/informazione/primo-piano/la-direttiva-nis2-ed-il-suo-recepimento-nella-normativa-nazionale-un-nuovo-standard-per-la-cybersecurity-in-europa

tività sicura tra i sistemi di difesa, in linea con l'approccio interforze e interagenzia, contribuendo alla protezione delle infrastrutture critiche e alla sicurezza nazionale in un contesto allargato di crescenti minacce informatiche.

Con la Legge 90/2024, nota come "Disposizioni per il rafforzamento di cybersicurezza nazionale e reati informatici," l'Italia si concentra sul miglioramento della cybersecurity e sulla lotta ai reati informatici, introducendo misure più stringenti per contrastare i cyber crimini, come l'accesso abusivo a sistemi informatici e la diffusione di strumenti per intercettare comunicazioni[10]. Integrando le disposizioni della Direttiva NIS 2, la Legge 90/2024 introduce anche specifici obblighi in campo di difesa militare, rafforzando il ruolo dell'Agenzia per la Cybersicurezza Nazionale (ACN) anche attraverso l'imposizione dell'adozione di misure tecniche e organizzative adeguate alla gestione dei rischi, la segnalazione tempestiva degli incidenti significativi entro 24 ore e l'implementazione di politiche di sicurezza più rigorose.

Per quanto riguarda l'interazione tra cybersecurity e intelligenza artificiale (IA), sebbene la Direttiva NIS 2 non regoli direttamente l'IA, incoraggia l'uso di tecnologie innovative per migliorare la sicurezza informatica. Le entità soggette alla NIS 2 che utilizzano IA devono però anche rispettare gli obblighi dell'AI Act, gestendo i rischi e garantendo trasparenza, soprattutto per i sistemi ad alto rischio, per questo il Regolamento sull'IA e la Direttiva sulla cybersecurity sono strettamente legate. Infatti, la NIS 2 impone misure di gestione del rischio e notifica degli incidenti applicabili anche ai sistemi che integrano IA. Pertanto, anche se non sia un requisito esplicito, la Direttiva promuove l'integrazione dell'IA nelle strategie di sicurezza, creando un quadro normativo che incoraggia il suo utilizzo strategico. La relazione tra IA e cybersecurity è complessa e ambivalente, caratterizzata da una dicotomia tra opportunità e rischi, da una parte rivoluziona il settore della sicurezza cibernetica e allo stesso tempo introduce nuove sfide e nuove minacce. Questi sistemi che integrano tecnologie così innovative devono essere maggiormente protetti contro accessi non autorizzati e manipolazioni. Tutte le organizzazioni e le aziende devono effettuare valutazioni di conformità, produrre apposita dichiarazione e implementare pratiche di sicurezza informatica robuste, inclusi test per identificare vulnerabilità (*penetration test*).

Per quanto riguarda l'intelligenza artificiale, l'Italia ha approntato un Disegno di Legge (DdL) specifico nel 2024 che recepisce i principi dell'AI Act, e ha redatto una strategia nazionale con il documento "Strategia Italiana per l'intelligenza artificiale 2024-2026". L'implementazione della strategia mira a posizionare l'Italia come leader nel settore dell'IA, in linea con il Regolamento europeo, concentrandosi su quattro macroaree: ricerca scientifica, pubblica amministrazione, imprese e

[10] https://www.giulianogroup.it/2024/09/10/normativa-sicurezza-informatica-legge-90/

formazione, con l'obiettivo di promuovere l'innovazione e migliorare la qualità della vita dei cittadini. La legge 90/2024, recentemente varata, supporta questa strategia promuovendo la cooperazione tra pubblico e privato e introducendo sanzioni per abusi nell'uso dell'IA. Questa legge, come anche l'*AI Act* europeo, mira a bilanciare innovazione e sicurezza con etica e protezione dei dati, in linea con il Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea (UE), che disciplina il modo in cui le aziende e le altre organizzazioni devono trattare i dati personali. La Strategia enfatizza l'importanza di etica, trasparenza e protezione dei dati, in particolare nei settori della sanità e giustizia[11], contribuendo a creare un ecosistema di IA sicuro e responsabile[12] e integra la cybersecurity come elemento chiave per garantirne lo sviluppo. Inoltre, il documento strategico sottolinea l'importanza della *cyber threat intelligence*[13], sfruttando l'IA per migliorare la capacità di rilevazione e risposta alle minacce informatiche, riconoscendo che i criminali informatici già utilizzano l'IA per rendere maggiormente sofisticate le loro tecniche di attacco, come la profilazione e il *social engineering*, in risposta alle quali propone di potenziare le difese cibernetiche nazionali anche attraverso l'adozione di soluzioni IA avanzate[14].

Infine, la strategia promuove la creazione di infrastrutture dati sicure e incentiva la ricerca scientifica per connettere le unità di ricerca nazionali con piattaforme internazionali, assicurando che l'Italia possa affrontare le sfide della cybersecurity in un contesto tecnologico in rapida evoluzione[15], includendo l'implementazione di "spazi di sperimentazione normativa" (*sandbox*) e fornendo un ambiente controllato che agevoli lo sviluppo e la validazione di soluzioni di IA. Queste *sandbox* sono progettate per promuovere l'innovazione e garantire un uso responsabile delle tecnologie IA, permettendo ai fornitori di sviluppare, addestrare e validare i loro sistemi in condizioni reali sotto supervisione regolamentare[16].

L'Agenzia per l'Italia Digitale (AgID) e l'Agenzia per la Cybersicurezza Nazio-

---

[11] https://www.ip4fvg.it/2024/07/31/la-strategia-italiana-per-lintelligenza-artificiale-2024-2026/

[12] https://ntplusdiritto.ilsole24ore.com/art/la-legislazione-sull-intelligenza-artificiale-italia-2024-innovazioni-etica-e-investimenti-AFoTawuD

[13] La Cyber Threat Intelligence (CTI) è una disciplina della sicurezza informatica che si concentra sulla raccolta, analisi e diffusione di informazioni strutturate riguardanti minacce informatiche potenziali o esistenti. L'obiettivo principale della CTI è fornire alle organizzazioni le informazioni necessarie per anticipare, prevenire e rispondere agli attacchi informatici, comprendendo il comportamento degli attori delle minacce, le loro tattiche e le vulnerabilità che sfruttano. Fonte: https://www.ibm.com/it-it/topics/threat-intelligence

[14] https://www.agid.gov.it/it/notizie/pubblicato-il-documento-completo-della-strategia-italiana-per-lintelligenza-artificiale-2024-2026

[15] https://www.cybersecurity360.it/cybersecurity-nazionale/litalia-ha-la-sua-strategia-sullai-anche-il-rischio-cyber-tra-i-punti-cardine/

[16] https://www.fiscoetasse.com/approfondimenti/16314-sandbox-ai-le-norme-previste-dal-ddl-sullintelligenza-artificiale.html

nale sono incaricate della gestione congiunta di questi spazi[17] che, auspicabilmente in collaborazione con il Ministero della Difesa, potrebbero essere utilizzati anche per gli aspetti relativi ai sistemi IA impiegabili in chiave "duale"[18]. Questo approccio permetterebbe di mirare a facilitare la transizione tecnologica del paese, supportando lo sviluppo di soluzioni innovative mentre si assicura la conformità con le normative europee e si protegge la sicurezza nazionale.

3. Cybersecurity e intelligenza artificiale in ambito Difesa

La sicurezza cibernetica nel settore della difesa nazionale è una priorità strategica con un'architettura complessa che coinvolge diverse istituzioni e agenzie. Il Ministero della Difesa, attraverso il Comando Operazioni in Rete (COR), guida le operazioni nel dominio cibernetico, proteggendo le reti e le infrastrutture critiche da minacce informatiche. L'ACN coordina gli sforzi tra vari attori, inclusa la Difesa e i servizi di intelligence come l'Agenzia Informazioni e Sicurezza Esterna (AISE) e l'Agenzia Informazioni e Sicurezza Interna (AISI)[19]. La strategia di cybersicurezza della difesa si concentra su innovazione, resilienza e contrasto alle minacce, promuovendo l'integrazione di tecnologie avanzate come l'intelligenza artificiale. Inoltre, la collaborazione con il settore privato e accademico è fondamentale per sviluppare capacità avanzate e garantire l'autonomia strategica del paese[20].

La Legge 90/2024 ha un impatto significativo sulla difesa nazionale, in quanto introduce misure per rafforzare la sicurezza cibernetica nazionale, con particolare attenzione alla protezione delle infrastrutture critiche e alla resilienza delle pubbliche amministrazioni. La legge amplia i confini tracciati della NIS 2, che non tratta il dominio militare, estendendoli al perimetro di sicurezza nazionale cibernetica, includendo anche i sistemi di interesse militare, prevedendo l'inasprimento delle pene per i reati informatici che li colpiscono. Inoltre, potenzia il ruolo dell'ACN nel coordinamento delle attività di difesa cibernetica e promuove la collaborazione tra il settore pubblico e privato per sviluppare capacità avanzate[21]. Queste misure sono in linea con la strategia della Difesa per la cybersicurezza, che mira a consolidare le

[17] https://documenti.camera.it/leg19/dossier/pdf/AP0124.pdf

[18] https://www.iassp.org/2020/11/classificazione-dinamica-del-concetto-di-dual-use/ https://www.ispionline.it/it/pubblicazione/il-dual-use-un-concetto-chiave-la-difesa-nel-sistema-paese-21593

[19] https://www.ispionline.it/it/pubblicazione/cybersecurity-larchitettura-della-difesa-italiana-24546

[20] https://www.cybersecitalia.it/la-strategia-per-la-cybersicurezza-della-difesa-in-3-azioni-intervista-a-carmine-masiello-sottocapo-di-stato-maggiore/26206/

[21] https://www.anitec-assinform.it/i-nostri-associati/aggiornamenti/eventi/legge-90-2024-sulla-cybersicurezza-e-reati-informatici-i-nuovi-obblighi-per-la-pa-e-l-impatto-sulle-imprese.kl

capacità di *cyber defence* e garantire il ripristino tempestivo delle infrastrutture in caso di attacchi.

Nell'ambito della interrelazione tra cybersecurity e IA, la Legge 90/2024 sostiene la Strategia italiana per l'intelligenza artificiale 2024-2026, che a sua volta ne riconosce l'importanza cruciale negli ambiti militare e della Difesa, puntando a migliorare le capacità operative e di sicurezza nazionale. La Strategia IA della Difesa italiana, insieme al documento di implementazione attualmente in sviluppo, si inserisce nel contesto più ampio della Strategia Nazionale per l'intelligenza artificiale 2024-2026 che, in aderenza anche a quanto definito dalla strategia NATO[22] sull'IA, mira a integrarla nella Difesa per migliorare le capacità militari anche nella condotta di operazioni. Ciò privilegiando un approccio collaborativo, responsabile e sicuro, come evidenziato anche in occasione degli ultimi seminari del Centro Alti Studi Difesa (CASD), ove sono stati discussi anche temi sulle implicazioni etiche, normative e strategiche dell'IA nella Difesa nel contesto delle nuove e future sfide digitali e dell'accelerazione nell'innovazione tecnologica[23].

In questo quadro, stabilire una governance integrata per la cybersecurity e l'IA che preveda anche degli spazi per la sperimentazione di nuove soluzioni tecnologiche anche dal punto di vista di una possibile regolamentazione in ambito della Difesa, potrebbe diventare un imperativo morale e strategico, oltre che un acceleratore tecnologico per l'adozione e l'adeguamento normativo che potrebbe rendersi necessario nell'impiego di tali soluzioni tecnologie sia in campo militare che civile (ambito duale o *dual use*), mantenendo al contempo un impegno verso un uso etico e regolamentato della tecnologia attraverso la sperimentazione in ambienti controllati.

La ricerca, lo sviluppo e la sperimentazione di nuove tecnologie legate alla cybersicurezza e all'IA, nel panorama normativo delineato, assume pertanto un ruolo cruciale nell'identificazione e sviluppo di tecnologie e soluzioni dirompenti che trova la sua massima espressione nell'alveo della cooperazione militare con il comparto industriale e quello accademico, ove l'opportunità di creare spazi di sperimentazione *ad-hoc* potrebbe aprire nuove opportunità nell'ambito delle sandbox regolamentari.

Sebbene il primo caso ufficiale di introduzione delle *sandbox* regolamentari sia stata un'iniziativa della *British Financial Conduct Authority* (FCA), tuttora attiva dal 2016 per i servizi finanziari[24], le *sandbox* regolamentari sono state introdotte e

[22] https://www.nato.int/cps/en/natohq/official_texts_227237.htm

[23] https://formiche.net/2024/04/intelligenza-artificiale-difesa-seminario-casd/

[24] https://whatnext.law/2023/05/19/e-u-regulatory-sandboxes-a-brief-overview/

utilizzate ad esempio dal Canada[25] anche nel contesto della Difesa, attraverso il programma *Innovation for Defence Excellence and Security* (IDEaS)[26], nell'ambito del *Counter Uncrewed Aerial Systems* (CUAS) *Sandbox*. Questi spazi di sperimentazione regolamentata offrono un ambiente controllato per testare tecnologie innovative di difesa, in particolare contro i droni.[27] Questi ambienti permettono di ricevere feedback da esperti militari e di sicurezza, facilitando lo sviluppo di tecnologie che rispondano alle esigenze operative reali delle Forze Armate ed anche alla loro regolamentazione e normativa di impiego.

Pertanto, anche se le applicazioni della cybersecurity e dell'intelligenza artificiale in ambito militare e di Difesa non sono direttamente regolamentate dalla normativa europea, l'introduzione di un *framework* basato sulle sandbox regolamentari potrebbe essere esteso alla sperimentazione di tecnologie di cybersecurity e AI anche di natura militare o *dual-use* nel settore della Difesa, estendendo il concetto ai *battle lab*, laboratori avanzati di simulazione per la sperimentazione di concetti operativi e tecnologie militari di prossima o futura introduzione, già in uso nella Difesa.

Tuttavia, né la Legge 90/2024 né il Documento Strategico sulla Cybersicurezza Nazionale 2022-2026 menzionano esplicitamente l'uso delle sandbox regolamentari nel contesto della cybersecurity. In questo scenario, l'uso di spazi di sperimentazione controllata in ambito IA e/o difesa cibernetica sembra al momento contemplato esclusivamente nel DdL sull'IA, rimandando nel documento di Strategia nazionale per l'intelligenza artificiale 2024-2026 alla stipula di specifici protocolli per la cybersicurezza.

4. Framework per un nuovo paradigma di regolamentazione per la cybersecurity e l'intelligenza artificiale

Da quanto esposto, sta emergendo un nuovo paradigma per la regolamentazione di tecnologie innovative con aree di sperimentazione fisiche e/o digitali (*phygital*), capace di integrare approcci partecipativi e adattivi per affrontare minacce cibernetiche avanzate, unendo la cybersicurezza e l'intelligenza artificiale nel

[25] https://www.canada.ca/en/government/system/laws/developing-improving-federal-regulations/modernizing-regulations/regulatory-sandbox.html

[26] https://www.cmisa.ca/articles/ideas-innovator-update-1

[27] https://science.gc.ca/site/science/en/blogs/defence-and-security-science/counter-drone-prototypes-undergo-real-world-testing-ideas-sandbox

riconoscimento della ormai super convergenza tra tutti i settori, abilitata dalla digitalizzazione e accelerata dai modelli di intelligenza artificiale, per proteggere infrastrutture critiche e strategiche.

Nonostante l'approccio normativo ancora precauzionale[28] che emerge dall'attuale panorama legislativo, che può essere particolarmente rilevante in ambiti come l'ambiente e la salute pubblica, ma può spesso risultare inefficace o - peggio - deleterio quando si regolamentano tecnologie emergenti, si intravedono nuove potenzialità di cambiamento, determinatesi anche dalla consapevolezza a livello europeo di poter perdere vantaggio competitivo nella corsa per lo sviluppo di tecnologie abilitanti, innovazione e sicurezza.

Intercettare innovazioni tecnologiche che avanzano a velocità considerevoli, vedasi i modelli fondazionali di *Large Language Model* (LLM) che, come il caso di *OpenAI* ed il suo *bot* conversazionale *ChatGPT*, in meno di un lustro stanno cambiando il modo di pensare e di lavorare delle persone, o tecnologie che già oggi stanno emergendo sottotraccia in ambiti relegati a settori di nicchia, ma che sono potenzialmente dirompenti una volta immessi nel sistema o nel mercato.

Regolamentare le nuove tecnologie emergenti è un vero e proprio dilemma metodologico, oggetto di studio dai primi anni 80 del Novecento, un punto di riferimento fondamentale nei dibattiti sulla valutazione della tecnologia di intelligenza artificiale, e prende il nome dal suo ideatore *David Collingridge.*

In *The Social Control of Technology"*[29], *Collingridge* enuncia che quando si cerca di influenzare o controllare lo sviluppo di una tecnologia, questo comporta un doppio vincolo: il problema informativo, dove gli impatti di una tecnologia non possono essere facilmente previsti per essere regolamentati finché essa non è sufficientemente sviluppata e ampiamente utilizzata, e il problema di potere, o meglio di abilità alla governance una volta che la tecnologia è diventata radicata, diventa difficile modificarla o controllarla.

Collingridge intercetta un momento, detto "*sweet spot*", più o meno ampio, ove la tecnologia non è sufficientemente matura o socialmente/economicamente introdotta e in cui le normative non sono ancora strettamente definite. In questo "momento magico" è possibile operare per una Valutazione Costruttiva della Sostenibilità (CSA)[30] e quindi dove rivedere gli attuali approcci a quella determinata inno-

---

[28] Il principio di precauzione, come definito dall'UE, stabilisce che "in caso di rischio di danno grave o irreversibile, l'assenza di una piena certezza scientifica non deve costituire un motivo per rinviare l'adozione di misure adeguate ed effettive" Comunicazione COM(2000) UE n.1

[29] The Social Control of Technology (New York: St. Martin's Press; London: Pinter) ISBN 0-312-73168-X

[30] Assessment che consente di applicare la valutazione della sostenibilità alle tecnologie emergenti

vazione, procedere alla valutazione analitica della sostenibilità e ridefinire quadri di governance deliberativa applicati a diversi contesti (fig.1).

L'innovazione responsabile e sicura prevede uno sviluppo concettuale della CSA, con quattro principi di progettazione - transdisciplinarità, apertura, esplorazione dell'incertezza e anticipazione - che possono essere seguiti quando si applicano, contestualmente al loro sviluppo, le valutazioni di sostenibilità delle tecnologie emergenti.[31]

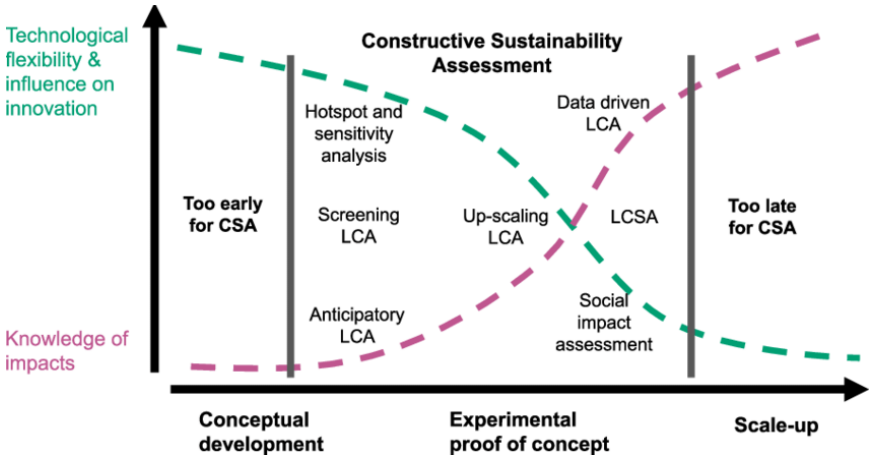


Fig. 1: *Collingridge Dilemma Diagramm: How to find the Sweet Spot in riferimento al Constructive Sustainability Assessment (CSA) delle tecnologie emergenti.*

La "Regolamentazione Anticipatoria"[32], un nuovo paradigma di regolamentazione, fornisce una serie di comportamenti e strumenti (in sostanza, un modo di lavorare) volti ad aiutare gli enti regolatori e il governo a identificare, costruire e testare soluzioni alle sfide emergenti, sia sociali che tecnologiche. Il procedimento include tra i suoi strumenti l'attuazione proprio delle "*sandbox*"[33] veri e propri banchi di prova sperimentali[34] dove l'uso di dati aperti, l'interazione tra regolatori e

come parte di un approccio deliberativo più ampio.

[31] Matthews, Nicholas & Stamford, Laurence & Shapira, Philip. (2019). Aligning sustainability assessment with responsible research and innovation: Towards a framework for Constructive Sustainability Assessment. Sustainable Production and Consumption. 20. 10.1016/j.spc.2019.05.002.

[32] Il termine è stato coniato al laboratorio di anticipazione sociale Nesta.co.uk sotto il Governo Tony Blair nel 1998.

[33] Sandbox è un termine ampiamente utilizzato in ambito informatico, è un ambiente di prova, spesso slegato dal normale flusso di ambienti predisposti per lo sviluppo e il test delle applicazioni. Il termine è mutuato dalla lingua inglese, nella quale indica il recinto della sabbia destinato ai giochi dei bambini.

[34] Nuovi approcci come il sandbox della Financial Conduct Authority https://www.fca.org.uk/firms/

innovatori nel processo e, in alcuni casi, il coinvolgimento attivo del pubblico rappresentano un approccio non più precauzionale, ma metodologico, in grado intercettare quel "*sweet spot*" individuato nel Dilemma di *Collingridge*.

Questo nuova forma di regolamentazione supera l'approccio tradizionale basato su regole statiche[35] in un sistema attuale globalizzato e interdipendente dove, parafrasando Eraclito[36]: "Tutto scorre" - "Nulla sta fermo", e dove occorre innestare un approccio di "neutralità tecnologica"[37] che non identifica le singole tecnologie all'interno di un quadro normativo o di un regolamento, ma piuttosto alla tutela di principi basilari. In risposta, è emersa una nuova serie di pratiche di regolamentazione in diversi stati e, a livello di normativa europea con l'AI Act all'Art.57 vengono introdotte le "*regulatory sandbox*", che rimodellano il ruolo del processo di governo nel supportare l'innovazione e se applicabile già durante il loro sviluppo, sperimentare tecnologie e definire normative *by design* in aree dove, per un predeterminato momento, è possibile applicare regole più blande concordate con le Autorità regolatorie. Infatti, le sandbox regolamentari[38] sono ambienti controllati e protetti che permettono di testare tecnologie, prodotti o servizi innovativi basati sull'IA in condizioni reali, sotto la supervisione delle autorità competenti e dove le attuali regolamentazioni, ad esempio, su privacy e AI, sono applicate con specifiche e deroghe, grazie al controllo e alla partecipazione diretta con le autorità competenti che presidiano le diverse fasi di sviluppo.

Le *sandbox* permettono di intercettare il "*sweet spot*" tra "abilità di controllo" e "impatto della conoscenza" previsto dal Dilemma di *Collingridge*, fornendo strumenti efficaci per una nuova modalità di creazione di regolamentazioni e leggi, facilitando così una transizione più fluida verso l'adozione collaborativa tra tecnici e regolatori, sicura e su larga scala di nuove tecnologie, nella fattispecie legate all'uso della IA nella cybersecurity.

Attualmente vi sono esempi di "regolamentazione anticipata" promosse direttamente dalle autorità competenti, che utilizzano lo strumento della *sandbox*: ad esempio, per il settore finanziario, la Banca d'Italia ha emanato di propri bandi per dare l'opportunità agli innovatori di proporre nuove soluzioni; oppure, come la Spagna, che ha attuato la prima *sandbox* regolamentare per modelli di AI direttamente

innovation/regulatory-sandbox

[35] https://anuariocompetencia.fundacionico.es/files/original/b954af06e25b99c4bfd9b52b30381c8b8437f6fe.pdf

[36] Tema filosofico del Divenire o Pánta rheî o panta rei (in greco antico: πάντα ῥεῖ?, "tutto scorre") celebre aforisma attribuito a Eraclito Eraclito, 500 a.C.

[37] https://www.ilsole24ore.com/art/auto-governo-punta-strada-neutralita-tecnologica-ecco-cosa-vuol-dire-AEGj1Z5C?refresh_ce=1

[38] https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733544/EPRS_BRI(2022)733544_EN.pdf

dal governo centrale.

In tema di cybersecurity, le autorità, le imprese e la Pubblica Amministrazione impegnate in sfide tecniche legate all'IA, hanno possibilità grazie alle *sandbox*, di testare, con approccio empirico[39], le difese dei sistemi di IA contro attacchi cibernetici orientati, ad es., a ingannare o manipolare l'algoritmo (attacchi "*adversarial*")[40]; la protezione dei modelli, valutando metodi per proteggere i modelli stessi da furti o da *reverse engineering*; l'integrità dei dati di addestramento, verificando la robustezza dei sistemi contro la manipolazione dei dati ed evitare così la produzione di *output* artefatti e dannosi (*data poisoning)*[41], che risultano particolarmente dannosi quando utilizzati per il supporto decisionale sia in campo civile che per la Difesa.

Le attuali minacce che interessano il settore della Difesa, non sono più solo attacchi di segregazione con conseguente richiesta di riscatto, oppure il blocco di sistemi operativi che governano le infrastrutture del sistema, oggi come non mai diviene imperativo porre interesse agli attacchi "silenziosi" rivolti ai furti di dati tramite *data-breach*[42] in specifiche banche dati.
Grandi archivi centralizzati stanno emergendo su database strategici, come lo Spazio Europeo dei Dati Sanitari (European Health Data Space, EHDS)[43], la banca delle Identità Digitali o *Digital Wallet* (electronic IDentification, Authentic and trust Services, eIDAS 2)[44] riconosciute da tutti gli Stati membri, e, nel settore privato, le banche dati genetiche di gruppi di ricerca impegnati nella creazione di passaporti farmacogenetici per la medicina di precisione[45]. Sebbene queste infrastrutture siano nate con i migliori presupposti, rappresentano anche significative criticità in termini di cybersicurezza generando un nuovo "perimetro di sicurezza" interconnesso. Essendo grandi *repository* centralizzati, custodiscono dati di enorme valore la cui riservatezza, integrità e disponibilità devono essere attentamente garantite. La mancanza di adeguata protezione potrebbe avere conseguenze disastrose per la sicurezza nazionale ed europea, oltre che per la privacy dei cittadini. L'accentramento di dati sensibili può innescare effetti a catena imprevedibili nell'ecosistema digitale, se

---

[39] Kousik Barik, Sanjay Misra, "Adversarial attack defense analysis: An empirical approach in cybersecurity perspective" Software Impacts, Volume 21, 2024, 100681, ISSN 2665-9638, https://doi.org/10.1016/j.simpa.2024.100681. (https://www.sciencedirect.com/science/article/pii/S2665963824000691)

[40] Gli Adversarial attacks sono cyber attacchi realizzati per ingannare i sistemi di intelligenza artificiale, inducendoli a fare previsioni o decisioni errate o non volute. Gli attori delle minacce introducono gli attacchi nei dati di input, alterando i dati originali o il modello di IA stesso modificandone i parametri o l'architettura (solitamente relativamente ai Deep Learning Models).

[41] https://www.cybersecurity360.it/outlook/data-poisoning-pericolo-ai/

[42] https://www.garanteprivacy.it/data-breach

[43] Spazio europeo dei dati sanitari https://eur-lex.europa.eu/legal-content/IT TXT/?uri=CELEX:52022PC0197

[44] eIDAS (electronic IDentification, Authentic and trust Services)

[45] https://www.insalutenews.it/in-salute/un-passaporto-farmacogenetico-basato-sul-dna-indichera-farmaci-e-dosi-piu-efficaci-per-ogni-paziente/

non adeguatamente mitigati. In particolare, se questi dati finissero nelle mani di organizzazioni terroristiche o avversarie, potrebbero diventare strumenti di guerra non convenzionale[46] estremamente potenti: dati biometrici, sanitari e genetici potrebbero essere utilizzati per creare informazioni false, generare sfiducia nelle istituzioni o per azioni di ricatto psicologico, alimentando conflitti interni di diversa natura (*Cognitive Warfare*[47]).

Viviamo in un mondo interconnesso, che coinvolge molti settori e discipline di studio in una grande convergenza tecnologica[48], e anche se la Direttiva NIS 2 enfatizza l'importanza di identificare e proteggere le attività strategiche con la loro mappatura, ci si chiede: cosa è veramente strategico e critico in un mondo interconnesso e in continuo cambiamento? Quali interconnessioni nascoste o meno esistono e di quale portata?

Il processo di mappatura identificato dalla norma NIS 2 non rispecchia la complessità degli ecosistemi interessati. Un mero elenco non costituisce una "mappa" capace di rappresentare un sistema sul quale è possibile comprendere quali sono o potrebbero essere gli effetti a catena di decisioni, di nuove regole o di un attacco cibernetico cibernetico.

Per aderire ai presupposti della Strategia Nazionale per l'IA, il *framework* qui proposto prevede non solo l'apertura di *regulatory sandbox* in maniera più estesa possibile, ma vi aggiunge la necessità di uno strumento di mappatura avanzato. In particolare, la realizzazione di un "*System Mapping* dinamico"[49] delle infrastrutture strategiche e critiche i cui "nodi" di sistema, sono composti dalle aziende elencate negli allegati della NIS 2, le sue "variabili" ed il sistema delle interconnessioni (tra loro dette "relazioni causali"), rende possibile visualizzare l'evoluzione delle interdipendenze tra i diversi nodi, monitorando tutto l'ecosistema in tempo reale e aggiornando ogni evento di natura regolatoria, evolutivo o turbativo proveniente da un attacco cibernetico, evidenziando le criticità di sistema.

Un vero e proprio "*Digital Twin*"[50] dell'ecosistema delle infrastrutture strate-

---

[46] UW, dall'inglese unconventional warfare — consiste nel tentativo di ottenere la vittoria sul nemico attraverso l'acquiescenza, la capitolazione o il sostegno clandestino di una parte del popolo (teoricamente) nemico.

[47] https://www.difesa.it/assets/allegati/29459/4.cognitive_warfare_-_la_competizione_nella_dimensione_cognitiva._ed.2023.pdf

[48] Jamie Metzl "Superconvergence: How the Genetics, Biotech, and AI Revolutions Will Transform our Lives, Work, and World" Timber Press (June 11, 2024)

[49] "Cluster Map" e la "Interconnected Circles Map"

[50] Un gemello digitale (Digital Twin) è un modello digitale di un prodotto, di un sistema o di un processo fisico del mondo reale, previsto o reale (un gemello fisico), che funge da controparte digitale effettivamente indistinguibile per scopi pratici, come la simulazione, l'integrazione, i test, il

giche e critiche, ma su cui poter anche simulare l'introduzione di innovazioni tecnologiche, attacchi, "*black swan*"[51], supportando l'implementazione delle misure di gestione dei rischi di cybersicurezza richieste dall'articolo 21 della Direttiva NIS 2.

L'obiettivo della protezione delle infrastrutture strategiche, a norma della direttiva europea NIS 2, dovrebbe provvedere a fornire strumenti nuovi alla pubblica amministrazione (PA), alle aziende e alla Difesa, prevedendo la creazione di *regulatory sandbox* nelle quali sia previsto un test di simulazione all'interno di una Mappa Dinamica di sistema, gestita e messa a disposizione a livello superiore (ACN con la NIS 2 è sicuramente l'ente maggiormente qualificato a definire compiti e attività).

Abbiamo citato esperienze di *sandbox* regolamentari in premessa relative al settore *Fintech*[52], la cybersicurezza del settore finanziario è strettamente legata alla sicurezza nazionale per diversi motivi, il sistema finanziario è infatti considerato un settore critico nazionale nella NIS 2 (All. II Altri Settori Critici). Attacchi informatici al settore potrebbero destabilizzare l'economia e, da non sottovalutare, la protezione dei dati bancari è essenziale per prevenire il finanziamento di attività illecite legate al terrorismo o al riarmo di stati sottoposti a sanzione.

A livello europeo, diverse iniziative rafforzano la cybersicurezza nel settore finanziario. L'*European Union Agency for Cybersecurity* (ENISA)[53] fornisce linee guida specifiche per la sicurezza informatica in questo ambito, mentre la Direttiva NIS 2 introduce requisiti più stringenti per la protezione delle infrastrutture finanziarie. Il *Digital Operational Resilience Act* (DORA)[54] mira a migliorare la resilienza digitale del settore finanziario, garantendo continuità operativa in caso di attacchi informatici, e un *framework* di cooperazione transfrontaliera facilita la condivisione di informazioni tra autorità di vigilanza, supportato da uno strumento messo a disposizione dei diversi istituti bancari *Digital Finance Platform*[55], dedicata alla gestione delle *regulatory sandbox* nel *Fintech*.

La Banca d'Italia si sta affermando come un importante promotore di innovazione nel *Fintech*, attraverso l'implementazione di un programma di sperimentazione controllata utilizzando Sandox Regolamentari. Questo programma, avviato grazie al Decreto MEF del 30 aprile 2021, n. 100, in attuazione del "Decreto Crescita"

monitoraggio e la manutenzione.

[51] https://it.wikipedia.org/wiki/Teoria_del_cigno_nero

[52] Il termine FinTech nasce dalla contrazione di 'Finance' e 'Technology'. Tale denominazione incapsula l'essenza di un approccio che ha come fulcro l'utilizzo di strumenti digitali avanzati per innovare e ottimizzare il settore finanziario.

[53] https://www.enisa.europa.eu/

[54] https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

[55] https://digital-finance-platform.ec.europa.eu

(Decreto-Legge 30 aprile 2019, n. 34), che disciplina il funzionamento del Comitato Fintech e delle sperimentazioni. La *sandbox* regolamentare, supervisionata congiuntamente da Banca d'Italia, CONSOB e IVASS, consente a startup, imprese consolidate e intermediari finanziari di operare con deroghe normative temporanee, partecipando a bandi pubblici, alcuni dei quali co-finanziati, favorendo così lo sviluppo di soluzioni innovative in un ambiente regolamentato flessibile.

I progetti accettati riguardano attività correlate al riconoscimento di chi accede ai siti e vi opera il c.d "o*nboarding*", dove è essenziale attivare procedure di sicurezza definite *Know Your Customer* (KYC) oggi normate dalla misura di sicurezza della PSD2[56]. Le proposte concluse sono state ad esempio lo sviluppo di una piattaforma innovativa per il monitoraggio in tempo reale delle operazioni di pagamento, aumentando così la capacità di prevenzione delle frodi e di strumenti di riconoscimento biometrico avanzato e soluzioni di identità digitale.

Sperimentare tali soluzioni di nel sistema di onboarding del riconoscimento tramite dati biometrici, o addirittura genetici, potrebbe fare emergere che tali strumenti di riconoscimento possono rivelarsi potenti ma estremamente fragili: una volta violate le credenziali, infatti, queste non possono essere sostituite come una *password*, impedendo ai cittadini di riottenere una propria *digital-ID* con notevoli conseguenze sul piano operativo, socio-economico, ma anche con notevoli implicazioni sotto il profilo della sicurezza nazionale.

Quando sussistono minacce provenienti da intelligenza artificiale, strategie cognitive, accessi fisici a dispositivi digitali in uso *consumer*[57], allora il livello di pensiero e gli strumenti per la regolamentazione devono evolvere verso un approccio più proattivo, adattivo e condiviso tra molte expertise, per trasformare attacco e difesa in un gioco a somma zero dove l'obiettivo del difensore non è solo prevenire le perdite, ma anche rendere gli attacchi meno redditizi per gli aggressori[58].

Conclusioni

L'Italia ha interpretato in maniera estensiva e integrato con visione pionieristica gli spunti normativi sulla sicurezza cibernetica offerti dal recepimento della NIS 2 e dell'*AI Act*, applicandoli alla normativa nazionale sulla cybersicurezza e al DdL

[56] La direttiva (UE) 2015/2366a PSD2 – Payment Service Directive 2 – è una direttiva europea messa in atto allo scopo di regolamentare i servizi di pagamento digitali nel territorio dell'UE e prevede il riconoscimento a due fattori.

[57] https://www.wired.it/article/nuovi-pos-rischio-violazione/

[58] https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/cyber-advisors-security-services-providers-can-use-zero-sum-game-theory-framework-to-benefit-clients

su IA, includendo il concetto di sperimentazione attraverso le *regulatory sandbox*.

Il *framework*, nel paradigma della regolamentazione anticipata, propone la creazione di un modello esteso di *regulatory sandbox*, quale strumento di innovazione responsabile per tutte le tecnologie emergenti e nella fattispecie della cybersicurezza. L'ACN potrebbe, al pari della Banca d'Italia per il *Fintech*, proporsi quale parte promotrice fornendo proattivamente anche gli strumenti di valutazione degli impatti sull'ecosistema. Tale modello "esteso" potrebbe contemplare l'adozione di una strategia di gestione collaborativa, facilitata da strumenti tecnici adeguati, quali mappe di sistema e strumenti di simulazione, creando quegli strumenti operativi che permettano di alleggerire, anche per gli aspetti di cybersecurity, i passaggi burocratici e un'inversione di tendenza nella produzione normativa, passando dal paradigma *top-down* a quello *bottom-up open-source*[59].

In ambito Difesa sarebbe auspicabile l'implementazione di un *framework* "esteso" per la creazione di spazi di sperimentazione controllata relativi a tecnologie emergenti in ambito militare e/o duale, con particolare riferimento alla fattispecie su cybersecurity e IA, atta a definire anche gli ambiti normativi e dottrinali di impiego in operazioni, con particolare riferimento anche ai settori classificati, ovvero quelli che trattano dati e informazioni di non pubblica divulgazione, che sono regolamentati da apposita normativa per la sicurezza nazionale.

Come nel caso di studio proposto relativo alla Banca d'Italia la creazione di tali spazi "estesi" potrebbe essere sostenuta dalle opportunità offerte da bandi ad-hoc di finanziamento o cofinanziamento per la ricerca e innovazione tecnologica come quelli offerti dal Piano Nazionale di Ricerca Militare (PNRM) e/o da altre iniziative bilaterali con università e industria, o ad esempio sul modello *sandbox* canadese, anche coinvolgendo i *battle lab* e i Centri di Valutazione (CEVA) e di Sperimentazione della Difesa.

[59] https://www.gartner.com/en/articles/this-new-strategy-could-be-your-ticket-to-change-management-success

N. 1 - 2025 - pp. 26-36

Data breach tra privacy e security: una proposta di sopravvivenza normativa, etica, logica e organizzativa in caso di violazioni nel trattamento dei dati

Andrea Lisi

Abstract: GDPR e Codice della protezione dei dati personali, da una parte, e Cybersecurity Act, le direttive NIS, la legge 90/2024 e il decreto legislativo 138/2024, dall'altra, non possono essere avvertite come normative parallele (come troppe volte accade) o peggio antinomiche, perché esse perseguono comuni finalità di tutela dell'individuo, in maniera diretta, nel primo caso, e indiretta, nel secondo, allorquando dal rischio sistemico di un'infrastruttura critica (ma anche di un sistema ritenuto essenziale o di particolare rilevanza per il nostro Paese) possono derivare danni a tutti i cittadini. Data Protection e Cybersecurity, quindi, lavorano insieme nella tutela della nostra dimensione individuale (protezione dei dati personali) o collettiva (sicurezza a tutela di servizi essenziali o di particolare rilevanza per il Sistema Paese). Questa duplice dimensione di tutela individuale e collettiva insita nelle due discipline ben si esprime in caso di violazioni di dati personali che ormai caratterizzano l'attuale periodo storico, contraddistinto da una particolare fragilità della nostra dimensione digitale, suscettibile di continui attacchi sia alle infrastrutture (anche critiche) del nostro Paese e sia a qualsiasi organizzazione (privata o pubblica).

GDPR and the Personal Data Protection Code, on the one hand, and the Cybersecurity Act, the NIS directives, Law 90/2024 and Legislative Decree 138/2024, on the other, cannot be perceived as parallel regulations (as too often happens) or worse, antinomian, because they pursue common goals of protecting the individual, directly, in the first case, and indirectly, in the second, when damage may be caused to all citizens by the systemic risk of a critical infrastructure (but also of a system considered essential or of particular importance for our country). Data Protection and Cybersecurity, therefore, work together in the protection of our individual dimension (protection of personal data) or collective dimension (security to protect services that are essential or of particular relevance for the Country System). This dual dimension of individual and collective protection inherent in the two disciplines is well expressed in the case of personal data breaches that now characterise the current historical period, marked by a particular fragility of our digital dimension, susceptible to continuous attacks both on the infrastructures (including critical infrastructures) of our country and on any organisation (private or public).

Parole chiave: data protection, cybersecurity, data breach

Sommario: 1. Il diritto alla protezione dei dati personali come presidio a tutela dei diritti e libertà fondamentali dell'uomo - 2. Data protection e Cybersecurity come espressione di due facce della stessa medaglia - 3. Data breach e personal data breach: due facce della medaglia della security e della privacy - 4. Conclusioni

1. Il diritto alla protezione dei dati personali come presidio a tutela dei diritti e libertà fondamentali dell'uomo

Il diritto alla protezione dei dati personali nel GDPR (Regolamento UE 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati) ha assunto una funzione piena di diritto fondamentale dell'uomo con una efficacia, quindi, universale. Funzione che ben si coglie leggendo il considerando 1) del GDPR nel quale si specifica proprio che "la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano". Inoltre, il considerando 2) sottolinea ancora che "i principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche".

Tale funzione di "essere al servizio dell'uomo", ben espressa che anche nel considerando 4)[1] del GDPR, dovrebbe farci comprendere l'importanza del diritto alla

[1] "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica"

protezione dei dati personali come presidio fondamentale, pur se non assoluto, a tutela di diritti e libertà che ci riguardano, i quali in caso di sua violazione rischiano di essere gravemente calpestati. Tale funzione, inoltre, spiega pienamente l'ambito di applicazione territoriale extra UE che viene sottolineato nel considerando 14) laddove si afferma che "è opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali", come poi peraltro si respira nei primi articoli del Regolamento UE dedicati all'oggetto, alle finalità e agli ambiti di applicazione materiale e territoriale[2].

Questa connotazione di diritto fondamentale ben rappresenta le intenzioni del legislatore di considerare la data protection come un diritto di cittadinanza globale, slegato quindi dai confini geografici dei singoli Stati nazionali, con una pienezza integrale di tutela dell'uomo in quanto tale, che lo avvicina funzionalmente alla visione di "Costituzione della Terra" ben espressa negli studi di Luigi Ferrajoli[3].

In quanto diritto fondamentale la protezione dei dati personali, insieme ad altri diritti come il diritto "alla vita, all'integrità fisica e psichica, alle libertà, alla salute, all'istruzione, alla sussistenza, alla sicurezza e al libero sviluppo della persona" andrebbe considerato[4] come diritto universale, spettante a tutti gli esseri umani e perciò – almeno secondo certi limiti - indivisibile e indisponibile[5].

In quanto diritto che è espressione diretta di cittadinanza digitale, quindi ab origine privo di confini territoriali, il diritto alla protezione dei dati personali deve ovviamente intendersi tutelante non degli interessi di ciascuno dei titolari del trattamento, ma di tutti i cittadini della Società dell'informazione che per partecipare in essa devono necessariamente essere trattati nei loro dati personali da qualcuno dei fornitori di servizi on line e, quindi, tale diritto deve essere integralmente considerato e interpretato nell'interesse pubblico dell'intera umanità. Non dovrebbe essere

(considerando 4).

[2] Per avere una prima ed esauriente lettura di inquadramento del GDPR si consigliano i due volumi a firma di Franco Pizzetti "Privacy e diritto europeo alla protezione dei dati personali", Giappichelli editore, 2016.

[3] Per comprendere appieno gli studi di Luigi Ferraioli sui diritti fondamentali dell'uomo si consiglia la lettura di "Iura Paria – i fondamenti della democrazia", 2017, Editoriale Scientifica.
Per apprendere l'importanza (e anche i possibili limiti) degli studi di Luigi Ferrajoli si consiglia la lettura di "La teoria dei diritti fondamentali di Luigi Ferrajoli. Considerazioni epistemologiche e politiche" di Alfonso Liguori, pubblicato su Jura Gentium - Rivista di filosofia del diritto internazionale e della politica globale, 2009, acquisibile alla pagina: https://www.juragentium.org/topics/rights/it/liguori.htm.
Infine, in merito alla lungimirante proposta di Costituzione della Terra si rinvia alla sua lettura qui: https://www.costituenteterra.it/introduzione-e-testo-della-costituzione-di-ferrajoli/.

[4] Anche secondo quanto si legge nella proposta di Costituzione della Terra di Luigi Ferrajoli.

[5] Art. 7 della proposta di Costituzione della Terra.

pertanto suscettibile di negoziazioni piene, né di rinuncia assoluta da parte dei cittadini digitalizzati, se non di volta in volta esposto a delicati bilanciamenti con altri diritti considerabili fondamentali, a piena e ineludibile tutela dei tanti e attualissimi rischi di manipolazione e profilazione selvaggia che caratterizza il mondo dell'informazione digitale[6]. In particolare, il diritto alla protezione dei dati personali, nella sua dimensione digitale che è ontologicamente a-nazionale, ha assunto una connotazione strategica ed essenziale di tutela universale, come presidio importantissimo di tanti altri diritti e libertà che rischiano a livello internazionale di essere sistematicamente indeboliti e messi in discussione dal capitalismo della sorveglianza[7].

2. Data protection e Cybersecurity come espressione di due facce della stessa medaglia

I vari regolamenti UE individuati con gli acronimi CRA[8], DSA[9], DGA[10], DMA[11], Data Act[12], Cybersecurity Act[13], GDPR[14] sino all'AI Act[15] sono ovviamente regolamen-

---

[6] Molto interessante è l'attuale dibattito sulla monetizzabilità dei dati personali. Si consiglia, in proposito, la lettura del manuale curato da Ginevra Cerrina Feroni "Commerciabilità dei dati personali", Il Mulino, 2024.

[7] Si consiglia la lettura di "Il capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri", di Soshana Zuboff, maggio 2023, Luiss University Press.

[8] Cyber Resilience Act (CRA) - Regolamento (UE) 2024/2847 relativo all'adozione di un sistema europeo comune di certificazione della cybersecurity basato sui Common Criteria.

[9] REGOLAMENTO (UE) 2022/2065 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Regolamento sui servizi digitali).

[10] REGOLAMENTO (UE) 2022/868 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).

[11] REGOLAMENTO (UE) 2022/1925 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828.

[12] REGOLAMENTO (UE) 2023/2854 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828.

[13] 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. 526/201

[14] 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 e che abroga la direttiva 95/46/CE.

[15] REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828.

tazioni stringenti[16], pensate proprio per arginare l'attuale situazione potenzialmente pericolosa per tutti i nostri diritti e libertà fondamentali[17]. Ma molti degli adempimenti ivi previsti alimentati da una ipertrofia normativa unionale senz'altro criticabile, da una parte straripano verso il mondo delle PMI, rischiando di costruire prigioni normative che non sempre fanno bene al diritto e senz'altro possono danneggiare alla lunga il nostro "piccolo" mercato europeo dedicato all'IT, dall'altra parte finiscono per disorientare anche lo stesso ambito di tutela che vorrebbero proteggere e, cioè, la costruzione di barriere di contenimento per tutti i diritti fondamentali così esposti a violazioni nell'attuale evoluzione del web e social web.

Alla luce di questo, risulta ineludibile l'esigenza di recuperare un'unica logica interpretativa che conferisca un senso comune al diluvio normativo europeo che caratterizza la "digitalità". Per farlo, oggi è indispensabile riprendere la lettura sistematica dei principi generali del diritto applicandoli, con razionalità e buon senso, a ciò che normativamente si va edificando nell'Unione Europea.

Per tale motivo, non si può non apprezzare il cammino interpretativo portato avanti nella Dichiarazione UE dei diritti e principi digitali[18], la quale ha proprio cercato di declinare i nostri diritti e libertà fondamentali in chiave digitale.

Il primo considerando della sopra citata Dichiarazione afferma solennemente che "l'Unione europea (UE) è un'«unione di valori», sancita dall'articolo 2 del trattato sull'Unione europea, e si fonda sul rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e sul rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Inoltre, secondo la Carta dei diritti fondamentali dell'Unione europea, l'UE si fonda sui valori indivisibili e universali della dignità umana, della libertà, dell'uguaglianza e della solidarietà. La Carta ribadisce, inoltre, i diritti derivanti in particolare dagli obblighi internazionali comuni agli Stati membri". Quindi, la Dichiarazione si fonda sulla Carta UE[19] dei

---

[16] Ai regolamenti richiamati sarebbe utile aggiungere le direttine NIS 1 (Direttiva UE 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione) e NIS 2 (Direttiva UE 2022/2555 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione.

[17] In proposito, ci si permette di proporre la lettura di un saggio a mia firma, dal titolo "Si può ottenere la fiducia dei cittadini digitali attraverso nuove regole?", pubblicato sulla Rivista trimenstrale Digeat (ISSN 3034-9591), in data 19 settembre 2024, disponibile alla pagina: https://digeat.info/articolo-rivista/digeat32024-lisi/ .

[18] Dichiarazione europea sui diritti e i principi digitali per il decennio digitale (2023/C 23/01), acquisibile in tutte le lingue dell'UE da questa pagina: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001.

[19] La Carta è stata proclamata ufficialmente a Nizza nel dicembre 2000 dal Parlamento europeo, dal Consiglio dell'Unione europea e dalla Commissione ed è diventata giuridicamente vincolante con l'entrata in vigore del trattato di Lisbona a dicembre 2009, e ora ha, quindi, lo stesso effetto giuridico dei trattati dell'Unione.
Il testo è acquisibile qui: https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex%3A12016P%2FTXT

diritti fondamentali, reinterpretandoli in un mondo profondamente mutato (che potrebbe metterne in discussione l'effettiva applicazione)[20].

La Dichiarazione, pertanto, costituisce guida e monito per le politiche legislative degli Stati membri e illustra in mondo efficace ai cittadini UE i diritti e le libertà fondamentali su cui si fonda l'ordinamento giuridico unionale[21]. Obiettivo esplicito della Dichiarazione è quello di promuovere un modello europeo per la trasformazione digitale, che metta al centro le persone, sia basato sui valori europei e sui diritti fondamentali dell'UE, riaffermi i diritti umani universali e apporti benefici a tutte le persone, alle imprese e alla società nel suo complesso. Per renderlo praticabile sono declinati in VI capitoli i vari principi fondamentali che devono guidare le future politiche legislative europee nel prossimo decennio[22].

---

[20] A presidio di tali diritti fondamentali esiste l'Agenzia dell'Unione europea per i diritti fondamentali (FRA) istituita nel 2007. L'agenzia sostiene la cooperazione in corso con le istituzioni dell'UE e i governi, fornendo loro consulenza indipendente e un'analisi della situazione dei diritti fondamentali. Ha istituito reti e creato legami con i paesi partner a tutti i livelli, in modo che le consulenze e le ricerche svolte possano servire ai responsabili politici dei governi nazionali e dell'UE. Info: https://fra.europa.eu/it.

[21] Esiste anche una versione semplificata della Dichiarazione per favorirne la lettura da arte dei minori. Info: https://op.europa.eu/it/publication-detail/-/publication/d39d5ad4-34d4-11ee-bdc3-01aa75ed71a1.

[22] Qui di seguito i contenuti dei vari Capitoli della Dichiarazione:
CAPITOLO I Mettere le persone al centro della trasformazione digitale
Le persone sono al centro della trasformazione digitale nell'Unione europea. La tecnologia dovrebbe essere al servizio e andare a beneficio di tutte le persone che vivono nell'UE, mettendole nelle condizioni di perseguire le loro aspirazioni, in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali.
CAPITOLO II Solidarietà e inclusione
La trasformazione digitale dovrebbe contribuire a una società e a un'economia eque e inclusive nell'UE.
declinato in:
Connettività
Ogni persona, ovunque nell'UE, dovrebbe avere accesso alla connettività digitale ad alta velocità a prezzi accessibili
Istruzione, formazione e competenze digitali
Ogni persona ha diritto all'istruzione, alla formazione e all'apprendimento permanente e dovrebbe poter acquisire tutte le competenze digitali di base e avanzate.
Condizioni di lavoro giuste ed eque
Ogni persona ha diritto a condizioni di lavoro eque, giuste, sane e sicure e a una protezione adeguata nell'ambiente digitale come nel luogo di lavoro fisico, indipendentemente dalla sua situazione occupazionale, dalle modalità o dalla durata dell'occupazione.
I sindacati e le organizzazioni di datori di lavoro svolgono un ruolo importante nella trasformazione digitale, in particolare in relazione alla definizione di condizioni di lavoro giuste ed eque, anche per quanto riguarda l'utilizzo degli strumenti digitali sul luogo di lavoro.
Servizi pubblici digitali online
Ogni persona dovrebbe avere accesso online ai servizi pubblici principali nell'UE. A nessuno deve essere chiesto di fornire dati più spesso di quanto necessario durante l'accesso ai servizi pubblici digitali e il loro utilizzo.
CAPITOLO III Libertà di scelta, declinato in:
Interazioni con algoritmi e sistemi di intelligenza artificiale
L'intelligenza artificiale dovrebbe fungere da strumento per le persone, con l'obiettivo ultimo di

aumentare il benessere umano.
Ogni persona dovrebbe essere messa nelle condizioni di godere dei benefici offerti dai sistemi algoritmici e di intelligenza artificiale, anche compiendo le proprie scelte informate nell'ambiente digitale, e rimanendo al contempo protetta dai rischi e dai danni alla salute, alla sicurezza e ai diritti fondamentali.
Un ambiente digitale equo.
Ogni persona dovrebbe essere in grado di scegliere realmente e liberamente quali servizi online utilizzare, sulla base di informazioni obiettive, trasparenti, facilmente accessibili e affidabili.
Ogni persona dovrebbe avere la possibilità di competere lealmente e innovare nell'ambiente digitale. Tutto ciò dovrebbe apportare benefici anche alle imprese, comprese le PMI.
CAPITOLO IV Partecipazione allo spazio pubblico digitale
Ogni persona dovrebbe avere accesso a un ambiente digitale affidabile, diversificato e multilingue. L'accesso a contenuti diversificati contribuisce a un dibattito pubblico pluralistico e alla partecipazione effettiva alla democrazia in modo non discriminatorio.
Ogni persona ha diritto alla libertà di espressione e di informazione, nonché alla libertà di riunione e di associazione nell'ambiente digitale.
Ogni persona dovrebbe poter accedere alle informazioni su chi possiede e controlla i servizi mediatici che utilizza.
Le piattaforme online, in particolare le piattaforme online di dimensioni molto grandi, dovrebbero sostenere il libero dibattito democratico online. Visto il ruolo svolto dai loro servizi nel plasmare l'opinione pubblica e il dibattito pubblico, le piattaforme online di dimensioni molto grandi dovrebbero attenuare i rischi derivanti dal funzionamento e dall'uso dei loro servizi, anche in relazione alle campagne di disinformazione e cattiva informazione, e tutelare la libertà di espressione.
CAPITOLO V Sicurezza, protezione e conferimento di maggiore autonomia e responsabilità, declinato in:
Un ambiente digitale sicuro, protetto e tutelato
Ogni persona dovrebbe avere accesso a tecnologie, prodotti e servizi digitali che siano sicuri e protetti e tutelino la vita privata fin dalla progettazione, traducendosi in un elevato livello di riservatezza, integrità, disponibilità e autenticità delle informazioni trattate.
Vita privata e controllo individuale sui dati
Ogni persona ha diritto al rispetto della vita privata e alla protezione dei propri dati personali. Quest'ultimo diritto prevede anche che i singoli individui abbiano il controllo di come sono utilizzati i propri dati e con chi sono condivisi.
Ogni persona ha diritto alla riservatezza delle proprie comunicazioni e delle informazioni sui propri dispositivi elettronici e a non essere sottoposta a sorveglianza online illecita, tracciamento pervasivo illecito o misure di intercettazione.
Ogni persona dovrebbe essere in grado di determinare la propria eredità digitale e decidere cosa succede, dopo la sua morte, ai propri account personali e alle informazioni che la riguardano.
Protezione dei bambini e dei giovani e conferimento di maggiore autonomia e responsabilità nell'ambiente digitale
I bambini e i giovani dovrebbero essere messi nelle condizioni di compiere scelte sicure e informate e di esprimere la propria creatività nell'ambiente digitale.
Si dovrebbero migliorare le esperienze, il benessere e la partecipazione all'ambiente digitale dei bambini e dei giovani attraverso materiali e servizi adeguati all'età.
Occorre prestare particolare attenzione al diritto dei bambini e dei giovani di essere protetti da tutti i reati commessi attraverso le tecnologie digitali o facilitati da tali tecnologie.
CAPITOLO VI Sostenibilità
Per evitare danni significativi all'ambiente, e al fine di promuovere l'economia circolare, i prodotti e i servizi digitali dovrebbero essere progettati, prodotti, utilizzati, riparati, riciclati e smaltiti in modo da attenuare il loro impatto negativo sull'ambiente e sulla società ed evitare l'obsolescenza prematura.
Ogni persona dovrebbe avere accesso a informazioni precise e di facile comprensione sull'impatto ambientale e sul consumo energetico dei prodotti e dei servizi digitali, nonché sulla loro riparabilità e sul loro ciclo di vita, in modo da essere in grado di compiere scelte responsabili.

fondamentale per l'interpretazione di qualsiasi normativa sui servizi e mercati digitali[23]. Andrebbe, quindi, favorita la sua conoscenza attraverso un'efficace azione di alfabetizzazione e divulgazione sui diritti e libertà fondamentali in ottica digitale all'interno di tutto il territorio unionale e sarebbe senz'altro apprezzabile una sua proiezione a livello sovranazionale.

Di particolare rilevanza ai nostri fini è senz'altro il capitolo 5 dedicato alla sicurezza, alla protezione dei dati personali e al conferimento verso i cittadini di maggiore autonomia e responsabilità. Questo capitolo va a correlare funzionalmente e correttamente la sicurezza con la protezione dei dati personali, inserendola così in quell'alveo di tutela della persona che giustamente le spetta, nel momento in cui essa agisce per attrezzare quelle misure adeguate a minimizzare i rischi di violazioni che possono ripercuotersi in modo diretto o indiretto su diritti e libertà fondamentali che ci riguardano.

Alla luce di quanto riferito, GDPR e Codice della protezione dei dati personali, da una parte, e Cybersecurity Act, le direttive NIS, la legge 90/2024[24] e il decreto legislativo 138/2024[25], dall'altra, non possono essere avvertite come normative parallele (come troppe volte accade) o peggio antinomiche, perché esse perseguono comuni finalità di tutela dell'individuo, in maniera diretta, nel primo caso, e indiretta, nel secondo, allorquando dal rischio sistemico di un'infrastruttura critica (ma anche di un sistema ritenuto essenziale o di particolare rilevanza per il nostro Paese) possono derivare danni a tutti i cittadini.

Data Protection e Cybersecurity, quindi, lavorano insieme nella tutela della nostra dimensione individuale (protezione dei dati personali) o collettiva (sicurezza a tutela di servizi essenziali o di particolare rilevanza per il Sistema Paese).

---

[23] È pregevole l'opera divulgativa di Agostino Ghiglia, componente dell'Authority italiana, sulla protezione dei dati personali, sui diritti di cittadinanza digitale, "Educazione civica digitale - Abbecedario essenziale", Maggioli Editore, 2023.
Si segnala, inoltre, che l'Agenzia per l'Italia ha pubblicato a sua volta una Guida sui diritti di cittadinanza digitale, in applicazione dell'art. 17, comma 1-quinquies del Codice dell'amministrazione digitale (D. Lgs. 82/2005). Purtroppo questa Guida, pur se di ottima fattura, non è stata mai stata accompagnata da un'opera di accurata diffusione per renderla utile allo scopo per cui era stata pensata dal legislatore. Si può leggerla qui: https://www.agid.gov.it/sites/default/files/repository_files/guida_riepilogo_diritti_cittadinanza_digitale_03-2022-acc.pdf.

[24] LEGGE 28 giugno 2024, n. 90 - Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici.

[25] DECRETO LEGISLATIVO 4 settembre 2024, n. 138 - Recepimento della direttiva (UE) 2022/2555, 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.

3. Data breach e personal data breach: due facce della medaglia della security e della privacy

Questa duplice dimensione di tutela individuale e collettiva insita nelle due discipline della data protection e della cybersecurity ben si esprime in caso di violazioni di dati personali che ormai caratterizzano l'attuale periodo storico, contraddistinto da una particolare fragilità della nostra dimensione digitale ,suscettibile di continui attacchi sia alle infrastrutture (anche critiche) del nostro Paese e sia a qualsiasi organizzazione (privata o pubblica)[26].

È vero che il (personal) data breach previsto nel GDPR viene percepito nell'art. 4 come una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l›accesso ai dati personali trasmessi, conservati o comunque trattati". Mentre nel D. Lgs. 138/2024 il data breach è definito come "un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informativi e di rete o accessibili attraverso di essi". Sono effettivamente definizioni differenti, ma – come abbiamo già sottolineato in precedenza - i piani di riferimento delle normative attualmente in vigore in materia di data protection e cybersecurity, pur non perfettamente coincidenti (dalle definizioni, alle tempistiche di azione, sino alle Autorità di riferimento o ai referenti da coinvolgere) finiscono per perseguire obiettivi comuni e interessi generali che ci riguardano, tutelando in maniera diretta o indiretta nostri diritti e libertà fondamentali.

Una violazione di dati, infatti, può compromettere gravemente tutti i principi generali del diritto alla protezione dei dati personali contenuti nell'art. 5 GDPR. E questo ben si può intuire dalla lettura del considerando 85 del GDPR, dove si evidenzia che "una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata". Per questo l'apparente antinomia normativa si ricompone funzionalmente nelle tempistiche di risposta che devono essere stringenti e nella necessità intrinseca di lavorare

[26] In proposito, si consiglia la lettura di "Truffe online e attacchi alle infrastrutture critiche: il report 2024 della Polizia Postale", di Chiara Ponti, pubblicato in data 08/01/2025 su Cybersecurity369 e disponibile alla pagina https://www.cybersecurity360.it/nuove-minacce/truffe-online-e-attacchi-alle-infrastrutture-critiche-il-report-2024-della-polizia-postale/.

insieme, in un'unica direzione, attraverso team interdisciplinari che adottino procedure comuni, dove i vari referenti della data protection (come il data protection officer) e della cybersecurity (come il referente previsto ad esempio dall'art. 8 della legge 90/2024) devono guardare verso un orizzonte comune, in dinamica sinergia, al fine di minimizzare l'impatto della violazione su diritti e libertà fondamentali degli individui coinvolti.

In poche parole, le decisioni da prendere in caso di attacchi informatici in corso sono tante e da dipanarsi in poche ore. Per questo, la sperimentazione di databreach simulati, attraverso la predisposizione di team di lavoro interdisciplinari, può essere fondamentale per prepararsi adeguatamente, passando così da una compliance solo teorica e formale a una compliance sostanziale. E solo quest'ultima si può considerare una piena applicazione del principio di accountability; principio quest'ultimo che investe trasversalmente la lettura e la comprensione delle due discipline della data protection e della cybersecurity.

Occorre riferire, peraltro, di una importante novità che si ricava dalla lettura della sopra richiamata definizione di evento di rischio, oggi contenuta nel D.lgs. 138/2024, che aggiunge alla classica triade della sicurezza (composta da integrità, riservatezza e disponibilità) la componente della autenticità. Questa opportuna integrazione terminologica costituisce una diretta applicazione del considerando 75 del Cybersecurity Act, allorché in esso si erano tracciati i confini della security by default dei prodotti, servizi o processi certificati specificando che "lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i prodotti TIC, servizi TIC e processi TIC certificati nel loro ambito siano conformi a determinati requisiti volti a proteggere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o delle funzioni di o dei servizi offerti da o accessibili tramite tali prodotti, servizi e processi per tutto il loro ciclo di vita". In questo modo acquisisce particolare valore anche quanto più volte precisato in recenti provvedimenti dall'Authority nazionale che si occupa di protezione dei dati personali e, cioè, che la protezione dei dati si persegue anche attraverso una protezione dell'autenticità delle informazioni e documenti gestiti attraverso sistemi di gestione e conservazione. Sul tema, il Garante ha avuto modo di precisare che "Occorre, a tal proposito, richiamare il costante orientamento di questa Autorità che, nei propri provvedimenti, ha sempre affermato che per assicurare l'ordinario svolgimento e la continuità dell'attività aziendale, è necessario predisporre sistemi di gestione documentale in grado di archiviare e conservare i documenti con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile"[27].

[27] Il passaggio è estratto dal recente provvedimento sulla conservazione delle e-mail dell'agente infedele, qui il link al provvedimento: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10053224. Si vedano anche il provvedimento n. 53 del 01/02/2018, doc. web n.

Risulta utile riferire, quindi, che mai come oggi la complessità di un attacco informatico vada perseguita attraverso reazioni interdisciplinari da parte di referenti di discipline solo apparentemente distanti (come referenti privacy, referenti security e referenti degli archivi digitali), i quali devono convergere in un'unica azione coordinata a tutela di diritti e libertà fondamentali.

4. Conclusioni

Abbiamo assistito una ventina di anni fa alla concentrazione a livello internazionale di oligopoli digitali portati avanti calpestando spensieratamente principi di trasparenza che erano già ampiamente presenti nella normativa europea. E in questi ultimi anni, con altrettanta passività, abbiamo accettato che i sistemi di intelligenza artificiale venissero alimentati da sterminati database, violando i principi di finalità per cui erano stati strutturati. Così come anni fa si riferiva che per custodire i propri dati su un PC occorreva disconnetterlo e chiuderlo in cassaforte. In realtà, l'obsolescenza di formati e supporti da tempo ci ha portato a consigliare di poggiare i nostri dati, informazioni e documenti su sistemi dinamici di custodia.

Oggi nessuno strumento a nostra disposizione può funzionare ed esserci utile senza essere (inter-) connesso. Dobbiamo, pertanto, virare il nostro sguardo verso una dimensione sia della "privacy" e sia della "security" dinamica, interconnessa, che valorizzi pienamente la circolazione di dati (personali e non personali) in archivi digitali e database che (ovviamente) devono essere ben presidiati da organizzazioni di controllo.

Queste organizzazioni (a livello locale, nazionale, europeo e internazionale) devono necessariamente fondarsi su tecnologie adeguate, ma anche su modelli e contratti strutturati da team interdisciplinari formati per controllare e custodire i nostri patrimoni digitali interconnessi.

Abbiamo davanti a noi una grande sfida e la tutela dei nostri diritti e libertà, ma anche di nostri valori fondamentali, tra cui la verifica delle fonti informative, dipende da una convergenza convinta di consapevoli azioni, in una fase di sviluppo digitale che consente facilmente profilazioni selvagge e manipolazioni cognitive.

8159221 e provvedimento n. 214 del 29/10/2020 doc. web 9518890.

N. 1 - 2025 - pp. 37-53

Il ruolo strategico dell'Agenzia per la cybersicurezza nazionale nella tutela integrata del dato

Stefano Marzocchi

Abstract: Dopo un quinquennio quasi interamente focalizzato sulla tutela del dato personale, eco dell'effetto dirompente del GDPR nelle vite di tutti noi, da qualche anno assistiamo ad un crescendo di attenzione verso la tutela delle informazioni *tout court*, che travalica l'orizzonte tipicamente segnato dalla privacy[1]. I tumultuosi scenari geopolitici, e gli scandali che hanno visto alcune big tech nel ruolo di protagoniste, hanno portato alla ribalta la tematica della cybersicurezza, che si affianca ora, completandola, a quella ormai socialmente metabolizzata e condivisa della protezione del dato personale. Spesso presentate come due facce della stessa medaglia, privacy e cybersicurezza possiedono un'innata differenziazione ontologica, che spiega ma non giustifica approcci spesso diametralmente opposti; come le due facce sono al tempo stesso opposte, ma parimenti necessarie perché la medaglia abbia valore, entrambe le discipline meritano e richiedono di essere affrontate con un approccio paritario e complementare, poiché ambedue sono in ultima analisi finalizzate alla tutela del medesimo bene: una società che è fatta di persone che operano all'interno di organizzazioni.

After a five-year period almost entirely focused on the protection of personal data, echoing the disruptive effect of GDPR in the lives of all of us, for the past few years we have been witnessing a growing focus on the protection of information tout court, which transcends the horizon typically marked by privacy[2]. The tumultuous geopolitical scenarios, and the scandals that have seen some big techs in the leading role, have brought the issue of cybersecurity to the forefront, which now complements and complements the now socially metabolized and shared issue of personal data protection. Often presented as two sides of the same coin, privacy and cybersecurity possess an innate ontological differentiation, which explains but does not justify approaches that are often diametrically opposed; just as the two sides are at once opposites but equally necessary for the coin to have value, both disciplines

[1] Al termine privacy ci si riferisce comunemente tuttora, seppur impropriamente, per riferirsi alla protezione dei dati personali - data protection. In questo elaborato useremo pertanto i due termini come sinonimi.

[2] The term privacy is still commonly referred to, albeit improperly, to refer to the protection of personal data-data protection. In this paper we will therefore use the two terms synonymously.

deserve and require to be approached with an equal and complementary approach, since both are ultimately aimed at protecting the same good: a society that is made up of people operating within organizations.

Parole chiave: privacy, cybersicurezza, ACN, GDPR

Sommario: 1. Introduzione – 2. Protezione e sicurezza implicano consapevolezza - 3. Sicurezza e protezione dei dati nell'Ordinamento giuridico – 4. Sinergia o sovrapposizione? - 5. Un matrimonio a rischio? - 6. Conclusioni

1.Introduzione

Come sappiamo, la tutela del dato è una priorità sia della cybersecurity che della data protection, è anzi una delle istanze che maggiormente differenzia la data protection dal nucleo originario, di derivazione prettamente statunitense, della privacy. Ci siamo poc'anzi riferiti alla cybersecurity e alla privacy come due facce della stessa medaglia, ricordando altresì che le due facce guardano in direzione diametralmente opposta; la differenza principale, ontologica, è ovviamente che la data protection si occupa esclusivamente del dato personale, tuttavia, le differenze non si esauriscono qui. Ad un occhio disattento, cybersicurezza e protezione dei dati potrebbero anzi apparire tematiche largamente divergenti, quando non antitetiche, in quanto ad oggetto di tutela. Sempre in un'ottica di estrema semplificazione, possiamo infatti dire che tutto lo scenario fattuale afferente alla security (e pertanto anche alla cybersecurity) sembra essere finalizzato a tutelare una determinata organizzazione dalle persone, esterne o interne che siano rispetto ad essa (financo infatti ai membri/dipendenti stessi, come sappiamo forieri di larga parte degli incidenti e delle violazioni di sicurezza), con una sua presunta ossessiva ricerca di una mole sempre più ampia di informazioni, che si sospettano poi indiscriminatamente vagliate e sfruttate ad uso e consumo esclusivo dell'organizzazione stessa. All'opposto, la data protection appare tutelare le persone dall'organizzazione, anche qui includendo quelle che ne sono membri (ed ancora ci riferiamo in particolare ai dipendenti). Ed è questo, in effetti, quello che avviene quando l'una si muove senza l'altra, è questo il rischio che si corre quando si enfatizza la potenzialità dello strumento e se ne perde di vista la finalità, di modo che il mezzo diventa il fine stesso. Quando invece si approcciano le due discipline in maniera filologicamente e teleologicamente orientata, e se ne comprende la ratio comune sottesa ad entrambe, non possono che emergerne i molteplici punti di contatto e la finalità condivisa, che è quella di proteggere un sistema che è fatto di persone che operano all'interno di organizzazioni. Nonostante, quindi, la direzione dello sguardo intrinsecamente opposta, senza entrambe le facce la medaglia non ha valore, e questo è esattamente il caso del binomio cybersecurity/data protection. Tale complementarità è altresì riconosciuta dalla

sensibilità del legislatore europeo e italiano, il quale, nel momento di disciplinare i due ordinamenti, non ha mancato di sottolinearne i punti di contatto e la necessità di procedere in parallelo per quanto riguarda le rispettive aree di compliance. Se, infatti, non è nemmeno pensabile la protezione del dato personale senza un'enclave di security (il GDPR[3] dedica pagine e pagine a questa tematica, in particolare uno dei suoi articoli di maggior impatto, il 32, alla sicurezza del trattamento, e quindi dei dati), come vedremo la normativa in tema di cybersicurezza non manca di sottolineare come la compliance con la disciplina privacy sia imprescindibile, appunto per evitare che le attività di cybersecurity diventino invasive, pervasive ed intrusive e si perda di vista quel nesso ineliminabile che ruota intorno ai concetti tipicamente privacy di necessità, proporzionalità e finalità, un fine legato ad ogni attività che deve sempre restare ancorato alla persona. In questo approccio necessariamente olistico, si inseriscono le autorità che istituzionalmente presiedono alla cybersicurezza (Agenzia per la cybersicurezza nazionale - ACN) ed alla protezione del dato personale (Garante per la protezione dei dati personali - GPDP).

L'ACN è stata istituita nel 2021 per rispondere alle crescenti minacce cibernetiche che riguardano infrastrutture critiche, aziende, istituzioni e cittadini[4]. La sua missione è proteggere il cyberspazio nazionale attraverso una serie di iniziative e strategie coordinate, attraverso la propria attività regolatoria[5], certificativa[6], ispettiva[7] e sanzionatoria, il tutto finalizzato in ultima istanza alla resilienza del sistema cibernetico

---

[3] Regolamento (UE) n. 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 (Regolamento Generale sulla Protezione dei Dati). Il GDPR ha abrogato la precedente direttiva 95/46/CE.

[4] A detta del Global Risk Report del World Economic Forum 2024, al quarto posto nella classifica dei rischi più rilevanti per i prossimi due anni vi sono quelli legati alla cyber (in)security. Sono rischi che si intensificano davanti al processo di digitalizzazione, sempre più pervasivo quanto necessario, e questo rende sempre più impellente, sottolinea il rapporto, comprendere le implicazioni immediate, a medio e lungo termine di queste tecnologie per la sicurezza informatica di ogni organizzazione. Le tecnologie emergenti possono fornire soluzioni all'insicurezza informatica, ma il divario tra le organizzazioni che sono in grado di rendersi cyber-resistenti e quelle che non lo sono sta crescendo, anche grazie all'uso, da parte degli aggressori informatici, di sempre nuove tecnologie come gli strumenti di AI generativa.

[5] Sia in proprio che in supporto alle istituzioni preposte per sviluppare normative e regolamenti che supportino la sicurezza cibernetica.

[6] L'ACN si occupa della supervisione della sicurezza nella catena di approvvigionamento e della protezione delle infrastrutture critiche nazionali, al fine di ridurre i rischi associati alla catena di fornitura e proteggere le infrastrutture essenziali, come energia, trasporti, sanità e finanza. A tal fine, essa esegue controlli e fornisce linee guida ai fornitori e alle aziende critiche per mantenere un alto livello di sicurezza in tutta la filiera.

[7] L'Agenzia ha il potere di vigilare sulla conformità degli enti pubblici e delle aziende alle normative di sicurezza cibernetica stabilite dalla legge, garantendo che tutti i soggetti rispettino le linee guida e le misure di sicurezza, riducendo così il rischio di vulnerabilità. A tale scopo, vengono effettuati audit e ispezioni, monitorata l'adozione delle misure di sicurezza e imposte eventuali sanzioni in caso di mancato rispetto delle disposizioni.

nazionale[8]. Essa, inoltre, definisce e coordina le strategie di cybersicurezza su tutto il territorio nazionale, con l'obiettivo di rafforzare l'infrastruttura di sicurezza del paese e garantire che tutti gli enti, le aziende e le amministrazioni pubbliche seguano procedure di sicurezza adeguate, promuovendo e supervisionando l'adozione di standard di sicurezza e misure di prevenzione per aumentare la resilienza contro gli attacchi informatici. L'Agenzia, inoltre, collabora con enti pubblici e privati e con le forze dell'ordine per identificare e neutralizzare le minacce cibernetiche e per proteggere le infrastrutture critiche nazionali da attacchi informatici, attraverso l'implementazione di sistemi avanzati per il monitoraggio e la rilevazione precoce di attività cibernetiche sospette. La raccolta e l'analisi delle informazioni sulle minacce cibernetiche viene usata per anticipare e prevenire attacchi, individuandone pattern e trend, fornendo indicazioni strategiche che vanno a immediato beneficio della collettività e permettono, in funzione preventiva ma anche reattiva, un intervento rapido, attivando team di risposta immediata in caso di attacchi cibernetici significativi, cosicché gli eventuali danni possano essere da subito mitigati. In caso di attacchi informatici, l'ACN ha il compito di gestire e coordinare la risposta a livello nazionale, onde minimizzare l'impatto degli incidenti e facilitare la condivisione delle informazioni necessarie tra tutti i soggetti coinvolti.

Alle organizzazioni colpite viene fornito dall'Agenzia il supporto tecnico per ripristinare la funzionalità dei sistemi compromessi[9], e alla collettività nel suo complesso sono indirizzati programmi di formazione per aumentare la consapevolezza sulle minacce cibernetiche e le migliori pratiche di sicurezza, con il lancio di sempre nuove campagne di sensibilizzazione pubblica per promuovere una cultura della sicurezza cibernetica unitamente all'innovazione (numerose sono le partnership con università, centri di ricerca e aziende tecnologiche per promuovere l'innovazione nella cybersicurezza[10]), investendo in progetti di ricerca e sviluppo per creare nuove tecnologie e soluzioni di sicurezza. Parallelamente, vengono sviluppati piani di contingenza per garantire la continuità operativa in caso di attacchi, creati protocolli di intervento e un sistema di allerta rapida per la comunicazione tempestiva delle minacce a enti pubblici e privati, ed effettuati regolari test di sicurezza e valutazioni delle vulnerabilità per migliorare le difese cibernetiche.

Inoltre, è sempre ACN a definire le policy[11] e a promuovere gli standard di sicurezza[12] per garantire che tutte le organizzazioni seguano le migliori pratiche, e

---

[8] ACN non si occupa di contrasto al cybercrime, che è di competenza della Polizia, né di intelligence in quanto anche quest'ultima è affidata alle cure delle specifiche autorità preposte.

[9] Negli ultimi due anni ACN ha fatto ripartire circa 60 strutture sanitarie bloccate da ransomware.

[10] La collaborazione tra settore pubblico e privato, insieme alla cooperazione internazionale, è essenziale per affrontare le minacce cibernetiche in modo efficace e garantire la sicurezza nazionale.

[11] v. https://www.acn.gov.it/portale/cloud/regolamento-cloud-per-la-pa

[12] v. https://www.garanteprivacy.it/temi/cybersecurity/password/conservazione-delle-password;

a partecipare a network internazionali di scambio di intelligence per combattere le minacce globali[13], offrendo consulenza tecnica alle istituzioni pubbliche e private per migliorare le loro difese cibernetiche ed organizzando simulazioni di attacchi cibernetici per preparare le organizzazioni a rispondere efficacemente alle emergenze. Dal punto di vista di governance & compliance, ACN è poi l'Autorità competente NIS, nonché una delle due autorità attualmente preposte a vigilare sull'intelligenza artificiale italiana.

Da ultimo, ma solo in omaggio a un criterio meramente cronologico, giova segnalare il ruolo centrale assegnato all'ACN dalla Legge c.d. Cybersicurezza, la n. 90 del 2024, emanata per rafforzare le misure di protezione e resilienza informatica in tutto il Paese. Questa legge rappresenta un aggiornamento delle normative italiane per rispondere alle crescenti minacce informatiche e l'ACN è chiamata da essa a guidare l'attuazione e il coordinamento di queste nuove disposizioni. La norma in questione consolida, infatti, il ruolo dell'Agenzia come organo principale per la protezione e la gestione della cybersicurezza in Italia, chiamata a coordinare le strategie nazionali, promuovere la cultura della sicurezza informatica, monitorare la conformità e intervenire in caso di attacchi. Grazie a questo ruolo, l'ACN contribuisce a garantire un ambiente digitale più sicuro e resiliente, sia per il settore pubblico che per quello privato.

Una cellula "totipotente", quindi, la cui impronta e portata innovativa è ancora tutta da percepire da parte del cittadino, ma che sin da subito ha fatto sentire la sua voce autorevole nel tessuto della compliance italiano, giocando un ruolo cruciale nella protezione del cyberspazio attraverso il coordinamento, la prevenzione, la risposta alle emergenze, la formazione e l'innovazione, e creando un ambiente digitale più sicuro e resiliente per tutti.

A ulteriore conferma del legame tra le due discipline della cybersecurity e della privacy, e pertanto delle autorità ad esse preposte, il legislatore italiano, nel momento di istituire l'ACN, ha previsto specifiche modalità di cooperazione con l'Autorità garante per la protezione dei dati personali, e il Protocollo di intenti finalizzato alla collaborazione con quest'ultima è stato cronologicamente la prima convenzione firmata dall'Agenzia. Le due autorità, quindi, hanno da subito stretto rapporti formali di collaborazione e reciproca assistenza al fine di garantire la coerente interazione e la corretta finalizzazione delle rispettive attività.

https://www.acn.gov.it/portale/crittografia

[13] L'ACN è incaricata di promuovere la cooperazione con le agenzie di cybersicurezza di altri paesi e con organizzazioni internazionali, al fine di favorire lo scambio di informazioni e la collaborazione per affrontare le minacce informatiche globali, partecipando a programmi di collaborazione internazionale, condividendo best practices e coordinare le strategie comuni di difesa cibernetica.

Si rende evidente, pertanto, come la cybersicurezza e la tutela dei dati personali non solo non si pongono in contrasto, ma sono l'una funzionale all'altra e, dunque, devono essere tenute egualmente in considerazione nel processo di sviluppo di prodotti ICT e nell'implementazione delle misure a tutela delle informazioni. Infatti, mentre da un lato, reti e sistemi ICT sicuri arginano il rischio di alterazione e distruzione, nonché di accesso illecito a dati personali (e della loro conseguente disseminazione), dall'altro, un trattamento dei dati personali svolto nel rispetto delle norme sulla protezione dei dati favorisce la sicurezza dei sistemi ICT (pensiamo a quanto il principio di necessità, quello di minimizzazione dei dati o le regole sulla data retention riducano sensibilmente l'esposizione al rischio della base dati).

Allo stesso tempo, si dovranno tenere presenti i fondamenti della data protection, che non è la privacy statunitense, per ricordarci che l'organizzazione che tratta i dati non è quello che oltreoceano chiamano il data owner; chi tratta il dato non è quasi mai il titolare del dato. Purtroppo il GDPR ha subito qualche torto in sede di traduzione, e nel nostro Paese abbiamo un *data controller* ed un *data processor* che diventano rispettivamente *titolare* e *responsabile*, poi opportunamente integrati della specificazione *del trattamento* ma che non è sufficiente a mettere in risalto come il titolare del trattamento non sia in realtà titolare di alcunché, è e deve rimanere un custode di qualcosa che appartiene ad altri, responsabile di un procedimento dove ad essere chiamato responsabile è invece qualcuno o qualcosa che - ancora - non è responsabile di nulla, a meno che non decida di fare l'unico gesto che potrebbe metterlo in difficoltà: disubbidire alle dettagliate istruzioni che in caso poi di mancato dettaglio lo priverebbero persino di quella residua responsabilità.

2. Protezione e sicurezza implicano consapevolezza

Per poter assicurare e mantenere un livello di protezione efficace e duraturo dell'ecosistema cibernetico, è indispensabile la consapevolezza del quadro della minaccia digitale, mediante un monitoraggio continuo degli eventi cibernetici e la condivisione delle relative risultanze. Questa identificazione ed analisi di informazioni, e soprattutto la loro condivisione, pone necessariamente il primo piano la considerazione del fatto che molte delle informazioni raccolte potrebbero rivelarsi dati personali, quindi essere riferite - o riferibili - a persone fisiche, dati la cui protezione è nel nostro Paese, così come nell'intera Unione europea, un diritto fondamentale della persona. Voler conoscere significa spesso dover indagare, e quanto più ampio è l'oggetto dell'indagine, maggiore è la quantità di dati raccolti, e quindi maggiore anche la possibilità che tali informazioni possano anche avere carattere personale.

Grazie all'enorme risonanza seguita all'introduzione del GDPR, oggi quando si parla di protezione del dato ci si riferisce comunemente alla tutela del dato personale, tanto è vero che il nome stesso del Regolamento non ha sentito il bisogno di questa specificazione. Per la restante parte del panorama informativo, che esula da questo ampio, enorme ambito (i dati personali sono infatti ovunque, o perlomeno non possiamo quasi mai escludere che ve ne siano), si preferisce parlare di *information security*, ma in ogni caso è - come abbiamo visto - evidente, se non altro per gli operatori ma auspichiamo presto per tutti, la complementarità, e non la conflittualità, della protezione dei dati personali e della cybersicurezza, nel comune obiettivo di tutelare la sicurezza nazionale (nel caso di ACN) e i diritti individuali - tra cui quello stesso alla sicurezza - dei cittadini nel cyberspazio, e questo è certamente di grande interesse non solo per i molteplici punti di contatto delle due aree, che ne determinano detta imprescindibile complementarietà, ma anche per l'ampiezza degli ambiti che vengono impattati. Consapevolezza quindi, al tempo stesso presupposto e risultato di una piena e sapientemente orientata applicazione di entrambe le discipline in esame.

3. Sicurezza e protezione dei dati nell'Ordinamento giuridico

Come anticipato, la sicurezza del dato digitale (obiettivo primario della cybersecurity) è preoccupazione primaria anche delle norme relative alla protezione del dato (personale - data protection), GDPR in testa. Abbiamo visto che l'art 32 di quest'ultimo, una delle articolazioni più estese ed analitiche dell'intero corpo normativo regolamentare, è dedicato alla "sicurezza del trattamento" e impone al titolare ed al responsabile del trattamento di *porre in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio* (questo adeguamento presuppone l'anzidetta consapevolezza, la quale prevede un *assessment* che ricomprende certamente, e anzi in particolar modo, le vulnerabilità), e che tengano *conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche*. Lo stesso articolo impone poi *una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*

Al secondo comma del medesimo articolo si esplicita poi nuovamente che "*nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento, che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati*".

Perdita, modifica e divulgazione che sono esattamente gli stessi eventi che la cybersicurezza da sempre mira ad evitare, e le misure di sicurezza individuate dalla corretta applicazione dell'articolo in esame non fanno che concretizzare la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza (termine particolarmente caro ad ACN, nonché profondamente connaturato alla cybersicurezza e alle strategie politiche a essa riferite) dei sistemi e dei servizi di trattamento.

Più in profondità, il Considerando 76 del GDPR afferma che *la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate con riguardo alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento. Il rischio dovrebbe essere considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati comportano un rischio o un rischio elevato.* Queste considerazioni oggettive fanno parte di quella valutazione del rischio, o *risk assessment* - che include necessariamente un *vulnerability assessment*, in quanto la vulnerabilità è un rischio intrinseco, connaturato all'attività o al mezzo con cui si opera - che non solo è consentita alle organizzazioni ma è dovuta, anche e soprattutto in virtù di espresse e molteplici disposizioni normative, come componente fondamentale ed imprescindibile della protezione del dato personale. È questa necessaria consapevolezza riguardo ai rischi, presupposto imprescindibile al cominciamento di qualunque attività di trattamento, che rende leciti, e abbiamo visto anzi dovuti, eventuali approfondimenti relativi a detti rischi – e ancora, incluse sempre le vulnerabilità – dove questi dovessero apparire, *prima facie* o successivamente alle prime valutazioni, elevati. Pensiamo quindi ad attività come i c.d. *penetration test*, attacchi mirati autoprodotti dal custode stesso del dato, o dietro sua autorizzazione, e dove la tenuta delle misure di sicurezza implementate viene testata principalmente nelle aree dove un accesso non autorizzato potrebbe causare i danni maggiori.

Sull'altro versante, quello del contributo delle normative sulla data protection alla disciplina dettata in tema di cybersicurezza, il legislatore europeo, consapevole dell'impossibilità di emanare una normativa contente obblighi puntuali, aggiornati e condivisi da tutti i settori sopra riportati, ha deciso di introdurre il concetto di Accountability anche in ambito di cybersecurity. Così, ai sensi dell'art. 21 della Direttiva NIS 2, viene sancito che gli Stati membri provvedano affinché i soggetti essenziali e importanti adottino misure tecniche, operative ed organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali soggetti utilizzano nelle loro attività o nella fornitura dei servizi, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi[14]. Anche dal punto di vista sanzionatorio infine, le best practice del GDPR stendono

[14] L'approccio è quello di responsabilizzare i soggetti interessati, che dovranno essere in grado di rendicontare il loro operato

la loro ombra sulla medesima Direttiva, il cui art. 34 prevede sanzioni molto alte in caso di violazione di una o più previsioni sancite agli articoli 21 o 23 da parte di un operatore di Servizi essenziali (fino a 10 milioni di euro o al 2% del totale del fatturato mondiale annuo per l'esercizio precedente) o di servizi importanti (fino a 7 milioni di euro o all'1,4% del fatturato mondiale annuo per l'esercizio precedente). Ancora più in là vanno gli importi dell'AI Act[15]. La sicurezza del dato diviene, dunque, un fondamentale prerequisito per il suo corretto trattamento e anche per la sua agevolata ma controllata circolazione, che poi sono gli obiettivi del GDPR stesso.

Sempre in ambito normativo, è doveroso menzionare che tale correlazione tra protezione dei dati personali e cybersicurezza è, in più parti, sempre più apertamente riconosciuta nella normativa UE e nazionale, ad esempio, nel decreto legislativo NIS[16] che impone, all'articolo 13, comma 5, che in caso di incidenti che comportano violazioni di dati personali, l'Autorità nazionale competente e, dunque, l'ACN, operi in stretta cooperazione con il Garante per la protezione dei dati personali. Lo stesso approccio è confermato dagli articoli 31 e 35 della più recente direttiva NIS 2, a cui è appena seguita una normativa nazionale di recepimento, una direttiva che sin dal principio specifica (Considerando 14) che a qualsiasi trattamento di dati personali ai sensi della direttiva si applica il diritto dell'Unione in materia di protezione dei dati personali e della vita privata (in particolare, si fa riferimento al GDPR e alla direttiva e-Privacy[17]). Non solo, tale applicazione è un concetto più volte ripreso all'interno del testo della Direttiva stessa, basti pensare a quanto stabilito fin dai primi articoli (art 2, par. 12) o a quanto previsto in relazione al trattamento di dati da parte del CSIRT e dalle Autorità competenti (art. 2, par. 14). Questa relazione tra autorità distinte a presidio di discipline complementari si estrinseca nel suo punto più alto all'interno della Direttiva quando giunge a stabilire una sussidiarietà tra la relativa attività sanzionatoria[18].

---

[15] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regolamento sull'intelligenza artificiale)

[16] D.Lgs. 4 settembre 2024, n. 138 - Recepimento della direttiva (UE) 2022/2555, 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.

[17] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

[18] Art.35, comma 2: Qualora le autorità di controllo di cui all'articolo 55 o 56 del regolamento (UE) 2016/679 impongano una sanzione amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del medesimo regolamento, le autorità competenti non impongono una sanzione amministrativa pecuniaria a norma dell'articolo 34 della presente direttiva per una violazione di cui al presente articolo, paragrafo 1, imputabile al medesimo comportamento punito con l'ammenda amministrativa pecuniaria a norma dell'articolo 58, paragrafo 2, lettera i), del regolamento (UE) 2016/679. Le autorità competenti possono tuttavia imporre le misure di esecuzione di cui all'articolo 32, paragrafo 4, lettere da a) a h), all'articolo 32, paragrafo 5, e all'articolo 33, paragrafo 4, lettere da a) a g) della presente direttiva.

Spaziando anche verso normative ulteriori in tema di cybersicurezza, vengono subito in evidenza i possibili punti di contatto e interferenze tra il Regolamento (UE) 2024/2847 (Cyber Resilience Act, di seguito CRA)[19], di recentissima adozione da parte del Consiglio[20], e la normativa in materia di protezione dei dati personali, in particolare relativamente alla potenziale e positiva incidenza delle regole contenute nel CRA sul principio di sicurezza e su quello di minimizzazione, principi che si trovano a ricoprire un ruolo fondamentale anche ai sensi di tale nuova normativa, risultando incorporati nell'elenco dei requisiti di cybersicurezza di cui all'Allegato 1. La definizione di un quadro giuridico uniforme in materia di requisiti essenziali di cybersicurezza per l'immissione di prodotti con elementi digitali è infatti essenziale per salvaguardare i diritti e le libertà fondamentali, compresi i diritti alla privacy e alla protezione dei dati personali, e di recente il Garante Europeo (EDPS) aveva auspicato un passaggio ulteriore, raccomandando ai regolatori UE di includere anche i principi di *privacy by design* e *by default* tra i requisiti di cybersicurezza dei prodotti con elementi digitali, e questo anche in considerazione del fatto che il GDPR non prevede obblighi diretti in capo ai produttori, limitandosi a incoraggiare tali operatori economici a tenere conto del diritto alla protezione dei dati in fase di sviluppo e progettazione (Considerando 78). Rilevano infine le sinergie previste dal Cyber Resilience Act tra i pertinenti organi e autorità in materia di standardizzazione e certificazione degli aspetti di cybersecurity, nonché avuto riguardo all'ambito della vigilanza e dell'enforcement.

In aggiunta, giova rilevare come l'approccio basato sul rischio - che caratterizza il GDPR ma anche il recentissimo Artificial Intelligence Act - abbia introdotto nel testo di quest'ultimo la Valutazione d'impatto sui diritti fondamentali (FRIA) sui sistemi ad alto rischio[21]. Essa dovrà essere effettuata solo per aspetti non coperti da

---

[19] Il "Cyber Resilience Act" è stato presentato dalla Commissione Europea il 15 settembre 2022. Il fine primario del regolamento è quello di avere, nel mercato dell'Unione, prodotti digitali più sicuri. Questo fine dovrebbe essere raggiunto stabilendo specifici requisiti essenziali di cybersicurezza a partire dalla manifattura dei prodotti digitali, hardware e software, quale precondizione necessaria all'immissione nel mercato dei prodotti stessi. A livello nazionale, si era già dato avvio a un processo similare nell'ambito del Perimetro di sicurezza nazionale cibernetica, stabilendo specifici obblighi, in capo ai soggetti perimetro, di comunicare al Centro di valutazione e certificazione nazionale (il CVCN, stabilito anch'esso in seno ad ACN), l'intenzione di acquisire beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici inseriti nel perimetro stesso, sui quali poi il CVCN effettuerà lo scrutinio tecnologico, anche questo riconducibile ad un vulnerability assessment. Tale norma, particolarmente efficace in relazione alla tutela della sicurezza nazionale nello spazio cibernetico è, al contempo, limitata solo allo specifico ambito di applicazione della normativa perimetro. Pertanto, è certamente apprezzabile la volontà della Commissione in termini di ampliamento dell'applicabilità dei requisiti di sicurezza sui prodotti digitali.

[20] Avvenuta il 10 ottobre 2024.

[21] La FRIA non era presente nella proposta di AI Act presentata dalla Commissione. Essa è stata infatti introdotta con appositi emendamenti dal Parlamento come adempimento ulteriore e distinto dalla c.d. Valutazione di conformità. Non si limita alla verifica documentata dei requisiti previsti per i

altri obblighi, come la Valutazione d'impatto (DPIA) ai sensi dell'art. 35 del GDPR e se uno qualsiasi degli obblighi relativi alla FRIA è già soddisfatto attraverso la Valutazione d'impatto (DPIA) condotta ai sensi dell'art. 35 del GDPR, la FRIA può o, meglio, deve essere effettuata congiuntamente alla DPIA[22].

Il profondo legame tra protezione dei dati e sicurezza cibernetica emerge quindi come abbiamo visto anche a livello legislativo, dove le fonti dei relativi diritti interagiscono sempre di più. All'interprete consapevole spetta infine il difficile ma intrigante compito di assemblare pazientemente tutte le tessere del mosaico.

4. Sinergia o sovrapposizione?

Detto questo, possiamo parlare di sovrapposizioni, se non di fungibilità tra rispetto della normativa in tema di cybersicurezza e di quella in tema di privacy? Esiste una norma o un complesso di norme all'interno dei due distinti scenari alla cui conformità si possa ancorare un'aspettativa generale di legittimità del proprio operato? La risposta è certamente negativa, perché diverse sono le angolazioni dalle quali si osserva il medesimo oggetto di tutela, ovvero i dati, le informazioni. Dalla prospettiva di sicurezza si insisterà quindi sugli adempimenti che assicurano il dato dalle compromissioni relative alla *integrità, disponibilità e confidenzialità*, definizioni che ora interessano parimenti l'operatore attento alla privacy e che sono state pedissequamente migrate nella normativa sulla data protection, ma la finalizzazione della privacy alla tutela di un diritto fondamentale della persona porta ad orientare le medesime attività di cybersecurity al bene fondamentale della persona. È poi la preoccupazione inerente alla privacy, innestata sulla normativa in tema di cybersecurity, che impedisce il concretizzarsi di un "grande fratello", perché senza considerarne il fine fondamentale non si potrebbe che cadere in un orwelliano controllo di tutto e tutti, a prescindere da *necessità, legittimità, proporzionalità*, e non da ultimo *eticità* del comportamento. E sono queste le definizioni che invece andranno migrate nel contesto cybersecurity, perché la piena complementarità tra le due discipline si concretizzi. Perché la sicurezza resti protezione e non avvenga quella sostituzione tra mezzo e fine a cui si accennava nelle pagine precedenti, è necessario che le

sistemi di AI ad alto rischio, ma comporta un'analisi più profonda dell'esposizione al rischio dei diritti fondamentali derivante dall'uso di un sistema di AI ad alto rischio. La FRIA deve essere svolta in ragione della natura del sistema e della sua riconducibilità ad un preciso elenco di casistiche, a prescindere dal fatto che lo stesso comporti un trattamento di dati personali. Deve dirsi, tuttavia, che nella quasi totalità dei casi i sistemi di AI ad alto rischio si nutrono di dati personali.

[22] La DPIA non indaga solo i rischi elevati che un trattamento può determinare per il diritto alla protezione dei dati personali, ma più in generale i rischi elevati, derivanti da quel trattamento, per tutti i diritti e tutte le libertà. Già ai sensi del GDPR, chi effettua una DPIA deve verificare se il trattamento con rischi elevati possa determinare, ad esempio, rischi per l'incolumità personale, per la reputazione, per la libertà di espressione, ecc.

specifiche tutele introdotte dalla normativa privacy vengano garantite, e ancora una volta è tale normativa stessa a venirci in soccorso, a evitare conflitti, ma anche sovrapposizioni e duplicazioni. Sempre nell'alveo dell'*accountability*, cardine e matrice di tutto il complesso normativo, fondamentali sono infatti le declinazioni concrete dei principi fondamentali relativi alla *necessità* del trattamento (le attività di security sono a tutti gli effetti dei trattamenti di dati, e questi devono essere posti in essere solo quando realmente indispensabili al raggiungimento del fine prefissato), la sua *proporzionalità* (entità e natura dei trattamenti di security devono essere giustificati, anche qui, dal fine prefissato) e non ultimo la *minimizzazione*, che si traduce banalmente nel cercare di raggiungere lo scopo utilizzando/indagando la minore quantità possibile di dati, per il minor tempo possibile e riducendone al massimo la loro circolazione. Come invece si innesteranno le molteplici normative in tema di cybersecurity sulla disciplina a presidio della privacy? Semplicemente passando attraverso il portone spalancato nel GDPR dal suo principio cardine, quello di *accountability*. Il GDPR non ha un allegato B come aveva un tempo il Codice privacy, non ha una lista della spesa la cui spunta possa presumibilmente portare ad una sensazione di sicurezza e intoccabilità, e questo volutamente in quanto una qualsiasi elencazione verrebbe ben presto resa desueta e obsolescente dal rapido avanzare della tecnica. Si parla invece, come abbiamo visto, di porre in essere tutto quello che lo stato dell'arte ci offre in relazione al rischio riscontrato. Come quantificare il rischio? Non c'è una disciplina privacy che ci aiuti ma linee guida delle organizzazioni che si occupano si cybersicurezza, in primis NIST[23] ed ENISA[24]. Quali sono le misure tecniche ed organizzative di cui parla il GDPR? Sono tutte tecniche già note alla cybersecurity, nessuna delle quali quindi è stata introdotta dal GDPR. Il rispetto della normativa, e delle linee guida degli organismi preposti è, pertanto, condizione necessaria ma non sufficiente perché si possa parlare di compliance privacy.

5. Un matrimonio a rischio?

Dato per scontato lo splendido rapporto tra le due discipline, non possiamo d'altro canto escludere che dei conflitti possano emergere, e questi ultimi non verranno però dalla natura delle due discipline stesse, ma da come le istituzioni e le corti decideranno di rapportarsi con le medesime.

[23] Il National Institute of Standards and Technology (NIST) è un'agenzia governativa statunitense che si occupa della gestione delle tecnologie di diverse discipline. Il Cybersecurity Framework sviluppato dal NIST fornisce best practice e linee guida a cui attenersi per migliorare la sicurezza delle informazioni e la gestione dei rischi per la sicurezza informatica.

[24] L'European Network and Information Security Agency (ENISA) è un'agenzia dell'Unione europea che si occupa di migliorare la sicurezza informatica e delle reti di telecomunicazioni dell'Unione europea.

Tutti siamo a conoscenza degli sconvolgimenti che ha portato con sé la sentenza Schrems della CGUE del 2015, che ha decretato l'invalidità di una decisione di adeguatezza della Commissione europea (il c.d. *Safe Harbor* del 2000) che per 15 anni aveva garantito il libero scambio di dati personali tra le due sponde dell'oceano. Di punto in bianco, la coperta giuridica di tale trasferimento è venuta a mancare, e i fornitori americani si sono trovati di colpo ghettizzati in quanto appartenenti a quello che sembrava divenuto uno stato canaglia in quanto a protezione del dato personale. La Direttiva Madre del 1995 prevedeva infatti, e il GDPR ha pedissequamente confermato, che il libero flusso di dati tra USA e UE dovesse essere preceduto da un *assessment* delle condizioni a cui di dati sarebbero stati sottoposti una volta trasferiti, e quelle formalizzate dall'ordinamento americano sono quanto di più distante dall'Europa si possa immaginare. Mancando una statuizione della Commissione circa l'adeguatezza del livello del protezione del paese via via preso in considerazione[25], tale *assessment* andrebbe svolto caso per caso dall'esportatore, ma è davvero molto difficile per un'organizzazione dichiarare che in terra statunitense i dati possano essere protetti quanto lo sono in Europa, specie tenuto conto dell'azione ultra interventista dei servizi di intelligence locali[26], il tutto aggravato dal fatto che gli USA non hanno (ancora, ma forse in queste ultimi mesi si sta provvedendo) una legislazione federale in proposito e che la privacy, teorizzata proprio da loro nel 1890, è rimasto sostanzialmente un blando diritto alla riservatezza, anni luce lontano dal concetto di diritto fondamentale alla protezione dei dati (e comunque legato al Quarto emendamento alla Costituzione, che in aggiunta non si applica ai non *permanent resident*).

A nulla varrebbero poi la firma delle clausole contrattuali standard (SCC) sviluppate a più riprese dalla Commissione, previse dalla Direttiva Madre e dal GDPR come suppletive alla decisione di adeguatezza, proprio perché uno strumento negoziale privato non può essere opposto alla legislazione federale, forte di poderosi strumenti di indagine come quelli previsti dalla Sezione 702 del Foreign Intelligence Surveillance Act (FISA) o dall'Ordine esecutivo 12333[27]. Affossato quindi il Safe Har-

---

[25] Sono meno di venti le decisioni di adeguatezza sinora emesse dalla Commissione ed oltretutto limitate, fino a pochi anni fa, perlopiù a paesi economicamente marginali.

[26] Nel 2013, un contractor della National Security Agency (NSA) statunitense di nome Edward Snowden fece trapelare una serie di diapositive dalla NSA che ha rivelato che le agenzie di intelligence statunitensi hanno accesso ai dati personali degli utenti europei attraverso programmi di sorveglianza come PRISM o Upstream. Entrambi questi programmi sono condotti ai sensi della Sezione 702 ma operano in modi diversi:
PRISM prevede la raccolta diretta "a valle" delle comunicazioni da parte della NSA attraverso l'assistenza forzata di fornitori di servizi di comunicazione elettronica (ad esempio Facebook o Google); Upstream, come suggerisce il nome, prevede invece la raccolta "upstream" di comunicazioni attraverso l'accesso alla dorsale di Internet (cavi, switch e router) stabilita dai fornitori di telecomunicazioni (es. AT&T e Verizon). Poiché i dati vengono ottenuti senza la conoscenza o l'assistenza dei fornitori a valle, Upstream è stato descritto come una forma di sorveglianza "backdoor".

[27] Sulla scia dei noti scandali emersi durante la presidenza Nixon, nel 1978 venne emanato il Foreign Intelligence Surveillance Act (FISA), un insieme di norme che attuano i principi emersi, nel corso degli

bor, la situazione di crisi - con i flussi di dati paralizzati e con interi servizi bloccati - venne prontamente risolta nel 2016 da una nuova decisione di adeguatezza, il c.d. Privacy Shield, "omaggiato" dalla Commissione a fronte di una modifica forse neppure formale dello *status quo* tra le diverse legislazioni. A fronte delle rimostranze emerse in ogni altra sede istituzionale che non fosse la Commissione stessa, con strali a dir poco inediti da parte del Parlamento, giunge quindi non certo inaspettata la seconda decisione di annullamento (2020) da parte della CGUE ancora intitolata all'intrepido giurista austriaco che aveva promosso l'attacco al Safe Harbor, e questa volta non sembrerebbe esserci verso di argomentare, la norma statunitense va cambiata. Ed invece a sorpresa, nuovamente la Commissione accetta blande dichiarazioni di principio, ed emette nel 2023 una terza decisione di adeguatezza (*Data Privacy Framework*). È questa che sembrerebbe ora aver tranquillizzato gli animi, ma se una Schrems III dovesse arrivare, cosa che ad oggi appare più che probabile, allora ci si potrebbe trovare nella situazione di dover scegliere tra un fornitore qualificato di servizi di cybersicurezza (buona parte dei quali localizzata nel USA) ed il rispetto della normativa europea in tema di protezione dei dati personali.

Ma da cosa deriva tutta questa difficoltà? Per quanto riguarda il mercato americano, che raggruppa la grandissima parte dei più blasonati fornitori di servizi di cybersecurity di alto livello, le piattaforme americane si sono affidate per decenni alle loro filiali locali per trattare i dati sul territorio europeo, e questa costituisce da

anni, da diverse decisioni della Corte Suprema Corte nonché dai dibattiti al Congresso sull'applicazione del Quarto Emendamento alla sorveglianza elettronica. Tende a regolamentare l'intercettazione delle comunicazioni (fisiche ed elettroniche) da parte dell'intelligence estera governativa. La disciplina è stata modificata, riformata e rafforzata nel corso degli anni, soprattutto dopo gli attentati dell'11 settembre 2001. Tuttavia, nel quadro originario, questa forma di controllo giurisdizionale che operava a priori era applicabile solo se la sorveglianza riguardava le comunicazioni tra cittadini statunitensi e cittadini stranieri situati nel territorio statunitense. Tuttavia, nel 2008 è entrato in vigore il FISA Amendments Act che ha creato la Sezione 702 per autorizzare l'acquisizione di informazioni di intelligence relative a cittadini non statunitensi (non-US person) che si trovano al di fuori del territorio statunitense. L'introduzione di questa norma particolarmente controversa è dovuta ad una delle numerose revisioni della FISA che il legislatore statunitense ha ritenuto necessarie dopo gli eventi dell'11 settembre 2001 e il conseguente culmine della minaccia alla sicurezza nazionale. Costituisce la principale base giuridica per la sorveglianza di massa oggi, è la legge antiterrorismo che autorizza la raccolta di qualsiasi comunicazione elettronica attraverso il computer o il telefono da parte di qualsiasi cittadino straniero al di fuori degli Stati Uniti, senza un mandato del giudice. La Sezione 702 non si applica ai cittadini e/o residenti negli Stati Uniti, che sono altrimenti soggetti ad altri meccanismi di sorveglianza. È specificamente progettato per gli individui stranieri che si trovano al di fuori degli Stati Uniti. Nei fatti, non esiste alcuna approvazione giudiziaria preventiva e individualizzata per i cittadini non statunitensi. Tecnicamente, se le comunicazioni tra cittadini non statunitensi e cittadini statunitensi avvenissero nel territorio di Paesi terzi – entriamo quindi nel caso delle comunicazioni internazionali – non si farebbe riferimento alla FISA, con le relative garanzie, ma all'Executive Ordine 12333/1981, firmato dal presidente Reagan e avente lo scopo di stabilire linee guida relative all'attività di intelligence posta in essere dai servizi segreti statunitensi, e che non pone limiti alla raccolta e all'analisi dei dati derivanti dalle comunicazioni internazionali. Sottopone infatti tutte le attività di intelligence, comprese quelle interne, a quelle della CIA (esterna), e consente la raccolta indiscriminata di informazioni dai fornitori di servizi digitali, sia riguardanti cittadini americani che stranieri.

tempo la loro più grande difesa contro le accuse di non garantire ai dati un livello adeguato di protezione, sostanzialmente equivalente a quella garantita dalle norme dell'Unione. Tuttavia, come evidenziato dalle sentenze della CGUE, è necessario garantire che eventuali flussi di dati "interni" verso gli USA rispettino gli standard europei. Va infatti tenuto presente che un'azienda americana è comunque soggetta alla normativa americana, indipendentemente dal luogo in cui hanno sede le sue filiali o sono conservati i suoi server[28], come oggi sottolinea espressamente il Cloud Act. Occorre(rebbe) quindi indagare concretamente se la società sia effettivamente soggetta agli obblighi previsti dalla normativa statunitense. Come abbiamo visto, questi obblighi non possono essere aggirati per via negoziale, poiché la legge statunitense imporrebbe comunque loro di violare il negozio stesso, così come gli obblighi previsti dal diritto dell'UE[29].

In pratica, il Governo statunitense emana direttive ai fornitori di servizi di comunicazione americani che obbligano questi ultimi a fornire immediatamente informazioni, documenti, materiali, assistenza relativi ai flussi comunicativi di volta in volta indicati, il tutto in segreto, senza possibilità di avvisare i propri utenti.

Come si comportano le corti americane in proposito? È necessario richiamare la tradizionale teoria che i tribunali americani adottano per bilanciare il diritto individuale alla privacy e gli interessi conflittuali con esso, il c.d. *test della ragionevole aspettativa* sviluppato dalla la Corte Suprema, secondo il quale il diritto alla privacy prevale solo se l'individuo può nutrire una "ragionevole aspettativa" di protezione della sua vita privata, a sua volta ricavabile applicando la c.d. *dottrina della terza parte*, secondo la quale un individuo non può far valere la ragionevole aspettativa di tutela del suo diritto alla privacy se ha volontariamente messo a disposizione di un terzo (ad esempio una banca, un operatore telefonico ma anche un fornitore di servizi) i suoi dati personali.

Nelle sentenze relative all'uso della sezione 702 del FISA, in particolare sulla questione se sia legittimo o meno effettuare tale sorveglianza senza la necessità, da parte del Governo, di ottenere alcuna autorizzazione (sorveglianza senza mandato), le corti hanno giustificato tale pratica principalmente sulla base del fatto che il Quarto Emendamento non si applica ai cittadini stranieri su suolo non statunitense. La sorveglianza degli stranieri da parte dei servizi segreti americani appare, quindi,

---

[28] Ai sensi della sezione 702, i "fornitori di servizi di comunicazione elettronica" statunitensi (come Google, Amazon, Apple, Microsoft, Facebook, Google e Yahoo) potrebbero infatti essere tenuti a garantire alle autorità di sicurezza statunitensi l'accesso alle informazioni personali su "persone non statunitensi".

[29] Questa questione è al centro di tutti i casi giudiziari che abbiamo visto coinvolgere Facebook, il signor Schrems, il commissario irlandese per la protezione dei dati (DPC), i tribunali irlandesi e la Corte di giustizia dell'Unione europea, poiché Facebook è chiaramente soggetto alla normativa statunitense.

particolarmente pervasiva[30]. Il regime della Sezione 702 sarebbe dovuto scadere nel gennaio 2018, ma il Congresso ha ripetutamente rinnovato l'applicabilità della FISA così come modificata nel 2008. Giova ricordare che la CGUE, con la sentenza Schrems II, nel dichiarare l'invalidità del Privacy Shield, ha ritenuto che il diritto interno degli Stati Uniti (in particolare l'Ordine Esecutivo 12333 e la Sezione 702 della FISA) comporti deroghe alle leggi sulla protezione dei dati che vanno oltre le restrizioni ritenute necessarie in una società democratica.

Si crea quindi un'inevitabile tensione tra la crescente domanda di protezione da parte europea e il quadro giuridico statunitense, la cui tendenza va inesorabilmente verso una significativa "riduzione" delle stesse garanzie.

6. Conclusioni

Siamo quindi in presenza di un approccio alla governance complesso e in continuo divenire, dove l'intimo e inscindibile rapporto che lega protezione dei dati personali e cybersecurity, e le autorità ad esse preposte, viene alla luce in maniera sempre più eclatante. Ciò è sicuramente e immediatamente evidente nella pratica. Una continua e profonda commistione che assume la forma di una vera e prioria interdipendenza, sia nelle fasi fisiologiche di trattamento e protezione degli assetti informativi, quanto in quelle patologiche.

Gli anzidetti, esemplificativi elementi di continuità tra protezione dati e cybersicurezza rendono evidente la complementarità delle due discipline di cui abbiamo parlato, ma anche quanto sia necessaria la loro interazione per un mondo digitale sicuro e rispettoso dei diritti costituzionali.

A livello normativo, diverse categorie tecniche della cybersecurity sono diventate di primaria importanza in ambiente data protection, pensiamo alla triade CIA (*confidentiality, integrity e availablity*) mentre oggi vediamo i pilastri della disciplina privacy estesi pedissequamente all'attività di cybersicurezza, prima tra tutti l'*accountability* (che ora fa mostra di sé nell'AI Act, come nella Direttiva NIS 2, mentre era assente nella precedente), ma anche la *proporzionalità* e la *minimizzazione*. In alcuni casi addirittura si arriva alla sussidiarietà dei rispettivi apparati sanzionatori

[30] Ci sono limiti e garanzie rispetto a queste attività investigative. Nel 2014, il presidente Obama ha emanato la Direttiva sulla politica presidenziale n. 28 (PPD-28) che ordinava alle agenzie di intelligence statunitensi di rivedere le proprie politiche relative al trattamento dei dati di soggetti non statunitensi in relazione ai programmi di intelligence, compresi quelli condotti ai sensi della Sezione 702 della FISA (più volte richiamata anche dal Garante Privacy italiano nel provvedimento del 9 giugno 2022 (n. 9782890) o dell'EO 12333. La CGUE ha ritenuto che le tutele offerte dalla PPD-28 non sono sufficienti a garantire un livello adeguato di protezione ai sensi del diritto dell'UE.

(nel caso in cui un incidente informatico abbia comportato una *data breach* ai sensi del GDPR, le sanzioni amministrative della NIS 2 non sono applicabili).

Alla luce di quanto detto, a fini di una tutela generale del Sistema Paese, è oltremodo necessario che la cybersicurezza e la protezione dei dati personali siano entrambe adeguate ed efficaci. Ciò richiede che questi temi siano considerati un ambito prioritario sin dalla fase di progettazione dei sistemi e prodotti ICT e fin dalle verifiche preliminari che devono necessariamente precedere l'inizio di ogni attività di trattamento. Questo è, tra l'altro, ciò che stabiliscono i principi di "privacy by design" e "security by design", che permeano rispettivamente le suddette aree disciplinari.

N. 1 - 2025 - pp. 54-62

Il Regolamento europeo 2024/1183 (eIDAS 2) e l'impatto della Direttiva 2022/2555 (NIS 2) sui servizi fiduciari

Giovanni Manca

Abstract: L'entrata in vigore della Direttiva europea 2022/2555, meglio nota come NIS 2, introduce nuovi scenari per la cibersicurezza. Uno scenario inedito è costituito dal coordinamento e dell'interazione significativa con il Regolamento europeo 2024/1183 (eIDAS 2 – electronic IDentification Authentication and trust Services) "*che modifica il regolamento (UE) n.910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale*". La Direttiva NIS 2 sopprime l'articolo 19 del Regolamento 910/2014 e quest'ultimo, più volte, stabilisce l'applicazione della NIS 2 per i servizi fiduciari. Tutto ciò impone attenzione all'azione congiunta delle due norme dell'Unione, anche perché sono numerose le differenze introdotte e le regole che si applicano sia ai servizi fiduciari qualificati che ai non qualificati.

The entry into force of the European Directive 2022/2555, better known as NIS 2, introduces new scenarios for cybersecurity. An unprecedented scenario is the coordination and significant interaction with the European Regulation 2024/1183 (eIDAS 2) "*amending Regulation (EU) No. 910/2014 as regards establishing the European Digital Identity Framework*". The NIS 2 Directive repeal Article 19 of Regulation 910/2014 and the latter, several times, establishes the application of NIS 2 for trust services. All this requires attention to the joint action of the two Union laws, also because there are numerous differences introduced and the rules apply to both qualified and non-qualified trust services.

Parole chiave: eIDAS, NIS 2, servizi fiduciari, cibersicurezza, vigilanza.

Sommario: 1. L'interazione tra NIS 2 ed eIDAS 2 – 2. I nuovi scenari di cibersicurezza nei servizi fiduciari – 3. Conclusioni

1. L'interazione tra NIS 2 ed eIDAS 2

Lo spirito generale dello scenario e degli obiettivi che si pone la Direttiva NIS 2 nella sua obbligatoria interazione con il Regolamento eIDAS 2 è ottimamente sintetizzato nell'introduzione dello standard ETSI EN 319 401.

"*Costruire la fiducia nell'ambiente online è fondamentale per lo sviluppo economico e sociale. La mancanza di fiducia, soprattutto a causa di una percepita mancanza di sicurezza, induce i consumatori, le imprese e le amministrazioni a esitare ad effettuare transazioni elettroniche e ad adottare nuovi servizi. I fornitori di servizi fiduciari sono spesso un elemento essenziale per stabilire la fiducia tra le parti che effettuano transazioni elettroniche, in particolare nelle reti pubbliche aperte, e possono essere utilizzati, ad esempio, per fornire informazioni sull'identità attendibili e contribuire a stabilire comunicazioni sicure tra le parti che effettuano transazioni.*
Esempi di tali fornitori di servizi fiduciari sono gli emittenti di certificati a chiave pubblica, i fornitori di servizi di marcatura temporale, i fornitori di servizi di generazione o convalida di firme elettroniche remote.
Affinché i partecipanti al commercio elettronico abbiano fiducia nella sicurezza di questi servizi fiduciari, devono avere fiducia che i fornitori di servizi fiduciari (TSP) abbiano stabilito una serie di procedure, processi e misure di sicurezza al fine di ridurre al minimo le minacce e i rischi operativi e finanziari associato.
Inoltre, la sicurezza informatica di tutti i servizi digitali essenziali è vitale per la trasformazione digitale dell'Europa con servizi digitali e transazioni elettroniche. La fornitura di servizi fiduciari eIDAS è identificata come un elemento essenziale dell'infrastruttura digitale europea. La Direttiva (UE) 2022/2555 [i.13] del Parlamento Europeo e del Consiglio del 14 dicembre 2022 recante misure per un livello comune elevato di cibersicurezza nell'Unione, che modifica il Regolamento (UE) 910/2014 e della Direttiva (UE) 2018/1972, e che abroga la Direttiva 2016/1148 (Direttiva NIS2 o NIS2) individua all'articolo 3 che i requisiti per le misure di gestione del rischio di sicurezza informatica sono applicabili, come entità essenziali, ai fornitori di servizi fiduciari qualificati di cui Regolamento eIDAS. Inoltre, poiché i servizi fiduciari eIDAS sono identificati come elemento fondamentale dell'infrastruttura digitale europea e NIS 2 è applicabile ai servizi fiduciari eIDAS, il presente documento mira anche a soddisfare i requisiti di NIS2"[1].

Il documento ETSI EN 319 401 è intitolato "*Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers* e specifica le politiche di sicurezza di base da applicare alle pratiche operative e di gestione dei prestatori di servizi fiduciari (Trust Service Providers - TSP) indipendentemente dal servizio fornito, compresi i requisiti di sicurezza informatica conformi alla Direttiva NIS2. Altri standard, riguardanti particolari tipologie di servizi fiduciari, possono basarsi sul presente documento per identificare requisiti aggiuntivi per particolari tipologie di servizi fiduciari. Quindi, ad esempio, un TSP che emettete certificati qualificati per la firma elettronica potrà soddisfare (nel rispetto dei principi base comunitari di neutralità tecnologica e non discriminazione) lo standard che tratta

[1] Traduzione dell'autore.

specificamente il servizio.

Nel seguito si ipotizza che il lettore sia a conoscenza dei principi della Direttiva NIS 2 e del Regolamento eIDAS 2[2].

Non ci sorprende che la Direttiva NIS 2 faccia riferimento decine di volte al *trust* e ai *trust services*. Già nel preambolo con il Considerando (11) si auspica che i prestatori di servizi fiduciari "*dovrebbero rientrare nell'ambito di applicazione della presente direttiva al fine di garantire un livello di requisiti di sicurezza e supervisione analogo a quello precedentemente stabilito in tale regolamento nei confronti dei prestatori di servizi fiduciari*".
Nel testo in italiano si è tradotto il termine *supervision* con quello di "supervisione", ma nel citato Regolamento 910/2014 la traduzione più aderente alla normativa nazionale risulta essere "vigilanza".
I prestatori di servizi fiduciari sono indicati anche nel Considerando (84), nell'ambito della esigenza di coordinamento generale della sicurezza a livello dell'Unione.
Un ulteriore aspetto di tale coordinamento è descritto nel Considerando (92).
Dal punto di vista della complementarità tra eIDAS e NIS è di particolare interesse il Considerando (94) che si riporta integralmente di seguito:

"Gli obblighi in materia di cibersicurezza stabiliti nella presente direttiva dovrebbero essere considerati complementari ai requisiti imposti ai prestatori di servizi fiduciari ai sensi del regolamento (UE) n. 910/2014. È opportuno chiedere ai prestatori di servizi fiduciari di adottare tutte le misure adeguate e proporzionate per gestire i rischi posti ai loro servizi, anche in relazione ai clienti e ai terzi che vi fanno affidamento, nonché di segnalare gli incidenti a norma della presente direttiva. Tali obblighi in materia di cibersicurezza e segnalazione dovrebbero riguardare anche la protezione fisica dei servizi forniti. I requisiti per i prestatori di servizi fiduciari qualificati stabiliti all'articolo 24 del regolamento (UE) n. 910/2014 continuano ad applicarsi."

I prestatori di servizi fiduciari operano in conformità alla NIS 2, ma l'articolo 24 "*Requisiti per i prestatori di servizi fiduciari qualificati*" continua ad applicarsi.
I prestatori di servizi fiduciari sono presenti nel testo della Direttiva già nell'articolo 2 dedicato all'ambito di applicazione. Sono nel paragrafo 2, lettera a, punto ii), ma per un palese errore di traduzione leggiamo "*prestatore di servizi di fiducia*".

Come appare evidente dai riferimenti richiamati, dunque, a tali soggetti si applica la Direttiva, in coordinamento con quanto stabilito nel 910/2014, modificato

[2] Per quest'ultimo Regolamento, qualora si voglia approfondire le tematiche, si può far riferimento alla pubblicazione seguente: https://www.clioedu.it/marketplace/elenco-completo/item/n-2024-4-rivista-elettronica-di-diritto-economia-management.

dal Regolamento 2024/1183.

Ai sensi dell'articolo 3 della NIS 2 i prestatori di servizi fiduciari sono individuati come soggetti essenziali, quindi, ad essi si applicano le norme più "stringenti", visti le criticità e l'impatto sulla società delle loro attività. Le sanzioni per questi soggetti sono più elevate[3].
Per concludere la descrizione dei principali aspetti di coordinamento e interazione tra eIDAS 2 e NIS 2, può essere utile mettere in evidenza l'articolo 24, paragrafo 1, che stabilisce regole per l'"*uso dei sistemi europei di certificazione della cibersicurezza*" e in base al quale gli Stati membri possono imporre ai soggetti essenziali e importanti prodotti certificati in Europa. Importante risulta anche la regola per cui "*gli Stati membri incoraggiano i soggetti essenziali e importanti a utilizzare servizi fiduciari qualificati*".

2. I nuovi scenari di cibersicurezza nei servizi fiduciari

Per comprendere meglio la stretta interazione in materia di cibersicurezza tra la Direttiva NIS 2 e il Regolamento eIDAS 2 appare corretto evidenziare i singoli punti di contatto, per poi commentarne lo scopo e l'azione operativa che ne consegue.
L'azione della NIS 2 su eIDAS 2 è puntuale nell'articolo 42, come già evidente nella rubrica dello stesso, "*Modifica del regolamento (UE) n. 910/2014*".
L'articolo stabilisce che: "*Nel regolamento (UE) n.910/2014, l'articolo 19 è soppresso con effetto a decorrere del 18 ottobre 2024*". L'articolo 19 è relativo ai "*Requisiti di sicurezza relativi ai prestatori di servizi fiduciari*" e la sua soppressione è indispensabile perché, vista la natura regolamentare di eIDAS 2 si creerebbe una disomogeneità tra i due provvedimenti, vin considerazione del rango normativo superiore del Regolamento rispetto alla normativa del singolo Stato membro.
La data del 18 ottobre 2024 è quella dell'obbligo di adozione da parte degli Stati membri della Direttiva NIS 2 tramite la normativa nazionale di recepimento.
In Italia il recepimento è stabilito con il Decreto Legislativo 4 settembre 2024, n. 138. Questo decreto introduce anche una serie di provvedimenti istituzionali che saranno indispensabili per l'attuazione del recepimento.

[3] Ulteriori informazioni sulle criticità e i settori coinvolti si possono trovare negli allegati della Direttiva.

Di seguito si illustrano i singoli riferimenti alla NIS 2 nel Regolamento eIDAS 2[4].

Il primo riferimento è nel Preambolo, Considerando (47), che all'interno di un testo dettagliato evidenzia l'importanza della NIS 2, del Regolamento sulla protezione dei dati personali (GDPR) e dell'uso degli elenchi di fiducia per *"…fissare le condizioni alle quali i quadri fiduciari dei paesi terzi potrebbero essere considerati equivalenti ai quadri fiduciari per i servizi fiduciari qualificati…"*.

Discorso analogo per il Considerando (50).
In questo caso si ritiene utile per il lettore riportare di seguito il testo integrale:
"(50) *Al fine di razionalizzare gli obblighi in materia di cibersicurezza imposti ai prestatori di servizi fiduciari, nonché di consentire a tali prestatori e alle rispettive autorità competenti di beneficiare del quadro giuridico istituito dalla direttiva (UE) 2022/2555, a norma di tale direttiva i servizi fiduciari sono tenuti ad adottare misure tecniche e organizzative adeguate, quali misure per far fronte a guasti del sistema, errori umani, azioni malevole o fenomeni naturali, per gestire i rischi posti alla sicurezza dei sistemi informativi e di rete che tali prestatori utilizzano nella prestazione dei loro servizi, nonché per notificare minacce informatiche e incidenti significativi conformemente alla medesima direttiva. Per quanto riguarda la segnalazione di incidenti, i prestatori di servizi fiduciari dovrebbero notificare eventuali incidenti che abbiano un impatto significativo sulla prestazione dei loro servizi, compresi quelli causati dal furto o dalla perdita di dispositivi o da danni ai cavi di rete, o quelli verificatisi nel contesto dell'identificazione di persone. I requisiti in materia di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione a norma della direttiva (UE) 2022/2555 dovrebbero essere considerati complementari ai requisiti imposti ai prestatori di servizi fiduciari a norma del presente regolamento. Ove opportuno, le autorità competenti designate a norma della direttiva (UE) 2022/2555 dovrebbero continuare ad applicare le prassi o gli orientamenti nazionali consolidati per quanto riguarda l'attuazione dei requisiti in materia di sicurezza e comunicazione e la vigilanza della conformità a tali requisiti a norma del regolamento (UE) n. 910/2014. Il presente regolamento fa salvo l'obbligo di notificare le violazioni dei dati personali a norma del regolamento (UE) 2016/679"*.

L'importanza del coordinamento tra gli organismi di vigilanza la troviamo descritta nel successivo Considerando (51).
Il primo riferimento nel testo dell'articolato normativo, che è anche quello maggiormente meritevole di attenzione, si trova nella nuova formulazione, con modifica dell'articolo 16 dedicato alle sanzioni. Il paragrafo 1 di questo articolo stabilisce che: *"1. Fatto salvo l'articolo 31 della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, gli Stati membri stabiliscono le norme relative alle sanzioni appli-*

[4] Il riferimento esplicito alla "2022/2555" è presente 23 volte, comprese le citazioni nelle note a piè di pagina.

cabili in caso di violazioni del presente regolamento. Tali sanzioni sono effettive, proporzionate e dissuasive".

Il testo del paragrafo ci suggerisce di commentare l'articolo 31 della NIS 2 che stabilisce gli "*Aspetti generali relativi alla vigilanza e all'esecuzione*". La necessità di soppressione dell'articolo 19 del Regolamento eIDAS 2 inizia a chiarirsi.

L'articolo stabilisce le regole per le autorità competenti, a partire dal fatto che "*gli Stati membri provvedono affinché le proprie autorità competenti monitorino efficacemente e adottino le misure necessarie a garantire il rispetto della presente direttiva*".

Nei paragrafi successivi si danno indicazioni sulle opzioni operative generali dello Stato membro nei confronti delle autorità competenti. In particolare, nel paragrafo 3 si stabilisce la stretta cooperazione con il Garante per la protezione dei dati personali quando questo è coinvolto, per competenza, in caso di incidente. L'articolo si chiude con il paragrafo 4 che richiede di coordinare i quadri legislativi e nazionali, che sono fatti salvi, con regole di vigilanza e poteri adeguati alle istituzioni che su questo tema devono agire.

Un altro articolo che richiama la Direttiva NIS 2 è il nuovo articolo 19 bis del Regolamento 2024/1183.
L'articolo stabilisce i "*Requisiti per i prestatori di servizi fiduciari non qualificati*" e questo aspetto costituisce una significativa novità rispetto alla versione originale del Regolamento eIDAS.

Per favorire la comprensione diretta del lettore, si riporta il testo completo dell'articolo:
"Articolo 19 bis
Requisiti per i prestatori di servizi fiduciari non qualificati
1. Un prestatore di servizi fiduciari non qualificato che presta servizi fiduciari non qualificati:

a. dispone di politiche adeguate e adotta misure corrispondenti per la gestione dei rischi giuridici, commerciali, operativi e di altro tipo, sia diretti che indiretti, per la prestazione del servizio fiduciario non qualificato, le quali, fatto salvo l'articolo 21 della direttiva (UE) 2022/2555, comprendono almeno misure relative:
   i. alla registrazione a un servizio fiduciario e alle relative procedure di onboarding;
   ii. ai controlli procedurali o amministrativi necessari per prestare servizi fiduciari;
   iii. alla gestione e all'attuazione dei servizi fiduciari;
b. alla notifica, senza indebito ritardo ma in ogni caso entro 24 ore dall'essere venuto a conoscenza di violazioni della sicurezza o perturbazioni, all'organismo

di vigilanza, alle persone interessate identificabili, al pubblico se è di pubblico interesse e, ove applicabile, ad altre autorità competenti interessate, di tutte le violazioni della sicurezza o perturbazioni connesse alla prestazione del servizio o all'attuazione delle misure di cui alla lettera a), punti i), ii) o iii), aventi un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.

2. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al paragrafo 1, lettera a), del presente articolo. Si presume che i requisiti di cui al presente articolo siano stati rispettati, ove siano rispettate tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2".

Il commento a questo articolo è utile che inizi dall'analisi dell'articolo 21 della Direttiva NIS 2.

Questo articolo è piuttosto lungo (circa una pagina nella pubblicazione nella Gazzetta dell'Unione) e stabilisce le "*Misure di gestione dei rischi di cibersicurezza*".

Il paragrafo 2 dell'articolo elenca gli elementi che devono essere tenuti in conto, in un approccio multirischio, nel definire e applicare le misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete adottati.

I singoli punti sono i seguenti:

a. *politiche di analisi dei rischi e di sicurezza dei sistemi informatici;*
b. *gestione degli incidenti;*
c. *continuità operativa, come la gestione dei backup e il ripristino in caso di disastro e gestione delle crisi;*
d. *sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;*
e. *sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;*
f. *strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;*
g. *pratiche di igiene informatica di base e formazione in materia di cibersicurezza;*
h. *politiche e procedure relative all'uso della crittografia e, del caso, della cifratura;*
i. *sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;*
j. *uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.*

La lettura di questi punti non sorprende, visto che si elencano gli elementi tipici di un sistema di gestione della sicurezza informatica. Naturalmente la loro puntuale ed esplicita presenza nella NIS 2 è indispensabile.
Il paragrafo 3 introduce e dettaglia regole per la valutazione della catena di approvvigionamento. Questo aspetto è sempre più critico nell'evoluzione degli scenari di rischio internazionali.

Una valutazione di sintesi dell'articolo 19 bis nel Regolamento n. 910/2014, così come modificato con il Regolamento n. 2024/1183, può essere indicata nella specializzazione delle regole della NIS 2 rispetto al contesto dei servizi fiduciari non qualificati. Questo passo è indispensabile per gestire l'intero insieme dei servizi fiduciari. Prima di questo approccio la qualifica e la conseguente vigilanza sui prestatori di servizi fiduciari lasciava spazio al rischio derivante dalla mancanza di regole dell'Unione sui servizi non qualificati.

Questo aspetto, senz'altro reale a livello di Unione europea, era già stato gestito in Italia nelle regole della PEC e della firma elettronica avanzata (FEA). Questi due servizi fiduciari non qualificati già sono trattati nella normativa nazionale di riferimento con un adeguato livello di sicurezza e con conseguente vigilanza, ad oggi, in capo all'Agenzia per l'Italia Digitale - Agid. Quello che mancava a livello di mercato interno dell'Unione era un quadro comune transnazionale e transettoriale che rendesse omogenee le regole per tutti gli attori coinvolti.

I riferimenti nel Regolamento 2024/1183 alla Direttiva NIS 2 proseguono con la modifica al paragrafo 1 dell'articolo 20.
"1.I prestatori di servizi fiduciari qualificati sono sottoposti, a proprie spese e almeno ogni 24 mesi, a una verifica da parte di un organismo di valutazione della conformità. Lo scopo della verifica è confermare che i prestatori di servizi fiduciari qualificati e i servizi fiduciari qualificati da essi prestati rispettano i requisiti di cui al presente regolamento e all'articolo 21 della direttiva (UE) 2022/2555. I prestatori di servizi fiduciari qualificati presentano la risultante relazione di valutazione della conformità all'organismo di vigilanza entro tre giorni lavorativi dalla sua ricezione.».

Dopo i servizi fiduciari non qualificati anche quelli qualificati devono mantenere i loro requisiti, periodicamente, con un ulteriore riferimento, che non ci sorprende, all'articolo 21 della NIS 2.

Nel testo del Regolamento n. 910/2014, modificato dal Regolamento 2024/1183, il riferimento alla NIS 2 è presente altre 10 volte. In questi casi oltre alle indispensabili norme di coordinamento tra i due provvedimenti, si sottolinea lo specifico riferimento alle autorità competenti nello Stato membro (in Italia l'AgID – Agenzia per

l'Italia Digitale e l'ACN – Agenzia per la Cybersicurezza Nazionale e, ovviamente, il Garante per la Protezione dei Dati Personali). Questi soggetti hanno poi degli obblighi di interazione con altre istituzioni e autorità dell'Unione, ai fini di un reciproco coordinamento sulla base dello scopo specifico, all'interno dei due provvedimenti citati.

3. Conclusioni

Le modifiche apportate al Regolamento europeo n. 910/2014 dal Regolamento 2024/1183 non potevano omettere i riferimenti all'indispensabile coordinamento con la Direttiva NIS 2. La gestione della sicurezza cibernetica doveva specializzarsi e potenziarsi nell'ambito dei servizi fiduciari anche sul piano operativo. Per raggiungere questo obiettivo, eIDAS 2 fa riferimento più volte all'applicazione dell'articolo 21 della NIS 2.

Le autorità nazionali competenti dovranno opportunamente coordinarsi per operare al meglio, anche limitando le duplicazioni di vigilanza sui prestatori di servizi fiduciari. In tal senso, è opportuno ricordare che le aziende sono soggette anche alle attività di certificazione e vigilanza per la qualità, il sistema di gestione di sicurezza informatica, la sostenibilità ambientale, le tematiche del cloud computing e della protezione dei dati personali. Altri regolamenti e norme dell'Unione incombono sugli stakeholder e le PMI avranno oneri significativi per ottenere e mantenere la conformità a tutte queste norme, regole tecniche e organizzative.

L'obiettivo finale è, in ogni caso, chiaro: per applicare la Direttiva NIS 2 in conformità con il Regolamento 2024/1183, è indispensabile integrare la gestione della sicurezza cibernetica con quella dei servizi fiduciari. La strategia di coordinamento è sempre basata su valutazioni del rischio, governance, notifiche di incidenti e collaborazione con le autorità nazionali e internazionali di riferimento.

Lo scenario operativo non è esso stesso esente da rischi. Come già detto in precedenza, l'impresa rischia di essere "intasata" da una serie di controlli istituzionali, interni ed esterni, relativi alla certificazione e all'audit. Il coordinamento tra soggetti e il buon senso dovranno essere protagonisti in questo nuovo scenario di regole, dove la cibersicurezza è cruciale e onnipresente, ma non sempre trattata in pratica a livelli attuativi e operativi adeguati.

N. 1 - 2025 - pp. 63-79

Condivisione Security Test per migliorare la difesa informatica attiva nella Pubblica Amministrazione

Christian Catalano, Mario Angelelli

Abstract: L'uso pervasivo delle nuove tecnologie in contesti sensibili (ad esempio, la gestione delle infrastrutture critiche) sta spingendo gli Stati nazionali a proteggere il dominio cibernetico attraverso la creazione di enti governativi con questa specifica responsabilità. Ciò richiede la definizione di protocolli specifici per gestire i diversi scenari di attacco, oltre a regole, linee guida e comportamenti. Le pubbliche amministrazioni devono seguire tali protocolli per sviluppare una capacità adeguata di difesa informatica.
L'obiettivo di questo articolo è introdurre un nuovo framework di alto livello per migliorare la difesa informatica proattiva nell'attuale Pubblica Amministrazione italiana. L'obiettivo generale è promuovere il riutilizzo delle informazioni derivanti dai test di sicurezza per ottimizzare le risorse locali, soddisfacendo al contempo i requisiti normativi a livello nazionale e le buone pratiche di cybersecurity. Vengono descritti i protocolli per diversi scenari e discussi gli effetti economici attesi, sia a livello micro che macro.

The pervasive use of new technologies in sensitive contexts (e.g. the management of critical infrastructures) is prompting nation states to protect the cyber domain through the creation of government agencies with this specific responsibility. This requires the definition of specific protocols to handle different attack scenarios, as well as rules, guidelines and behaviour. Public administrations must follow these protocols to develop an adequate cyber defence capability.
The objective of this article is to introduce a new high-level framework to improve proactive cyber defence in the current Italian public administration. The overall objective is to promote the reuse of information from security tests to optimise local resources, while meeting national regulatory requirements and good cybersecurity practices. Protocols for different scenarios are described and the expected economic effects, both at micro and macro level, are discussed.

Parole chiave: difesa cibernetica della PA, riuso, strategie di sicurezza, effetti economici

1. Introduzione

L'evoluzione della trasformazione digitale e la crescente interconnessione dei sistemi informatici hanno reso la cybersicurezza una priorità critica per le pubbliche amministrazioni[1]. In questo contesto, l'Italia ha recentemente implementato importanti normative per rafforzare la protezione del proprio spazio cibernetico. In particolare, la Legge 28 giugno 2024, n. 90, recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", rappresenta un passo significativo per affrontare le sfide poste dalle minacce informatiche. Questa Legge introduce obblighi di notifica degli incidenti informatici, definisce le responsabilità delle pubbliche amministrazioni, e prevede sanzioni in caso di inosservanza.

La Legge 90/2024, che fa riferimento anche al Decreto Legge 21 settembre 2019, n. 105[2], prevede l'identificazione di una struttura e di un referente per la cybersicurezza in ogni amministrazione, con il compito di sviluppare politiche di sicurezza delle informazioni e di attuare misure di potenziamento delle capacità di gestione dei rischi informatici. Queste figure fungono da punto di contatto con l'Agenzia per la cybersicurezza nazionale.

Parallelamente, l'Unione Europea ha emanato la Direttiva NIS2, che mira a rafforzare la cybersicurezza in tutta l'Unione, recepita in Italia con il Decreto Legislativo 138/2024, che amplia il novero dei soggetti tenuti a rispettare gli standard minimi di sicurezza, includendo enti pubblici e privati che operano in settori critici, e rafforzando gli obblighi di segnalazione degli incidenti informatici.

Questo contesto normativo evidenzia la necessità di un approccio proattivo alla cybersicurezza, che vada oltre la semplice reazione agli attacchi informatici, in quanto risulta necessario implementare strategie di prevenzione e protezione che minimizzino i rischi e aumentino la resilienza delle infrastrutture digitali, anche attraverso la condivisione delle informazioni e lo svolgimento di periodici test di sicurezza.

L'uso delle tecnologie ICT in contesti pubblici sensibili e strategici (ad esempio, sanità pubblica, gestione di centrali elettriche, ecc.), combinato con l'uso della tecnologia da parte dei cittadini privati, sta spingendo le organizzazioni pubbliche

[1] Per il presente contributo, cfr. diffusamente Catalano, C., Afrune, P., Angelelli, M., Maglio, G., Striani, F., & Tommasi, F. (2021). Security Testing Reuse Enhancing Active Cyber Defence in Public Administration. In ITASEC (pp. 120-132).

[2] Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica, convertito con modificazioni dalla Legge 18 novembre 2019, n. 133

a considerare la conformità alle normative e la difesa contro gli attacchi informatici malevoli come una questione di vitale importanza.

A causa dell'alto livello di connettività introdotto dalla trasformazione digitale, la gestione delle informazioni, da sempre un elemento cruciale ma trasversale a diversi settori, è oggi riconosciuta come un asset con caratteristiche proprie. In questo contesto, il termine "cyberwarfare" viene definito come l'uso delle tecnologie ICT per supportare attacchi militari contro un paese[3]. Inoltre, si fa riferimento alla quinta dimensione della guerra, che include l'"informazione" tra i domini da proteggere, accanto a quelli tradizionali (aria, terra, spazio e mare).

Di conseguenza, gli Stati nazionali stanno proteggendo attivamente questo nuovo dominio attraverso la creazione di enti governativi con responsabilità specifiche, definendo protocolli specifici per determinate circostanze e scenari di attacco, regole, linee guida[4] e comportamenti[5] che le organizzazioni pubbliche devono seguire.

Le amministrazioni devono conformarsi con le norme interne definite dai singoli Stati per la propria protezione e con direttive e regolamenti Europei che gli stati membri dell'Unione Europea seguono come la Direttiva NIS 2[6] (Direttiva UE 2022/2555), il Cybersecurity Act (Reg. UE n. 881/19) e il Regolamento Generale sulla Protezione dei Dati, noto come GDPR (Reg. UE n. 679/16)[7].

---

[3] J. Carr, Inside cyber warfare: Mapping the cyber underworld, O'Reilly Media, Inc., 2012 e V. A. Almeida, D. Doneda, J. de Souza Abreu, Cyberwarfare and digital governance, IEEE Internet Computing 21 (2017) 68–71.

[4] In proposito, si vedano i seguenti documenti di AgID:
- Linee guida di sicurezza nello sviluppo delle applicazioni, https://www.agid.gov. it/sites/default/files/repository_files/documentazione/lineeguidasicurezza-introduzione.pdf, 2017;
- Linee guida per l'adozione di un ciclo di sviluppo di software sicuro, https://www.agid.gov.it/sites/default/files/repository_files/allegato_1-_linee_guida_per_ladozione_di_un_ciclo_di_sviluppo_di_software_sicuro.pdf, 2020;
- Linee guida per lo sviluppo sicuro, https://www.agid.gov.it/sites/default/files/repository_files/allegato_2_-_linee_guida_per_lo_sviluppo_sicuro_di_codice.pdf, 2020;
- Linee guida per la configurazione per adeguare la sicurezza del software di base, https://www.agid.gov.it/sites/default/files/repository_files/allegato_3_linee_guida_per_la_configurazione_per_adeguare_la_sicurezza_del_software_di_base.pdf, 2020;
- Linee guida per la modellazione delle minacce ed individuazione delle azioni di mitigazione conformi ai principi del secure/privacy by design, https://www.agid.gov.it/sites/default/files/repository_files/allegato_4_-_linee_guida_per_la_modellazione_delle_minacce-dlt.pdf, 2020.

[5] Cfr R. Baldoni, R. De Nicola, P. Prinetto, Il futuro della cybersecurity in italia: Ambiti progettuali strategici progetti e azioni per difendere al meglio il paese dagli attacchi informatici, Laboratorio Nazionale di Cybersecurity (CINI)-Consorzio Interuniversitario Nazionale per l'Informatica (2018).

[6] 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 NIS 2).

[7] P. Voigt, A. Von dem Bussche, The eu general data protection regulation (GDPR), A Practical Guide,

La difesa di questo nuovo dominio non è né semplice né lineare, neanche seguendo le raccomandazioni degli Stati nazionali o dell'Unione Europea: diversi fattori contribuiscono infatti alla discrepanza tra il ritmo dell'evoluzione tecnologica e il tempo necessario alle strutture organizzative pubbliche o agli enti interni per adattarsi.

Nel presente contributo, si presenta una nuova proposta per migliorare la difesa cibernetica proattiva in uno scenario specifico, ovvero l'attuale Pubblica Amministrazione italiana (da qui in avanti PA). Questo obiettivo si basa sull'adattamento operativo e organizzativo dei processi della PA alle tecnologie già esistenti, spingendoci a concentrarci su descrizioni di alto livello e non tecniche delle fasi che caratterizzano la difesa proattiva attraverso il riutilizzo dei test di sicurezza.

Si inizia con una breve introduzione al contesto italiano attuale, evidenziando i punti di forza e le sfide organizzative legate alla difesa cibernetica nella PA. Successivamente, si fornisce una descrizione della proposta, che mira a migliorare la resilienza del sistema-paese e a sviluppare una capacità di difesa cibernetica "attiva" (cioè proattiva).

Nello specifico, si propone una variante del riutilizzo del codice, ovvero il riutilizzo dei risultati dei test di sicurezza eseguiti localmente (ad esempio, i vulnerability assessment e penetration test condotti dai nodi locali della PA presenti sul territorio nazionale) attraverso una centralizzazione a livello nazionale. L'obiettivo principale di questo nuovo framework è rafforzare la protezione dei collegamenti più vulnerabili (le PA locali) di un sistema complesso (la PA nazionale), ottimizzando al contempo le risorse pubbliche.

2. Specifica dello Scenario

Situazione attuale nella Pubblica Amministrazione Italiana

Il contesto in cui è stata concepita la presente proposta è lo stato attuale della cybersicurezza nella Pubblica Amministrazione italiana. Partendo dalla necessità di proteggere il dominio dell'informazione, la nozione di difesa dell'informazione è stata definita nell'ordinamento italiano con l'obiettivo di delineare protocolli per la gestione di situazioni critiche.

1st Ed., Cham: Springer International Publishing 10 (2017) 3152676.

L'attuale definizione del sistema nazionale di difesa cibernetica coinvolge diversi attori, tra cui il Presidente del Consiglio dei Ministri, il Comitato Interministeriale per la Sicurezza della Repubblica (CISR), il Dipartimento delle Informazioni per la Sicurezza (DIS), l'Agenzia Informazioni e Sicurezza Esterna (AISE) e l'Agenzia Informazioni e Sicurezza Interna (AISI). Più recentemente (2019)[8], i regolatori hanno fornito una definizione più chiara degli standard nazionali di cybersicurezza, riguardo alla prevenzione e alla risposta agli eventi cibernetici, con l'obiettivo di garantire un elevato livello di sicurezza delle reti, delle ICT e dei servizi IT per le Pubbliche Amministrazioni e per gli enti pubblici o privati operanti sul territorio nazionale.

Sviluppo software e Pubbliche Amministrazioni

Oltre alla reazione agli attacchi in corso, un approccio fondamentale per evitare danni nel dominio dell'informazione è prevenire gli attacchi informatici ("Prevenzione per Mitigazione"). Per quanto riguarda la difesa proattiva, l'AgID ha definito le linee guida per l'acquisizione e il riuso del software per le pubbliche amministrazioni (9 maggio 2019) con l'obiettivo di ridurre i costi delle PA. Queste linee guida richiedono che il codice sorgente del software prodotto dalle PA (sia su commissione che attraverso risorse interne) venga rilasciato come progetto open source, in modo che altre PA possano riutilizzare il software. Tuttavia, un nodo della PA non è obbligato a utilizzare il software prodotto da altre PA. Infatti, le linee guida descrivono il processo di selezione in tre fasi[9]:

- 1. *prima fase*: identificazione delle esigenze;
- 2. *seconda fase*: analisi delle soluzioni disponibili nel catalogo del codice riutilizzabile e delle soluzioni open source;
- 3. *terza fase*: analisi di altre soluzioni.

Ogni fase è preliminare e obbligatoria per le successive. La terza fase è suddivisa in due sottofasi, durante le quali vengono analizzate sia la fattibilità dell'implementazione di una nuova soluzione, sia l'adozione di quelle proprietarie già esistenti; le amministrazioni sono tenute a effettuare entrambe le analisi, che saranno confrontate durante la fase di scelta (valutazione "make or buy").

In particolare, le soluzioni prese in considerazione durante la fase di ricerca

[8] D.L. 21 settembre 2019, n. 105, Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica.

[9] Cfr. AgID, Linee guida su acquisizione e riuso di software per le pubbliche amministrazioni, https://www.agid.gov.it/sites/default/files/repository_files/lg-acquisizione-e-riuso-software-per-pa-docs_pubblicata.pdf, 2019.

devono soddisfare una serie di vincoli e criteri; in ogni caso, se anche solo uno dei vincoli non è soddisfatto, la soluzione non può essere considerata idonea. Tuttavia, vincoli esterni (tempi, specificità della problematica sollevata dal nodo PA, ecc.) possono portare le PA a trovare e adottare soluzioni proprietarie che soddisfino tutti i vincoli, più facilmente rispetto a soluzioni basate sul riuso del software.

Si sottolinea inoltre che il software proprietario è spesso progettato per un contesto specifico; pertanto, le sue caratteristiche e configurazioni dipendono fortemente dalla legislazione e dall'organizzazione dello Stato (nel caso in questione, l'Italia). Questo porta a considerare tali soluzioni proprietarie come "prodotti di nicchia", poiché il software prodotto per la PA italiana spesso non è oggetto di attenzione da parte della comunità di ethical hacker e le software house raramente organizzano programmi di bug bounty[10].

Punti di forza e limiti del sistema attuale

Lo sviluppo di strategie nazionali di cybersicurezza ha suscitato interesse poiché hanno il potenziale di allineare le esigenze della sicurezza nazionale con quelle della crescita economica: queste ultime promuovono la sicurezza proattiva per la progettazione di tutte le politiche digitali. Infatti, una difesa proattiva può aumentare la capacità di prevenire, dissuadere e rilevare attacchi informatici, rispondendo in modo coordinato e coinvolgendo le diverse istituzioni nell'ambito della cybersicurezza.

Esistono diversi approcci riguardo alle contromisure che un'azienda privata o un ente pubblico può adottare per prevenire possibili attacchi alle proprie infrastrutture.

Tra questi, si citano:

1. *Vulnerability Assessment (VA) e Penetration Test (PT)*[11]: la prima consente di identificare possibili vulnerabilità all'interno di una rete, mentre il secondo consiste nell'identificare e sfruttare le vulnerabilità (sia quelle già conosciute

[10] A. Kuehn, M. Mueller, Analyzing bug bounty programs: An institutional perspective on the economics of software vulnerabilities, in: 2014 TPRC Conference Paper, 2014.

[11] In proposito si vedano: J. N. Goel, B. M. Mehtre, Vulnerability assessment & penetration testing as a cyber defence technology, Procedia Computer Science 57 (2015) 710–715; I. Yaqoob, S. A. Hussain, S. Mamoon, N. Naseer, J. Akram, A. ur Rehman, Penetration testing and vulnerability assessment, Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org 7 (2017); P. S. Shinde, S. B. Ardhapurkar, Cyber security analysis using vulnerability assessment and penetration testing, in: 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), 2016, pp. 1–5. doi:10.1109/STARTUP. 2016.7583912.

che nuovi 0days[12]) al fine di prendere il controllo del sistema, come avviene negli attacchi reali.

2. *Analisi statica*[13] *e dinamica delle applicazioni*[14]: l'analisi statica permette di analizzare un programma senza eseguirlo. Questa analisi può essere effettuata sul codice sorgente o sull'eseguibile del software (reverse engineering). L'analisi dinamica, invece, consiste nell'analizzare il software durante la sua esecuzione. A differenza dell'analisi statica, il risultato dell'analisi dinamica può dipendere dall'input utilizzato.
3. *Strumenti semi-automatici*: questi strumenti eseguono un controllo per vulnerabilità note. Successivamente, i risultati vengono analizzati da analisti[15].

Sebbene tali approcci siano ben adatti per anticipare possibili conseguenze in caso di attacchi informatici, in pratica presentano problematiche che non possono essere ignorate. Riprendendo alcune delle sfide presentate nel White Paper "Il futuro della Cybersecurity in Italia: Aree strategiche di interesse"[16], citiamo:

1. **Costi di verifica**: questo è probabilmente l'aspetto più importante. Infatti, non tutte le aziende o gli enti possono sostenere i costi della sicurezza, soprattutto quando l'infrastruttura da proteggere cambia frequentemente.
2. **Certificabilità e verificabilità delle analisi**: garantiscono che una vulnerabilità individuata durante un'analisi sia riproducibile e quindi verificabile.
3. **Limiti degli strumenti automatici:** gli strumenti automatizzati possono solo fornire un'idea delle possibili vulnerabilità negli asset analizzati. In particolare, alcuni errori derivanti da fattori umani non possono essere individuati automaticamente. Inoltre, alcuni software rendono difficile l'analisi automatica a causa del linguaggio adottato.
4. **Vulnerabilità in ambienti e contesti IT specifici**: questo aspetto è collegato al precedente. Alcune vulnerabilità possono emergere principalmente a seguito dell'introduzione di un determinato set di input. Pertanto, il verificarsi di vulnerabilità improbabili in uno scenario generico potrebbe diventare più probabile in contesti applicativi specifici. Queste vulnerabilità possono

---

[12] M. A. McQueen, T. A. McQueen, W. F. Boyer, M. R. Chaffin, Empirical estimates and observations of 0day vulnerabilities, in: 2009 42nd Hawaii International Conference on System Sciences, IEEE, 2009, pp. 1–12.

[13] P. Ferrara, F. Spoto, Static analysis for GDPR compliance., in: ITASEC, 2018.

[14] T. Ball, The concept of dynamic analysis, in: Software Engineering—ESEC/FSE'99, Springer, 1999, pp. 216–234.

[15] Y. Stefinko, A. Piskozub, R. Banakh, misc and automated penetration testing. benefits and drawbacks. modern tendency, in: 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), IEEE, 2016, pp. 488–491.

[16] R. Baldoni, R. De Nicola, P. Prinetto, Il futuro della cybersecurity in italia: Ambiti progettuali strategici progetti e azioni per difendere al meglio il paese dagli attacchi informatici, Laboratorio Nazionale di Cybersecurity (CINI)-Consorzio Interuniversitario Nazionale per l'Informatica (2018).

quindi aumentare la probabilità di intrusioni e rappresentare punti deboli per l'intera infrastruttura ICT.

5. **Ambienti per l'analisi di sicurezza di sistemi interoperabili**: testbed reali per analisi sperimentali di soluzioni di terze parti o soluzioni provenienti da fonti non affidabili.

3. Framework proposal

Basandoci sulla discussione precedente, introduciamo una proposta per promuovere la sicurezza proattiva e aumentare la capacità di prevenire, dissuadere e rilevare attacchi informatici in modo coordinato con le varie istituzioni coinvolte, al fine di affrontare alcune delle sfide evidenziate nel citato White Paper.

La proposta consiste nella progettazione ad alto livello di una nuova classe di processi per gestire i contenuti informativi relativi ai test di sicurezza come risorsa. L'effetto atteso di questo design è introdurre un nuovo criterio osservabile, ossia il contenuto informativo utile relativo ai test di sicurezza, per formalizzare e migliorare l'implementazione concreta di connessioni sicure tra i nodi della PA. Questo criterio non solo può integrare gli approcci efficaci e le raccomandazioni attualmente in uso con capacità di difesa cibernetica attiva, ma rappresenta anche una discriminante esplicita tra i diversi nodi della PA: il contenuto informativo può essere condiviso e accessibile solo in base alle effettive esigenze di sicurezza dei diversi nodi della PA, oltre le loro funzionalità.

Inoltre, la nostra soluzione comprende in modo naturale le linee guida emesse da AgID riguardo al riuso del codice per le PA: in particolare, risolve diverse limitazioni dell'organizzazione attuale, evidenziate anch'esse nel White Paper, affrontando direttamente il paradigma del riuso del codice.

Per chiarire i punti affrontati dalla proposta, si parte dalla riduzione dei costi di verifica, che rappresenta una limitazione significativa per alcune istituzioni (come le piccole PA). Successivamente, le soluzioni software adottate in nodi distinti con esigenze simili possono beneficiare del riuso dei test di sicurezza e delle informazioni relative alla correzione dei bug: questo può portare a un insieme più ampio di soluzioni in uso da valutare e aggiornare prima di passare ad altri software proprietari, favorendo così la riduzione dei costi e l'adozione di soluzioni certificate e verificate.

Infine, vale la pena sottolineare che questo approccio potrebbe anche risolvere la limitazione introdotta dagli strumenti automatizzati, poiché il tempo

risparmiato nella fase di analisi consente di trasferire risorse per analisi aggiuntive e più approfondite. A questo proposito, potrebbero essere necessari test multipli sugli asset software per esplorare vulnerabilità che emergono in diverse configurazioni: si sottolinea che questi test non rappresentano una ridondanza, ma migliorano l'accuratezza di PT/VA nell'esplorare potenziali vulnerabilità in diversi ambienti.

Dettagli della proposta

Così come per il software, dietro il concetto di "riuso" vi è l'osservazione che diverse PA operanti in un contesto comune spesso condividono le stesse soluzioni, sia attraverso il riuso promosso dall'AgID sia tramite soluzioni proprietarie. Di conseguenza, nel caso di VA/PT, gli stessi componenti potrebbero essere analizzati. La prima implicazione è la violazione di uno dei principali requisiti che si vogliono soddisfare, ovvero la minimizzazione dei costi. Un approccio per risolvere questo problema è evitare controlli ridondanti condividendo i report dei VA e/o PT effettuati dalle PA. In particolare, questo consente di:

1. **Minimizzare i costi**: è la conseguenza ovvia della condivisione. In questo modo, è possibile analizzare in dettaglio solo quelle soluzioni che non dispongono ancora di risultati di test di sicurezza o che presentano configurazioni specifiche.
2. **Supportare le piccole PA nella protezione dei loro asset**: i risultati condivisi dovrebbero essere accessibili a tutte le PA (limitatamente a quelle interessate, per ovvi motivi di sicurezza). In questo modo, anche le PA che non sono in grado di effettuare analisi approfondite possono garantire un livello adeguato di sicurezza. A un livello di dettaglio più profondo, i risultati potrebbero essere accessibili solo a un determinato insieme di nodi PA, ad esempio quei nodi che hanno adottato lo stesso software (approccio nominale) o quelli che svolgono funzioni simili (approccio funzionale).
3. **Notificare nuove vulnerabilità**: il responsabile tecnico di una PA può essere notificato direttamente riguardo nuove vulnerabilità negli asset di cui è responsabile. Inoltre, queste comunicazioni possono certificare che gli aggiornamenti sono stati notificati, rendendo il responsabile obbligato ad aggiornare il sistema di conseguenza.

Dato il contesto sensibile, i risultati non possono essere condivisi pubblicamente e l'accesso deve essere garantito solo a specifiche entità. Inoltre, i risultati dovrebbero essere resi disponibili senza fornire informazioni sulla PA che ha eseguito il test, per evitare di rivelare la sua infrastruttura tecnologica. In ogni caso, le informazioni possono essere condivise solo dopo che i bug di sicurezza trovati sono stati risolti

(caso zero).

Operativamente, questa proposta richiede sia una piattaforma dedicata, che stabilisca un canale ufficiale di comunicazione per notifiche e scambio di informazioni a livello di rete, sia una partecipazione attiva del personale tecnico incaricato della sua gestione.

Per ciascun nodo PA, i responsabili tecnici dovrebbero essere coinvolti sia quando la PA riceve un report dopo un test di sicurezza, sia dopo una modifica degli asset. Nel dettaglio:

1. La PA che ha effettuato il test di sicurezza verifica innanzitutto che le vulnerabilità scoperte siano state risolte dal fornitore; successivamente, la PA carica i risultati sulla piattaforma specificando il fornitore, il prodotto, la versione e l'impatto della vulnerabilità (score CVSS[17]) con una descrizione di tale vulnerabilità. È anche possibile indicare chi ha effettuato il test.
2. La PA che modifica la propria infrastruttura tecnologica, sia in termini di asset hardware che software, aggiorna tali modifiche sulla piattaforma. In questo modo, può essere notificata per eventuali problemi già noti o per quelli futuri.

Organizzazioni come i CSIRT sono candidati naturali per gestire la piattaforma, ma il framework proposto introduce un approccio bottom-up oltre il mandato dei CSIRT: le informazioni e le richieste sui test di sicurezza provengono dai nodi PA e coinvolgono attivamente l'intera rete PA, incluse le piccole PA.

Rappresentazione grafica dei processi da implementare

Il flusso logico delle interazioni per abilitare il riuso dei Test di Sicurezza è principalmente determinato dai requisiti. Si parte dai vincoli derivanti dalle attuali linee guida AgID sulla sviluppo di software sicuro e dalle buone pratiche in PT/VA.

- **L'esecuzione dei Test di Sicurezza** (ad esempio PT) deve essere condotta da un fornitore terzo e non può essere effettuata né dalla PA né dal fornitore che ha sviluppato il software.

- **Scenari standard**: devono essere considerati da qualsiasi PA i seguenti scenari:
    - acquisizione di informazioni relative a nuovo software introdotto nel nodo PA;

[17] P. Mell, K. Scarfone, S. Romanosky, A complete guide to the common vulnerability scoring system version 2.0, in: Published by FIRST-forum of incident response and security teams, volume 1, 2007, p. 23.

- recupero e aggiornamento delle informazioni relative al software esistente nel nodo PA;
- recupero e aggiornamento delle informazioni relative a nuovo software nel nodo PA.

- **Scenari non standard basati sul contesto**: questi scenari possono generare nuovi schemi di processo. Tale eventualità deve essere considerata di default, al fine di tracciare, valutare e possibilmente accettare il processo o correggerlo.

Per contestualizzare i seguenti schemi di processo nello stesso scenario, rispettando i requisiti precedenti indipendentemente dal software analizzato, adotteremo la convenzione di due attori distinti, associati rispettivamente alla vendita del software e ai servizi di PT/VA.

Attori:
- PA (1, 2, 3, ...): pubblica amministrazione;
- SW-1: Fornitore di software. Questo attore sviluppa, personalizza e vende il software alle PA;
- PT-1: Fornitore di test di sicurezza. Questo attore vende test di sicurezza alle pubbliche amministrazioni;
- PLATFORM: la piattaforma.

Schema di processo 1

1. PA1 acquista il software da SW-V1.
2. SW-V1 fornisce il software a PA1 (ad esempio, sw_calcoloImu v1.0).
3. PA1 richiede un servizio di test di sicurezza a PT-V2.
4. PT-V2 esegue il test di sicurezza e fornisce a PA1 il report riguardante i bug di sicurezza e gli 0day.
5. PA1 invia a SW-V1 i bug di sicurezza e gli 0day trovati durante il test di sicurezza e richiede la correzione dei bug nel software (ad esempio, sw1_calcoloImu v1.0).
6. SW-V1 esegue la correzione dei bug sul software in conformità agli accordi tra le parti (ad esempio, sw_calcoloImu v1.0).
7. SW-V1 rilascia la versione corretta del software (ad esempio, sw1_calcoloImu v2.0).
8. PA1 carica sulla piattaforma i bug di sicurezza trovati durante il test di sicurezza (ad esempio, bug di sicurezza e/o 0day) per la versione 1 del software (ad esempio, sw1_calcoloImu v1.0) sviluppata da SW-V1.
9. La PLATFORM notifica a tutte le PA che hanno registrato il software sulla piattaforma le vulnerabilità che sono state aggiunte per la versione specifica del software.
10. Ogni singola PA verifica il software per il quale è stata segnalata una vulnerabilità.

A questo punto, ci sono due possibilità:

a. la PA possiede il software vulnerabile;
b. la PA non ha più il software tra i propri asset.

11. PA2 richiede a SW-V1 l'ultima versione del software.
12. SW-V1 rilascia a PA2 l'ultima versione del software (ad esempio, sw1_calcoloImu v2.0).

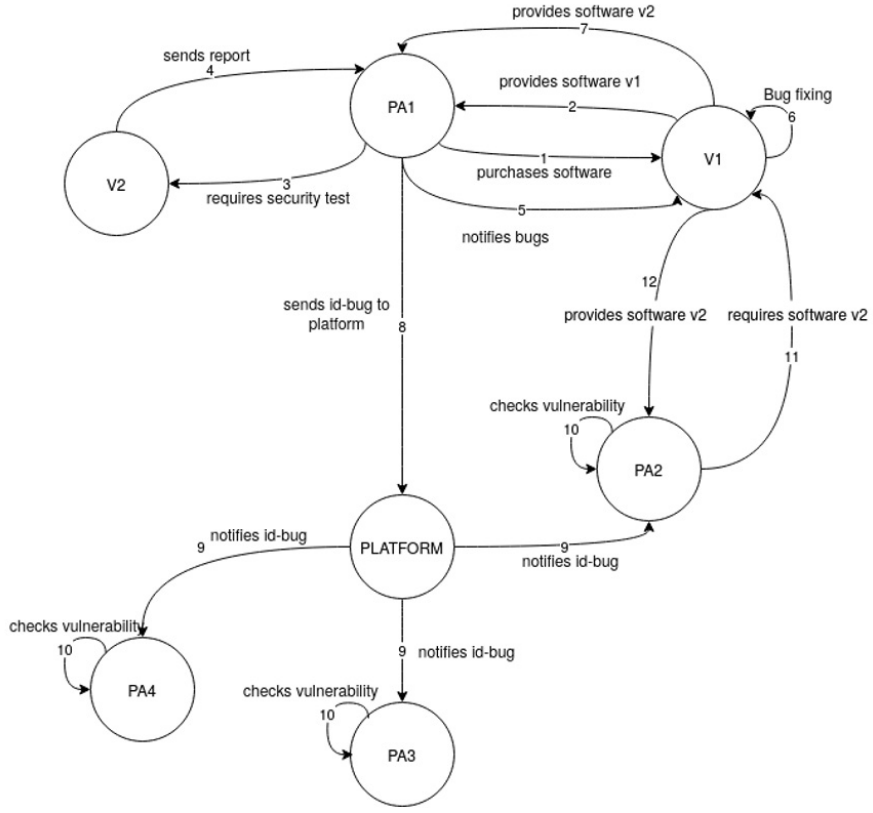


Figure 1: schema di processo 1

Schema di processo 2

1. PA1 richiede alla PLATFORM un elenco aggiornato delle vulnerabilità relative ai propri asset software.
2. La PLATFORM fornisce a PA1 l'elenco delle vulnerabilità per ogni singolo software posseduto da PA1.
3. PA1 analizza l'elenco delle vulnerabilità fornito dalla PLATFORM. L'elenco può essere così suddiviso:

a. Contiene informazioni recenti per alcuni componenti posseduti da PA1:
   i. PA1 contatta SW-V1 per la correzione dei bug relativi alle informazioni che soddisfano il punto 3.(a).
   ii. SW-V1 fornisce la versione corretta.
b. Contiene informazioni obsolete (ad esempio, la data dell'ultimo test di sicurezza eseguito su una singola versione del software è più vecchia di 6 mesi) o non contiene informazioni (ad esempio, un test di sicurezza non è mai stato eseguito su quella specifica versione del software) per alcuni componenti posseduti da PA1.
   i. PA1 richiede un test di sicurezza a PT-V2 per gli asset che soddisfano il punto 3.(b).
   ii. PT-V2 esegue il test di sicurezza e fornisce a PA1 il report relativo ai bug di sicurezza agli 0day.
   iii. PA1 aggiorna i propri asset sulla base del report fornito da PT-V2.
   iv. PA1 carica i risultati del test di sicurezza sulla PLATFORM.

Si noti che gli attributi "informazioni recenti" e "informazioni obsolete" nel Punto 3 dello Schema di processo 2 sono relativi ad aspetti di implementazione indipendenti dalla struttura logica proposta. Gli attributi, infatti, possono dipendere da fattori come l'aggiunta di nuove funzionalità al software in esame, valutazioni individuali della PA o criteri legati alla periodicità dei test in base alle linee guida per una gestione sicura del software (ad esempio, "da eseguire preferibilmente ogni 6 mesi").

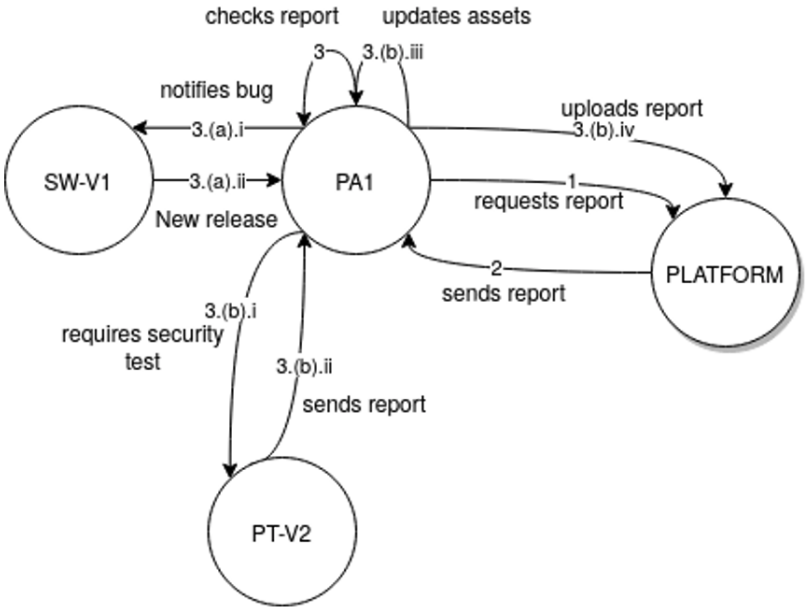


Figure 2: schema di processo 2

Schema di processo 3

1. PA1 acquista nuovi asset software da SW-V1.
2. SW-V1 fornisce gli asset a PA1.
3. PA1 aggiorna il proprio inventario aggiungendo gli asset appena acquisiti.
4. PA1 aggiunge i nuovi asset acquisiti alla PLATFORM.
5. La PLATFORM fornisce un elenco delle vulnerabilità note riguardanti gli ultimi asset aggiunti, basandosi sulle informazioni disponibili sulla piattaforma.
6. PA1 analizza il report per verificare che tutti i nuovi asset siano aggiornati e privi di vulnerabilità note.

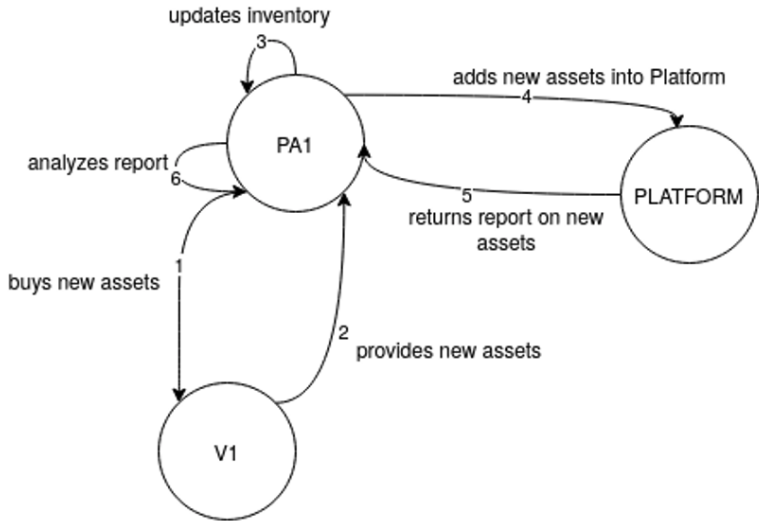


Figure 3: schema di processo 3

4. Effetti economici misurabili attesi

L'implementazione del riuso dei risultati dei PT descritta sopra potrebbe portare vantaggi effettivi sia da un punto di vista microeconomico che macroeconomico. Questi vantaggi rappresentano effetti tangibili, ovvero misurabili, poiché è possibile valutare gli indicatori economici per analizzare l'efficacia dell'approccio proposto a diverse scale:

- **Migliore valutazione delle politiche di spesa pubblica:** se la descrizione di alcune vulnerabilità emerge durante l'esecuzione di un PT e le informazioni sulla versione corretta dello stesso software sono disponibili, la spesa pubblica può essere riallocata su investimenti differenti.
- **Vantaggio competitivo per gli ecosistemi territoriali**: l'intero sistema paese trarrebbe vantaggi competitivi, ad esempio tramite il potenziamento delle PA che non riescono a eseguire PT in modo regolare e costante a causa di problemi di bilancio o difficoltà nel trovare personale specializzato.
- **Supporto ai decisori politici nella revisione della spesa:** basato su

informazioni sicure provenienti da una rete affidabile.

- **Scelta dei settori in cui intervenire:** i risparmi in un settore consentono potenziali reinvestimenti in altri (ad esempio, beni culturali, ambiente, sanità, ecc.).

Dal punto di vista microeconomico, si possono individuare alcuni vantaggi utilizzando il concetto di economie di scopo: con questo termine si fa riferimento ai risparmi derivanti dalla produzione congiunta di diversi prodotti o dal perseguimento di diversi obiettivi attraverso l'uso degli stessi fattori produttivi. In questo modo, è possibile produrre diversi tipi di beni con la stessa classe di risorse. Utilizzando questa nozione, è facile identificare gli effetti del riuso dei risultati dei PT come i benefici degli investimenti effettuati da un singolo ente della PA per tutti gli altri enti che condividono lo stesso bisogno.

D'altro canto, la proposta avrebbe anche un effetto macroeconomico grazie ai notevoli risparmi per la PA. Per quantificarli, si parte dalla formula del risparmio pubblico:

$$
S_{pubb} = T - G
$$

Una riduzione della spesa pubblica (G) comporterebbe un aumento del risparmio pubblico, che potrebbe consentire una riduzione delle tasse (T). Inoltre, è utile ricordare che il risparmio complessivo è dato da:

$$
S = S_{priv} + S_{pubb}
$$

Quindi, maggiori risparmi pubblici porterebbero a maggiori risparmi complessivi. Nella teoria keynesiana, vale l'identità macroeconomica:

$$
S = I
$$

Pertanto, un incremento del risparmio complessivo corrisponde a un aumento degli investimenti (I), determinando un miglioramento complessivo del PIL nazionale.

Il vantaggio macroeconomico emerge non solo da maggiori risorse economico-finanziarie che possono coprire diverse necessità, ma anche in termini di ridefinizione delle strategie condivise tra i diversi nodi locali della PA. Una modifica della struttura

di condivisione delle informazioni comporta un corrispondente cambiamento nell'insieme delle soluzioni o politiche possibili per l'allocazione delle risorse; in particolare, l'approccio presente non esclude strategie possibili, ma ne introduce di nuove.

Un esempio pratico è il riuso delle informazioni utili provenienti da VA/PT effettuati su specifici componenti di un dato asset: se un nodo PA non dispone di risorse sufficienti per garantire il rispetto di tutti i criteri richiesti dalle linee guida nazionali, può limitarsi a recuperare le informazioni mancanti, assumendo che informazioni complementari siano già disponibili grazie ad azioni di testing e condivisione effettuate da altri nodi. In linea di principio, questa conoscenza può supportare la pianificazione amministrativa strategica dei singoli nodi, portando possibili benefici reciproci.

Infine, il riuso dei test di sicurezza o, più precisamente, delle informazioni utili che essi forniscono, può portare vantaggi anche a livello sovranazionale, ad esempio a livello europeo. Questo aspetto riguarda la conformità delle politiche adottate dall'UE in materia di open data. Inoltre, il riuso delle informazioni provenienti dai test di sicurezza può configurarsi come un canale di comunicazione secure-by-design tra due tipi di attori: il livello puramente nazionale (PA) e il livello internazionale (fornitori).

5. Conclusione e sviluppi futuri

Il presente contributo propone un nuovo framework che mira a supportare la PA nazionale nel soddisfare i requisiti posti dalla trasformazione digitale in conformità con le raccomandazioni europee. Inoltre, questo framework apre la strada a nuovi risparmi e opportunità di business per organizzazioni pubbliche e private.

Esistono diverse direzioni di ricerca per affinare questa proposta: innanzitutto, le informazioni derivanti dal riuso dei test di sicurezza assumono un nuovo valore, che può diventare un nuovo asset per le organizzazioni. Il valore aggiunto portato dalla condivisione delle informazioni può essere sfruttato per esplorare nuovi modelli di incentivazione organizzativa con l'obiettivo di migliorare la trasparenza nella cybersicurezza orientata alla PA. Questa prospettiva si configura come una forma di economia circolare con risorse immateriali, strategicamente importante non solo per i singoli nodi della PA, ma anche per il sistema paese e, più in generale, per l'UE. Anche i fornitori potrebbero trarre vantaggi da un tale framework: una maggiore trasparenza nei requisiti di test di sicurezza per un nodo specifico della rete potrebbe integrare le informazioni parziali già disponibili per le PA, sia in termini di riduzione delle falle nel processo di testing (ad esempio, violazioni delle

condizioni nelle Linee guida) sia nell'accesso al mercato oltre la scala locale (ad esempio, a livello nazionale).

In questo lavoro è stata presentata una struttura ad alto livello senza fornire un contesto specifico di caso reale: questo approccio è motivato dalle possibilità offerte da questo livello di astrazione, poiché lo schema proposto può essere adattato a diversi contesti distinti. Potrebbero esistere situazioni in cui diverse esigenze di sicurezza e requisiti conflittuali (ad esempio, riservatezza vs. accessibilità) portano a implementazioni ad hoc di questo framework. Ad esempio, potrebbero essere introdotti nuovi livelli di sicurezza, in cui diversi uffici o entità all'interno della struttura stratificata della PA hanno i propri requisiti di sicurezza e le relative contromisure.

L'opportunità di adattare la struttura logica alle caratteristiche contestuali dei nodi si adatta bene alla complessità della PA italiana e potrebbe migliorare la condivisione sicura delle informazioni tra i livelli centrali e locali/periferici. D'altra parte, l'implementazione del framework proposta, che è tipica dei sistemi tecnologici su larga scala, richiede procedure di validazione specifiche per ciascun contesto.

In questo modo, il framework proposto:

- Introduce la separazione dei dati nell'accesso alle informazioni, rendendo lo scambio di informazioni asimmetrico tra questi livelli come formalmente definito dal Principio del Minimo Privilegio[18]: i livelli locali non possono accedere alle informazioni centrali, prevenendo l'escalation di privilegi verticali.
- Può supportare la definizione di livelli di comunicazione (ad esempio, avvisi) basati su specifici livelli di qualificazione di sicurezza attesi o richiesti in ciascun nodo. Questo miglioramento può stimolare una definizione più chiara dei campi di competenza e delle responsabilità legate alla cybersicurezza nella PA, al fine di inviare informazioni rilevanti a entità target capaci di interpretarle e contrastare i rischi cibernetici.
- Permette di condividere informazioni senza accedere ai dati originali (ad esempio, report originali), che potrebbero essere riservati. È possibile accedere alle informazioni senza divulgazione, fornendo solo conferme per specifiche richieste da parte di un nodo della PA relative ai propri asset software. Questo approccio promuove le contromisure richieste e migliora, anziché compromettere, la sicurezza della rete PA.

[18] F. B. Schneider, Least privilege and more, in: Monographs in Computer Science, Springer- Verlag, 2003, pp. 253–258. URL: https://doi.org/10.1007%2F0-387-21821-1_38. doi:10.1007/0-387-21821-1_38.

N. 6 - 2024 - pp. 80-97

Direttiva NIS 2:
genesi, attuazione, impatti

Corrado Giustozzi

Abstract: La cosiddetta Direttiva NIS 2, pubblicata in Gazzetta ufficiale dell'Unione europea a fine 2022 e le cui rispettive norme di recepimento si applicano in tutti gli Stati membri dell'Unione Europea a decorrere dal 18 ottobre 2024, non è un provvedimento a sé stante e soprattutto non nasce, contrariamente a quanto molti credono, come "correzione" della precedente Direttiva NIS del 2016: è invece la più recente tappa di un percorso organico e sistematico tracciato dalla Commissione oltre un decennio fa ed avente l'ambizioso obiettivo di innalzare, in modo comune e coordinato, la protezione cibernetica dell'intera infrastruttura produttiva e di servizio su cui si poggiano lo sviluppo e la sostenibilità dell'Europa. Interviene, quindi, su di un ecosistema diffuso formato non solo da poche e grandissime infrastrutture critiche, ma anche e soprattutto da organizzazioni grandi e medie, che operano in molteplici settori pubblici e privati, e sono interconnesse da catene di approvvigionamento caratterizzate da complesse e spesso fragili relazioni di interdipendenza funzionale.

The so-called NIS 2 Directive, which was published in the Official Journal of the European Union at the end of 2022 and whose respective transposition rules will apply in all EU Member States as of 18 October 2024, is not a stand-alone measure and, above all, does not originate, contrary to what many believe, as a 'correction' of the previous NIS Directive of 2016:: it is instead the most recent stage of an organic and systematic path traced by the European Commission over a decade ago, and having the ambitious goal of enhancing, in a common and coordinated way, the cyber protection of the entire production and service infrastructure on which the development and sustainability of Europe are based. It therefore intervenes on a widespread ecosystem made up not only of a few and very large critical infrastructures but also of large and medium-sized organizations, which operate in multiple public and private sectors, and are interconnected by supply chains characterized by complex and often fragile relationships of functional interdependence.

Parole chiave: NIS, NIS 2, servizi essenziali, infrastrutture critiche, cybersecurity, supply chain.

Sommario: 1. Premessa – 2. Origine della Direttive NIS e NIS 2 – 3. La Direttiva NIS – 4. La Direttiva NIS 2 – 5. Conclusioni.

1. Premessa: il "nuovo" approccio del Legislatore Europeo

Per poter analizzare compiutamente la portata della Direttiva NIS 2 è opportuno preliminarmente sottolineare come essa si inserisca concettualmente in una linea di norme caratterizzate da un approccio comune, e relativamente nuovo per l'ordinamento europeo, alle misure di sicurezza.

Si può in effetti rilevare che il Legislatore europeo, nel declinare le prescrizioni di sicurezza per i settori regolati, stia sistematicamente adottando da una decina di anni a questa parte una modalità di indirizzo filosoficamente opposta a quella che aveva seguito in precedenza: mentre, infatti, in passato veniva adottato un approccio meramente *prescrittivo*, ossia basato su una logica che potremmo definire *dell'adempimento* da parte del soggetto interessato, da circa dieci anni si adotta, invece, un approccio *finalizzato ai risultati* e basato sulla logica *della responsabilizzazione* del soggetto in questione. Ciò si declina, in sostanza, nel non consegnare più al soggetto interessato una lista predefinita e puntuale di misure di sicurezza da adottare (solitamente definite "minime"), lasciandolo invece libero di scegliere quelle che ritiene maggiormente idonee al fine di raggiungere gli obiettivi assegnatigli (solitamente definite "appropriate" o "adeguate").

Tale profondo mutamento prospettico, peraltro da sempre caldeggiato da parte della comunità degli esperti di sicurezza e sostenuto dalle principali *best practice* di settore, parte dalla considerazione che ciascun soggetto operante è diverso dagli altri, perfino se appartenente al medesimo settore di attività; ed è profondamente caratterizzato dalle proprie particolari specificità relativamente a "cosa fa" e "come lo fa". Risulta, pertanto, concettualmente erroneo, e senz'altro poco efficace, imporre a tutti gli operatori, siano essi del medesimo settore o - peggio ancora - di settori differenti, le medesime misure di sicurezza, soprattutto se formulate in modo aprioristico e aspecifico, perché certamente in questo modo non si ottengono i risultati sperati.

In primo luogo infatti tali misure "universali", così come la proverbiale maglietta a taglia unica "che va bene a tutti", finiranno in realtà per non andare bene a nessuno, risultando cioè insufficienti per qualcuno e sovrabbondanti per qualcun altro. Ma soprattutto l'imposizione stessa di un elenco predefinito di misure ne favorirà un'adozione totalmente acritica da parte dei soggetti a cui sono destinate, i quali si limiteranno a recepirle per puro obbligo formale e senza alcuna comprensione del loro reale valore: di fatto, quindi, attuando una deresponsabilizzazione dei destinatari rispetto alle esigenze di protezione che dovrebbero invece fare proprie, e dunque vanificando ogni processo di miglioramento continuo.

È invece assai più corretto, sia sul piano metodologico che su quello della reale

efficacia, che ciascun operatore definisca e adotti le misure di sicurezza più adatte a sé e al proprio contesto, non limitandosi ad estrarle asetticamente da qualche elenco predefinito di uso generale, ma derivandole autonomamente da una analisi del rischio attenta e personalizzata che tenga in considerazione, appunto, le proprie specificità. La sicurezza, in altre parole, per essere efficace deve essere costruita su misura da ciascun operatore, in modo da adattarsi ai propri processi e poter così contrastare i propri rischi specifici.

Si tratta evidentemente di un approccio assai più difficile da attuare, in quanto richiede molta maturità e disciplina nel soggetto operante: tuttavia, è l'unico in grado di garantire non solo l'efficacia nel tempo delle misure di sicurezza, ma anche la loro efficienza, perché consente a chi lo adotta di poter modulare consapevolmente gli investimenti in sicurezza, e quindi ottimizzarli, anziché procedere secondo criteri attuativi eterodeterminati e mal compresi.

Di fatto, questo è l'approccio adottato sistematicamente dal Legislatore europeo in tutte le recenti normative rilevanti, a partire dal Regolamento (UE) 2014/910 noto come eIDAS, emanato esattamente dieci anni fa e rivolto a quei soggetti che forniscono servizi di fiducia nel mondo digitale. Lo ritroviamo poi, cosa ben più nota, nel Regolamento (UE) 2016/679 noto come GDPR, dove rientra come requisito nel novero più ampio del concetto di *accountability*, ovvero la capacità di poter dimostrare e sostenere in modo oggettivo le proprie scelte anche per quanto riguarda l'adozione delle misure di sicurezza. E naturalmente lo ritroviamo nella coeva, ancorché precedente come concezione, Direttiva (UE) 2016/1148 nota come «NIS», recentemente abrogata dalla Direttiva (UE) 2022/2555 «NIS 2» che ne riprende ed estende l'impianto.

È interessante a tal proposito vedere come in tutte queste norme, ancorché scritte in tempi e da mani differenti, si manifesti una singolare unità di pensiero e di espressione quando si tratti, appunto, di definire i requisiti di sicurezza ai quali devono attenersi i rispettivi destinatari:

- il Regolamento eIDAS, all'art. 19 "Requisiti di sicurezza relativi ai prestatori di servizi fiduciari", stabilisce che: «*1. I prestatori di servizi fiduciari qualificati e non qualificati adottano le misure tecniche e organizzative appropriate per gestire i rischi legati alla sicurezza dei servizi fiduciari da essi prestati. Tenuto conto degli ultimi sviluppi tecnologici, tali misure assicurano un livello di sicurezza commisurato al grado di rischio esistente. In particolare, sono adottate misure per prevenire e minimizzare l'impatto degli incidenti di sicurezza e informare le parti interessate degli effetti negativi di eventuali incidenti.*»;
- il GDPR, all'art. 32 "Sicurezza del trattamento", stabilisce che: «*1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'og-*

getto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, […]»;

- infine, la Direttiva NIS 2, all'art. 21 "Misure di gestione dei rischi di cibersicurezza", stabilisce che: «*1. Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino misure tecniche, operative e organizzative adeguate e proporzionate per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete […]. Tenuto conto delle conoscenze più aggiornate in materia, […] nonché dei costi di attuazione, le misure […] assicurano un livello di sicurezza dei sistemi informatici e di rete adeguato ai rischi esistenti. […]*».

Questa pur rapida lettura sinottica ben chiarisce come l'assenza nelle recenti norme europee di prescrizioni specifiche e puntuali relative a misure minime di sicurezza, talvolta criticata da qualche osservatore superficiale che l'ha attribuita a leggerezza o addirittura dimenticanza del Legislatore, sia invece frutto di una corretta applicazione dell'approccio metodologico, secondo il quale ogni soggetto operante deve definire i propri criteri di protezione: in applicazione, quindi, di quel principio di responsabilizzazione degli operatori che risulta necessario per innescare un circolo virtuoso di miglioramento continuo in tutto il sistema.

2. Origine delle Direttive NIS e NIS 2

Per poter meglio contestualizzare la Direttiva NIS 2 nel panorama ove si inserisce, inoltre, è utile conoscere il relativamente lungo ed articolato excursus storico e concettuale che ha portato alla sua definizione. Essa, infatti, non nasce *ex abrupto* nel 2022, ma ha origine nella prima Direttiva NIS, risalente all'ormai lontano 2013: ed è per questo, tra l'altro, che essa porta tuttora nel proprio nome l'esplicito riferimento alla "sicurezza delle reti e delle informazioni"[1], che al giorno d'oggi suona piuttosto obsoleto e anche limitativo. Va anche sottolineato che, contrariamente a quanto qualcuno fallacemente sostiene, essa non è stata istituita per sopraggiunte esigenze di "correggere in corsa" la NIS, ma era già prevista *ab origine* come sua naturale evoluzione. Per inquadrare correttamente la sua valenza conviene, quindi, preliminarmente ripercorrerne le tappe evolutive e soprattutto analizzare i razionali che portarono alla sua emanazione, partendo appunto dalla genesi della prima Direttiva NIS.

[1] L'acronimo NIS sta infatti per «Network and Information Security».

Nel marzo 2013, a margine delle attività previste dalla titanica iniziativa Europe 2020 finalizzata allo sviluppo e al rafforzamento delle tecnologie digitali per supportare la crescita e l'occupazione nell'Unione, la Commissione Europea sottopose al Parlamento e al Consiglio due atti di indirizzo in materia di cybersecurity, chiedendone la rapida approvazione. Il primo era un documento strategico sulla protezione dello spazio cibernetico comune europeo, la cosiddetta European Cyberstrategy; il secondo era una proposta di direttiva contenente *«misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno»*, subito soprannominata NIS per via degli ambiti da essa interessati. Lo scopo di questa iniziativa della Commissione era quello di promuovere rapidamente l'adozione sia di una politica di indirizzo che di misure operative atte a rafforzare la postura di protezione cibernetica dell'Unione, alla luce dei segnali di crescita della minaccia che già da qualche tempo si stavano chiaramente delineando all'orizzonte.

Come auspicato dalla Commissione, la cyberstrategy venne effettivamente approvata in tempi rapidissimi dal Consiglio e dal Parlamento e fu quindi ufficialmente emanata nell'aprile dello stesso anno, diventando così immediatamente vincolante per gli Stati Membri e segnando l'avvio di un percorso evolutivo che ancora oggi prosegue sulle stesse linee programmatiche[2]. Invece, i membri del Consiglio e del Parlamento si trovarono subito in disaccordo politico sulla proposta di direttiva, che, essendo la prima iniziativa tesa ad armonizzare una situazione di forte disomogeneità tra gli Stati Membri, fu accolta dai rappresentanti degli stessi con valutazioni di merito decisamente contrastanti.

In effetti, le controversie furono tali che la discussione sulla proposta di direttiva proseguì a porte chiuse per oltre due anni e mezzo, e fu solo alla fine del 2015 che in sede di Trilogo si riuscì ad ottenere la convergenza su un testo ritenuto soddisfacente da tutte le parti interessate. Era così nata, come soluzione di compromesso, la Direttiva NIS: la quale venne, quindi, formalmente approvata nei primi mesi del 2016 e infine pubblicata in Gazzetta Ufficiale dell'Unione a luglio dello stesso anno[3]. Agli Stati Membri furono dati due anni di tempo per recepirla nel proprio ordinamento nazionale ed adeguarsi al suo mandato: così, essa divenne completamente efficace solo nel giugno del 2018[4].

---

[2] La prima Cyberstrategy europea del 2013, denominata «An open, safe and secure cyberspace», è stata sinora aggiornata due volte: la prima nel 2017 con un documento denominato «Resilience, Deterrence and Defence: Building strong cybersecurity for the EU», e la seconda nel 2020 con un documento denominato «The EU's Cybersecurity Strategy for the Digital Decade».

[3] Formalmente: «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».

[4] In Italia fu recepita con il Decreto legislativo 18 maggio 2018, n. 65, pubblicato in GU n.132 (SG) del 9 giugno 2018, successivamente modificato dal Decreto Legge 14 giugno 2021 n° 82 «Definizione

Proprio in quanto frutto di compromesso, la Direttiva non poté indirizzare sin da subito tutti gli aspetti originariamente proposti dalla Commissione: essa fu, invece, disegnata in modo da attuare i suoi obiettivi con un approccio più cauto e graduale e, quindi, maggiormente protratto nel tempo. Si decise, infatti, di affrontare in un primo momento il solo ambito dei soggetti a maggior criticità, quelli che in precedenza venivano appunto denominati "infrastrutture critiche", circoscrivendo così il mandato della norma ad un numero relativamente ristretto di operatori e di settori di attività; per lasciare poi ad una successiva direttiva, da definirsi anche alla luce dell'esperienza maturata nei primi anni di attuazione di quella in emanazione, il compito di ampliare sia il numero di operatori, per ricomprendervi anche soggetti di dimensioni minori, che il numero e la tipologia dei rispettivi settori di attività.

Fu, pertanto, stabilito *ab origine* che la successiva direttiva sarebbe stata emanata quattro anni dopo la prima. Tale intervallo di tempo fu giudicato come il più adeguato, tanto per consentire alla Commissione di valutare i risultati conseguiti sul campo dall'attuazione della Direttiva iniziale, quanto per dare modo agli Stati Membri di rodare le loro strutture organizzative ed operative in vista dell'ampliamento di portata che essa avrebbe comportato. Con evidente poca fantasia, la futura emananda Direttiva fu da subito informalmente identificata come «NIS 2», e tale denominazione le è poi rimasta ufficialmente anche in seguito.

Di conseguenza, nel 2020, e quindi dopo due anni di reale esercizio della Direttiva NIS, la Commissione avviò in tutta l'Unione un'ampia azione di ricognizione finalizzata a valutare come essa fosse stata effettivamente recepita ed attuata, quali punti di forza e di debolezza si fossero manifestati nella reale operatività quotidiana, quali eventuali aspetti di miglioramento fossero emersi, come avessero funzionato le strutture tecniche ed operative predisposte dagli Stati Membri per supportare le attività previste; e, più in generale, quali lezioni si potessero apprendere dall'esperienza sino ad allora fatta sul campo. Tutte le informazioni così raccolte servirono a preparare il terreno per la discussione politica e tecnica su come mettere a punto la successiva NIS 2 la quale, come originariamente previsto, avrebbe dovuto estendere il regime di protezione a molti più settori, nonché ad operatori di dimensioni molto minori, rispetto alla precedente.

L'elaborazione della nuova direttiva durò quasi due anni: infatti, benché essa fosse stata annunciata nelle sue linee generali già nel dicembre 2020, l'accordo politico sul testo fu effettivamente raggiunto solo nel maggio 2022. La formulazione definitiva della NIS 2 fu quindi approvata dal Parlamento Europeo a ottobre 2022, ratificata ufficialmente il 14 dicembre e pubblicata in Gazzetta Ufficiale EU il 27 di-

dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale».

cembre[5] dello stesso anno, entrata in vigore il 17 gennaio 2023, con obbligo di recepimento entro il 17 ottobre 2024, contestualmente all'abrogazione della precedente Direttiva NIS. Agli Stati Membri, quindi, in linea con quanto già fatto con la prima Direttiva NIS, furono dati circa due anni di tempo per familiarizzare con la nuova normativa, predisporre le proprie Autorità e le strutture operative ad attuarla, e soprattutto sensibilizzare i nuovi operatori relativamente agli impegni che li avrebbero interessati.

3. La prima Direttiva NIS

La Direttiva NIS, come già detto, fu la prima norma europea ad affrontare in modo sistematico il problema, allora appena agli albori, della protezione cibernetica dei soggetti responsabili dell'erogazione nella UE di quei servizi ritenuti essenziali per l'ordinato funzionamento della società civile. A tal fine, il suo approccio fu piuttosto innovativo sotto vari aspetti significativi, che ritroviamo poi nella successiva NIS 2.

In primo luogo, essa ampliava e rimodulava il precedente concetto di «infrastruttura critica», trasformandolo nelle due nuove categorie degli «operatori dei servizi essenziali» e dei «fornitori di servizi digitali». Questi comprendevano, oltre ai "classici" operatori elettrici, del gas o dei trasporti, anche soggetti che sino a quel momento erano stati considerati estranei a questo mondo, quali ad esempio le banche, le strutture sanitarie, i fornitori di servizi in cloud e i motori di ricerca su Internet.

In particolare, venivano definiti come «operatori dei servizi essenziali» quei soggetti, particolarmente rilevanti per via della loro dimensione o del bacino d'utenza interessato, operanti nei seguenti sette settori specifici, qui elencati nei loro titoli principali, ma che venivano ulteriormente qualificati nel dettaglio dalla norma mediante diverse articolazioni di livello inferiore:

1. Energia
2. Trasporti
3. Settore bancario
4. Infrastrutture dei mercati finanziari
5. Settore sanitario

[5] Formalmente: «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».

6. Fornitura e distribuzione di acqua potabile
7. Infrastrutture digitali

Erano, invece, definiti «fornitori di servizi digitali» quegli operatori, anch'essi rilevanti per dimensione o bacino d'utenza, che fornivano servizi di:

1. Mercato online
2. Motore di ricerca online
3. Servizi di cloud computing

Allo scopo di assicurare la continuità dei servizi essenziali e dei servizi digitali erogati, la norma imponeva ai rispettivi operatori di adottare misure tecnico-organizzative idonee ed adeguate per ridurre il rischio e limitare l'impatto di incidenti informatici, in applicazione di quel principio di responsabilizzazione illustrato in premessa. Obbligava, altresì, gli operatori ad auto-vigilarsi durante la propria attività, e a riportare tempestivamente alle apposite autorità nazionali tutti gli incidenti eventualmente subiti, i quali avessero avuto impatto rilevante sulla fornitura dei propri servizi.

La norma italiana di recepimento declinò il mandato della Direttiva attribuendo il ruolo di Autorità nazionale NIS alla Agenzia Nazionale per la Cybersicurezza[6], e nominando Autorità di settore quei Ministeri aventi competenza sugli specifici settori NIS, con l'aggiunta di Banca d'Italia e Consob a supporto del Ministero dell'Economia e delle Finanze per quanto riguardava il settore bancario e dei mercati finanziari.

Gli operatori interessati dalla norma vennero identificati individualmente mediante l'applicazione di specifici criteri predefiniti che, di fatto, selezionavano solo quelli di maggiore dimensione o di maggiore rilevanza rispetto al proprio bacino d'utenza. Numero e identità di tali operatori non furono resi noti, in quanto sottoposti dal Governo italiano ad un regime di riservatezza, ma è noto che fossero complessivamente meno di cinquecento: di fatto, dunque, furono interessati solo i grandissimi operatori nazionali o regionali dei rispettivi settori.

La Direttiva prevedeva naturalmente un regime sanzionatorio per le inadempienze, dando tuttavia ampia libertà a ciascuno Stato Membro nel definire l'entità delle sanzioni e le modalità di applicazione. L'Italia adottò un modello basato su sanzioni fisse, ovvero definite in valore assoluto, che alla luce dell'esperienza si è

[6] Inizialmente, tale Autorità era il Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri, che all'epoca era la struttura del Governo competente per la sicurezza cibernetica nazionale. Quando venne istituita l'Agenzia Nazionale per la Cybersicurezza, ad essa vennero trasferite tutte le competenze sulla sicurezza cibernetica, comprese quelle derivanti dall'attuazione della Direttiva NIS.

dimostrato poco efficace.

4. La Direttiva NIS 2: struttura e punti di attenzione

La Direttiva NIS 2, entrata in vigore in tutta l'Unione il 18 ottobre 2024 contestualmente all'abrogazione della NIS originaria, riprende sostanzialmente l'impianto di quest'ultima, ma ne estende la portata sia in senso "orizzontale" che "verticale": orizzontale, in quanto amplia significativamente il novero dei settori di attività interessati, portandoli da sette a dieci; verticale, in quanto accresce enormemente il numero degli operatori coinvolti, affiancando alle imprese "grandissime" anche quelle "grandi" e "medie" secondo la definizione ufficiale europea[7]. È assai significativo che tra i settori di nuova introduzione vi sia la Pubblica Amministrazione, la quale per la prima volta viene riconosciuta come "soggetto critico" a livello europeo.

La nuova Direttiva cancella, inoltre, la categorizzazione precedentemente operata dalla NIS sulle entità interessate, le quali come già detto erano suddivise in «operatori dei servizi essenziali» e «fornitori di servizi digitali», e parla più omogeneamente di «soggetti»: questi sono classificati semplicemente come «essenziali» o «importanti» in funzione della loro dimensione e dell'appartenenza a settori di attività identificati come più o meno critici.

Nel testo adottato dall'Italia, la norma comprende ben quattro allegati per la determinazione dei settori interessati, i quali vengono specificati con grande dettaglio e ricomprendono un novero estremamente ampio di ambiti di attività.

L'Allegato I raccoglie i cosiddetti «settori ad alta criticità» che, sempre ad alto livello, comprendono:

1. Energia
2. Trasporti
3. Settore bancario
4. Infrastrutture dei mercati finanziari
5. Settore sanitario
6. Fornitura e distribuzione di acqua potabile
7. Acque reflue

[7] Secondo la definizione contenuta nell'articolo 2 dell'allegato alla Raccomandazione 2003/361/CE le imprese sono considerate "piccole" se hanno da 10 a 49 addetti e un fatturato inferiore a 10 milioni di euro; "medie" se hanno da 50 a 249 addetti e un fatturato compreso fa i 10 e i 50 milioni di euro; "grandi" se hanno 250 o più addetti e un fatturato superiore ai 50 milioni di euro.

8. Infrastrutture digitali
9. Gestione dei servizi TIC (business-to-business)
10. Spazio

L'Allegato II raccoglie i cosiddetti «altri settori critici», che comprendono:

1. Servizi postali e di corriere
2. Gestione dei rifiuti
3. Fabbricazione, produzione e distribuzione di sostanze chimiche
4. Produzione, trasformazione e distribuzione di alimenti
5. Fabbricazione
6. Fornitori di servizi digitali
7. Ricerca

L'Allegato III raccoglie la categoria delle «amministrazioni», identificate come:

1. Amministrazioni centrali
2. Amministrazioni regionali
3. Amministrazioni locali
4. Altri soggetti pubblici

E, infine, l'Allegato IV elenca le «ulteriori tipologie di soggetti», consistenti in:

1. Soggetti che forniscono servizi di trasporto pubblico locale
2. Istituti di istruzione che svolgono attività di ricerca
3. Soggetti che svolgono attività di interesse culturale
4. Società in house, società partecipate e società a controllo pubblico

La norma stabilisce che, salvo specifiche eccezioni debitamente elencate, sono considerati «soggetti essenziali»:

- i soggetti di cui all'allegato I che superano i massimali per le medie imprese;
- indipendentemente dalle loro dimensioni, i soggetti identificati come soggetti critici ai sensi del decreto legislativo, che recepisce la Direttiva (UE) 2022/2557 (CER);
- i fornitori di reti pubbliche di comunicazione elettronica e i fornitori di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese;
- indipendentemente dalle loro dimensioni, i prestatori di servizi fiduciari qualificati e i gestori di registri dei nomi di dominio di primo livello, nonché i prestatori di servizi di sistema dei nomi di dominio;
- indipendentemente dalle loro dimensioni, le pubbliche amministrazioni centrali;

- tutti quei soggetti che l'Autorità NIS decida per fondati motivi di considerare essenziali.

Sono, invece, considerati «soggetti importanti» tutti quelli non essenziali che:

- sono negli allegati I o II e superano i massimali per le piccole imprese;
- sono negli allegati III o IV indipendentemente dalle loro dimensioni.

Le eccezioni a questo criterio generale sono molteplici e tendono di fatto a includere nel novero dei soggetti NIS anche quelle entità che per dimensioni o tipologia di attività non vi rientrerebbero, ma svolgono comunque attività critiche per il proprio settore o per il Paese.

Ad esempio sono inclusi, indipendentemente dalle dimensioni, gli operatori di cui agli allegati I, II, III o IV che, a seguito di valutazione da parte dell'Autorità nazionale NIS:

- sono «operatori dei servizi essenziali» già identificati ai sensi della precedente Direttiva NIS;
- sono l'unico fornitore nazionale di un servizio che è essenziale per il mantenimento di attività sociali o economiche fondamentali;
- forniscono servizi la cui perturbazione potrebbe avere un impatto significativo sulla sicurezza pubblica, l'incolumità pubblica o la salute pubblica;
- forniscono servizi la cui perturbazione potrebbe comportare un rischio sistemico significativo, in particolare per i settori nei quali tale perturbazione potrebbe avere un impatto transfrontaliero;
- sono critici in ragione della loro particolare importanza a livello nazionale o regionale per quel particolare settore o tipo di servizio o per altri settori indipendenti nel territorio dello Stato;
- sono considerati critici quali elementi sistemici della catena di approvvigionamento, anche digitale, di uno o più soggetti considerati essenziali o importanti.

Sono infine incluse, indipendentemente dalle loro dimensioni, tutte quelle imprese collegate ad un soggetto essenziale o importante, che soddisfano almeno uno dei seguenti criteri:

- adottano decisioni o esercitano una influenza dominante sulle decisioni relative alle misure di gestione del rischio per la sicurezza informatica di un soggetto importante o essenziale;
- detengono o gestiscono sistemi informativi e di rete da cui dipende la fornitura dei servizi del soggetto importante o essenziale;
- effettuano operazioni di sicurezza informatica del soggetto importante o es-

senziale;
- forniscono servizi ICT o di sicurezza, anche gestiti, al soggetto importante o essenziale.

In queste ultime eccezioni si legge chiaramente la spasmodica attenzione che la norma pone sulla protezione della *supply chain*, ossia l'intera filiera di servizi che lega gli operatori l'uno all'altro e all'utente finale. Tale attenzione nasce dalla considerazione secondo la quale ogni operatore essenziale, per quanto grande, può essere messo in crisi dalla mancata fornitura di un servizio critico da parte di un suo fornitore anche piccolissimo; e siccome ogni disservizio o perturbazione può riverberarsi sull'intera catena di fornitura a valle, e produrre ulteriori perturbazioni a cascata per effetto domino, il Legislatore correttamente assegna elevati livelli di criticità a tutti quegli anelli della catena di fornitura che erogano servizi critici ad un operatore essenziale o importante.

Da quanto precede appare evidente che il numero di operatori soggetti alla NIS2 nel nostro Paese sarà assai elevato, dell'ordine delle migliaia o decine di migliaia: la norma infatti riguarda tutte le aziende medie e grandi dei settori elencati, che sono moltissimi e spesso dalla portata molto ampia. Di fatto con questo nuovo regime normativo gli obblighi di sicurezza e resilienza incombono non più su un limitato numero di soggetti grandissimi e in qualche modo "speciali", ma su un novero estremamente ampio di soggetti anche sostanzialmente "comuni"[8].

Per quanto riguarda gli aspetti attuativi, la norma di recepimento italiana agisce in continuità col passato assegnando il ruolo di Autorità nazionale NIS all'ACN e quelli di Autorità di settore ai Ministeri aventi competenza sugli specifici settori NIS, sempre con l'aggiunta di Banca d'Italia e Consob a supporto del Ministero dell'Economia e delle Finanze per quanto riguarda il settore bancario e dei mercati finanziari. Tuttavia, per i settori ICT, PA e partecipate, Spazio, che sono di nuova introduzione, il ruolo di Autorità di settore viene assunto direttamente dalla Presidenza del Consiglio, il che costituisce una novità importante.

Gli obblighi a cui i soggetti interessati devono ottemperare, pur analoghi concettualmente a quelli previsti dalla precedente Direttiva NIS, sono ora declinati in modo più preciso e soprattutto assai più attento alla sicurezza di filiera. La norma prescrive, infatti, che i soggetti interessati debbano adottare misure di sicurezza le quali «*assicurino un livello di sicurezza dei sistemi informativi e di rete adeguato ai rischi esistenti, tenuto conto delle conoscenze più aggiornate e dello stato dell'arte in materia […] nonché dei costi di attuazione*» e «*siano proporzionate al grado di espo-*

[8] Si consideri, a tal proposito, che nei settori interessati dall'Allegato II ricadono attività produttive del tutto ordinarie quali, a mero titolo di esempio, la fabbricazione di apparecchiature elettriche o di rimorchi e semirimorchi.

sizione a rischi del soggetto, alle dimensioni del soggetto e alla probabilità che si verifichino incidenti, nonché alla loro gravità, compreso il loro impatto sociale ed economico»; specificando, inoltre, che per valutare l'adeguatezza i soggetti debbano tenere conto «*delle vulnerabilità specifiche per ogni diretto fornitore e fornitore di servizi e della qualità complessiva dei prodotti e delle pratiche di sicurezza informatica dei propri fornitori e fornitori di servizi, comprese le loro procedure di sviluppo sicuro*». Dunque, ciascun soggetto ha l'obbligo di identificare e di valutare, nella propria analisi dei rischi, anche le vulnerabilità dei propri fornitori: un onere non indifferente, e soprattutto di non facile attuazione pratica.

Contrariamente alla precedente NIS che, in piena attuazione del già citato principio di responsabilizzazione, non forniva agli operatori interessati alcuna indicazione sugli aspetti di sicurezza da indirizzare, ma lasciava loro la massima libertà nello sceglierle, la NIS 2 fornisce invece un elenco ad alto livello e ben strutturato di tematiche che devono essere necessariamente coperte dalle misure di sicurezza adottate o da adottare. Esse comprendono in particolare:

- politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
- gestione degli incidenti, incluse le procedure e gli strumenti per eseguire le notifiche;
- continuità operativa, backup e ripristino in caso di disastro, gestione delle crisi;
- sicurezza della catena di approvvigionamento;
- sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi;
- politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi cyber;
- pratiche di igiene di base e di formazione in materia di sicurezza informatica;
- politiche e procedure relative all'uso della crittografia;
- sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli asset;
- uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.

Ma l'aspetto forse più dirompente della NIS 2, vero punto di svolta nello stabilire l'approccio più corretto e moderno che ogni soggetto deve adottare nell'indirizzare le tematiche di sicurezza, è laddove viene esplicitamente (e finalmente!) sancito un principio che la comunità mondiale degli esperti di settore sosteneva inascoltata da anni: ossia che la cybersecurity sia un tema strategico e non meramente tecnico, e dunque debba essere una precisa responsabilità dell'Alta Direzione.

La legge di recepimento[9], all'Art. 23, stabilisce infatti che: *«gli organi di amministrazione e gli organi direttivi dei soggetti interessati approvano le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica adottate, sovrintendono all'implementazione degli obblighi, […], sono responsabili delle violazioni»*. Inoltre: *«sono tenuti a seguire una formazione in materia di sicurezza informatica, e promuovono l'offerta periodica di una formazione coerente a quella propria ai loro dipendenti, per favorire l'acquisizione di conoscenze e competenze sufficienti al fine di individuare i rischi e valutare le pratiche di gestione dei rischi per la sicurezza informatica e il loro impatto sulle attività del soggetto e sui servizi offerti»*. Infine: *«sono informati su base periodica o, se opportuno, tempestivamente, degli incidenti e delle notifiche»*. Si tratta di un mandato preciso ed estremamente forte, corroborato per di più dall'elevata entità delle sanzioni comminabili per eventuale inadempienza: le violazioni a questo articolo, infatti, ricadono tra quelle più gravi previste dalla norma, che possono arrivare a importi decisamente rilevanti.

Per quanto riguarda gli altri obblighi a carico dei soggetti interessati, la NIS 2 riprende l'impianto della NIS nell'imporre loro quel regime di auto-vigilanza richiamato in precedenza. Il quale, se da un lato comporta implicitamente l'adozione di modelli e processi organizzativi atti a mantenere un regime di miglioramento continuo dell'efficacia delle misure di protezione, dall'altro impone esplicitamente di accorgersi in modo tempestivo di eventuali incidenti significativi e di saperli non solo gestire, ma anche innanzitutto notificare all'Autorità NIS tramite la struttura operativa del CSIRT.

In particolare, sul tema della notifica degli incidenti occorre fare alcune specifiche valutazioni. Innanzitutto, i suoi tempi sono decisamente stringenti: entro 24 ore, infatti, va inoltrata una pre-notifica che, ove possibile, indichi se l'incidente possa ritenersi il risultato di atti illegittimi o malevoli o possa avere un impatto transfrontaliero; entro 72 ore, poi, va inoltrata la notifica vera e propria che, sempre ove possibile, aggiorni le informazioni della pre-notifica e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché gli eventuali indicatori di compromissione se disponibili. I tempi vanno naturalmente contati dal momento in cui il soggetto ha evidenza dell'incidente, non dal momento in cui l'incidente si è realmente verificato, perché questo potrebbe non essere noto, almeno in un primo momento.

Entro 30 giorni dalla data dell'incidente va, inoltre, presentata una relazione finale che dia conto compiutamente dell'accaduto, includendo almeno: una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto; il tipo di

[9] D.Lgs. 4 settembre 2024 n. 138, Recepimento della Direttiva (UE) 2022/2555, 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 2016/1148.

minaccia o la causa originale che ha probabilmente innescato l'incidente; le misure di attenuazione adottate e in corso; e infine, l'eventuale impatto transfrontaliero dell'incidente, se noto. Nel caso in cui allo scadere dei 30 giorni l'incidente fosse ancora in corso, va invece presentata una relazione provvisoria che dia conto dei progressi svolti nella sua gestione; tale relazione deve essere presentata, aggiornata, ogni 30 giorni sino alla conclusione dell'incidente; dopo di che, entro ulteriori 30 giorni, andrà finalmente presentata la relazione definitiva.

Ma l'aspetto forse più importante, e anche di maggiore impatto, di questo già oneroso regime di notifica è che i soggetti operanti devono segnalare non solo gli incidenti che hanno effettivamente prodotto significativi effetti indesiderati sui servizi erogati, ma anche quelli che, pur non avendo avuto conseguenze, avrebbero potuto averne. Sono questi gli incidenti potenziali, i cosiddetti *near miss* o "quasi-incidenti"; e sono altrettanto importanti da analizzare quanto gli incidenti veri e propri perché rappresentano comunque una situazione in cui qualcosa non ha funzionato, anche se la bravura o la semplice fortuna hanno fatto sì che non producessero effettive conseguenze. In altri settori nei quali la sicurezza è cruciale, ad esempio in ambito aeronautico, la prassi di segnalare e analizzare i *near-miss* è consolidata da sempre, perché è un ottimo modo per imparare dagli errori e migliorare sistemi e procedure senza aver dovuto contare le vittime; nel settore della cybersecurity è un concetto nuovo, ma è assai importante averlo introdotto e messo a regime per migliorare la tenuta complessiva del sistema.

Particolare attenzione va posta al fatto che l'ACN, se lo ritiene, può informare il pubblico riguardo un incidente significativo di cui riceva segnalazione. Può farlo ad esempio per evitare ulteriori incidenti significativi o per gestire un incidente significativo in corso, o qualora ritenga che la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico. Tale facoltà è analoga a quella che può esercitare il Garante per la protezione dei dati personali ai sensi del GDPR nel caso di significativi *data breach*.

Naturalmente, occorre definire cosa sia un incidente "significativo"[10]. La norma dice a tal proposito che un incidente è considerato tale se *«ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato»*, oppure se *«ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli»*. La logica è quindi sempre quella di considerare non solo

[10] A tal proposito il Regolamento di esecuzione (UE) 2024/2690 della Commissione del 17 ottobre 2024 al suo art. 3 fornisce una definizione in termini assoluti, la quale tuttavia riguarda solo i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari.

gli impatti che interessano direttamente il soggetto operante, ma anche quelli che possono riverberarsi su altri soggetti esterni.

È evidente come questo insieme di prescrizioni relativo alla notifica degli incidenti possa risultare oneroso e di non facile attuazione per gli operatori chiamati ad adottarlo, soprattutto per quei soggetti più piccoli e che non abbiano esperienza o cultura specifiche. L'unico modo per adempiere efficacemente al mandato della norma è dotarsi di una corretta e rigorosa procedura per la gestione degli incidenti e seguirla con disciplina, magari facendosi supportare nell'operatività da una piattaforma in grado di automatizzare almeno in parte il relativo workflow.

L'ultimo aspetto di interesse in cui la norma attuale differisce significativamente rispetto alla versione precedente risiede, infine, nel regime sanzionatorio. Se, infatti, l'Italia nel recepire la NIS originale aveva scelto di adottare il vecchio modello basato su sanzioni dall'importo assegnato in valore assoluto, nel recepire la NIS 2 ha invece optato per un più efficace modello mutuato sull'impianto del GDPR, che prevede sanzioni dall'importo parametrato al fatturato del soggetto autore della violazione. Fanno eccezione a questo schema le sole Pubbliche Amministrazioni, per le quali invece la sanzione è espressa in valore assoluto e con importi, peraltro, sensibilmente ridotti rispetto al caso degli operatori privati.

Più in dettaglio, la citata norma licenziata dall'Italia prevede due sole tipologie di violazione, ossia più e meno grave; ciascuna è a sua volta suddivisa in due livelli, a seconda che il contravventore sia un soggetto essenziale o importante. Per le violazioni più gravi la sanzione per i soggetti essenziali può arrivare fino a un massimo di dieci milioni di euro o del 2% del totale del fatturato annuo su scala mondiale per l'esercizio precedente del soggetto, se tale importo è superiore; per i soggetti importanti questi limiti sono di sette milioni di euro o dell'1,4% del fatturato. Per le violazioni meno gravi, invece, la sanzione per i soggetti essenziali può arrivare ad un massimo dello 0,1% del totale del fatturato annuo su scala mondiale per l'esercizio precedente, mentre per i soggetti importanti tale limite è dello 0,07% del fatturato. Si tratta, come si vede, di sanzioni decisamente rilevanti, che dovrebbero quindi raggiungere l'obiettivo di svolgere un'efficace azione deterrente nei confronti di potenziali tentativi di violazione. Da notare, inoltre, che tra le sanzioni più gravi sono esplicitamente rubricate le inosservanze agli obblighi e alle responsabilità gravanti sugli organi di amministrazione e direttivi del soggetto.

5. Conclusioni

Con l'emanazione della Direttiva NIS 2 l'Europa raggiunge finalmente un ambizioso obiettivo perseguito da oltre dieci anni: questa norma, infatti, non è un

provvedimento tardivo e raffazzonato, come purtroppo alcuni osservatori superficiali hanno sostenuto, ma un deciso passo in avanti lungo un percorso sistematico e coordinato, avente l'obiettivo di innalzare non solo la protezione cibernetica, ma soprattutto la resilienza del diffuso ecosistema produttivo e di servizio che sostiene l'economia dell'Unione stessa.

Il coinvolgimento di moltissimi soggetti pubblici e privati di dimensioni non solo grandi, ma addirittura medie, e soprattutto appartenenti anche a settori di per sé non particolarmente critici, serve infatti a mettere sotto protezione non tanto - e non solo - i singoli operatori, quanto tutte le possibili filiere produttive che, tramite complessi ed imperscrutabili incroci, forniscono quei servizi realmente essenziali per il buon funzionamento dell'intera comunità globale. In questo modo si interviene in profondità proprio su quella che oggi è la vera vulnerabilità sistemica della nostra società basata sull'intermediazione tecnologica, ossia la debolezza della *supply chain*. Le filiere di approvvigionamento, e in particolare gli anelli costituiti dai piccoli operatori, sono infatti oggetto di attacchi sempre più numerosi, mirati e sofisticati, da parte di chi ha interesse a ottenere illeciti profitti o perfino a destabilizzare il sistema: metterle in sicurezza tutte assieme è l'unico modo efficace per assicurare stabilità e fiducia a tutta l'Unione.

Naturalmente, ora che il Legislatore e i Governi hanno fatto la propria parte, la palla sta adesso a chi ha l'onere e la responsabilità di attuare quanto prescritto. Gli operatori, dunque, soprattutto i soggetti più piccoli e quelli che non sono mai stati sfiorati da tematiche di cybersecurity globale, devono comprendere l'importanza del loro ruolo nel grande disegno e capire che solo dalla sicurezza di ciascuno si può ottenere e mantenere la sicurezza di tutto l'ecosistema di cui fanno parte. Devono, quindi, fare un significativo salto di qualità: realizzare che la cybersecurity non è solo un obiettivo globale, ma anche e soprattutto una responsabilità condivisa; sviluppare strumenti concettuali idonei alle nuove sfide; dotarsi di modelli di governo della sicurezza adeguati ed efficaci; adottare con diligenza un approccio difensivo basato su un'attenta e accurata analisi dei rischi; ragionare non solo in ottica di prevenzione ma specialmente di resilienza; attuare processi di monitoraggio e miglioramento continui, senza mai abbassare la guardia. Certo non è facile: non solo serve tanta maturità, ma ci vogliono anche risorse adeguate, e queste si possono ottenere solo se vi sarà un forte e serio *committment* da parte delle Alte direzioni dei soggetti interessati. La sfida è globale, e la risposta deve esserlo altrettanto.

È, infine, chiaro che le cose non si fermano qui, anzi sono solo all'inizio. Mettere a regime una macchina così ciclopica richiederà probabilmente diversi aggiustamenti in corso d'opera, e questa sarà responsabilità delle Autorità NIS nazionali, tramite le varie strutture trasversali di coordinamento appositamente istituite. Un altro importante problema operativo consisterà nel trovare la giusta armonizzazione tra le molteplici norme che oramai insistono sullo stesso tema (DORA, GDPR, CER,

NIS 2, solo per citare quelle sovranazionali) e che spesso si rivolgono contemporaneamente ad un medesimo soggetto, costringendolo a fare più volte le stesse cose in modi solo leggermente diversi: e questo sarà compito del Legislatore.

Infine, dobbiamo tenere presente che la minaccia evolve continuamente, e quindi ogni progresso fatto nella difesa verrà prima o poi contrastato da un nuovo salto di qualità da parte degli attaccanti. Forse in futuro ci sarà bisogno di una NIS 3: per ora, tuttavia, non se ne vede la necessità, dato che la NIS 2 sembra offrire sufficienti garanzie di tenuta per un ragionevole lasso di tempo futuro. Farla davvero funzionare, tuttavia, è non solo un obbligo normativamente imposto ai soggetti interessati, ma soprattutto una responsabilità sociale e morale di ciascuno di noi.

N. 1 - 2025 - pp. 98-108

La Cibersicurezza per la fornitura di servizi fiduciari in Italia

Luigi Foglia

Abstract: Il D.Lgs. 138/2008 recepisce anche in Italia quanto previsto dalla Direttiva UE, comunemente conosciuta come NIS 2. La Direttiva, con l'obiettivo di rafforzare la sicurezza informatica e la resilienza delle infrastrutture critiche e dei fornitori di servizi digitali all'interno dell'Unione Europea, individua tra i soggetti "essenziali" i fornitori di servizi fiduciari qualificati e tra i soggetti "importanti" i fornitori di servizi fiduciari non qualificati ai sensi nel Regolamento 910/2014 - eIDAS. Occorre, anche alla luce della citata norma di recepimento italiana, analizzare i reali impatti della Direttiva NIS 2 sui fornitori di servizi fiduciari e gli obblighi, in tema di misure di gestione del rischio e segnalazione degli incidenti, di recente specificati con il Regolamento di esecuzione della Commissione UE 2024/2690.

Legislative Decree 138/2008 implements, also in Italy, the provisions of the EU Directive, commonly known as NIS 2. The Directive, with the aim of strengthening IT security and the resilience of critical infrastructures and digital service providers within of the European Union, identifies qualified trust service providers, pursuant to Regulation 910/2014 - eIDAS, among the "essential" subjects and non-qualified trust service providers among the "important" subjects. It is necessary, also considering the Italian transposition of the NIS 2 EU Directive, to analyze the real impacts of this EU Directive for the Italian trust service providers and the obligations, in terms of risk management measures and incident reporting, recently specified with the Implementing Regulation of the EU Commission n° 2024/2690.

Parole chiave: cibersicurezza, NIS 2, prestatori di servizi fiduciari, obblighi

1. La strategia UE per la cibersicurezza

La Cibersicurezza ha assunto negli ultimi anni un ruolo sempre più strategico all'interno delle strategie dell'Unione Europea mirate a garantire la sicurezza dell'Unione. Tale ruolo strategico è confermato anche dalla vigente strategia dell'Unione Europea per la sicurezza 2020-2025 (EU Security Union Strategy), che prevede l'ulteriore implementazione di quando già previsto con il Regolamento (UE) n. 2019/881, relativo all'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (regolamento sulla cibersicurezza).

All'interno di tale quadro, assume una rilevanza fondamentale, anche per i suoi impatti sulle imprese dell'UE, l'aggiornamento della Direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS). Introdotta nella sua prima versione nel 2016 quale prima misura legislativa in assoluto per tutta l'UE volta ad accrescere la cooperazione tra gli Stati membri sulla questione vitale della cibersicurezza, la Direttiva (UE) 2016/1148 (NIS) ha definito obblighi di sicurezza per gli operatori di servizi essenziali (in settori critici come l'energia, i trasporti, la sanità e la finanza) e i fornitori di servizi digitali (mercati online, motori di ricerca e servizi cloud).

Nel 2022, sotto la spinta degli incessanti attacchi informatici che colpivano in maniera sempre più efficace istituzioni e imprese dell'Unione, l'UE ha approvato la nuova Direttiva (UE) 2022/2555 (NIS 2) che con la sua entrata in vigore nel gennaio 2023 ha abrogato la precedente Direttiva (UE) 2016/1148 (cd. NIS 1) e ha posto le basi per realizzare un nuovo e più elevato livello comune di cybersecurity nell'Unione Europea.

I principali obiettivi che con la Direttiva NIS 2 l'Unione ha inteso perseguire possono essere così sintetizzati:

- rafforzare la gestione dei rischi per la cibersicurezza: viene chiesto alle organizzazioni rilevanti di implementare misure di gestione del rischio complete per identificare, valutare e gestire i propri rischi per la cibersicurezza;
- potenziare la segnalazione degli incidenti: le organizzazioni dovranno notificare tempestivamente alle autorità competenti gli incidenti informatici significativi;
- implementare misure di sicurezza su tutta la catena dei fornitori: le organizzazioni dovranno implementare misure per proteggere le proprie catene di fornitura dalle minacce informatiche.

2. NIS 2 e i prestatori di servizi fiduciari eIDAS

Secondo quanto previsto dall'art. 3 della Direttiva NIS 2, i requisiti per la gestione dei rischi di cibersicurezza sono applicabili anche ai Prestatori di Servizi fiduciari qualificati ai sensi del Regolamento eIDAS, considerati come "soggetti essenziali" ai fini della Direttiva. Inoltre, poiché tutti i servizi fiduciari eIDAS sono identificati come elemento fondamentale dell'infrastruttura digitale europea, anche i fornitori di servizi fiduciari non qualificati sono considerati comunque "soggetti importanti" ai fini dell'applicazione della NIS 2.

Trattandosi di una Direttiva UE, la NIS 2 è stata recepita (entro lo scorso 17 ottobre 2024) in ogni singolo Stato membro per divenire pienamente efficace nei confronti di istituzioni pubbliche e imprese stabilite nei rispettivi territori.

Con il D.Lgs. 138 del 4 settembre 2024 l'Italia ha recepito la Direttiva NIS 2, le cui prescrizioni sono quindi vigenti nel nostro Stato dal 1° ottobre 2024. Il Decreto di recepimento citato ha sostanzialmente ribadito quanto previsto dalla NIS 2 e, in tema di fornitori di servizi fiduciari, ha ribadito il ruolo di soggetti essenziali dei fornitori di servizi qualificati ai fini dell'applicazione della NIS 2. Allo stesso modo, è stato ribadito il ruolo di soggetti importanti dei fornitori di servizi fiduciari non qualificati a prescindere dalle dimensioni in termini di capitale e/o numero di dipendenti.

Si tratta, quindi, di un elevato numero di imprese (ma anche di pubbliche amministrazioni) fornitori di servizi fiduciari che dal 1° dicembre 2024 al 28 febbraio 2025 dovranno manifestarsi all'Agenzia per la Cybersicurezza Nazionale – ACN, registrandosi sull'apposita piattaforma digitale secondo modalità e termini definiti con Determinazione del Direttore Generale di ACN 38565/2024[1].

Terminata la fase di registrazione, l'ACN unitamente alle Autorità di settore[2] vaglieranno le dichiarazioni per costituire l'elenco dei soggetti NIS entro fine marzo 2025. Nel mese di aprile 2025, l'ACN elaborerà e adotterà anche una serie di obblighi di base che dovranno essere rispettati dai differenti soggetti essenziali e importanti. Entro aprile 2026, invece, saranno elaborati e adottati ulteriori obblighi di lungo termine.

Dal 1° maggio al 30 giugno di ogni anno, i soggetti essenziali e i soggetti importanti dovranno comunicare o aggiornare, tramite la piattaforma digitale di ACN,

[1] https://www.acn.gov.it/portale/documents/d/guest/detacn_nis_piattaforma_2024_38565_signed

[2] Al fine di assicurare l'efficace attuazione del Decreto Legislativo 138/2024 (recepimento della Direttiva NIS 2) a livello settoriale, sono individuate le Autorità di settore NIS che supportano l'Autorità nazionale competente NIS e collaborano con essa.

un elenco delle proprie attività e dei propri servizi, comprensivo di tutti gli elementi necessari alla loro caratterizzazione e della relativa attribuzione di una categoria di rilevanza.

Diventa, quindi, fondamentale riconoscersi e manifestarsi per tempo come soggetti NIS 2, così da pianificare gli investimenti necessari al fine di rispettare le scadenze previste e predisporsi all'implementazione delle misure sicurezza che via via saranno elaborate da ACN.

Se per i fornitori qualificati esistono elenchi specifici tenuti da AgID, lo stesso non può dirsi per i fornitori non qualificati, molti dei quali, fino ad oggi, non sapevano neanche di rientrare in tale definizione. Basti pensare a numerosi servizi di firma elettronica erogati da differenti fornitori o ai servizi di conservazione a norma dei documenti informatici che, dall'entrata in vigore del nuovo Regolamento eIDAS (c.d. eIDAS 2) avvenuta lo scorso maggio, rientrano tra il novero dei fornitori di servizi fiduciari non qualificati di e-archiving.

Per comprendere quali soggetti rientrino tra i fornitori di servizi fiduciari non qualificati e, quindi, tra i soggetti importanti ai fini dell'applicabilità della NIS 2, occorre richiamare la definizione data dall'art. 3 del Regolamento eIDAS, secondo la quale è un servizio fiduciario *un servizio elettronico prestato normalmente dietro remunerazione e consistente in uno qualsiasi degli elementi seguenti:*

a. *il rilascio di certificati di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari;*
b. *la convalida di certificati di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari;*
c. *la creazione di firme elettroniche o sigilli elettronici;*
d. *la convalida di firme elettroniche o sigilli elettronici;*
e. *la conservazione di firme elettroniche, sigilli elettronici, certificati di firme elettroniche o certificati di sigilli elettronici;*
f. *la gestione di dispositivi per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza;*
g. *il rilascio di attestati elettronici di attributi;*
h. *la convalida di attestati elettronici di attributi;*
i. *la creazione di validazioni temporali elettroniche;*
j. *la convalida di validazioni temporali elettroniche;*
k. *la prestazione di servizi elettronici di recapito certificato;*
l. *la convalida dei dati trasmessi tramite servizi elettronici di recapito certificato e relative prove;*
m. *l'archiviazione elettronica di dati elettronici e di documenti elettronici;*

n. la registrazione di dati elettronici in un registro elettronico;

3. Requisiti di sicurezza stabiliti da eIDAS per i prestatori di servizi fiduciari

Restando in tema di servizi fiduciari, lo stesso Regolamento eIDAS - nella versione definita con il Regolamento UE 2024/1183 - ha previsto specifici requisiti, in termini di sicurezza, che tutti i prestatori di servizi fiduciari devono soddisfare.

In particolare, il nuovo art. 19 bis del Regolamento eIDAS, sostituendo di fatto il precedente articolo 19 che già si occupava di sicurezza dei sistemi per la fornitura dei servizi fiduciari, ha individuato nuovi requisiti in termini di sicurezza.

Secondo quanto previsto dal nuovo art. 19 bis anche un prestatore di servizi fiduciari non qualificato che presta servizi fiduciari non qualificati:

a) *dispone di politiche adeguate e adotta misure corrispondenti per la gestione dei rischi giuridici, commerciali, operativi e di altro tipo, sia diretti che indiretti, per la prestazione del servizio fiduciario non qualificato, le quali, fatto salvo l'articolo 21 della direttiva (UE) 2022/2555, comprendono almeno misure relative:*
    i. *alla registrazione a un servizio fiduciario e alle relative procedure di onboarding;*
    ii. *ai controlli procedurali o amministrativi necessari per prestare servizi fiduciari;*
    iii. *alla gestione e all'attuazione dei servizi fiduciari;*
b) *alla notifica, senza indebito ritardo ma in ogni caso entro 24 ore dall'essere venuto a conoscenza di violazioni della sicurezza o perturbazioni, all'organismo di vigilanza, alle persone interessate identificabili, al pubblico se è di pubblico interesse e, ove applicabile, ad altre autorità competenti interessate, di tutte le eventuali violazioni della sicurezza o perturbazioni connesse alla prestazione del servizio o all'attuazione delle misure di cui alla lettera a), punti i), ii) o iii), aventi un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.*

Viene poi stabilito che entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, debba stabilire un elenco di norme di riferimento e, se necessario, specifiche e procedure applicabili in materia di sicurezza.

L'art. 19 bis, quindi, individua (o comunque pone le basi per individuare) ulteriori misure di sicurezza specifiche per i fornitori di servizi fiduciari rispetto a quanto già previsto dall'art. 21 della Direttiva NIS 2. Tale art. 21, infatti, individua già numerose e diversificate misure di sicurezza, prevedendo che tali misure siano basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti, e comprendono almeno gli elementi seguenti:

a. *politiche di analisi dei rischi e di sicurezza dei sistemi informatici;*
b. *gestione degli incidenti;*
c. *continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;*
d. *sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;*
e. *sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;*
f. *strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza;*
g. *pratiche di igiene informatica di base e formazione in materia di cibersicurezza;*
h. *politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;*
i. *sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;*
j. *uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.*

Se le misure di cui all'art. 19 bis del Regolamento eIDAS e quelle sopra richiamate di cui all'art. 21 del Regolamento NIS 2 sono applicabili a tutti i fornitori di servizi fiduciari, le recenti modifiche al Regolamento eIDAS introdotte con il Regolamento UE del 11/04/2024 n. 1183 stabiliscono ulteriori misure specifiche per i fornitori di servizi fiduciari che abbiano ottenuto la relativa qualifica. Il nuovo art. 20 del Regolamento eIDAS prescrive, quindi, che *I prestatori di servizi fiduciari qualificati sono sottoposti, a proprie spese e almeno ogni 24 mesi, a una verifica da parte di un organismo di valutazione della conformità. Lo scopo della verifica è confermare che i prestatori di servizi fiduciari qualificati e i servizi fiduciari qualificati da essi prestati rispettano i requisiti di cui al presente regolamento e all' articolo 21 della direttiva (UE) 2022/2555 (NIS2). I prestatori di servizi fiduciari qualificati presentano la risultante relazione di valutazione della conformità all'organismo di vigilanza entro tre giorni lavorativi dalla sua ricezione.*

Inoltre, il par. 3 bis dell'art. 20 del Regolamento eIDAS prevede che qualora

l'ACN (autorità designata come competente per la NIS in Italia) rilevi che un fornitore di servizi fiduciari qualificati non soddisfi uno qualsiasi dei requisiti di cui all'articolo 21 della Direttiva NIS 2, debba informare immediatamente AgID (in qualità di Organismo di vigilanza eIDAS) il quale potrà, se ciò è giustificato in particolare dalla portata, dalla durata e dalle conseguenze di tale inadempienza, revocare la qualifica di tale prestatore o del servizio interessato da esso prestato.

Infine, sempre in tema di requisiti di sicurezza per i fornitori di servizi fiduciari, è doveroso sottolineare come anche l'Ente di Standardizzazione europeo (ETSI - European Telecommunications Standards Institute) ha iniziato ad aggiornare alcuni standard di sicurezza integrandoli con le nuove previsioni contenute nella NIS2. In particolare, lo scorso giugno, ETSI ha aggiornato il proprio standard ETSI EN 319 401 (General Policy Requirements for Trust Service Providers) alla versione V3.1.1 (06-2024): sono stati rivisti e specificati i requisiti previsti dalle precedenti versioni dello standard, adeguandoli e integrandoli con i requisiti di sicurezza previsti da NIS 2, indipendentemente dal servizio fornito. Probabilmente, nei prossimi mesi, verranno aggiornati anche gli altri standard riguardanti i singoli servizi fiduciari, così da identificare i requisiti aggiuntivi per particolari tipologie di servizi fiduciari.

4. Il Regolamento di esecuzione (UE) 2024/2690: requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza

Con il proprio Regolamento di esecuzione 2024/2690 del 17 ottobre 2024 la Commissione UE ha indicato le modalità di applicazione della Direttiva (UE) 2022/2555 (NIS 2) per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza e ha ulteriormente specificato i casi in cui un incidente deve essere considerato significativo.

In merito ai requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza di cui all'art 21 della Direttiva NIS 2, la Commissione ha elaborato uno specifico elenco di requisiti contenuto nell'Allegato A al Regolamento di esecuzione[3], basandosi su norme europee e internazionali, quali ISO/IEC 27001, ISO/IEC 27002 ed ETSI EN 319401, e su specifiche tecniche, quali CEN/TS 18026:2024, pertinenti per la sicurezza dei sistemi informativi e di rete.

Inoltre, soprattutto attraverso i considerando del citato Regolamento di ese-

[3] https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=OJ:L_202402690#anx_1

cuzione, sono state fornite alcune interessanti indicazioni in ordine all'attuazione e all'applicazione dei requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza individuati nell'Allegato A al Regolamento. In particolare, nel conformarsi a tali requisiti tecnici e metodologici, il considerando 4 al Regolamento ritiene opportuno che i soggetti essenziali e importanti tengano debitamente conto della loro effettiva esposizione al rischio, della propria criticità, delle loro dimensioni e della loro struttura, nonché della probabilità che si verifichino incidenti, della loro gravità e del loro impatto sociale ed economico.

5. Gli obblighi di segnalazione degli incidenti

In attesa della definizione delle misure di sicurezza da parte di ACN (in qualità di Autorità competente per la NIS 2)[4] e della definizione di ulteriori requisiti e oneri specifici per i prestatori di servizi fiduciari da parte della Commissione UE[5] è possibile concentrarsi su uno degli obblighi che, seppur con nomenclature e forme leggermente divergenti, è presente nella maggior parte delle recenti discipline che si occupano, a vario titolo, di protezione dei dati e di sicurezza informatica: la segnalazione degli incidenti.

Accanto, infatti, agli obblighi di segnalazione dei cosiddetti *data breach* previsto dagli articoli 33 e 34 del Regolamento UE 679/2016 - Gdpr, sia il Regolamento NIS 2 che il Regolamento eIDAS, qui presi in esame, individuano uno specifico obbligo di segnalazione degli incidenti.

In particolare, come abbiamo avuto modo di vedere, il nuovo art. 19 bis del Regolamento eIDAS prevede in capo a tutti i fornitori di servizi fiduciari uno specifico obbligo di notifica all'Organismo di vigilanza (AgID) e, ove applicabile, alle Autorità competenti (ACN/CSIRT Italia e Garante per la protezione dei dati personali), senza indebito ritardo, ma in ogni caso entro 24 ore dall'esserne venuti a conoscenza, di violazioni della sicurezza o perturbazioni, connesse alla prestazione del servizio aventi un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.

Il Regolamento eIDAS ha così ripreso gli obblighi di segnalazione previsti dall'art. 23 del Decreto NIS 2 che, è alla base della formulazione degli obblighi di notifica degli incidenti previsti dal Decreto Legislativo 138/2024 che recepisce la

[4] ACN dovrà elaborare ed adottare misure di sicurezza di base (entro l'aprile 2025) e misure di sicurezza a lungo termine (entro aprile 2026).

[5] La Commissione UE dovrà indicare entro il 21 maggio 2025 un elenco di norme di riferimento e, se necessario, specifiche e procedure applicabili in materia di sicurezza.

Direttiva NIS 2 in Italia. Tale Decreto Legislativo, all'art. 25, prevede che i soggetti essenziali e i soggetti importanti notifichino, senza ingiustificato ritardo, al CSIRT Italia ogni incidente che abbia un impatto significativo sulla fornitura dei loro servizi.

Per i prestatori di servizi fiduciari[6], la notifica dovrà avvenire senza indebito ritardo e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo e dovrà contenere l'indicazione della possibile origine dell'incidente, del suo eventuale impatto transfrontaliero e una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto.

Entro un mese dalla notifica dell'incidente, dovrà poi essere inviata una relazione finale contenente:

1. una descrizione dettagliata dell'incidente, ivi inclusi la sua gravità e il suo impatto;
2. il tipo di minaccia o la causa originale (root cause) che ha probabilmente innescato l'incidente;
3. le misure di attenuazione adottate e in corso;
4. ove noto, l'impatto transfrontaliero dell'incidente.

In caso di incidente in corso al momento della trasmissione della relazione finale, andrà inviata una relazione mensile sui progressi e un'ulteriore relazione finale entro un mese dalla conclusione della gestione dell'incidente.

Gli operatori saranno tenuti al rispetto degli obblighi di notifica trascorsi nove mesi dalla ricezione della comunicazione di inserimento nell'elenco dei soggetti essenziali o importanti che sarà inviata da ACN entro aprile 2025. Le modalità di adempimento degli obblighi di notifica degli incidenti saranno disciplinate con una determinazione di ACN da adottare sempre entro aprile 2025.

Il comma 4 dell'art 25 citato specifica che un incidente dev'essere considerato significativo se:

a. *ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato;*
b. *ha avuto ripercussioni o è idoneo a provocare ripercussioni su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli.*

Sull'esatta definizione degli incidenti significativi è intervenuto anche il già

[6] Per gli altri soggetti essenziali e importanti viene, invece, prevista una pre-notifica (con la sola indicazione della possibile origine dell'incidente e/o del suo possibile impatto transfrontaliero) entro le 24 ore con l'obbligo di notifica vera e propria entro le 72 ore dalla conoscenza dell'incidente.

menzionato Regolamento di esecuzione della Commissione 2024/2690 secondo la quale un incidente è considerato significativo quando:

1) ha causato o è in grado di causare al soggetto pertinente una perdita finanziaria diretta superiore a 500 000 EUR o, se tale importo è inferiore, al 5 % del suo fatturato totale annuo dell'esercizio precedente;
2) ha causato o è in grado di causare l'esfiltrazione di segreti commerciali, quali definiti all'articolo 2, punto 1), della Direttiva (UE) 2016/943, del soggetto pertinente;
3) ha causato o è in grado di causare il decesso di una persona fisica;
4) ha causato o è in grado di causare danni considerevoli alla salute di una persona fisica;
5) si è verificato un accesso non autorizzato ai sistemi informativi e di rete, che si sospetta essere malevolo ed è in grado di causare gravi perturbazioni operative;
6) l'incidente è considerato ricorrente[7];
7) l'incidente soddisfa uno o più criteri specifici per settore: per quanto riguarda i prestatori di servizi fiduciari, un incidente è considerato significativo, se soddisfa uno o più dei criteri seguenti:
   a. *un servizio fiduciario è completamente indisponibile per più di 20 minuti;*
   b. *un servizio fiduciario non è disponibile per gli utenti o per le parti facenti affidamento sulla certificazione per più di un'ora calcolata sulla base di una settimana di calendario;*
   c. *oltre l'1 % degli utenti o delle parti facenti affidamento sulla certificazione nell'Unione o oltre 200 000 utenti o parti facenti affidamento sulla certificazione nell'Unione, a seconda di quale valore sia inferiore, risentono della disponibilità limitata di un servizio fiduciario;*
   d. *l'accesso fisico a un'area in cui sono ubicati i sistemi informativi e di rete e il cui accesso è limitato al personale di fiducia del prestatore di servizi fiduciari o la protezione di tale accesso fisico sono compromessi;*
   e. *l'integrità, la riservatezza o l'autenticità dei dati conservati, trasmessi o elaborati relativi alla fornitura di un servizio fiduciario è compromessa con un impatto su oltre lo 0,1 % degli utenti o delle parti facenti affidamento sulla certificazione o su oltre 100 utenti o parti facenti affidamento sulla certificazione del servizio fiduciario nell'Unione, a seconda di quale valore sia inferiore.*

[7] Gli incidenti che singolarmente non sono considerati un incidente significativo sono considerati collettivamente come un unico incidente significativo se soddisfano tutti i criteri seguenti: a) si sono verificati almeno due volte nell'arco di sei mesi; b) presentano la stessa causa di fondo apparente; c) hanno causato o sono in grado di causare collettivamente al soggetto pertinente una perdita finanziaria diretta superiore a 500 000 EUR o, se tale importo è inferiore, al 5 % del suo fatturato totale annuo dell'esercizio precedente.

Per completezza, infine, si segnala che, ad oggi, per i prestatori di servizi fiduciari qualificati, per i gestori di posta elettronica certificata, per i gestori dell'identità digitale e per i conservatori che conservano documenti per conto delle pubbliche amministrazioni (ai sensi dell'art. 34 comma 1-bis, lett. b del CAD), l'art. 32 bis del D.Lgs. 82/2005 prevede già, al comma 2, un obbligo di segnalazione ad AgID di qualsiasi malfunzionamento nei servizi forniti che determini l'interruzione del servizio.

N. 1 - 2025 - pp. 109-121

NIS2-Ready? L'applicazione della direttiva NIS 2 nelle imprese italiane. Tempistiche e nodi da sciogliere

Eleonora Faina, Carlo Didonè

Abstract: Negli ultimi anni i legislatori europeo e italiano hanno adottato diversi provvedimenti volti al rafforzamento delle capacità di cybersecurity di imprese e pubblica amministrazione. Queste misure si prefiggono l'obiettivo di rispondere all'aumento della minaccia cyber: secondo dati Clusit, l'Italia ha visto un aumento degli attacchi del 65% nel 2023 rispetto all'anno precedente. Tra le misure adottate, la più significativa è la Direttiva NIS 2, trasposta nell'ordinamento italiano il 1° ottobre 2024. La Direttiva mira a garantire la continuità operativa delle catene del valore critiche di fronte a potenziali attacchi cyber. A questo fine, impone in particolare obblighi riguardanti le misure di gestione del rischio e di segnalazione degli incidenti. La trasposizione nell'ordinamento italiano, così come in altri Paesi europei, lascia spazio all'Agenzia per la Cybersicurezza Nazionale di definire standard tecnici riguardanti l'applicazione della NIS 2 nelle aziende dei diversi settori. L'articolo, soffermandosi sulle misure della Direttiva e le specificità della sua applicazione in Italia, approfondirà gli aspetti regolatori definiti finora e quanto invece rimane ancora aperto, oltre che le tempistiche che le imprese si possono attendere per i propri obblighi di compliance.

In recent years, European and Italian lawmakers have adopted several measures aimed at strengthening the cybersecurity capabilities of businesses and public administration. These measures aim to respond to the increase in the cyber threat: according to Clusit data, Italy saw a 65 percent increase in attacks in 2023 over the previous year. Among the measures taken, the most significant is the NIS 2 Directive, which was transposed into Italian law on October 1, 2024. The Directive aims to ensure the business continuity of critical value chains in the face of potential cyber attacks. To this end, it specifically imposes obligations regarding risk management and incident reporting measures. The transposition into Italian law, as well as in other European countries, leaves room for the National Cybersecurity Agency to define technical standards regarding the application of NIS 2 in companies in different sectors. Focusing on the measures of the Directive and the specifics of its implementation in Italy, the article will delve into the regulatory aspects defined so far and how much, on the other hand, remains open, as well as the timelines that companies can expect for their compliance obligations.

Parole chiave: cybersecurity, Direttiva NIS 2, applicazione, imprese

1. Introduzione

Negli ultimi anni, il numero e l'intensità degli attacchi informatici hanno subito un incremento significativo, alimentato da minacce ibride che si inseriscono in un contesto di crescente frammentazione geopolitica. La crescente digitalizzazione di prodotti, servizi e processi – accelerata da nuovi paradigmi tecnologici – ha offerto ai cybercriminali e agli attori statali opportunità di accesso senza precedenti. L'invasione russa in Ucraina ha ulteriormente intensificato la frequenza degli attacchi, innescando campagne di attacchi mirati in tutta Europa.

I dati raccolti dall'Associazione Italiana per la Sicurezza Informatica (CLUSIT) evidenziano la portata di questa escalation: tra il 2018 e il 2022, il numero di attacchi cyber a livello mondiale è aumentato del 60%, con una crescita particolarmente marcata negli attacchi gravi – ovvero quelli che generano danni economici e perdite di dati considerevoli per le vittime. Anche l'Italia ha visto un incremento allarmante: nel primo semestre del 2023, il Paese ha registrato 132 attacchi gravi, un dato che rappresenta un incremento di nove volte rispetto ai 15 attacchi del 2018. Risulta particolarmente colpita la pubblica amministrazione, che subisce il 23% degli attacchi totali, seguita dal settore manufatturiero.

Per contrastare questa minaccia crescente, l'Unione Europea e il Governo italiano hanno adottato un insieme di normative che mirano a rafforzare le capacità di risposta agli attacchi informatici di imprese e amministrazioni pubbliche, garantendo al contempo la continuità operativa dei settori critici delle economie europea e italiana. Tra queste misure, la Direttiva 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (*Network Information Security directive*, NIS 2) rappresenta il provvedimento più ampio, imponendo alle organizzazioni soggette una serie di obblighi che spaziano dalla gestione del rischio cyber alla segnalazione degli incidenti.

In Italia, la trasposizione della Direttiva ha adottato un approccio basato sul rischio e su una certa flessibilità, per evitare costi di compliance eccessivi per gli operatori. In questo contesto, l'Agenzia per la Cybersicurezza Nazionale (ACN) avrà un ruolo centrale, con ampi margini di discrezionalità nell'elaborazione di criteri e

modalità di implementazione della Direttiva.

Questo approccio flessibile ha il vantaggio di potersi adattare rapidamente alle evoluzioni tecnologiche e alle nuove minacce cibernetiche. Tuttavia, sarà fondamentale garantire agli operatori certezze sulle misure di conformità richieste, oltre a fornire loro il necessario supporto nell'adozione delle previsioni normative. Se infatti i comparti produttivi italiani si stavano già muovendo verso un livello elevato di sicurezza informatica, l'intervento legislativo non deve sostituirsi a questo sforzo, imponendo obblighi generalizzati e di ridotta applicabilità per le imprese. La Direttiva NIS2 può invece essere un'opportunità per le Autorità per guidare la transizione verso la sicurezza informatica, indicando standard e tecnologie alle imprese a cui dovessero mancare competenze e capacità di investimento.

2. Panoramica delle Politiche di Cybersecurity in Europa e in Italia

La Direttiva NIS 2 si colloca all'interno di una strategia regolatoria più ampia, sviluppata a livello europeo e nazionale per rispondere al crescente numero di attacchi informatici. Questo quadro è stato progressivamente arricchito da misure volte a garantire la resilienza delle infrastrutture critiche, a partire dal Perimetro di Sicurezza Nazionale Cibernetica (PSNC). Introdotto dal governo italiano nel 2019, il PSNC è stato progettato per proteggere gli enti pubblici e privati che rivestono un ruolo essenziale per la sicurezza nazionale. Gli enti inclusi nel PSNC sono selezionati in base all'impatto che un eventuale attacco informatico potrebbe avere su funzioni e servizi essenziali dello Stato. Oggi il PSNC rappresenta la principale misura di sicurezza informatica per le infrastrutture critiche italiane.

La Direttiva NIS 2 adotta un approccio simile a quello del PSNC, ma estende il perimetro di protezione a una gamma più ampia di settori considerati cruciali per il funzionamento dell'economia europea e nazionale. L'obiettivo della NIS 2 è garantire la continuità operativa di tali settori anche in presenza di gravi attacchi cyber, preservando così la stabilità dei mercati e la sicurezza dei servizi essenziali. Con l'adozione di misure di gestione del rischio e l'obbligo di segnalare gli incidenti, la NIS 2 ambisce a migliorare la resilienza delle organizzazioni nei settori chiave, offrendo una copertura complementare rispetto a quella garantita dal PSNC.

Un ulteriore provvedimento rilevante è la Direttiva sulla Resilienza degli Enti Critici, la quale amplia il raggio di intervento oltre la sicurezza informatica, con l'intento di evitare qualsiasi tipo di interruzione nei settori critici. Tale Direttiva copre non solo i rischi cyber ma anche altre minacce imprevedibili, come incidenti

e disastri naturali, che potrebbero compromettere il normale funzionamento delle infrastrutture fondamentali. Il principio di ispirazione della norma rimane l'autonomia operativa, integrando la cybersicurezza con misure più ampie di prevenzione e risposta a situazioni di crisi.

Nel contesto delle misure specifiche di settore, emerge il Digital Operational Resilience Act (DORA), concepito per il settore bancario e dei pagamenti online. DORA rappresenta il primo intervento normativo a livello europeo che punta a garantire la resilienza operativa del settore finanziario, rispondendo ad una proliferazione di regolazione nazionale in materia che minacciava la coesione nel mercato unico europeo. La Commissione Europea ha inoltre avviato valutazioni su ulteriori provvedimenti settoriali, specialmente per il settore automobilistico, a fronte di una crescente digitalizzazione dei veicoli e delle infrastrutture di mobilità.

A completamento di questa strategia, si inserisce il Cyber Resilience Act (CRA), che definisce standard di conformità per i prodotti con componenti digitali, imponendo requisiti per la sicurezza dei dispositivi stessi. Il CRA mira a stabilire un livello di protezione uniforme per tutti i dispositivi digitali presenti sul mercato europeo, rendendo obbligatori gli assessment di conformità per assicurare la robustezza e la sicurezza dei prodotti. Questo approccio aggiunge un ulteriore livello di sicurezza, integrando la protezione a livello di prodotto con la sicurezza informatica interna alle aziende come prevista dalle altre normative citate.

Queste iniziative rappresentano i pilastri di una strategia regolatoria europea e italiana che non si limita a proteggere le infrastrutture e le imprese da attacchi cyber, ma mira a costruire un sistema resiliente, in grado di resistere alle diverse minacce che possono impattare il funzionamento dei settori essenziali e delle reti digitali.

3. Campo di Applicazione della Direttiva NIS 2

L'ambito di applicazione della Direttiva NIS 2, come recepita in Italia nell'art. 3 del decreto legislativo di attuazione (dlgs 138/2024), è stato definito per includere i comparti ritenuti fondamentali al funzionamento dei mercati e all'economia nazionale, comprendendo settori quali digitale, energia, trasporti, alimentare, ricerca e sanità. Le medie e grandi imprese operanti in questi settori rientrano automaticamente nella categoria dei soggetti NIS 2, conformemente alle definizioni di dimensione di impresa stabilite nella raccomandazione 2003/361/CE della Commissione Europea: una media impresa ha tra i 50 e i 250 dipendenti e un fatturato annuo compreso tra 10 e 50 milioni di euro. Al di sotto e al di sopra di questi limiti si collocano, rispettivamente, le piccole e le grandi imprese. Alcuni settori specifici, particolarmente rilevanti per la sicurezza informatica, includono invece tutte le imprese indipenden-

temente dalle dimensioni. Tra questi, le reti di comunicazione elettronica, i servizi fiduciari, e l'infrastruttura internet (ad esempio registri TLD, sistemi DNS) che presentano un rischio elevato per la sicurezza digitale su scala nazionale e europea. ACN stima che i soggetti NIS 2 così identificati siano circa 50.000.

Nell'ambito della Direttiva, i soggetti NIS sono distinti tra essenziali e importanti a seconda delle dimensioni e del settore. Questa classificazione è rilevante non solo per il livello di protezione richiesto, ma anche per determinare gli obblighi di sicurezza e le sanzioni applicabili. Tale suddivisione permette di concentrare gli interventi regolatori laddove la vulnerabilità della catena di valore risulta più elevata e quindi necessiti di una protezione specifica.

In aggiunta, il legislatore italiano ha previsto una clausola di salvaguardia per garantire una attuazione proporzionata della Direttiva. Questa clausola richiede che l'applicazione della raccomandazione UE sulle dimensioni aziendali consideri "l'indipendenza del soggetto dalle sue imprese collegate" sia per quanto riguarda i sistemi informativi sia per i servizi forniti. In tal modo, le imprese che, pur superando i limiti dimensionali stabiliti, non rappresentano un rischio significativo per la sicurezza nazionale a causa della propria indipendenza da clienti e fornitori, potranno richiedere una deroga in fase di registrazione. I criteri di applicazione di tale clausola dovranno essere specificati da un decreto del Presidente del Consiglio dei ministri, che al momento in cui si scrive (gennaio 2025) non è ancora stato pubblicato.

L'Agenzia per la Cybersicurezza Nazionale (ACN) avrà inoltre il compito di ampliare il campo di applicazione per includere le catene del valore dei soggetti NIS 2, con l'obiettivo di garantire la protezione della filiera in modo più ampio e omogeneo. Questo intervento assicura un approccio completo alla sicurezza informatica, ma resta da chiarire il numero esatto di imprese che verranno incluse nella normativa attraverso questa estensione.

Per le imprese transnazionali, l'art. 5 del decreto legislativo stabilisce le regole sulla giurisdizione. In particolare, le imprese di servizi ICT come i sistemi dei nomi di dominio DNS, i registri di nomi di dominio di primo livello, i servizi di cloud computing, i data center, le reti di distribuzione dei contenuti, i servizi gestiti e i social network sono soggetti alla giurisdizione dello Stato membro in cui si trova lo stabilimento principale. Quest'ultimo è identificato in base alla sede in cui vengono prese le decisioni principali in materia di sicurezza informatica.

La configurazione giuridica così composta consente una certa flessibilità e capacità di adattamento della Direttiva rispetto all'evoluzione delle minacce cibernetiche e delle tecnologie. Tuttavia, il successo della NIS2 richiederà significative capacità di coordinamento tra l'ACN, i ministeri, la Presidenza del Consiglio dei ministri e gli altri enti coinvolti, al fine di garantire certezza giuridica e coerenza applicativa.

Un punto di discrezionalità particolarmente significativo riguarda i criteri di inclusione dei fornitori dei soggetti essenziali o importanti nel campo di applicazione. Il ruolo dell'ACN sarà centrale in questo contesto, per monitorare e adattare tali disposizioni in risposta alle rapide trasformazioni delle catene del valore e dei mercati digitali.

Infine, le previsioni sulla giurisdizione italiana, coerenti con il quadro normativo europeo, richiederanno una stretta cooperazione e un coordinamento con gli altri Stati membri. La realizzazione di un *level playing field* tra imprese soggette a diverse giurisdizioni sarà fondamentale, visto le potenziali disparità competitive derivanti dall'applicazione nazionale. Questo punto potrebbe rivelare la debolezza dello strumento legislativo della Direttiva, inadatto a garantire una attuazione uniforme di norme estremamente rilevanti per il mercato unico. Tuttavia, un forte coinvolgimento e responsabilizzazione delle autorità nazionali era indispensabile per assicurare un approccio basato sul rischio, contrario a disposizioni centralistiche e prescrittive.

Dal punto di vista operativo, l'elenco dei soggetti NIS 2 sarà redatto dall'Agenzia per la Cybersicurezza Nazionale (ACN) entro aprile 2025. La lista si baserà sull'auto registrazione delle imprese che soddisfano i criteri settoriali e dimensionali richiesti, utilizzando una piattaforma disponibile sul sito dell'ACN. Nel rispetto del principio di flessibilità adottato dal decreto, la registrazione non comporta automaticamente l'inclusione come soggetto NIS. Una tale inclusione automatica risulterebbe infatti inefficace, poiché i settori sono identificati tramite il codice ATECO aziendale, che non sempre riflette con precisione tutte le attività svolte dall'impresa. L'ACN condurrà verifiche a campione sull'elenco delle imprese registrate, sebbene non siano ancora chiare le modalità con cui tali verifiche saranno effettuate.

4. Obblighi nella Direttiva

Il decreto di recepimento della Direttiva NIS 2 stabilisce una serie di obblighi di sicurezza e gestione degli incidenti per i soggetti NIS, adottando un approccio flessibile e basato sul rischio per adattarsi ai diversi contesti aziendali. Per bilanciare la necessità di proteggere le infrastrutture critiche con l'esigenza di ridurre gli oneri regolatori, il legislatore ha previsto ampi margini di discrezionalità per l'Agenzia per la Cybersicurezza Nazionale (ACN), che potrà modulare l'applicazione degli obblighi, intervenendo in base alle necessità specifiche dei diversi tipi di impresa.

L'assortimento di misure di gestione del rischio che le imprese devono implementare si estende a diversi aspetti cruciali della sicurezza informatica aziendale. Si parte dall'analisi approfondita dei rischi, che comporta una valutazione continua della sicurezza dei sistemi informativi e delle reti utilizzate. Questa analisi preventi-

va rappresenta il primo passo di un'architettura di sicurezza completa, pensata per individuare e ridurre le vulnerabilità prima che possano essere sfruttate. La Direttiva evidenzia anche l'importanza della continuità operativa: le imprese devono avere in atto politiche per il ripristino dei dati e delle operazioni in caso di disastro, inclusi protocolli di backup e gestione delle crisi, così da garantire una rapida ripresa delle attività.

Tra le misure di sicurezza richieste vi è anche la protezione della catena di approvvigionamento. Questo obbligo mira a garantire che la sicurezza si estenda non solo all'impresa, ma anche ai rapporti con fornitori e partner esterni, i cui standard di sicurezza devono essere monitorati e controllati per ridurre le vulnerabilità lungo tutta la filiera. La sicurezza informatica deve inoltre essere integrata in ogni fase del ciclo di vita dei sistemi aziendali, dall'acquisizione e sviluppo alla manutenzione, e richiede una gestione scrupolosa delle vulnerabilità. La Direttiva sottolinea anche l'importanza delle procedure di sicurezza interne: ogni impresa deve formare costantemente il proprio personale sulle pratiche di sicurezza, adottando infine linee guida chiare per l'utilizzo di strumenti critici come la crittografia e prevedendo controlli per l'accesso ai dati e ai sistemi informatici. La protezione delle risorse aziendali richiede infine una valutazione dell'affidabilità del personale, con politiche di controllo dell'accesso e una gestione rigorosa degli asset aziendali.

L'applicazione di queste misure mira a garantire un livello di sicurezza proporzionale al rischio. In questo senso, la Direttiva NIS 2 non fornisce una lista rigida di obblighi da adempiere, bensì un atlante delle misure a cui l'impresa deve fare attenzione, sulla base del proprio grado di esposizione ai rischi, alle dimensioni e al potenziale impatto di incidenti sul contesto sociale ed economico esterno.

Se da un lato la Direttiva è flessibile sui requisiti di sicurezza, gli obblighi di notifica degli incidenti sono invece più rigidi. I soggetti NIS sono tenuti a segnalare tempestivamente al Computer System Incident Response Team (CSIRT) ogni incidente significativo che possa minare la continuità dei loro servizi, "senza ingiustificato ritardo". Un incidente viene considerato significativo se può causare un'interruzione grave o perdite economiche rilevanti per l'impresa, oppure se presenta il rischio di impattare terze parti, generando danni materiali o immateriali considerevoli. La segnalazione dell'incidente deve avvenire secondo tempistiche precise: entro 24 ore dalla scoperta, l'impresa è obbligata a inviare una pre-notifica iniziale che chiarisca se l'incidente sia legato ad atti malevoli e se possa avere un impatto transfrontaliero. Entro le successive 72 ore, è necessaria una notifica completa, in cui viene fornita una valutazione della gravità dell'incidente e dei possibili indicatori di compromissione. Infine, entro un mese dalla notifica iniziale, si richiede un rapporto dettagliato che includa una descrizione dell'incidente, le cause alla base del problema, le misure di mitigazione adottate e, se noto, l'eventuale impatto su altri Stati membri.

In attesa delle determinazioni di ACN che chiariranno i criteri per identificare gli incidenti significativi, è possibile già oggi ravvisare un approccio troppo "narrativo" nell'impostazione della Direttiva, come evidente per esempio nell'atto di esecuzione approvato dalla Commissione europea, che già oggi stabilisce i criteri per i settori dei servizi ICT. Soffermandosi sulla pura descrizione delle misure di gestione del rischio e di notifica degli incidenti, l'atto di esecuzione utilizza spesso formulazioni che mirano a descrivere qualitativamente i tipi di incidenti e i requisiti per la gestione del rischio informatico. Questo approccio può portare a disposizioni ambigue per le PMI e di difficile applicazione per le organizzazioni più grandi. In questo modo non si aiutano realmente le PMI a comprendere cosa devono fare e si spingono le organizzazioni più grandi a adattare individualmente le descrizioni qualitative alle proprie procedure interne e certificazioni, rinunciando implicitamente ad una visione d'insieme. Le disposizioni di attuazione della Direttiva sarebbero più accessibili a tutte le entità NIS 2 se facessero esplicitamente riferimento a framework e standard esistenti. Questi riferimenti potrebbero inoltre rivelarsi preziosi in futuro, con l'evolversi delle problematiche e delle pratiche di cybersecurity, poiché gli standard vengono aggiornati regolarmente. Al contrario, le descrizioni qualitative tendono a diventare rapidamente obsolete.

5. L'applicazione della Direttiva nelle imprese italiane

La Direttiva NIS 2 richiede che le imprese adottino una strategia di cybersicurezza più approfondita e complessa, che non può limitarsi a un semplice approccio "plug-and-play" con l'acquisto di nuove tecnologie. Per raggiungere il livello di protezione richiesto, le aziende sono chiamate a ripensare sia la propria intera infrastruttura informatica e quella dei fornitori, sia la struttura organizzativa e le procedure di gestione delle crisi. Un simile ripensamento implica un coordinamento interno efficace e una chiara strategia di gestione del rischio.

Dal punto di vista organizzativo, per garantire un'efficace gestione della sicurezza informatica, diventa cruciale dotarsi di figure specializzate in risk management e crisi, da collocare nei nodi critici dell'infrastruttura aziendale. Queste figure devono essere coordinate a livello aziendale, con un buon equilibrio tra centralizzazione e flessibilità, così da poter rispondere rapidamente e da vicino agli incidenti. La cooperazione tra i team IT, operations e compliance diventa dunque essenziale per assicurare l'integrazione delle misure di sicurezza in tutte le attività aziendali.

Anche dal punto di vista tecnologico, le imprese devono rivedere periodicamente le proprie infrastrutture critiche e valutare come queste interagiscono sia

all'interno dell'azienda che con clienti e fornitori. La Direttiva NIS 2 spinge le aziende a condurre analisi del rischio su larga scala, includendo la valutazione delle tecnologie e dei processi di comunicazione. Questa valutazione potrebbe portare all'adozione di nuove tecnologie che, per essere efficaci, dovranno integrarsi correttamente nell'infrastruttura ICT preesistente.

Questa trasformazione strutturale richiede risorse significative, sia finanziarie che umane, e un'effettiva capacità di innovazione e adattamento, competenze che potrebbero risultare scarse non solo nelle piccole imprese, ma anche nelle medie. Le imprese medie, definite come quelle con 50-250 dipendenti e fatturati tra 10 e 50 milioni di euro, potrebbero non disporre facilmente né dei fondi necessari né del personale adeguato a soddisfare pienamente i requisiti della Direttiva. In tal senso, uno dei principali ostacoli resta la carenza di professionisti qualificati in ambito cybersecurity, un problema particolarmente sentito nel mercato del lavoro italiano e soprattutto nelle PMI.

D'altra parte, la Direttiva NIS 2 arriva in un contesto di crescente aumento degli attacchi informatici. Secondo l'indagine OAD[1] recentemente pubblicata, il 72,4% dei rispondenti ha subito attacchi digitali ai propri sistemi informativi nel 2023, che rappresentano una minaccia economica significativa per le imprese. Ancora più gravi sono le perdite di dati, che, sebbene non gli venga spesso riconosciuto, costituiscono l'asset aziendale più importante per l'innovazione e il mantenimento della competitività di impresa.

Esiste quindi una necessità oggettiva per le imprese di garantire le proprie capacità di cybersicurezza. Sebbene il mercato stesse già provvedendo a diffondere le tecnologie e buone pratiche necessarie, la Direttiva interviene correttamente sulle intere catene di approvvigionamento, mirando a ridurre i punti di vulnerabilità che potrebbero essere sfruttati da attacchi cyber. Le aziende, infatti, non possono garantire la sicurezza dei dati una volta che essi escono dai propri sistemi, e questo rende essenziale un approccio collettivo alla cybersicurezza.

Analogamente a quanto previsto per la rendicontazione sulle pratiche ESG, la transizione verso la cybersicurezza delineata dalla Direttiva dovrà essere inizialmente guidata dalle imprese capofila di settore, le medie e grandi aziende a cui si applica direttamente la NIS 2. Queste imprese fungeranno da punto di riferimento per la propria catena del valore: in futuro le imprese collegate ai soggetti NIS, così come definite da ACN, dovranno rispettare standard di cybersicurezza in linea con quelli del proprio capofiliera. Si auspica che, seguendo l'esempio delle imprese di maggiori dimensioni, le PMI possano adattarsi più agevolmente, facendo leva sull'e-

[1] *Rapporto dell'Osservatorio Attacchi Digitali (OAD) in Italia 2024*, Associazione Italiana Professionisti della Sicurezza Informatica (AIPSI), 2024. Rapporto OAD 2024 di AIPSI.pdf

sempio e l'esperienza dei propri clienti che hanno già adottato le misure necessarie.

6. Nodi da sciogliere per garantire una applicazione efficace della NIS 2

Il recepimento della Direttiva NIS 2 nell'ordinamento italiano ha fornito un quadro istituzionale chiaro, ma sussistono ancora aspetti da definire affinché l'applicazione della Direttiva sia completa e uniforme. Tra i principali nodi ancora aperti vi sono:

- I criteri di applicazione della clausola di salvaguardia, previsti dall'art. 3, comma 4 del decreto legislativo di recepimento e attesi entro gennaio 2025 tramite Decreto del Presidente del Consiglio dei Ministri (DPCM). Questi criteri delineeranno le condizioni in cui le imprese possono essere esentate, con possibili implicazioni sull'ampiezza del campo di applicazione della Direttiva.
- Estensione dell'applicazione della Direttiva ai fornitori dei soggetti NIS, come previsto dall'art. 3, comma 9. La responsabilità di questa determinazione spetta all'Agenzia per la Cybersicurezza Nazionale (ACN).
- Obblighi di gestione del rischio e di notifica degli incidenti, come richiesto dall'art. 31, comma 1, e soggetti a pubblicazione entro aprile 2025 da parte di ACN. Si tratta in questo caso degli obblighi di base, che saranno integrati successivamente, ad aprile 2026, da previsioni settoriali più avanzate.
- L'utilizzo degli schemi di certificazione, ai sensi dell'art. 27, comma 1-2. Sarà necessario attendere la piena applicabilità delle certificazioni europee, quali la *EU Cybersecurity Certification* (EUCC) e lo *European Cybersecurity Certification Scheme for Cloud Services* (EUCS).
- L'interpretazione di alcune disposizioni del dlgs 138/2024, in particolare sulla giurisdizione italiana nei confronti dei gruppi internazionali.

Il modo in cui saranno sciolti questi nodi determinerà l'efficacia della Direttiva. Non sarebbe efficace, ad esempio, prevedere una clausola di salvaguardia dalle maglie troppo ampie, così come restringere eccessivamente il numero di imprese nella catena del valore dei soggetti NIS: un approccio di questo tipo, pur riducendo il numero di imprese che dovranno incorrere nei costi di compliance alla Direttiva, ignorerebbe la necessità oggettiva di garantire un miglioramento delle capacità di cybersicurezza del tessuto industriale, e troverebbe comunque una contraddizione con l'impulso dato dalle imprese stesse, che avranno necessità sempre maggiori di imporre ai propri fornitori standard di sicurezza elevati. Lo stesso principio si può applicare alla determinazione degli obblighi di gestione del rischio e di notifica degli

incidenti. Non gioverà ridurre al minimo gli obblighi, confondendo la flessibilità con una diluzione dell'ambizione della Direttiva.

Allo stesso tempo, è necessario evitare un approccio eccessivamente prescrittivo, come già precedentemente evidenziato. Un rischio significativo legato all'implementazione della Direttiva è che molte imprese, in particolare le PMI, possano limitarsi a un'aderenza puramente formale ai requisiti normativi, senza che ciò produca un reale impatto sulla sicurezza informatica. L'approccio orientato al risk assessment, adottato da ACN, punta a scongiurare questa cosiddetta "paper compliance" e a favorire invece un adeguamento sostanziale. Grazie a questa strategia, le imprese sono spinte a considerare le proprie vulnerabilità specifiche e a implementare misure concrete per mitigare i rischi, contribuendo così a costruire una cultura della sicurezza informatica più robusta e autentica. È auspicabile che questo approccio venga mantenuto lungo l'intero ciclo di applicazione della Direttiva.

L'equilibrio da raggiungere tra spinta trasformativa e approccio basato sul rischio non è semplice da mantenere, soprattutto in presenza di difficoltà delle imprese meno dinamiche a investire e integrare nuove tecnologie. Sarà dunque fondamentale che ACN sfrutti appieno le indicazioni provenienti dal dlgs di recepimento riguardanti il supporto e l'accompagnamento delle imprese, basandosi sulla loro dimensione e il rischio sistemico che possono porre. Questo compito potrebbe non essere semplice da adempiere, viste le risorse limitate di cui dispone l'Autorità e il già gravoso compito di valutare il rischio e l'efficacia delle misure di cybersecurity dei soggetti NIS.

Diventa quindi necessario puntare su strumenti facilmente accessibili e applicabili per garantire alle imprese un'adozione semplificata delle misure della Direttiva. Le certificazioni europee, come EUCC ed EUCS, rivestono un ruolo fondamentale. Queste certificazioni garantiscono che i prodotti rispettino determinati standard di sicurezza e possano essere integrati per rispondere agli obblighi normativi. Oltre a EUCC, recentemente adottata, è in fase di sviluppo EUCS, e si prevede che nuovi schemi di certificazione riguarderanno tecnologie emergenti, tra cui Intelligenza Artificiale, crittografia e identità digitali. Per i vendor che dovranno certificare i proprio prodotti di cybersecurity sarà essenziale che i costi e benefici delle certificazioni siano chiari e prevedibili.

Tuttavia, le certificazioni non possono garantire che le tecnologie siano integrate correttamente nell'infrastruttura ICT di impresa. Di conseguenza, le certificazioni devono essere affiancate dalle linee guida e raccomandazioni previste dall'art. 31, comma 4 e 5 del decreto di recepimento. Questi strumenti possono offrire un supporto progettuale efficace, semplificando il lavoro delle imprese con meno risorse. Gli strumenti più efficace e di più immediata comprensione per le imprese sono però gli standard tecnici ISO, che garantiscono un approccio olistico alla sicurezza

informatica e la sua applicabilità e integrazione. Utilizzarli come base di partenza per la definizione e l'illustrazione degli obblighi di gestione del rischio può essere un fattore di successo fondamentale per l'applicazione della Direttiva.

Le decisioni delle autorità italiane su questi aspetti saranno fondamentali anche a livello europeo, poiché il nostro Paese è tra i primi ad aver trasposto la Direttiva e applicato alcune delle sue disposizioni. L'importanza dell'approccio adottato dall'Autorità è già emersa nell'interpretazione dell'art. 5 del D.lgs. 138/2024, che recepisce l'art. 26 della Direttiva. Quest'ultimo consente ai gruppi aziendali internazionali operanti nei settori delle infrastrutture e dei servizi digitali di individuare uno stabilimento principale nell'Unione Europea, riducendo così il peso della compliance a una sola disciplina nazionale. Tuttavia, un'interpretazione estensiva di questa norma da parte dell'Italia, che imponesse a tutte le filiali dei gruppi internazionali di sottostare alla propria giurisdizione, rischierebbe di compromettere l'efficacia della Direttiva. Tale approccio potrebbe infatti moltiplicare gli obblighi di gestione del rischio e le segnalazioni di incidenti, aggravando il carico normativo per imprese operanti in settori tipicamente transnazionali.

Dunque, le imprese dovranno attendere il quadro tecnologico e normativo completo che l'Autorità metterà a disposizione per una piena applicazione della NIS 2. Per questo motivo, contrariamente agli allarmismi che si sono diffusi in questi mesi, ACN ha definito tempistiche di compliance dilazionate, per permettere una applicazione graduale della Direttiva:

- 28 febbraio 2025: scadenza per la registrazione sulla piattaforma ACN.
- Aprile 2025: comunicazione ufficiale dell'inclusione tra i soggetti NIS.
- 1° gennaio 2026: entrata in vigore degli obblighi di notifica degli incidenti.
- 1° ottobre 2026: entrata in vigore degli obblighi di gestione del rischio.

Il primo adempimento obbligatorio per le imprese è, quindi, la registrazione sulla piattaforma ACN. Durante questa fase sarà possibile richiedere eccezioni specifiche in base alle necessità di ciascuna azienda.

7. Conclusioni

L'implementazione della Direttiva NIS 2 in Italia rappresenta una sfida significativa per le imprese dei settori critici, in particolare le medie e piccole realtà. La norma richiede un ripensamento profondo della strategia di cybersicurezza, che deve andare ben oltre l'adozione di nuove tecnologie per integrarsi nelle strutture organizzative e nei processi aziendali.

Sebbene il tessuto imprenditoriale italiano si stesse già muovendo verso standard di sicurezza informatica più elevati, la Direttiva NIS 2 introduce un approccio più sistematico e obbligatorio, imponendo alle imprese specifici oneri di gestione del rischio e notifica degli incidenti. Questo rappresenta un'opportunità per sviluppare una cultura aziendale più attenta alla protezione delle infrastrutture critiche e delle catene del valore, ma allo stesso tempo pone sfide significative in termini di risorse e competenze, soprattutto per le PMI.

Il ruolo chiave dell'Agenzia per la Cybersicurezza Nazionale sarà determinante nel guidare questa transizione. La definizione puntuale dei criteri di applicazione, degli obblighi specifici e degli strumenti di supporto alle imprese rappresenterà un fattore critico per il successo dell'applicazione della Direttiva. Sarà inoltre fondamentale che le Autorità riescano a trovare il giusto equilibrio tra un approccio basato sul rischio e la spinta trasformativa della regolazione, evitando sia un'attuazione eccessivamente prescrittiva sia una mera compliance formale da parte delle aziende.

Per i motivi elencati, la Direttiva NIS 2 ha il potenziale per migliorare in modo significativo la sicurezza informatica del sistema economico italiano di fronte alle crescenti minacce cibernetiche, a condizione che le istituzioni e le imprese siano in grado di collaborare efficacemente per superare le sfide organizzative e tecnologiche poste dalla normativa.

N. 1 - 2025 - pp. 122-133

Autenticità dei dati: l'altro pilastro fondamentale della cybersecurity

Sarah Ungaro

Abstract: La Direttiva NIS 2, recepita nell'ordinamento italiano con il D.Lgs. 138/2024, rappresenta un'evoluzione più matura nell'approccio alla sicurezza, poiché sancisce la necessità di considerare anche l'autenticità nella valutazione dei rischi per la sicurezza dei dati, che si affianca alla nota triade della sicurezza (Riservatezza, Integrità, Disponibilità).
In effetti, l'autenticità dei dati, insieme al principio di non ripudio, risulta fondamentale per garantire la certezza del diritto, specialmente in relazione alle transazioni online, ma rappresenta un requisito essenziale anche per la qualità dei dati, con particolare riferimento alla corretta metadatazione.
L'elemento dell'autenticità dei dati non costituisce neppure una novità. In tema di corretta gestione documentale, infatti, è noto che l'autenticità rappresenta uno dei requisiti dei sistemi di conservazione a norma di dati e documenti informatici, che devono assicurare, dalla presa in carico fino all'eventuale scarto, la conservazione degli oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, idonei a garantirne le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.

The NIS 2 Directive, transposed into Italian law by Legislative Decree 138/2024, represents a more mature development in the approach to security, since it sanctions the need to also consider authenticity in the assessment of data security risks, which goes hand in hand with the well-known triad of security (Confidentiality, Integrity, Availability).
Indeed, data authenticity, together with the principle of non-repudiation, is fundamental to guarantee legal certainty, especially in relation to online transactions, but it is also an essential requirement for data quality, with particular reference to correct metadata.
The element of data authenticity is also not new. On the subject of proper document management, in fact, it is well known that authenticity is one of the requirements of computerised data and document preservation systems, which must ensure, from the time they are taken in charge until their eventual discard, the preservation of the digital objects stored therein, through the adoption of rules, procedures and technologies, suitable to guarantee their characteristics of authenticity, integrity, reliability, readability, and retrievability.

Parole chiave: autenticità dei dati, sicurezza, valutazione dei rischi, certezza del diritto, non ripudio, conservazione, metadati

Sommario: 1. Autenticità dei dati come elemento da valutare nella gestione della sicurezza – 2. Autenticità dei dati e certezza del diritto – 3. Autenticità come requisito fondamentale per la qualità dei dati – 4. Autenticità dei dati come fattore da considerare nell'analisi dei rischi – 5. Conclusioni

1. Autenticità dei dati come elemento da valutare nella gestione della sicurezza

L'entrata in vigore della Direttiva (UE) 2022/2555, nota come NIS 2, rappresenta un'importante evoluzione nell'ambito della sicurezza delle reti e dei sistemi informativi nell'Unione Europea. Tale Direttiva, insieme al D.Lgs. 138/2024 che ne recepisce le disposizioni nell'ordinamento italiano, delinea un quadro normativo rafforzato per la protezione dei dati e la resilienza delle infrastrutture digitali, ricomprendendo espressamente per la prima volta l'autenticità dei dati quale ulteriore elemento cruciale nel contesto della cybersecurity, esaminando i rischi correlati alla sua compromissione e alla sua interdipendenza con i più noti principi fondamentali della triade RID (o CIA) della sicurezza, relativa ai fattori della Riservatezza (Confidentiality), dell'Integrità (Integrity) e della Disponibilità (Availability).

L'Autenticità, quale ulteriore elemento di analisi e valutazione del rischio, infatti, viene espressamente menzionato sin dal Considerando 79 del Direttiva NIS 2, in cui si evidenzia la necessità che le misure di gestione dei rischi di cibersicurezza siano basate su un approccio multirischio, mirante a proteggere i sistemi informatici e di rete, con particolare riferimento ai rischi derivanti dalle interferenze "che possano compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi".

In effetti, è proprio la Direttiva NIS 2, recepita in Italia con il D.Lgs. 138/2024[1], a sancire in modo esplicito l'autenticità come elemento fondamentale per la valutazione dei rischi sulla sicurezza dei dati, facendo espresso riferimento a tale requisito sia nella definizione di "sicurezza dei sistemi informatici e di rete"[2] che in quella di

[1] Decreto Legislativo 4 settembre 2024, n. 138, Recepimento della Direttiva (UE) 2022/2555, 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.

[2] «Sicurezza dei sistemi informatici e di rete»: la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità,

"quasi incidente"[3] e di "incidente"[4](art. 6, par. 1, nn. 2, 5 e 6)[5].

Pertanto, risulta opportuno proporre un aggiornamento degli elementi sui quali sono state finora sviluppate le analisi dei rischi per la sicurezza dei dati, configurando l'innesto del fattore dell'autenticità in quella che si potrebbe definire come la nuova quadrìade della sicurezza, identificabile con l'acronimo CIAA (Confidentiality, Integrity, Availability, Authenticity).

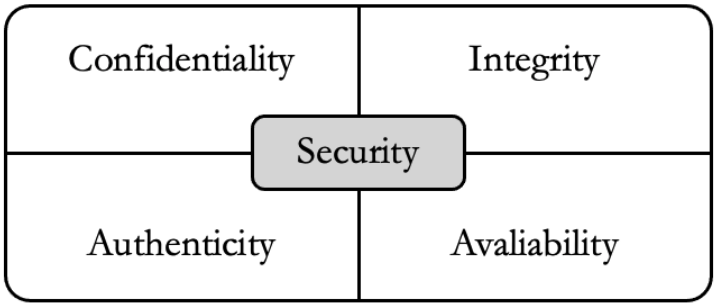


Fig. 1

Ovviamente, tale novità non può essere considerata un mero dettaglio terminologico, ma il punto di arrivo di un processo di maturità nell'approccio alla security, frutto di una maggiore consapevolezza circa la crescente complessità che connota la gestione dei dati in ambiente digitale e che, al contempo, deve comportare il necessario ripensamento dei fattori di rischio nell'ambito della sicurezza dei dati. Questi, in effetti, dovranno includere anche gli elementi in base ai quali valutare i rischi per l'autenticità dei dati, prendendo come riferimento, in primis, gli elementi della ISO/IEC 27000:2018, in cui l'autenticità (insieme al principio di non ripudio) viene riferita alla garanzia che la provenienza di un dato sia esattamente attribuibile all'entità o al soggetto a cui risulta imputabile, e che un'informazione sia conforme, verificabile e fidata.

l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili attraverso di essi.

[3] «Quasi incidente»: un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato.

[4] «Incidente»: un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi.

[5] Analoghe definizioni di "sistemi informativi e di rete" e "incidente" che riportano espliciti riferimenti all'autenticità dei dati sono rinvenibili all'art. 2, comma 1, lett. q) e t) del D.lgs. n. 138/2024.

In estrema sintesi, l'autenticità è quell'elemento che esprime la garanzia che i dati siano attribuibili (e le relative azioni/conseguenze siano giuridicamente imputabili) ai soggetti ai quali gli stessi dati risultino riconducibili e ascrivibili, escludendo inoltre che possano essere stati modificati da soggetti non autorizzati.

Tale principio appare strettamente connesso a quello dell'integrità dei dati, ma rispetto a quest'ultimo risulta incentrato sull'identificazione del soggetto che ha generato i dati (i.e. il titolare di un certificato di firma digitale utilizzato per la sottoscrizione di un documento o come mezzo di identificazione informatica per l'espletamento di una procedura in ambiente digitale, il soggetto al quale è ascrivibile una transazione online, l'utente autenticato per l'accesso a un account, etc.) e sugli aspetti legati alla provenienza dei dati stessi (i.e. sistema che ha generato un file di log, apposizione di un numero di protocollo, utilizzo di un servizio di recapito elettronico certificato, etc.).

2. Autenticità dei dati e certezza del diritto

L'autenticità dei dati, come già chiarito, è un principio riconosciuto a livello internazionale e sancito nello standard ISO/IEC 27000:2018 che fornisce una panoramica essenziale per la gestione della sicurezza delle informazioni, introducendo concetti chiave come l'autenticità dei dati e il principio del non ripudio. Questi elementi risultano cruciali per garantire la fiducia nei sistemi informativi e prevenire abusi o manipolazioni dei dati.

L'autenticità dei dati e il non ripudio, in effetti, rappresentano due principi fondamentali nella gestione della sicurezza delle informazioni, sicuramente complementari, poiché non perfettamente sovrapponibili: in effetti, mentre il principio di autenticità si riferisce alla garanzia che i dati informatici provengano da una fonte attendibile e non siano stati alterati, il principio del non ripudio assicura che un'entità (o soggetto giuridico) non possa negare di aver effettuato una determinata azione, operazione, transazione in un ambiente digitale (i.e. l'acquisto tramite una piattaforma di e-commerce, l'invio di una comunicazione tramite un sistema di recapito, l'accesso in un'area riservata, l'autorizzazione a una transazione finanziaria, etc.), a cui l'ordinamento giuridico ricollega determinati effetti, in relazione ai quali è necessario garantire l'irrinunciabile e fondamentale principio di certezza del diritto[6].

[6] Intesa quale obiettiva prevedibilità delle conseguenze che l'ordinamento giuridico determina per i nostri comportamenti (cfr. S. Margiotta, Certezza del diritto e diritto positivo, in Nomos, le attualità nel diritto, n. 1/2021).
Si veda anche G. Gometz, La certezza giuridica come prevedibilità, Torino, Giappichelli, 2005, secondo il quale il concetto di certezza del diritto, sfuggente in una prospettiva filosofica così come in teoria generale, si esprime, da un punto di vista giuspositivistico soprattutto in termini prevedibilità, vale

Nel nostro ordinamento, in considerazione dell'importanza ai fini della certezza del diritto e dell'alto valore strategico di alcune banche dati per il buon andamento delle funzioni dello Stato, i richiamati principi di riservatezza, integrità, disponibilità e autenticità dei dati in ambiente digitale trovano espressione anche nella disciplina della tutela delle basi di dati di interesse nazionale[7], di cui all'art. 60 del D.Lgs. n. 82/2005[8] (Codice dell'amministrazione digitale – CAD) e, più di recente, nelle Linee guida dell'Agenzia per la Cybersicurezza Nazionale per il rafforzamento della protezione delle banche dati rispetto al rischio di utilizzo improprio[9].

3. Autenticità come requisito fondamentale per la qualità dei dati

In tale prospettiva, il concetto di autenticità dei dati si lega indissolubilmente al requisito di qualità dei dati e, in ossequio alla disciplina sul documento informatico contenuta all'art. 20 del CAD e alle Linee guida AgID in materia di formazione, gestione e conservazione dei documenti informatici[10] (in particolare, all'Allegato 5

a dire come «possibilità diffusa di prevedere la gamma delle conseguenze giuridiche effettivamente suscettibili di essere spontaneamente o coattivamente ricondotte ad atti o fatti, nonché l'ambito temporale in cui tali conseguenze giuridiche verranno in essere».

[7] Le basi di dati di interesse nazionale sono basi di dati affidabili, omogenee per tipologia e contenuto, rilevanti per lo svolgimento delle funzioni istituzionali delle Pubbliche amministrazioni e per fini di analisi. Esse costituiscono l'ossatura del patrimonio informativo pubblico, da rendere disponibile a tutte le PA, facilitando lo scambio di dati ed evitando di chiedere più volte la stessa informazione al cittadino o all'impresa.

[8] Art. 60 Base di dati di interesse nazionale
1. Si definisce base di dati di interesse nazionale l'insieme delle informazioni raccolte e gestite digitalmente dalle pubbliche amministrazioni, omogenee per tipologia e contenuto e la cui conoscenza è rilevante per lo svolgimento delle funzioni istituzionali delle altre pubbliche amministrazioni, anche solo per fini statistici, nel rispetto delle competenze e delle normative vigenti e possiedono i requisiti di cui al comma 2.
2. Ferme le competenze di ciascuna pubblica amministrazione, le basi di dati di interesse nazionale costituiscono, per ciascuna tipologia di dati, un sistema informativo unitario che tiene conto dei diversi livelli istituzionali e territoriali e che garantisce l'allineamento delle informazioni e l'accesso alle medesime da parte delle pubbliche amministrazioni interessate. Tali sistemi informativi possiedono le caratteristiche minime di sicurezza, accessibilità e interoperabilità e sono realizzati e aggiornati secondo le Linee guida e secondo le vigenti regole del Sistema statistico nazionale di cui al decreto legislativo 6 settembre 1989, n. 322, e successive modificazioni.
2-bis. Le pubbliche amministrazioni responsabili delle basi dati di interesse nazionale consentono il pieno utilizzo delle informazioni ai soggetti di cui all'articolo 2, comma 2, secondo standard e criteri di sicurezza e di gestione definiti nelle Linee guida e mediante la piattaforma di cui all'articolo 50-ter (omissis).

[9] Novembre 2024, reperibili all'indirizzo https://www.acn.gov.it/portale/w/online-le-linee-guida-per-il-rafforzamento-della-protezione-delle-banche-dati-rispetto-al-rischio-di-utilizzo-improprio-

[10] Linee Guida sulla formazione, gestione e conservazione dei documenti informatici, AgID, maggio 2021.

delle Linee guida), anche – e soprattutto - ai metadati[11], poiché tali disposizioni sanciscono espressamente che i documenti informatici devono essere formati (e successivamente gestiti e conservati) con modalità tali da garantire "la sicurezza, l'integrità e l'immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore". Proprio tale ultimo elemento, a ben vedere, sembra fare riferimento proprio al concetto di autenticità, intesa sia come attribuibilità e imputabilità giuridica sia come verifica della provenienza.

Nello specifico, nel Glossario di cui all'Allegato 1 delle menzionate Linee guida di AgID, l'autenticità è definita come la "caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze".

Appare utile rilevare, inoltre, che la necessità di garantire il requisito di autenticità finalizzato ad assicurare la qualità dei dati risulta trovare implicito riscontro sia nel GDPR (Regolamento 2016/679/EU) sia nel AI Act (Regolamento 2024/1689/EU). In effetti, non esiste accountability senza una preventiva analisi e valutazione dei rischi e ciò vale soprattutto in tema di sicurezza dei dati (in relazione alla quale, appunto, occorre garantire riservatezza, integrità, disponibilità e autenticità). Questa viene valorizzata, per citare alcuni riferimenti normativi:

- nel GDPR, con specifico riferimento ai rischi per i diritti e le libertà delle persone fisiche nel trattamento dei dati personali (art. 35);
- nell'AI Act, in relazione ai sistemi ad alto rischio, in relazione a salute, sicurezza e diritti fondamentali (art. 9);
- nella NIS 2, con riferimento all'adozione di politiche di analisi dei rischi e di sicurezza dei sistemi informatici da parte dei soggetti essenziali e importanti (art. 21).

In proposito, come è stato evidenziato dalla Commissione UE nella Relazione alla proposta di Regolamento europeo sull'intelligenza artificiale[12], per i sistemi di

[11] Definiti nel Glossario di cui all'Allegato 1 delle Linee guida AgID in materia di formazione, gestione e conservazione dei documenti informatici come "Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017".

[12] Relazione - A9-0188/2023 sulla proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, successivamente adottato con il Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i Regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le Direttive 2014/90/UE, (UE)

IA ad alto rischio, i requisiti di qualità elevata dei dati - insieme a quelli di documentazione e di tracciabilità, di trasparenza, di sorveglianza umana, di precisione e di robustezza - sono strettamente necessari per mitigare i rischi per i diritti fondamentali e la sicurezza connessi all'utilizzo di sistemi di IA, soprattutto al fine di ridurre al minimo proprio i rischi derivanti dai c.d. *bias*.

Anche l'AI Act, in relazione ai sistemi di intelligenza artificiale ad alto rischio, richiama l'attenzione sulla necessità di valutare i rischi per la sicurezza e i diritti fondamentali, includendo espressamente l'autenticità dei dati e dei contenuti tra gli elementi da garantire, soprattutto nell'ottica di arginare il fenomeno dei c.d. deepfake.

Tali rischi, nello specifico, sono oggetto del Considerando 133, ove si osserva che "Diversi sistemi di IA possono generare grandi quantità di contenuti sintetici, che per gli esseri umani è divenuto sempre più difficile distinguere dai contenuti autentici e generati da esseri umani. L'ampia disponibilità e l'aumento delle capacità di tali sistemi hanno un impatto significativo sull'integrità e sulla fiducia nell'ecosistema dell'informazione, aumentando i nuovi rischi di cattiva informazione e manipolazione su vasta scala, frode, impersonificazione e inganno dei consumatori. Alla luce di tali impatti, della rapida evoluzione tecnologica e della necessità di nuovi metodi e tecniche per risalire all'origine delle informazioni, è opportuno imporre ai fornitori di tali sistemi di integrare soluzioni tecniche che consentano agli output di essere marcati in un formato leggibile meccanicamente e di essere rilevabili come generati o manipolati da un sistema di IA e non da esseri umani. Tali tecniche e metodi dovrebbero essere sufficientemente affidabili, interoperabili, efficaci e solidi nella misura in cui ciò sia tecnicamente possibile, tenendo conto delle tecniche disponibili o di una combinazione di tali tecniche, quali filigrane, identificazioni di metadati, metodi crittografici per dimostrare la provenienza e l'autenticità dei contenuti, metodi di registrazione, impronte digitali o altre tecniche, a seconda dei casi".

4. Autenticità dei dati come fattore da considerare nell'analisi dei rischi

Con specifico riferimento alle metodologie di sviluppo di un'analisi dei rischi che comprenda anche il fattore di rischio dell'autenticità, oltre a quelli consueti di riservatezza, integrità e disponibilità, proprio sulla scorta delle indicate misure di gestione dei rischi di cibersicurezza, di cui all'art. 21, par. 2, lett. a) della Direttiva NIS 2, i soggetti essenziali e importanti devono dotarsi anche di politiche di analisi dei rischi e di sicurezza dei sistemi informatici, che – come espressamente richiesto dal

2016/797 e (UE) 2020/1828 (Regolamento sull'intelligenza artificiale).

punto 2.1 dell'Allegato al Regolamento di esecuzione (UE) 2024/2690 della Direttiva NIS 2 del 17 ottobre 2024[13] - comprendano anche la necessaria individuazione e documentazione dei rischi per la sicurezza dei sistemi informativi e di rete, anche in termini di autenticità, con indicazione dei singoli punti di vulnerabilità (*points of failure*)[14].

Pertanto, appare utile considerare quali potrebbero essere alcuni esempi di tipologie di minacce informatiche da considerare nelle politiche di analisi dei rischi e di sicurezza dei sistemi informatici, ai fini della richiesta valutazione dei rischi specifici per l'autenticità dei dati:

- Attacchi di spoofing: un soggetto si finge un'entità affidabile per ottenere informazioni sensibili o per eseguire azioni non autorizzate;
- Attacchi di phishing: l'utente viene indotto con l'inganno a fornire credenziali di accesso o altre informazioni personali;
- Attacchi Man-in-the-Middle: un soggetto si interpone tra due entità che comunicano, intercettando e manipolando il traffico dati;

---

[13] Regolamento di esecuzione (UE) 2024/2690 della Commissione del 17 ottobre 2024 recante modalità di applicazione della Direttiva (UE) 2022/2555 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza e l'ulteriore specificazione dei casi in cui un incidente è considerato significativo per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari.

[14] Ai fini del punto 2.1.1 del Regolamento di esecuzione, i soggetti pertinenti devono stabilire procedure per l'individuazione, l'analisi, la valutazione e il trattamento dei rischi («processo di gestione dei rischi di cibersicurezza»). Il processo di gestione dei rischi di cibersicurezza deve essere parte integrante del processo generale di gestione dei rischi dei soggetti pertinenti, se applicabile. Nell'ambito del processo di gestione dei rischi di cibersicurezza, i soggetti pertinenti devono:
a) seguire una metodologia di gestione dei rischi;
b) stabilire il livello di tolleranza per i rischi conformemente alla propensione al rischio dei soggetti pertinenti;
c) stabilire e mantenere criteri di rischio pertinenti;
d) in linea con un approccio multirischio, individuare e documentare i rischi per la sicurezza dei sistemi informativi e di rete, in particolare in relazione a terzi, come pure i rischi che potrebbero causare perturbazioni in termini di disponibilità, integrità, autenticità e riservatezza dei sistemi informativi e di rete, compresa l'individuazione dei singoli punti di vulnerabilità (single points of failure);
e) analizzare i rischi per la sicurezza dei sistemi informativi e di rete, compresi la minaccia, la probabilità, l'impatto e il livello di rischio, tenendo conto delle informazioni di intelligence relative alle minacce informatiche e delle vulnerabilità;
f) valutare i rischi individuati sulla base dei criteri di rischio;
g) individuare le opzioni e le misure adeguate per il trattamento dei rischi e attribuirvi la priorità;
h) monitorare costantemente l'attuazione delle misure di trattamento dei rischi;
i) individuare i soggetti competenti per l'attuazione delle misure di trattamento dei rischi e la tempistica per tale attuazione;
j) documentare in un piano di trattamento dei rischi, in modo comprensibile, le misure di trattamento dei rischi scelte e le ragioni che giustificano l'accettazione di rischi residui.

- Modifica o manipolazione dei dati durante la trasmissione o l'archiviazione: un soggetto sfrutta la mancanza di misure a presidio della garanzia di autenticità per creare transazioni o documenti falsi o manipolare il contenuto degli stessi.

In proposito, le vulnerabilità che possono essere considerate come idonee ad esporre i sistemi al rischio di perdita di autenticità includono:

- Mancanza di sistemi di autenticazione forte[15], in quanto l'utilizzo di password deboli o di sistemi di autenticazione a singolo fattore facilita l'accesso non autorizzato;
- Mancanza di sistemi di cifratura per i dati e di crittografia[16] o di utilizzo di protocolli di sicurezza nelle comunicazioni, che espongono i dati al rischio di intercettazione e manipolazione;
- Inadeguata gestione delle identità e degli accessi[17], poiché la mancanza di un sistema di gestione centralizzata delle identità e degli accessi può portare a una proliferazione di account con privilegi eccessivi;
- Inadeguata classificazione delle risorse[18], che incide negativamente su un'adeguata mappatura e controllo delle stesse;
- Obsolescenza e mancato aggiornamento di software e sistemi[19] che, se non aggiornati, risultano più vulnerabili agli attacchi informatici, in quanto possono presentare falle di sicurezza note;
- Mancanza di un'adeguata formazione e sensibilizzazione del personale[20], atta a promuovere la conoscenza delle regole di igiene informatica di base e a prevenire l'incidenza di errori umani, in quanto gli utenti di un sistema possono essere indotti con l'inganno a fornire informazioni sensibili o a eseguire azioni non autorizzate.

---

[15] Misura prevista dall'articolo 21, paragrafo 2, lettera j), della Direttiva (UE) 2022/2555 e specificata nell'art.11.7 dell'Allegato al Regolamento di esecuzione (UE) 2024/2690 della stessa Direttiva NIS 2.

[16] Misura prevista dall'articolo 21, paragrafo 2, lettera h), della Direttiva (UE) 2022/2555 e specificata nell'art. 9 dell'Allegato al Regolamento di esecuzione (UE) 2024/2690 della stessa Direttiva NIS 2.

[17] Misura prevista dall'articolo 21, paragrafo 2, lettere i) e j), della Direttiva (UE) 2022/2555 e specificata nell'art. 11 dell'Allegato al Regolamento di esecuzione (UE) 2024/2690 della stessa Direttiva NIS 2.

[18] In tema di gestione delle risorse, nel richiamato Allegato al Regolamento di esecuzione della Direttiva NIS 2 del 17 ottobre 2024, al punto 12.1 si chiarisce che i soggetti pertinenti devono:
a) stabilire un sistema di livelli di classificazione per le risorse;
b) associare tutte le risorse a un livello di classificazione, in base a requisiti di riservatezza, integrità, autenticità e disponibilità, al fine di indicare la protezione richiesta in base alla sensibilità, alla criticità, al rischio e al valore commerciale di tali risorse;
c) allineare i requisiti di disponibilità delle risorse agli obiettivi di consegna e ripristino stabiliti nei loro piani di continuità operativa e di ripristino in caso di disastro.

[19] Misura prevista dall'articolo 21, paragrafo 2, lettera e), della Direttiva (UE) 2022/2555 e specificata nell'art. 6 dell'Allegato al Regolamento di esecuzione (UE) 2024/2690 della stessa Direttiva NIS 2.

[20] Misura prevista dall'articolo 21, paragrafo 2, lettera g), della Direttiva (UE) 2022/2555 e specificata nell'art. 8 dell'Allegato al Regolamento di esecuzione (UE) 2024/2690 della stessa Direttiva NIS 2.

Più in generale, il Considerando 20 del menzionato Regolamento di esecuzione 2024/2690/EU, recante modalità di applicazione della NIS 2 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza, specifica che a norma dell'articolo 21, paragrafo 2, lettera g), della Direttiva (UE) 2022/2555, gli Stati membri devono provvedere affinché i soggetti essenziali e importanti applichino pratiche di igiene informatica di base e forniscano formazione in materia di cibersicurezza. Tra le pratiche di igiene informatica di base possono figurare principi zero trust, aggiornamenti del software, configurazione dei dispositivi, segmentazione della rete, gestione delle identità e degli accessi o sensibilizzazione degli utenti, organizzazione di attività di formazione per il personale e sensibilizzazione in merito alle minacce informatiche, al phishing o alle tecniche di ingegneria sociale. Le pratiche di igiene informatica costituiscono parte di diversi requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza[21].

5. Conclusioni

L'introduzione dell'autenticità dei dati quale elemento fondamentale della cybersecurity non è un mero dettaglio terminologico, ma un punto di arrivo di un processo di maturità nell'approccio alla sicurezza, che comporta un ripensamento dei fattori di rischio nella sicurezza dei dati, sancito espressamente dalla Direttiva NIS 2.

Tale evoluzione, che sottolinea un'innovativa attenzione anche alla certezza delle conseguenze giuridiche connesse all'autenticità dei dati stessi, deve includere elementi specifici per valutare i rischi propri di tale fattore, prendendo come riferimento le definizioni della ISO/IEC 27000:2018, dove l'autenticità e il principio di non ripudio garantiscono che la provenienza di un dato sia esattamente attribuibile all'entità o al soggetto a cui risulta imputabile e che l'informazione sia conforme, verificabile e fidata.

In sintesi, l'autenticità dei dati è finalmente un pilastro riconosciuto della cybersecurity che richiede un'attenta valutazione dei rischi e l'implementazione di misure di sicurezza appropriate, soprattutto, ad esempio, nell'ambito della sicurezza dei dati delle transazioni on-line, i.e. quelle finanziarie o bancarie, in cui è necessario garantire il requisito dell'autenticità dei dati per poter fare affidamento sulla non ripudiabilità dei dati relativi all'origine della transazione stessa in capo alle parti a

[21] Tra le pratiche di igiene informatica di base per gli utenti, tra quelli che i soggetti pertinenti dovrebbero prendere in considerazione sono menzionati: una politica «clear desk» (scrivania pulita) e «clear screen» (schermo pulito), l'uso di mezzi di autenticazione a più fattori e di altro tipo, pratiche sicure per l'uso della posta elettronica e della navigazione sul web, la protezione dal phishing e dall'ingegneria sociale e pratiche sicure di lavoro a distanza.

cui tale transazione è giuridicamente attribuita.

L'elemento dell'autenticità dei dati non costituisce neppure una novità. In tema di corretta gestione documentale, infatti, è noto che l'autenticità rappresenta uno dei requisiti dei sistemi di conservazione a norma di dati e documenti informatici, che devono assicurare, dalla presa in carico fino all'eventuale scarto, la conservazione degli oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità.

In conclusione, tenuto conto dei menzionati elementi di valutazione di rischio in relazione alla perdita di autenticità dei dati, risulta utile provare a individuare alcune specifiche misure - oltre ai più noti controlli da implementare[22] - al fine specifico di mitigare i rischi per l'autenticità dei dati (ma anche in ossequio al correlato principio del non ripudio):

- Identificazione univoca e persistente del dato o del documento in un sistema informativo o di gestione documentale che adotti idonee misure di sicurezza (es. sistema di protocollo informatico[23] o sistemi di registro elettronico[24]);

---

[22] Oltre alle misure e ai controlli che sono raccomandati in via generale (sulla scorta delle indicazioni rinvenibili anche nel citato standard ISO/IEC 27000:2018, nella Direttiva NIS 2 e nel relativo Regolamento di esecuzione 2024/2690/EU) e che dovrebbero essere comunque oggetto di implementazione, di seguito sintetizzati a livello macro sulla scorta delle misure indicate nei documenti innanzi richiamati:
Misure e controlli organizzativi
- Definizione di politiche di sicurezza;
- Analisi e valutazione dei rischi;
- Gestione delle identità e degli accessi;
- Gestione della catena di approvvigionamento (supply chain);
- Formazione del personale sui principi di sicurezza e sulle migliori pratiche di igiene informatica;
- Definizione di un piano di risposta agli incidenti;
- Pianificazione e svolgimento di audit periodici.

Misure e controlli tecnici
- Implementazione di sistemi di autenticazione forte (es. Multi Factor Authentication, MFA);
- Crittografia end-to-end;
- Utilizzo di firme digitali;
- Implementazione di protocolli di sicurezza (come SSL/TLS);
- Implementazione di sistemi di monitoring e alert;
- Protezione e segmentazione della rete;
- Aggiornamento costante dei sistemi;
- Backup regolari e verifica dell'integrità dei backup;
- Utilizzo di sistemi di gestione dei log;
- Monitoraggio continuo dei sistemi.

[23] Cfr. paragrafo 2.1 delle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici

[24] Si veda il Regolamento 2024/1183/EU (c.d. eIDAS 2) del Parlamento europeo e del Consiglio dell'11 aprile 2024 che modifica il Regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale. I registri elettronici sono descritti al Considerando 68 come "una sequenza di registrazioni di dati elettronici che dovrebbero garantirne l'integrità e l'accuratezza

- Utilizzo di sistemi di blockchain, che forniscono una prova in un sistema distribuito dell'esistenza e dell'attribuibilità di un dato o documento;
- Adozione di sistemi di registrazione di log e di audit trail immutabili[25], che registrano le azioni e le operazioni all'interno di un sistema, permettendo di implementare conseguenti sistemi di monitoring e alert, al fine di identificare le violazioni di sicurezza, individuando chi ha avuto accesso ai dati, quali modifiche sono state apportate e quando si è verificata un'azione;
- Apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata[26], che permettono di avere evidenza di eventuali modifiche al documento apportate successivamente all'apposizione dei dati connessi alla firma.
- Trasmissione di dati e documenti attraverso sistemi di recapito certificato, che consentono di ottenere una garanzia circa la provenienza della comunicazione;
- Versamento di dati e documenti in un sistema di conservazione a norma, in modo da assicurare le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei dati e dei documenti versati.

In ogni caso, come già evidenziato, per assicurare l'autenticità a dati e documenti in ambiente digitale[27], non si può prescindere da una corretta metadatazione degli stessi, in linea con quanto indicato dalle richiamate Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici[28].

dell'ordine cronologico. I registri elettronici dovrebbero stabilire una sequenza cronologica delle registrazioni di dati". In tema di registri elettronici e della loro utilità nel garantire il requisito dell'autenticità, appare utile evidenziare che l'art. 45 *terdecies* del menzionato Regolamento specifica che i registri elettronici qualificati, in particolare, "stabiliscono l'origine delle registrazione dei dati nel registro".

[25] Sul punto, in relazione ai documenti informatici formati mediante "memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente" (lett. c del paragrafo 2.1 delle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici), oppure mediante "generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica" (lett. d del medesimo paragrafo), tra le modalità idonee ad assicurare l'immodificabilità e l'integrità dei documenti informatici così formati, le menzionate Linee guida AgID indicano la registrazione dei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema.

[26] In tal senso, si veda l'art. 2.1.1 delle Linee guida AgID sulla formazione, gestione e conservazione dei documenti informatici.

[27] Sulle tematiche relative alla formazione progressiva del documento informatico si veda A. Lisi, L'evoluzione del documento Informatico nel nuovo quadro giuridico dell'eIDAS 2, in Rivista elettronica di Diritto, Economia e Management, n. 4/2024.

[28] Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati (cfr. par. 2 delle Linee guida).

N. 1 - 2025 - pp. 134-138

Autori di questo numero

Mario Angelelli
Collaboratore di ricerca e professore a contratto presso il Dipartimento di Scienze Umane e Sociali dell'Università del Salento. Ha conseguito il dottorato di ricerca in Fisica teorica presso l'Università del Salento, concentrandosi sui metodi formali e modelli matematici per lo studio di sistemi complessi. La sua ricerca attuale si concentra su modelli di equazioni strutturali e rappresentazione di incertezza in Psicometria, combinando approcci statistici, geometrico-algebrici e della teoria dell'informazione per formalizzare ambiguità, incertezza epistemica e percezione del cyber-rischio. È membro della SIS (Società Italiana di Statistica), dell'AIP (Associazione Italiana di Psicologia: Sezione Sperimentale) e dell'INdAM (Istituto Nazionale di Alta Matematica).
email: *mario.angelelli@unisalento.it*

Marco Biagini
Ph.D., è un esperto di Intelligenza artificiale e cybersecurity con particolare riferimento alla ricerca e innovazione tecnologica in ambito Difesa. Attualmente è coinvolto nella definizione del documento di implementazione della strategia per l'Intelligenza Artificiale della Difesa.
email: *marcobia71@gmail.com*

Christian Catalano
Ricercatore in cybersecurity e cyber social security presso il Dipartimento di Informatica dell'Università degli Studi di Bari, Aldo Moro. Ha conseguito il dottorato di ricerca in ingegneria dei sistemi complessi presso l'Università del Salento, concentrandosi su modellazione di nuove tipologie di cyber attacchi, malware analysis e social engineering. La sua ricerca attuale si concentra nell'ambito delle nuove tipologie di attacco cyber e difesa e su algoritmi di AI applicati alla cyber social security.
email: *christian.catalano@unisalento.it*

Carlo Didonè
Senior Public Policy Manager presso Anitec-Assinform. Dopo la laurea triennale in Economia e Scienze Sociali dell'Università Bocconi, ha conseguito una doppia laurea magistrale in Public Policy presso l'Institut de Sciences Politiques di Parigi e la Hertie School of Governance di Berlino.
Da 6 anni lavora a politiche pubbliche europee ed italiane, prima a Bruxelles al Parlamento europeo e poi in Anitec-Assinform, dove segue gli affari europei, la digitalizzazione delle PMI e i temi legati alla cybersicurezza.
email: *carlo.didone@anitec-assinform.it*

Eleonora Faina
Direttore Generale di Anitec-Assinform, laureata in scienze politiche, ha conseguito Master in Antitrust e regolazione dei mercati, da oltre 15 anni si occupa di politiche pubbliche e affari istituzionali per associazioni di categoria e imprese di settori regolati, in Italia e a Bruxelles.
Nel suo percorso professionale ha maturato una solida esperienza nell'attività di advocacy e lobby, lavorando a stretto contatto con le Istituzioni a ogni livello (Parlamento, Governo, Autorità di regolazione, enti locali). Inoltre, grazie a oltre 9 anni nel sistema confindustriale (2008-2017), ha acquisito competenze specifiche nell'attività di policy making in particolare in materia di infrastrutture, appalti pubblici, politiche industriali e digitalizzazione. Fino a luglio 2019 è stata Senior Manager Institutional Affairs presso Italiana petroli S.p.A. e da agosto 2019 è stata Responsabile delle politiche industriali di FederlegnoArredo.
email: *eleonora.faina@anitec-assinform.it*

Luigi Foglia
Avvocato del Foro di Lecce, è partner dello Studio Legale Lisi dal 2009 e collabora con la Digitalaw S.r.l. dal 2011 occupandosi principalmente di diritto dell'innovazione digitale, contratti di outsourcing informatico, formazione e conservazione digitale del documento informatico, firme elettroniche, altri servizi fiduciari, fatturazione elettronica, innovazione nella PA, privacy, contratti IT, licenze d'uso software e disaster recovery.
Attualmente è Segretario Generale di Anorc (Associazione Nazionale per Operatori e Responsabili della Conservazione digitale dei documenti). Iscritto nell'Elenco di ANORC Professioni dei "Professionisti della digitalizzazione" - Livello Expert.
Ricopre il ruolo di Responsabile della Conservazione esterno per diverse aziende. Relatore in numerosi convegni nazionali e autore di pubblicazioni su note testate di settore in materia di diritto applicato alle nuove tecnologie. Nelle materie di sua competenza ha fornito servizi di docenza e consulenza in favore di enti pubblici, società partecipate, aziende private.
email: *luigifoglia@studiolegalelisi.it*

Corrado Giustozzi
Ingegnere delle tecnologie dell'informazione e della comunicazione, si occupa di sicurezza informatica da oltre trentacinque anni.
È docente di cybersecurity nel corso di Laurea magistrale in Ingegneria dei sistemi intelligenti dell'Università Campus Bio-medico e nei Master universitari di 1° e 2° livello di LUISS, Campus Bio-medico, Link Campus, SIOI. È membro del Comitato Scientifico dell'Area di Diritto e Informatica del Collegio Ghislieri – Università di Pavia, del Comitato Scientifico di Clusit, del Comitato Scientifico di ANSSAIF.
È stato membro dell'Advisory Group dell'Agenzia dell'Unione europea per la Cybersecurity (ENISA) dal 2010 al 2020, responsabile dello sviluppo del CERT della Pubblica Amministrazione presso l'Agenzia per l'Italia Digitale (AgID) dal 2014 al 2020,

membro del Consiglio Direttivo di Clusit dal 2015 al 2024.
È giornalista pubblicista dal 1990, e membro dell'Unione Giornalisti Italiani Scientifici (UGIS).
email: *c.giustozzi@nightgaunt.it*

Andrea Lisi
Avvocato, si occupa di diritto applicato all'informatica da più di 20 anni. Oltre allo Studio Legale Lisi, coordina le realtà di Digitalaw e D&L NET. È il Presidente di ANORC Professioni e il Direttore della Rivista di divulgazione scientifica DIGEAT. Docente universitario e direttore scientifico di Master universitari e percorsi specialistici di settore. È Direttore del Dipartimento DigitaLaw presso CUIRIF - Centro Universitario Internazionale di Ricerca e Innovazione Integral Intelligence. È membro dei quattro Osservatori nati dalla collaborazione tra Oikos Mediterraneo, CNF, Autorità Garante per la protezione dei dati personali e AgID con la Pontificia Università Antonianum. Dal 2024 è iscritto nell'Elenco dei Manager dell'Innovazione gestito da Unioncamere. Con DPCM del 26 gennaio 2023 è stato indicato come Componente del Comitato di Esperti di comprovata esperienza e qualificazione in materia di innovazione tecnologica e transizione digitale della PA per guidare la trasformazione digitale del Paese, ricoprendeo questo ruolo fino a dicembre 2024.
É componente della lista tenuta dal Comitato europeo per la Protezione dei Dati "Experts for the implementation of the EDPB's Support Pool of Experts" relativamente ai settori "Technical expertise in new technologies and information security" e "Legal expertise in new technologies".
È componente della Commissione sull'Intelligenza Artificiale dell'Ordine degli Avvocati di Lecce.
Riveste il ruolo di Direttore scientifico di numerosi Master e percorsi specialistici di settore, organizzati in collaborazione con Università ed Enti di Formazione nazionali.
Attualmente, in qualità di Professore della Pontificia Università Antonianum, è componente di Osservatori istituzionali attivi presso l'Autorità Garante per la protezione dei dati personali, presso l'Agenzia per l'Italia Digitale e presso il Consiglio Nazionale Forense.
email: *andrealisi@studiolegalelisi.it*

Giovanni Manca
Ingegnere elettronico esperto di digitalizzazione, sicurezza informatica e trasformazione digitale.
A partire dal 1986 si è occupato di identità digitale, dematerializzazione (conservazione e gestione) dei documenti informatici, sottoscrizioni informatiche, Digital Transaction Management, sicurezza informatica anche applicata al regolamento 679/2016 sulla protezione dei dati personali (GDPR).
Nel periodo 1986-1999 ha lavorato in SOGEI per la digitalizzazione del sistema del Catasto, i servizi di rete fino alla messa in linea del primo sito di natura fiscale su Internet.

Dal maggio 2001 fino all'aprile 2010 ha svolto attività direttive presso il Centro Tecnico per la RUPA, l'AIPA e il CNIPA. Tali attività hanno riguardato l'accreditamento e controllo delle aziende che operavano come certificatori di firma digitale o come gestori di posta elettronica certificata, il supporto tecnico al legislatore sulle problematiche di trasformazione digitale e la consulenza alle Pubbliche Amministrazioni sull'utilizzo sicuro dei servizi di rete e sulla integrazione nei flussi documentali di strumenti abilitanti come la firma o la PEC.
Dal maggio 2010 ha proseguito le attività professionali come consulente in numerose aziende ICT. Dal dicembre 2015 è in LAND Srl dove è Responsabile della formazione e prosegue le già citate attività di consulenza.
È coautore di norme primarie, come il Codice dell'Amministrazione Digitale, e delle normative tecniche in materia di firma digitale, conservazione documentale e documenti di identità digitale come la Carta Nazionale dei Servizi (CNS) e la CIE (Carta di Identità Elettronica).
È docente in attività di alta formazione anche presso atenei e soggetti privati
Ha pubblicato centinaia di articoli sui temi della trasformazione digitale ed è autore dei libri "Le firme elettroniche" e "Memorie del digitale".
Già Presidente di ANORC (Associazione Nazionale per Operatori e Responsabili della Custodia di contenuti digitali) nel biennio 2016-2018 è stato rieletto per il biennio 2022-2024. Attualmente ricopre la carica di Vice presidente.
email: *mncgnn59@gmail.com*

Stefano Marzocchi
Laurea in legge nel 2001, dopo alcuni nella consulenza milanese approda alla Ferrero nel 2008, occupandosi dapprima di proprietà industriale ed anticontraffazione e successivamente di licensing, digital brand protection e segreti industriali; infine, dal 2012, di protezione dei dati personali. Dal 2015 al 2022 è ricopre la carica di Group Privacy Officer e dal 2018 al 2022 quella di Data Protection Officer (DPO) dell'headquarter lussemburghese del Gruppo. Dal 2022 è DPO dell'Agenzia per la cybersicurezza nazionale (ACN). Attivo come relatore in seno a molteplici iniziative formative e autore di numerose pubblicazioni, collabora gratuitamente con diverse università italiane ed estere.
email: *s.marzocchi@acn.gov.it*

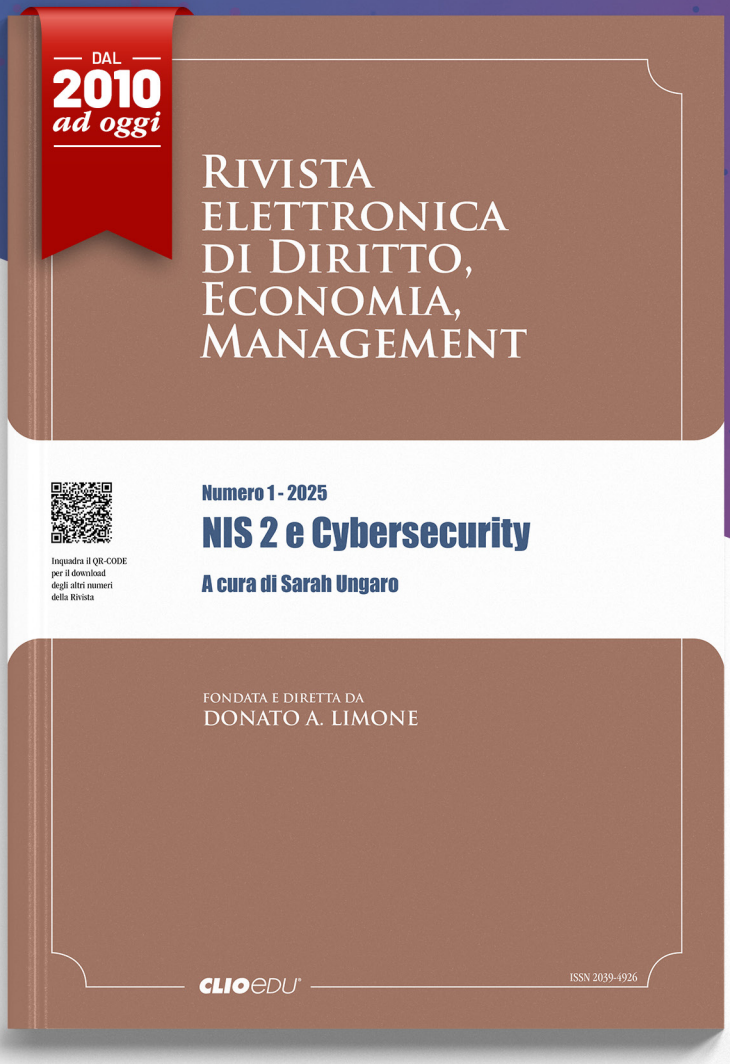
Sarah Ungaro
Avvocato, dopo la laurea in giurisprudenza conseguita con lode presso l'Università del Salento, ha conseguito il titolo della Scuola di Specializzazione per le professioni legali presso lo stesso Ateneo.
Collabora dal 2010 con lo Studio Legale Lisi in qualità di Senior Partner in materia di diritto dell'informatica, protezione dei dati personali, e-government, contratti IT e cloud, e-health, fascicolo sanitario elettronico, telemedicina, documento informatico, trasparenza amministrativa, open data, riuso, firme elettroniche, dematerializzazione dei documenti contabili e fiscali, conservazione

digitale, appalti e e-procurement.
In relazione a tali materie, è docente per Università ed enti di formazione specialistica pubblici e privati, partecipa in qualità di relatrice a seminari e convegni.
Vicepresidente dell'associazione ANORC Professioni, ne è componente della Commissione di valutazione ed è iscritta nell'Elenco della sezione "Professionisti della digitalizzazione" – Livello Expert e nell'Elenco della sezione "Professionisti della privacy" – Livello Expert, tenuti dalla stessa associazione.
Ha partecipato in qualità di autrice alla redazione del Syllabus "Competenze digitali per la PA", il documento realizzato dal Dipartimento della funzione pubblica – Presidenza del Consiglio dei Ministri nell'ambito del progetto "Competenze digitali per la PA" finanziato sul Programma Operativo Nazionale "Governance e capacità istituzionale" 2014-2020 – giunto alla sua seconda edizione (febbraio 2022).È Rappresentante esperto per l'Associazione ANORC all'interno dell'Osservatorio Regionale dell'Agenda Digitale Pugliese.
È componente del gruppo di ricerca dell'Osservatorio permanente sulla diplomazia digitale e l'Intelligenza artificiale nato dalla collaborazione tra OIKOS Mediterraneo e la Pontificia Università Antonianum.
È componente della Commissione sull'Intelligenza Artificiale dell'Ordine degli Avvocati di Lecce.
email: *sarahungaro@studiolegalelisi.it*

Giorgia Zunino
Dirigente di ricerca al Policlinico San Martino IRCCS di Genova, si occupa di Innovazione in campo Manageriale dei Sistemi Sanitari e di Strategic Foresight. Esperto della Regione Liguria per il Nuovo Ospedale Computazionale degli Erzelli, è anche uno dei componenti del Board Etico per le Tecnologie Emergenti della Città di Torino.
email: *reginadquadri.gz@gmail.com*

CLIOEDU®

Soluzioni digitali d'*eccellenza* per progetti di prestigio



FONDATA E DIRETTA DA
DONATO A. LIMONE

La "Rivista elettronica di Diritto, Economia, Management" è un periodico totalmente digitale, accessibile e fruibile gratuitamente.

INQUADRA IL QR-CODE PER IL DOWNLOAD DEGLI ALTRI NUMERI

www.clioedu.it/rivistaelettronica

CLIOEDU®