unione europea e diritti

L'alba di un diritto alla cybersicurezza? Profili emergenti nell'ordinamento dell'Unione europea

Enza Cirone*

SOMMARIO: 1. Considerazioni introduttive. - 2. Oltre la definizione: la cybersicurezza tra prassi e stato. - 3. Il quadro normativo di diritto dell'Unione europea in materia di cybersicurezza. - 4. Verso un diritto alla cybersicurezza? – 5. Osservazioni conclusive.

1. Considerazioni introduttive

Come ben noto, nei tempi più recenti, la cybersicurezza è divenuta una componente centrale dell'architettura giuridica dell'Unione europea, collocandosi al crocevia del triplice obiettivo di integrazione del mercato unico digitale e della tutela dei diritti fondamentali e della sicurezza pubblica[1]. Ciò è avvenuto in parallelo con la crescente penetrazione delle tecnologie digitali nei servizi pubblici essenziali, nelle infrastrutture strategiche e nelle dinamiche economiche, modificando progressivamente la percezione stessa della sicurezza informatica. Se in passato essa era prevalentemente considerata nei suoi elementi squisitamente tecnici e quindi affidata a specialisti incaricati di gestire vulnerabilità e incidenti, oggi la sua rilevanza appare sempre più cruciale in quanto condizione necessaria per il regolare funzionamento delle istituzioni e

* Assegnista di ricerca in Diritto dell'Unione europea, Università degli Studi di Firenze.

[1] Sulle implicazioni costituzionali del processo di ampliamento del diritto UE della cybersicurezza, si rimanda a F. CASOLARI, F. FERRI, S. VILLANI, *La costituzionalizzazione della cybersicurezza nell'ordinamento dell'Unione europea*, in R. BRIGHI, G. ADINOLFI (a cura di), *Governare la sicurezza degli (eco)sistemi cyberfisici*, Torino, 2025, pp. 27-49.

la continuità delle attività essenziali per la vita sociale ed economica degli Stati membri[2] e, più in generale, dell'Unione[3].

Si è dunque compreso che la protezione dalle minacce cibernetiche non riguarda più soltanto la preservazione dell'integrità delle reti, ma incide direttamente, tra gli altri, sulla tutela dei dati personali degli utenti della rete stessa e, in senso più ampio, sulla stabilità dell'ambiente digitale europeo nel suo complesso[4].

In risposta all'innovazione tecnologica e al conseguente ripensamento dell'assetto politico, economico e sociale, l'Unione europea ha costruito un articolato quadro normativo volto a rafforzare la capacità di prevenire, gestire e contenere gli incidenti informatici. A partire dalla strategia del 2013[5], fino alla revisione della direttiva NIS[6] e all'adozione del più recente *Cyber Solidarity Act*[7], si è delineato un assetto normativo sempre più strutturato, fondato su obblighi organizzativi a carico degli operatori, su meccanismi di cooperazione tra autorità nazionali e su strumenti comuni di certificazione per prodotti e servizi digitali[8].

Ciononostante, tale evoluzione non ha comportato né la definizione di una politica autonoma in materia di cybersicurezza, né l'introduzione all'interno

---

[2] Per approfondimenti di carattere generale, si veda A. ADINOLFI, *Evoluzione tecnologica e tutela dei diritti fondamentali: qualche considerazione sulle attuali strategie normative dell'Unione*, in *Quaderni AISDUE*, n. 15, 14 marzo 2023, pp. 321-343; M. DUNN CAVELTY, C. KAVANAGH, *Cybersecurity and human rights*, in B. WAGNER, M. C. KETTEMANN, K. VIETH-. DITLMANN, S. MONTGOMERY (eds.), *Research Handbook on Human Rights and Digital Technology. Global Politics, Law and International Relations*, Cheltenham, 2025, pp. 70-93.

[3] M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds and Machines*, 2019, p. 352; M. HILDEBRANDT, *Digital security and human rights: a plea for counter-infringement*, in M. SUSI (ed.), *Human Rights, Digital Society and the Law: A Research Companion*, Milton Park, 2019, p. 266.

[4] S.A. SALVAGGIO, N. GONZÁLEZ, *The European framework for cybersecurity: strong assets, intricate history*, in *International Cybersecurity Law Review*, 2023, p. 137 ss.

[5] Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013) 1 final.

[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.

[7] Regolamento (UE) 2025/38 del Parlamento europeo e del Consiglio, del 19 dicembre 2024, che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti informatici e di preparazione e risposta agli stessi, e che modifica il regolamento (UE) 2021/694.

[8] G. SZPOR, *The Evolution of Cybersecurity Regulation in the European Union Law and Its Implementation in Poland,* in *Review of European and Comparative Law*, vol. 46, n. 3, 2019, p. 219 ss.

dei Trattati di una base giuridica specifica per il settore[9]. Sebbene la disciplina trovi prevalentemente fondamento nell'articolo 114 TFUE[10], sarebbe tuttavia riduttivo ricondurla esclusivamente alla logica dell'armonizzazione del mercato interno.

Lo sviluppo della normativa dell'UE in materia di cybersicurezza appare piuttosto il risultato di un graduale adattamento delle competenze esistenti dell'Unione, attraverso le quali esigenze legate alla sicurezza dell'ambiente digitale[11] sono state ricondotte all'interno di ambiti di intervento già previsti dai Trattati. La crescente interdipendenza tra le diverse politiche dell'Unione ha infatti consentito di collocare la cybersicurezza all'intersezione tra mercato interno, regolazione delle infrastrutture digitali e tutela dei diritti fondamentali, ampliando di fatto lo spazio di intervento dell'UE[12].

Un passo particolarmente significativo per tale evoluzione si è avuto con il progetto del Mercato Unico Digitale, avviato dalla Commissione europea con

[9] G.G. FUSTER, L. JASMONTAITE, *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights*, in M. CHRISTEN, B. GORDIJN, M. LOI (eds.), *The Ethics of Cybersecurity*, Cham, 2020, p. 98.

[10] Fatta eccezione per il *Cyber Solidarity Act* che è basato sugli artt. 173 e 322, par. 1, lett. a), TFUE, ovvero sulla politica industriale e sulle modalità relative alla formazione e all'esecuzione del bilancio, al rendiconto e alla verifica dei conti. Sul punto è interessante notare che la Corte di giustizia ha confermato la legittimità dell'art. 114 TFUE come base giuridica per gli atti di diritto derivato dell'Unione che presentano profili inerenti alla cybersicurezza nella sentenza del 2 maggio 2006, C-217/04, *Regno Unito/Parlamento e Consiglio*. In dottrina v. anche Y. MIADZVETSKAYA, R. A. WESSEL, *The Externalisation of the EU's Cybersecurity Regime: The Cyber Diplomacy Toolbox*, in *EP*, 2022, pp. 418-421.

[11] Un ambiente definito come "ubiquo", v. Parlamento europeo, *Ubiquità del mercato unico digitale*, www.europarl.europa.eu/factsheets/it/sheet/43/ubiquita-del-mercato-unico-digitale.

[12] Per lungo tempo, la disciplina in materia di cybersicurezza si è sviluppata al di fuori delle logiche proprie del mercato interno, trovando piuttosto fondamento in strumenti riconducibili all'area della cooperazione in materia penale e di sicurezza. In una prima fase, infatti, il riferimento normativo era rappresentato da una decisione quadro adottata nell'ambito del pilastro "Giustizia e affari interni", successivamente sostituita dalla direttiva del 2013 sugli attacchi contro i sistemi di informazione (dir. (UE) 2013/40), fondata sull'art. 83, par. 1, TFUE, che consente l'adozione di norme minime in materia penale per reati gravi a dimensione transnazionale. Parallelamente, le prime iniziative in materia di cybersicurezza sono state ricondotte all'obiettivo della protezione delle reti e delle infrastrutture critiche (dir. (UE) 2016/1148), un ambito inizialmente disciplinato in modo frammentario dal diritto derivato, come dimostra la direttiva 2008/114/CE. Quest'ultima si basava sull'art. 308 del Trattato CE, espressione della teoria dei poteri impliciti, che consentiva al Consiglio di intervenire anche in assenza di una specifica base giuridica, purché la misura fosse adottata all'unanimità e fosse necessaria al conseguimento degli obiettivi della Comunità, nell'ambito del funzionamento del mercato comune (con il Trattato di Lisbona la norma è stata sostituita dall'art. 352 TFUE che non richiede il collegamento con il funzionamento del mercato interno).

la strategia del 2015[13], attraverso vari atti vincolanti[14] con cui l'Unione ha promosso la costruzione di uno spazio digitale integrato fondato sulla libera circolazione di servizi, dati e tecnologie, all'interno del quale la sicurezza delle reti e dei sistemi informativi è emersa come elemento imprescindibile per il funzionamento dell'ecosistema digitale europeo.

La progressiva espansione della normativa dell'Unione in questo ambito mostra infatti come la cybersicurezza sia sempre più considerata fattore rilevante per la tutela delle persone nello spazio digitale e per l'effettivo esercizio dei diritti e delle libertà garantiti dall'ordinamento dell'Unione.

In tale prospettiva, si pone un interrogativo di carattere sistematico: la cybersicurezza costituisce soltanto un obiettivo normativo funzionale al corretto funzionamento del mercato, oppure l'attuale sviluppo normativo consente di intravedere l'emersione di una posizione giuridica autonoma, suscettibile di essere ricondotta al sistema dei diritti fondamentali?[15] È proprio alla luce di questa tensione tra dimensione regolatoria e possibile dimensione soggettiva della cybersicurezza che si colloca la presente ricerca.

Per sviluppare questa riflessione, il contributo si articola in tre parti. In primo luogo, verrà esaminata la definizione di cybersicurezza, evidenziando come l'assenza di una definizione comune abbia indotto parte della dottrina a distinguere tra cybersicurezza come prassi e cybersicurezza come stato, utile per chiarire la natura e le possibili implicazioni giuridiche del concetto nell'ordinamento dell'Unione (paragrafo 2).

Su queste basi, l'analisi si concentra poi sull'evoluzione del quadro normativo di diritto dell'UE in materia di cybersicurezza, ricostruendo i

---

[13] Commissione europea e Alto Rappresentante dell'UE per gli affari esteri e la politica di sicurezza, *Strategia per il mercato unico digitale in Europa*, COM(2015) 192 final.

[14] Per approfondire si v. S. GARBEN, I. GOVAERE (eds.), *The Internal Market 2.0*, Oxford-New York, 2020; G. CAGGIANO, *Il quadro normativo del Mercato unico digitale*, in F. ROSSI DAL POZZO (a cura di), *Mercato unico digitale, dati personali e diritti fondamentali*, in *EJ,* fascicolo speciale, 2020, p. 13 ss.; P. MANZINI, G. CONTALDI, G. CAGGIANO, (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021; L. D. DABROWSKI, M. SUSKA (eds.), *The European Union Digital Single Market: Europe's Digital Transformation*, New York, 2022; V. PAPAKONSTANTINOU, P. DE HERT, *The Regulation of Digital Technologies in the EU, Actification, GDPR Mimesis and EU Law Brutality at Play*, New York, 2024.

[15] P. G. CHIARA, *The Balance Between Security, Privacy and Data Protection in IoT Data Sharing*, in *EDPL*, 2021, p. 18; A. KASPER, V. VERNYGORA, *The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market?*, in *Cuadernos Europeos de Deusto*, 2021, p. 29; D. M. VICENTE, S. DE V. CASIMIRO, C. CHEN, *The Legal Challenges of the Fourth Industrial Revolution: The European Union's Digital Strategy*, Cham, 2023.

principali strumenti adottati e verificando se e in che termini essi riflettano la crescente rilevanza della sicurezza informatica per la tutela delle persone nello spazio digitale (paragrafo 3).

La terza parte del lavoro è dedicata alla configurabilità di un diritto alla cybersicurezza nell'ordinamento dell'Unione europea[16], di cui si analizza il fondamento e il rapporto con il sistema dei diritti fondamentali (paragrafo 4).

2. *Oltre la definizione: la cybersicurezza tra prassi e stato*

A livello europeo, la definizione di cybersicurezza si inserisce in un contesto ancora segnato da incertezza concettuale e pluralità di approcci.

Il Regolamento sulla cybersicurezza[17] la definisce come «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche» (art. 2, par. 1, n.1). Si tratta di una formulazione volutamente ampia, che estende il raggio della tutela oltre l'integrità tecnica dei sistemi, includendo espressamente le persone tra i destinatari della protezione. Tuttavia, come evidenziato in dottrina, la cybersicurezza resta un concetto "avvolgente", difficilmente riducibile a una definizione univoca e stabile[18].

Tale difficoltà emerge anche nei lavori degli organismi di standardizzazione europea, come il CEN-CENELEC, nei quali si evidenzia come la cybersicurezza sfugga a una definizione tradizionale, poiché designa un insieme eterogeneo di rischi, strumenti e pratiche[19] intrinsecamente dinamico e soggetto a continua evoluzione. In questa prospettiva, più che tentare una delimitazione rigida, si è ritenuto preferibile adottare definizioni tecniche,

[16] Cfr. V. PAPAKONSTANTINOU, *The Need to Introduce a New Individual Right to Cybersecurity*, in L. MARTINO, N. GAMAL (eds.), *European Cybersecurity in Context: A Policy-Oriented Comparative Analysis: Techno-Politics Series,* Brussels, 2022, pp. 77-83; P. G. CHIARA, *Towards a right to cybersecurity in EU law? The challenges ahead*, in *Computer Law & Security Review*, 2024, pp. 1-9.

[17] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013.

[18] V. ad esempio, A. REFSDAL, B. SOLHAUG, K. STØLEN, *Cybersecurity*, in *Cyber-Risk Management, SpringerBriefs in Computer Science*, Cham, 2015; D. SCHATZ, R. BASHROUSH, J. WALL, *Towards a More Representative Definition of Cyber Security*, in *Journal of Digital Forensics, Security and Law*, 2017, pp. 53-74; M. BAY, *What is cybersecurity - In search of an encompassing definition for the post-Snowden era*, in *French Journal For Media Research*, 2016, pp.1-28; J. KOSSEFF, *Defining Cybersecurity Law*, in *Iowa Law Review*, 2018, pp. 985-1031.

[19] V. Cen/Cenelec, Cyber Security Focus Group (CSCG), *Definition of Cybersecurity, Recommendation,* V. 01.08.

calibrate sugli specifici ambiti di applicazione con una catalogazione di minacce e rischi. Analogamente, anche parte di altra dottrina[20] ha proposto definizioni ancorate ai processi di gestione del rischio e alla protezione della riservatezza, integrità e disponibilità dei dati, mettendo in luce, tuttavia, come tali formulazioni finiscano per descrivere un complesso di attività e politiche più che individuare un concetto dotato di confini netti. Altri autori, ancora, hanno messo in luce come, nel contesto dell'Unione, la nozione di cybersicurezza si collochi all'intersezione tra resilienza delle infrastrutture, contrasto alla criminalità informatica, difesa cibernetica e tutela dei diritti fondamentali, confermandone la natura composita e multidimensionale[21].

Proprio alla luce di tale *impasse* definitoria, la presente analisi si avvale della distinzione tra "cybersicurezza come prassi" e "cybersicurezza come stato"[22] proposta in dottrina.

Nel primo senso, la "cybersicurezza come prassi" designa l'insieme delle misure, delle attività organizzative e degli strumenti tecnici posti in essere dai soggetti destinatari degli obblighi normativi al fine di prevenire e gestire i rischi informatici. L'accento cade sull'azione che consiste nella adozione di strategie nazionali, nella implementazione di misure tecniche e organizzative e nella cooperazione tra autorità competenti. In questa prospettiva, la cybersicurezza si configura prevalentemente come un dovere di condotta imposto a determinati attori pubblici e privati[23].

Tale impostazione solleva tuttavia due questioni preliminari: chi sono i destinatari di tali obblighi e chi ne sono i beneficiari[24]. Sotto il primo profilo, la cybersicurezza può essere concepita secondo due modelli alternativi: uno inclusivo, che coinvolge l'insieme dei soggetti, chiamati a contribuire attraverso comportamenti e misure adeguate, e uno selettivo, che limita gli obblighi a categorie specifiche, individuate dal legislatore, come le infrastrutture critiche o determinati operatori.

Una simile alternativa si riflette anche sul piano dei beneficiari: mentre una prospettiva ampia riconosce una legittima aspettativa di sicurezza a tutti i soggetti che operano nello spazio digitale, un'impostazione più restrittiva tende

[20] D. SCHATZ, R. BASHROUSH, J. WALL, *op. cit.*
[21] G. G. FUSTER, L. JASMONTAITE, *op. cit.*
[22] V. PAPAKONSTANTINOU, *Cybersecurity as praxis and as a state: The EU law path towards acknowledgement of a new right to cybersecurity?,* in *Computer Law & Security Review,* 2022, pp. 1-15.
[23] J. ODERMATT, *The European Union as a cybersecurity actor*, in S. BLOCKMANS, P. KOUTRAKOS (eds.), *Research Handbook on EU Common Foreign and Security Policy,* Cheltenham, 2018, pp. 354-373.
[24] V. PAPAKONSTANTINOU, *op. cit.*, p. 5.

a circoscrivere tale protezione a un numero limitato di destinatari. Tuttavia, la natura stessa della cybersicurezza e il suo stretto collegamento con la sicurezza in senso lato rendono difficilmente sostenibile una delimitazione rigida dei beneficiari, che appaiono piuttosto destinati a coincidere con l'intera platea degli utenti digitali.

Diversamente, la «cybersicurezza come stato» rinvia a una condizione protettiva che si realizza quando le attività di prevenzione e gestione del rischio informatico risultano efficaci: una sfera entro la quale persone fisiche e giuridiche possono ritenersi al riparo da minacce informatiche. Questa dimensione non coincide con le misure adottate, ma con la situazione di sicurezza che ne deriva. Si tratta di una costruzione teorica che presuppone l'esistenza di un ambito di protezione riconoscibile, rispetto al quale i soggetti possono vantare un'aspettativa di sicurezza e pretendere il rispetto della integrità del proprio spazio digitale[25].

Tale aspettativa, tuttavia, non equivale automaticamente al conseguimento effettivo di una condizione di sicurezza, ma esprime piuttosto una pretesa a una sfera di protezione, la cui concreta realizzazione dipende dalle azioni intraprese e dai mezzi disponibili. In questo senso, la cybersicurezza come stato implica non solo la delimitazione di un ambito protetto, ma anche la possibilità, per i soggetti interessati, di esercitare un controllo su di esso e di difenderlo rispetto a interferenze esterne, a fronte di un correlato obbligo di rispetto in capo ai terzi.

I mezzi attraverso cui tale condizione può essere garantita e mantenuta non si esauriscono nelle misure tecniche e organizzative proprie della fase della prassi, ma comprendono anche strumenti di natura giuridica, che consentono ai destinatari della protezione di rivendicare e preservare la propria sfera di sicurezza. Ne deriva che, una volta instaurata, la condizione di cybersicurezza richiede anche di essere costantemente mantenuta attraverso un insieme di azioni che possono coinvolgere tanto i soggetti originariamente obbligati quanto gli stessi beneficiari.

Per quanto interessante sul piano teorico, suddetta distinzione, come verrà messo in evidenza nel paragrafo seguente, non sembra trovare riscontro nel quadro normativo che appare invece incentrato sulla cybersicurezza come prassi. Gli strumenti vigenti delineano infatti obblighi di gestione del rischio e

[25] *Ivi,* p. 6.

meccanismi di cooperazione[26], ma non riconoscono espressamente una pretesa alla protezione in capo ai singoli.

3. *Il quadro normativo di diritto dell'Unione europea in materia di cybersicurezza*

L'evoluzione della normativa dell'Unione in materia di cybersicurezza può essere ricostruita, in chiave analitica, come un percorso articolato in tre momenti: una prima fase di definizione strategica, una seconda fase di costruzione degli strumenti regolatori e una terza di consolidamento del quadro normativo. Attraverso queste fasi, l'Unione europea è progressivamente passata da un approccio settoriale alla sicurezza informatica a una strategia politica e giuridica più integrata e trasversale. La crescente sofisticazione e la frequenza delle minacce informatiche[27] hanno infatti evidenziato la necessità per l'Unione di sviluppare un *corpus* normativo più coerente e integrato, sebbene il quadro attuale risulti ancora frammentato[28].

Prima del 2013, le questioni relative alla cybersicurezza erano trattate principalmente all'interno di specifiche normative settoriali. Queste prime iniziative hanno avuto il merito di gettare le basi per la protezione delle infrastrutture e dei dati[29], ma mancavano di un approccio unitario. Nel processo evolutivo della materia, un momento significativo, come già anticipato, si è verificato nel 2013, quando la Commissione Barroso II presentò la prima Strategia dell'Unione europea per la cybersicurezza, intitolata *Un Ciberspazio aperto e sicuro*[30]. Tale documento programmatico mirava a delineare uno spazio digitale accessibile a tutti e, al contempo, dotato di strumenti adeguati a proteggere la riservatezza dei dati e delle informazioni in esso contenute. Questa strategia ha avuto il merito di includere formalmente la cybersicurezza tra le priorità politiche dell'Unione, riconoscendo sia la

[26] A. VERHELST, J. WOUTERS, *Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives*, in *International Organisations Research Journal,* 2020, pp. 105-124.
[27] ENISA, *ENISA Threat Landscape 2024. Global Cybersecurity Challenges and EU Preparedness*, 2024, p 6, disponibile a www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
[28] D.M. VICENTE, S. CASIMIRO, C. CHEN, *op. cit.*; A. BARRINHA, G. CHRISTOU, *Speaking Sovereignty: The EU in the Cyber Domain*, in *European Security*, 2022, pp. 356-376.
[29] Decisione quadro 2005/222/GAI del Consiglio, del 24 febbraio 2005, relativa agli attacchi contro i sistemi di informazione.
[30] Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN(2013) 1 final.

crescente minaccia della criminalità informatica, sia la necessità di un modello di governance multilivello fondato sulla cooperazione tra settore pubblico e privato.

Su queste basi, la Commissione presieduta da Juncker ha avviato una fase di implementazione di tali indirizzi politici, promuovendo l'adozione dei primi due strumenti normativi di portata generale in materia di cybersicurezza, la direttiva NIS[31] e il regolamento sulla cybersicurezza (*Cybersecurity Act*)[32].

La direttiva NIS, muovendo dalla premessa che le reti e i sistemi informativi svolgono un ruolo essenziale nel facilitare la libera circolazione di beni, servizi e persone, ha introdotto obblighi specifici di sicurezza e di notifica degli incidenti a carico degli operatori di servizi essenziali e dei fornitori di servizi digitali, nonché meccanismi di cooperazione tra le autorità nazionali. Tuttavia, prevedendo un'armonizzazione minima[33], essa ha lasciato agli Stati membri un ampio margine di discrezionalità nell'attuazione, determinando un'applicazione disomogenea e significative differenze nei livelli di protezione tra gli ordinamenti nazionali, con effetti sull'uniformità delle condizioni di sicurezza nel mercato interno.

Riprendendo la distinzione delineata nel paragrafo precedente, un'analisi più attenta della direttiva NIS mostra come il suo impianto normativo rimanga ancorato a una concezione della cybersicurezza intesa quale insieme di obblighi organizzativi e tecnici posti a carico di specifiche categorie di operatori. La disciplina si rivolge infatti a un numero limitato di soggetti - principalmente operatori di servizi essenziali e fornitori di servizi digitali - chiamati ad adottare misure di gestione del rischio e di notifica degli incidenti.

In questa prospettiva, la sicurezza delle reti e dei sistemi informativi è perseguita principalmente in funzione del corretto funzionamento del mercato interno, senza che vengano individuati in modo esplicito i beneficiari della tutela né riconosciute posizioni giuridiche soggettive azionabili. La protezione delle persone rimane così un obiettivo mediato, solo indirettamente rilevante.

A fronte di tali limiti, le iniziative successive mostrano un tentativo di superare un'impostazione meramente funzionale, collocando la cybersicurezza all'interno di un quadro più ampio di sicurezza dell'Unione, come emerge sia

[31] G. BELLA, G. CASTIGLIONE, D. F. SANTAMARIA, *An ontological approach to compliance verification of the NIS 2 directive*, in *CEUR Workshop Proceedings,* 2023.
[32] Regolamento (UE) 2019/881, cit.
[33] C. CALLIESS, A. BAUMGARTEN, *Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective*, in *GLJ*, 2020, pp. 1149–1179.

dalla comunicazione *Plasmare il futuro digitale dell'Europa*[34] sia dalla Strategia per l'Unione della sicurezza 2020–2025[35].

In tali documenti, la sicurezza digitale non è più trattata come un ambito settoriale, ma come componente di un quadro integrato che comprende la lotta al terrorismo e alla criminalità organizzata, la gestione delle minacce ibride e il rafforzamento della resilienza delle infrastrutture critiche. In questa stessa traiettoria si colloca la Strategia europea per la cybersicurezza del dicembre 2020[36], che segna un passaggio ulteriore: la cybersicurezza viene qualificata come elemento strutturale della trasformazione digitale dell'Unione, e non più soltanto come insieme di misure tecniche o di gestione del rischio.

In questa stessa direzione si colloca l'adozione del regolamento sulla cybersicurezza, che ha consolidato il ruolo dell'Agenzia dell'Unione europea per la cybersicurezza (ENISA) [37], ampliandone le funzioni di supporto tecnico e coordinamento a livello europeo, e ha introdotto un sistema europeo di certificazione della cybersicurezza per prodotti, servizi e processi digitali. Pur mantenendo il riferimento al funzionamento del mercato interno quale base giuridica, il regolamento affianca a tale obiettivo il perseguimento di un livello elevato di cybersicurezza e di fiducia nell'ambiente *online*.

Come anticipato nel paragrafo precedente, particolarmente significativa è la definizione di cybersicurezza in esso contenuta, che estende la protezione non solo alle reti e ai sistemi informativi, ma anche agli utenti e, più in generale, alle persone esposte alle minacce informatiche. Emerge così lo spostamento da una concezione prevalentemente tecnica della sicurezza digitale a una che incorpora anche la dimensione della tutela degli individui[38].

---

[34] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Plasmare il futuro digitale dell'Europa*, COM(2020) 67 final.

[35] Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni sulla *strategia dell'UE per l'Unione della sicurezza*, COM(2020) 605 final.

[36] Comunicazione congiunta al Parlamento europeo, al Consiglio europeo, al Consiglio**,** *La strategia dell'UE in materia di cibersicurezza per il decennio digitale***,** JOIN(2020)18 final; A. KASPER, V. VERNYGORA, *The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market?*, in *Cuadernos Europeos de Deusto*, 2021*,* pp. 29-71.

[37] L'Agenzia è stata istituita con il regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione.

[38] A tal riguardo, il 20 gennaio 2026 la Commissione europea ha presentato una proposta di revisione del Cybersecurity Act, volta a superare le criticità emerse nell'attuazione del quadro vigente, in particolare con riferimento al funzionamento del sistema europeo di certificazione, alla frammentazione degli obblighi e ai rischi connessi alle *supply chain* ICT.

Il mutamento del contesto geopolitico, accentuato dal conflitto tra Russia e Ucraina, ha poi contribuito ad una traslazione della cybersicurezza verso la dimensione della sicurezza e difesa dell'Unione. La *Bussola strategica per la sicurezza e la difesa* del 2022[39] segna, in tal senso, un passaggio rilevante, inserendo stabilmente la dimensione cibernetica tra gli strumenti della politica di sicurezza europea.

In questa prospettiva si inserisce la *comunicazione sulla politica di ciberdifesa dell'UE*[40], che non si limita a promuovere la cooperazione e lo sviluppo di capacità tecniche, ma riflette una più ampia integrazione tra cybersicurezza e logiche di autonomia strategica[41]. Ne deriva un ulteriore ampliamento del perimetro della cybersicurezza, ormai esteso ben oltre la gestione del rischio tecnico e sempre più intrecciato con le politiche di sicurezza dell'Unione.

Coerentemente con questa impostazione, l'Unione ha avviato un processo di rafforzamento dell'architettura normativa esistente, in particolare attraverso l'adozione della direttiva NIS 2[42], che amplia significativamente l'ambito di applicazione della disciplina e introduce requisiti più stringenti in materia di gestione del rischio e sicurezza delle reti[43].

La proposta si articola attorno a tre direttrici principali. In primo luogo, essa ridefinisce il mandato di ENISA, attribuendole funzioni rafforzate in materia di supporto all'attuazione del diritto dell'Unione, cooperazione operativa tra Stati membri e gestione delle capacità di risposta agli incidenti. In secondo luogo, interviene sul *European Cybersecurity Certification Framework* (ECCF), modificandone le procedure di adozione e manutenzione, ampliandone l'ambito applicativo e valorizzandone la funzione quale strumento di semplificazione degli obblighi di conformità previsti dalla normativa settoriale. In terzo luogo, introduce un quadro armonizzato a livello dell'Unione per la gestione dei rischi non tecnici nelle catene di distribuzione ICT, fondato su valutazioni coordinate del rischio e sulla possibilità di adottare misure restrittive nei confronti di fornitori considerati ad alto rischio. Commissione europea, *proposta di regolamento del Parlamento europeo e del Consiglio relativo all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al quadro europeo di certificazione della cibersicurezza e alla sicurezza delle catene di approvvigionamento delle TIC e che abroga il regolamento (UE) 2019/881 ("regolamento sulla cibersicurezza 2")*, COM(2026) 11 final.

[39] Consiglio dell'Unione europea, *Una bussola strategica per la sicurezza e la difesa – Per un'Unione europea che protegge i suoi cittadini, i suoi valori e i suoi interessi e contribuisce alla pace e alla sicurezza internazionali*, adottata il 21 marzo 2022.

[40] Comunicazione congiunta al Parlamento europeo e al Consiglio, *La politica di ciberdifesa dell'UE*, JOIN(2022) 49 final.

[41] V. REMONDINO, *L'Unione europea come standard-setter in materia di cybersicurezza nel contesto della sua autonomia strategica aperta,* in *Quaderno AISDUE, Fascicolo V ed. Incontro fra giovani studiosi di diritto UE*, 2025, pp. 1-36.

[42] Direttiva (UE) 2022/2555, cit.

[43] U. JUKNEVIČIŪTĖ, V. MURACHOV, *Navigating the Legal Landscape of Cybersecurity Regulation in Lithuania*, in *Vilnius University Open Series*, 2024, pp. 144-161.

Pur mantenendo un impianto fortemente incentrato sulla gestione dei rischi e sugli obblighi a carico delle entità essenziali e importanti, la nuova disciplina si inserisce in una cornice normativa già influenzata dalla definizione di cybersicurezza introdotta dal *Cybersecurity Act*. In tale quadro, la sicurezza delle reti e dei sistemi informativi non appare più riconducibile esclusivamente alle esigenze di funzionamento del mercato interno, ma tende progressivamente a essere collegata alla protezione degli utenti e delle persone esposte alle minacce digitali.

A questo intervento si aggiungono ulteriori atti normativi complementari, tra cui il regolamento sulla resilienza operativa digitale del settore finanziario (DORA) [44], il regolamento sulla cyber-resilienza[45] e il *Cyber Solidarity Act*[46] del 2025. Nel loro insieme, tali strumenti, inseriti in un contesto di revisione ancora *in fieri* della normativa[47], contribuiscono alla costruzione di una vera e propria architettura normativa multilivello della cybersicurezza europea.

L'espansione del quadro normativo solleva tuttavia anche una questione di ordine costituzionale relativa al rapporto tra l'intervento dell'Unione e la competenza degli Stati membri in materia di sicurezza nazionale. Ai sensi dell'articolo 4, paragrafo 2, TUE, la sicurezza nazionale resta infatti di esclusiva competenza degli Stati membri ed è qualificata come una delle funzioni

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

[45] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828.

[46] Regolamento (UE) 2025/38, cit.

[47] Il 20 gennaio 2026, assieme alla proposta di revisione del regolamento sulla cybersicurezza, la Commissione europea ha presentato una proposta di direttiva che modifica la direttiva (UE) 2022/2555 (NIS 2), inserita nel più ampio pacchetto di revisione del quadro europeo di cybersicurezza. L'intervento mira principalmente a semplificare e rendere più coerente l'attuazione della disciplina vigente, intervenendo su alcuni profili critici emersi nella pratica applicativa. In particolare, la proposta chiarisce l'ambito di applicazione della direttiva, riduce gli oneri di compliance e valorizza il ricorso a strumenti di certificazione per facilitare la dimostrazione della conformità. Al contempo, rafforza il ruolo di ENISA nella cooperazione tra Stati membri e introduce misure di maggiore armonizzazione, anche in relazione alla gestione dei rischi, alla sicurezza delle *supply chain* e alla raccolta di dati sugli attacchi *ransomware*, oltre a promuovere la transizione alla crittografia post-quantistica. Nel complesso, l'iniziativa sembra orientata più a razionalizzare e coordinare il quadro esistente che a introdurre nuovi obblighi sostanziali, confermando una progressiva integrazione della cybersicurezza nelle politiche di sicurezza dell'Unione. Commissione europea, *proposta di direttiva del Parlamento europeo e del Consiglio che modifica la direttiva (UE) 2022/2555 per quanto riguarda le misure di semplificazione e l'allineamento alla [proposta di regolamento sulla cibersicurezza 2],* COM(2026) 13 final.

essenziali dello Stato che l'Unione è tenuta a rispettare. Ciò sembrerebbe, almeno in linea teorica, escludere qualsiasi intervento dell'Unione in ambiti direttamente riconducibili alla sicurezza degli Stati.

Tuttavia, lo sviluppo di un articolato sistema di atti normativi di diritto dell'UE in materia di cybersicurezza dimostra come, nella prassi, la separazione tra dimensione nazionale e dimensione sovranazionale risulti difficilmente tracciabile in modo netto. La giurisprudenza della Corte di giustizia ha infatti chiarito che il richiamo alla sicurezza nazionale non può essere utilizzato dagli Stati membri per sottrarsi agli obblighi derivanti dal diritto dell'Unione[48]. Pur restando ferma l'esistenza di una sfera di competenza primaria degli Stati, la linea di demarcazione tra sicurezza nazionale e intervento dell'Unione appare quindi più flessibile di quanto possa emergere da una lettura meramente formale dei Trattati[49].

In questo scenario si osserva una graduale convergenza tra esigenze di sicurezza nazionale e obiettivi di sicurezza dell'Unione, favorita anche dalla natura transnazionale delle minacce cibernetiche e dalla necessità di risposte coordinate a livello europeo.

In tale evoluzione, la cybersicurezza tende a sottrarsi a una qualificazione meramente tecnica o funzionale, assumendo una rilevanza sistemica nell'ordinamento dell'Unione. Proprio questa trasformazione apre lo spazio per interrogarsi sulla sua possibile qualificazione in termini di posizione giuridica soggettiva, e dunque sulla configurabilità di un vero e proprio diritto alla cybersicurezza.

4. *Verso un diritto alla cybersicurezza?*

Per delineare le caratteristiche di un (per adesso, potenziale) diritto alla cybersicurezza, occorrerebbe innanzitutto considerare quest'ultima come una condizione indispensabile per l'esercizio effettivo di altri diritti, sia nel cyberspazio sia al di fuori di esso. In assenza di un adeguato livello di sicurezza

[48] V. Corte giust. 6 ottobre 2020, C-511/18, C-512/18 e C-520/18, *La Quadrature du Net*, punto 99.

[49] Sul punto v. G. DI FEDERICO, *L'identità nazionale degli Stati membri nel diritto dell'Unione europea: natura e portata dell'art. 4, par. 2, TUE,* Napoli, 2017, p. 156 ss.; B. DE WITTE, *Les compétences exclusives des états membres existent-elles?*, in AA.VV., *Liber amicorum per Antonio Tizzano: de la Cour CECA à la Cour de l'Union: le long parcours de la justice Européenne*, Torino, 2018, p. 301 ss.; F. FERRARO, *Brevi note sulla competenza esclusiva degli Stati membri in materia di sicurezza nazionale*, in *I Post di AISDUE*, I, 2019, pp. 95-115; F. CASOLARI, *Supranational Security and National Security in Light of the EU Strategic Autonomy Doctrine: The EU-Member States Security Nexus Revisited,* in *European Foreign Affairs Review*, 2023, vol. 28, n. 4, p. 339.

delle reti e dei sistemi informativi, diritti quali la libertà di espressione online, la partecipazione politica attraverso strumenti digitali, la protezione dei dati personali e, in taluni casi, perfino la sicurezza fisica degli individui risulterebbero gravemente compromessi. Da questo punto di vista, la cybersicurezza opererebbe (e, in un certo qual senso, già opera) come presupposto funzionale per il godimento di una pluralità di diritti fondamentali.

Tale constatazione, tuttavia, non sarebbe di per sé sufficiente. Affermare semplicemente che la cybersicurezza costituisce un requisito necessario per l'esercizio di altri diritti non comporterebbe un automatico riconoscimento ai singoli di una posizione giuridica autonoma, idonea a proteggerli rispetto ai rischi propri dell'ambiente digitale. È proprio qui che pare emergere l'esigenza di un diritto alla cybersicurezza: non solo perché, in assenza di diritti e obblighi chiaramente configurati, anche le politiche più progressiste potrebbero rischiare di restare affidate alla sola logica della *compliance* e dell'*enforcement* amministrativo, ma soprattutto perché gli individui potrebbero rimanere altrimenti privi di strumenti adeguati a difendere la propria sfera digitale da minacce, interferenze e pregiudizi provenienti da terzi[50].

In questa prospettiva, il riconoscimento di un diritto alla cybersicurezza assolverebbe una duplice funzione. Da un lato, esso trasformerebbe la sicurezza informatica da obiettivo dell'azione pubblica a posizione giuridica azionabile; dall'altro, imporrebbe ai soggetti pubblici e privati un dovere di rispetto della sfera digitale altrui. È proprio la distinzione tra cybersicurezza come prassi e cybersicurezza come stato a rendere più evidente tale passaggio: se la prima riguarda l'insieme delle misure tecniche, organizzative e comportamentali necessarie a prevenire e gestire i rischi, la seconda rinvia alla condizione di sicurezza che i destinatari della tutela devono poter effettivamente godere e mantenere. In assenza di un diritto, questa condizione resta esposta, affidata alla diligenza dei soggetti obbligati e priva di un presidio giuridico direttamente riferibile ai beneficiari della protezione.

Sotto questo profilo, il *Cybersecurity Act* segna un passaggio rilevante ma non conclusivo. Come si è visto, il regolamento adotta una nozione di cybersicurezza più ampia rispetto a quella sottesa alla prima direttiva NIS, includendo non solo la protezione delle reti e dei sistemi informativi, ma anche quella degli utenti e, più in generale, delle persone suscettibili di subire effetti

[50] R. WESSEL, T. NASCIMENTO HEIM, *The Various Dimensions of Cyberthreats: (In)consistencies in the Global Regulation of Cybersecurity,* in *Anales de Derecho,* 2023, pp. 41-65.

pregiudizievoli da minacce informatiche. Ne emerge una nozione non più esclusivamente tecnica, ma più vicina a una logica di tutela della persona. Tuttavia, proprio qui si manifesta il limite dell'assetto vigente: il regolamento lascia intravedere una cybersicurezza come stato, cioè come condizione di protezione da garantire a una platea ampia di soggetti, ma non attribuisce ancora agli individui mezzi giuridici propri per difendere tale condizione quando le attività necessarie a realizzarla risultino inadeguate, omesse o inefficaci.

Si potrebbe obiettare che l'ordinamento già offre tutele attraverso altri settori normativi, come ad esempio la protezione dei dati personali, la proprietà intellettuale, il diritto penale. Ma proprio questo argomento mostra il punto critico, anziché risolverlo. Tali strumenti intervengono solo indirettamente rispetto alla cybersicurezza e tutelano interessi specifici, non la sicurezza della sfera digitale in quanto tale. Alcuni di essi poi operano prevalentemente *ex post*, quando il pregiudizio si è già prodotto, e non colmano la mancanza di una posizione soggettiva riferita alla condizione di sicurezza che l'ordinamento dell'Unione dichiara di voler promuovere. In altri termini, il fatto che altri rami del diritto possano offrire rimedi non elimina il problema della assenza di un diritto alla cybersicurezza propriamente inteso.

In termini più generali, il riconoscimento di un diritto alla cybersicurezza non avrebbe soltanto una funzione protettiva, ma anche una funzione ordinante e responsabilizzante. Esso contribuirebbe infatti a chiarire che la sicurezza digitale non è soltanto un onere di *compliance* per operatori economici e autorità pubbliche, ma anche una pretesa riferibile alle persone. Inoltre, potrebbe incentivare comportamenti di consapevolezza e di autodifesa nello spazio digitale, favorendo pratiche di igiene cibernetica analoghe a quelle che, nel mondo fisico, accompagnano l'idea stessa di sicurezza quotidiana. In questo senso, il diritto alla cybersicurezza non si limiterebbe a rafforzare il sistema dei rimedi, ma parteciperebbe alla costruzione di un modello di responsabilità condivisa tra istituzioni, operatori economici e utenti.

La possibilità di configurare un simile diritto deve tuttavia essere valutata alla luce della struttura delle competenze dell'Unione e dell'evoluzione del quadro normativo europeo in materia di cybersicurezza. Sebbene l'Unione non disponga ancora di una competenza espressa e generale in materia, l'evoluzione del diritto derivato mostra una progressiva espansione della prospettiva di intervento. La direttiva NIS era ancora fortemente ancorata a una concezione funzionale della sicurezza delle reti, connessa al buon funzionamento del mercato interno e rivolta a categorie determinate di

operatori. Il *Cybersecurity Act*, pur mantenendo l'articolo 114 TFUE[51] come base giuridica e conservando un impianto prevalentemente funzionale, ha tuttavia introdotto elementi che consentono di leggere la cybersicurezza in termini più ampi: il rafforzamento del ruolo di ENISA, il quadro europeo di certificazione e, soprattutto, una definizione di cybersicurezza aperta, non circoscritta a una cerchia chiusa di destinatari né a un gruppo limitato di beneficiari. In questa prospettiva, la cybersicurezza tende a essere concepita non più solo come presidio del mercato interno, ma come condizione generale di protezione dell'ecosistema digitale europeo.

In tale evoluzione si intravede un passaggio da una logica centrata sul paradigma della riservatezza, integrità e disponibilità dei sistemi a una logica maggiormente sensibile alla protezione delle persone. Non si tratta ancora di un pieno approccio basato sui diritti, e sarebbe eccessivo sostenere che il regolamento abbia già introdotto un vero diritto soggettivo. Tuttavia, è plausibile ritenere che esso abbia predisposto alcune delle premesse teoriche e normative per una sua futura emersione. Il punto è importante perché potrebbe consentire di sostenere che il diritto alla cybersicurezza non rappresenti una rottura rispetto al quadro vigente, bensì l'esplicitazione di una traiettoria già in atto nel diritto dell'Unione.

Sotto questo profilo, il percorso evolutivo della protezione dei dati personali costituisce un precedente particolarmente significativo[52]. Anche in quel caso, l'originaria disciplina era stata costruita a partire dalla logica del mercato interno, per poi evolvere verso il riconoscimento di una posizione autonoma nella Carta dei diritti fondamentali e di una base giuridica espressa nei Trattati (art. 16 TFUE)[53]. Tale precedente dimostra che, nell'ordinamento giuridico dell'Unione, il processo normativo non è necessariamente lineare: la legislazione derivata può anticipare la configurazione di diritti che trovano solo in un momento successivo piena consacrazione a livello primario. In questa

[51] A. ENGEL, *Licence to Regulate: Article 114 TFEU as Choice of Legal Basis in the Digital Single Market*, in A. ENGEL, X. GROUSSOT, G.T. PETURSSON (eds.), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights*, London, 2024, p. 13; P. DE PASQUALE, *Dalla flessibilità delle basi giuridiche alla normazione integrata: tecniche legislative funzionali alla rigidità del riparto di competenze nell'UE*, in *DUE*, 2025, pp. 43-71; P. DE PASQUALE, O. PALLOTTA, *Art. 114 TFUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, II ed., Milano, 2014, p. 1263.

[52] I. BERZINS, *Cybersecurity and Data Protection in the European Union: The Role of GDPR and the NIS Directive*, 18 febbraio 2025, disponibile al seguente link: ssrn.com/abstract=5142708.

[53] R. DAL POZZO, L. ZOBOLI, *To protect or (not) to protect: definitional complexities concerning personal (and non-personal) data within the EU*, in *EJ*, 2021, pp. 316-322.

chiave, l'articolo 114 TFUE potrebbe ancora costituire, almeno in una fase intermedia, una base giuridica sufficiente per ulteriori sviluppi della disciplina europea della cybersicurezza, senza che sia necessario postulare da subito una riforma dei Trattati che, allo stato attuale, non pare praticabile.

Neppure il tema delle competenze appare, di per sé, insuperabile. Certamente, permangono ambiti sottratti all'intervento dell'Unione, in particolare quelli connessi alla sicurezza nazionale, alla difesa e, in parte, al diritto penale. Ma proprio la protezione dei dati personali mostra come possano coesistere, entro uno stesso quadro normativo, profili rientranti e profili non rientranti nelle competenze dell'Unione. Anche il *Cybersecurity Act*, del resto, preserva espressamente le competenze degli Stati membri in tali materie[54]. Ne consegue che l'emersione di un diritto alla cybersicurezza non dovrebbe essere intesa come attribuzione all'Unione di una competenza generale sulla sicurezza in senso ampio, ma piuttosto come consolidamento di una posizione giuridica riferita alla dimensione civile e digitale della protezione, entro i limiti già tracciati dall'ordinamento dell'Unione.

L'affermazione di un potenziale diritto alla cybersicurezza non potrebbe tuttavia prescindere dalla sua interazione con altri diritti fondamentali già riconosciuti nell'ordinamento dell'Unione. In tale prospettiva, particolare rilievo assume il diritto alla libertà e alla sicurezza sancito dall'articolo 6 della Carta, quale principale riferimento normativo per la protezione dell'individuo rispetto a minacce che, pur tradizionalmente riferite alla dimensione fisica, sussistono oggi anche nello spazio digitale.

Proprio con riferimento a questa disposizione si pone la questione se l'ordinamento dell'Unione necessiti effettivamente di un nuovo diritto fondamentale alla cybersicurezza, ovvero se una modifica del diritto generale alla sicurezza già riconosciuto o una sua interpretazione estensiva, tale da ampliarne l'ambito applicativo alla sfera digitale, non siano già sufficienti a ricomprendere le sfide poste dalla trasformazione tecnologica.

Una prima linea argomentativa, valorizzata anche a livello istituzionale, depone in favore di questa seconda opzione. Nella Strategia europea per la cybersicurezza per il decennio digitale, la Commissione afferma espressamente che la cybersicurezza costituisce parte integrante della sicurezza dei cittadini europei[55]. In questo senso, il diritto alla sicurezza potrebbe essere letto in chiave evolutiva, come comprensivo anche della dimensione cibernetica, alla luce

[54] Art. 1, par. 2; art. 3, par. 3.

[55] Comunicazione congiunta al Parlamento europeo, al Consiglio europeo, al Consiglio, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, JOIN(2020)18 final, p. 1.

dello sviluppo delle politiche dell'Unione in materia e della crescente rilevanza della sicurezza digitale per la protezione delle persone. Tale impostazione si inserisce in un più ampio paradigma di equivalenza normativa, secondo cui i diritti fondamentali tradizionali sarebbero in grado di assorbire anche le sfide poste dall'ambiente digitale[56].

Questa lettura trova un ulteriore supporto nell'evoluzione dell'azione normativa dell'Unione, sempre più orientata al rafforzamento della propria autonomia strategica nel dominio digitale[57]. In tale contesto, la crescente attenzione alla protezione di infrastrutture, dati e servizi essenziali contribuisce a ridefinire la nozione stessa di sicurezza, estendendola oltre la dimensione fisica. Ne consegue che, pur in una logica complementare rispetto agli Stati membri ma nell'ottica del principio di leale cooperazione[58], l'intervento dell'Unione potrebbe apparire idoneo a incidere anche sul contenuto del diritto alla sicurezza, includendovi progressivamente la protezione nello spazio cibernetico.

Tuttavia, tale ricostruzione incontra limiti rilevanti. Sotto il profilo sistemico, essa presuppone una sostanziale continuità tra sicurezza e cybersicurezza, che appare solo parzialmente convincente. Pur essendo vero che le trasformazioni tecnologiche tendono a sfumare i confini tra dimensione digitale e dimensione fisica, le minacce informatiche presentano caratteristiche peculiari, tanto sul piano tecnico quanto su quello normativo, che non trovano un immediato corrispettivo nelle forme tradizionali di tutela della sicurezza personale.

Sotto il profilo strettamente giuridico, poi, l'ipotesi di un'estensione dell'articolo 6 incontra un limite significativo nella sua connessione con l'articolo 5 della Convenzione europea dei diritti dell'uomo, di cui, come precisato nelle Spiegazioni della Carta, riproduce contenuto e portata. Come chiarito dalla giurisprudenza della Corte europea dei diritti dell'uomo[59], tale

---

[56] V. PAPAKONSTANTINOU, *op. cit.,* p. 7.

[57] Il termine sovranità strategica è presente nel vocabolario dell'Unione a partire dal 2017, quando il presidente francese Macron, in un discorso all'Università Sorbona di Parigi, sottolineò la necessità di costruire una "Europa sovrana". Da allora, il concetto si è notoriamente diffuso, anche a livello istituzionale e dottrinale. Si v. a titolo di esempio la comunicazione della Commissione europea del 29 gennaio 2020, intitolata *Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE,* COM(2020) 50 final; F. HOFFMEISTER, *Strategic Autonomy in the European Union's External Relations Law*, in *CMLR*, 2023, pp. 667-700; Editorial Comments, *Keeping Europeanisation at Bay? Strategic Autonomy as a Constitutional Problem*, in *CMLR*, 2022, pp. 319–321.

[58] F. CASOLARI, *op. cit.,* p. 338.

[59] European Court of Human Rights, *Guide on Article 5 of the European Convention on Human Rights: Right to Liberty and Security*, aggiornata il 31 agosto 2025,

disposizione è finalizzata alla tutela della libertà fisica della persona e non appare, allo stato attuale, suscettibile di essere interpretata nel senso di includere la protezione dalle minacce informatiche.

A ciò si aggiunge un ulteriore elemento di complessità, emerso anche nella giurisprudenza della Corte di giustizia. Le pronunce relative all'articolo 6 della Carta, seppur ancora limitate[60], si collocano prevalentemente in contesti in cui la sicurezza è declinata come interesse generale, in particolare con riferimento alla lotta al terrorismo e alla criminalità grave[61]. Pur essendo formalmente configurato come diritto individuale, esso viene dunque in concreto mobilitato in una dimensione funzionalmente orientata alla tutela della collettività. Ne deriva una tensione tra la dimensione soggettiva del diritto e la sua funzione sistemica di garanzia della sicurezza pubblica.

In questo quadro, l'interpretazione dell'articolo 6 della Carta come comprensivo della cybersicurezza, pur non essendo priva di fondamento, rischia di non offrire una tutela sufficientemente determinata e mirata rispetto alle specifiche esigenze di protezione che emergono nello spazio digitale.

Tale limite emerge con maggiore evidenza ove si consideri il più ampio intreccio tra cybersicurezza e altri diritti fondamentali. La sicurezza informatica si collega infatti in modo diretto al diritto al rispetto della vita privata e familiare, al diritto alla protezione dei dati personali e alla libertà di espressione e di informazione. La sicurezza delle reti e dei sistemi informativi costituisce una condizione essenziale affinché tali diritti possano essere esercitati in ambiente digitale, ma le misure adottate in nome della cybersicurezza possono al contempo incidere su di essi, rendendo necessario un costante bilanciamento[62].

Ne deriva che la cybersicurezza si configura come uno spazio di intersezione tra più diritti fondamentali, rispetto al quale l'articolo 6 della Carta, pur rilevante, non appare di per sé sufficiente a ricomprendere l'intero spettro delle esigenze di tutela coinvolte. In questo senso, la Carta svolge indubbiamente una funzione interpretativa centrale, offrendo, attraverso la

---

ks.echr.coe.int/documents/d/echr-ks/guide_art_5_eng; Corte EDU 23 febbraio 2017, ric. n. 43395/09, *De Tommaso/Italia*, punto 80; 23 febbraio 2012, ric. n. 29226/03, *Creanga/Romania,* punto 92; 18 marzo 2008, ric. n. 11036/03, *Ladent/Polonia*, punti 45 e 46; 8 giugno 1976, ricc. nn. 5100/71, 5101/71, 5102/71, 5354/71 e 5370/71, *Engel e a./Paesi Bassi*, punto 58.

[60] Alcune delle più recenti e rilevanti ai fini della presente analisi: Corte giust. 4 settembre 2025, C-313/25 PPU, *Adrar,* punto 76; *La Quadrature du Net,* cit., punto 123.

[61] Corte giust. 8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland,* punto 42.

[62] M. LOI, M. CHRISTEN, *Ethical Frameworks for Cybersecurity*, in *The International library of ethics, law and technology*, Berlin, 2020, p. 73; J. ODERMATT, *op. cit.*

combinazione degli articoli 6, 7 e 8, un terreno normativo e assiologico idoneo a sostenere la possibile emersione di una posizione giuridica più specificamente riferita alla cybersicurezza. A ciò si aggiunge, in un orizzonte più programmatico ma non irrilevante, la Dichiarazione europea sui diritti e i principi digitali per il decennio digitale[63], che valorizza l'idea di un ambiente digitale sicuro e affidabile e richiama l'esigenza che tecnologie, prodotti e servizi digitali siano progettati in modo da garantire elevati livelli di sicurezza e tutela della vita privata. Pur priva di effetti vincolanti, essa segnala un'evoluzione del lessico e delle priorità delle istituzioni dell'Unione, sempre più attente alla dimensione soggettiva della sicurezza digitale e alla distribuzione delle responsabilità lungo l'intera catena del valore delle tecnologie digitali.

Occorre, tuttavia, tenere fermo il limite strutturale posto dall'articolo 6, paragrafo 1, TUE: la Carta non può estendere le competenze dell'Unione oltre quelle attribuite dai Trattati. Il riconoscimento di un nuovo diritto fondamentale non sarebbe di per sè sufficiente a fondare un'autonoma capacità normativa generale dell'Unione in materia di cybersicurezza, ma andrebbe piuttosto collocato nel più ampio processo di progressiva costituzionalizzazione della materia[64].

5. *Osservazioni conclusive*

L'analisi svolta consente di cogliere come la cybersicurezza stia assumendo una funzione che eccede la sua originaria configurazione tecnica, collocandosi all'intersezione tra esigenze di gestione del rischio e tutela della persona nello spazio digitale.

In questo contesto, il profilo più significativo non riguarda tanto il riconoscimento formale di un diritto alla cybersicurezza, quanto il mutamento del modo in cui la sicurezza digitale viene giuridicamente concepita. L'evoluzione del diritto derivato mostra infatti una apertura verso una lettura che, pur restando legata al funzionamento del mercato interno, tende a includere in modo sempre più esplicito la protezione delle persone tra le finalità dell'azione normativa.

[63] Commissione europea, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, COM(2022) 28 final; P. DE PASQUALE, *Verso una Carta dei diritti digitali (fondamentali) dell'Unione europea?*, in *DUE,* 2022, pp. 1-15.
[64] V. F. CASOLARI, F. FERRI, S. VILLANI, *op. cit.*

Ciò non consente ancora di configurare un diritto soggettivo pienamente definito né di individuare una posizione giuridica immediatamente azionabile in capo agli individui. Tuttavia, limitarsi a qualificare tale evoluzione come un'estensione delle politiche esistenti rischierebbe di non coglierne appieno la portata. Piuttosto, essa sembra indicare l'emergere di una diversa impostazione della sicurezza digitale, nella quale obblighi, standard e meccanismi di coordinamento vengono progressivamente riletti anche alla luce della loro incidenza sulla sfera giuridica degli individui. Le più recenti iniziative della Commissione [65], pur muovendosi dichiaratamente nella direzione della semplificazione e dell'efficienza del quadro normativo, confermano al contempo la centralità crescente della cybersicurezza nell'assetto economico e istituzionale dell'Unione, con ricadute che si proiettano, seppur indirettamente, anche sulla tutela delle persone.

In questa prospettiva, il processo di valorizzazione della protezione dei dati personali assume un valore paradigmatico. Esso mostra come, nell'ordinamento dell'Unione, il riconoscimento di nuove posizioni giuridiche possa essere preceduto da un graduale consolidamento normativo, nel quale strumenti di regolazione e principi interpretativi preparano il terreno a possibili sviluppi ulteriori.

Resta, naturalmente, il limite posto dal principio di attribuzione e dalla conseguente centralità degli Stati membri nei settori più direttamente connessi alla sicurezza nazionale. Ciò nondimeno, l'evoluzione del quadro normativo evidenzia come lo spazio di intervento dell'Unione nella dimensione organizzativa ed economica della sicurezza digitale si sia via via ampliato, rendendo meno netta la distinzione tra sicurezza come prerogativa statale e sicurezza come oggetto di regolazione sovranazionale.

È probabilmente su questo terreno che si giocheranno gli sviluppi futuri della disciplina, in un contesto nel quale la sicurezza digitale non può essere intesa come una alternativa alla libertà, bensì come una delle condizioni attraverso cui essa prende forma. In questo scenario, la riflessione sul possibile riconoscimento di un diritto alla cybersicurezza appare meno come un esercizio teorico e più come un tentativo di dare forma giuridica a trasformazioni già in atto nell'ordinamento dell'Unione.

[65] Il riferimento è alle proposte di modifica del Regolamento sulla cybersicurezza e della direttiva NIS 2 presentate dalla Commissione il 20 gennaio scorso (si rimanda alle note nn. 37 e 46 del presente contributo).

ABSTRACT (ita)

Il contributo esamina il ruolo della cybersicurezza nell'ordinamento dell'Unione europea, interrogandosi se essa debba essere intesa come mero obiettivo funzionale al mercato interno o se i più recenti interventi normativi consentano di intravedere l'emersione di una posizione giuridica autonoma. A partire dalla distinzione tra cybersicurezza come prassi e come stato, l'analisi evidenzia come il diritto dell'Unione resti ancorato a una logica di gestione del rischio, ma al tempo stesso manifesti una crescente attenzione verso la tutela delle persone nello spazio digitale. Pur in assenza di un diritto soggettivo pienamente definito, tali dinamiche non segnano ancora un vero mutamento di paradigma, ma riflettono una trasformazione nel modo in cui la cybersicurezza viene concepita, con effetti sempre più rilevanti sulla sfera giuridica degli individui.

ABSTRACT (eng)

This article examines the role of cybersecurity within the European Union legal order, asking whether it should be understood merely as a regulatory objective serving the internal market or whether recent legislative developments allow for the emergence of an autonomous legal position. Building on the distinction between cybersecurity as practice and as state, the analysis shows that EU law remains largely grounded in a risk management logic, while at the same time displaying an increasing concern for the protection of individuals in the digital environment. Although a fully-fledged subjective right has not yet emerged, these developments do not amount to a genuine paradigm shift, but rather reflect a transformation in the way cybersecurity is conceived, with increasingly significant implications for the legal sphere of individuals.