

1/2026 anteprima

Rivista di diritto dei media

ISSN 2532-9146

La *governance* della cibernsicurezza nell'era digitale: una rilettura costituzionale globale*

Omar Caramaschi

Sommario

1. Premessa: la cibernsicurezza nello spazio cibernetico – 2. Il ruolo dell'Unione europea nell'ambito della sicurezza digitale – 3. La dimensione internazionale della cibernsicurezza – 4. È possibile una *governance* (costituzionale) globale della cibernsicurezza?

1. Premessa: la cibernsicurezza nello spazio cibernetico

La digitalizzazione globale e la sempre maggiore interconnessione digitale hanno determinato l'avvio di una serie di processi e di cambiamenti riguardanti anche la dimensione costituzionale degli ordinamenti giuridici, non solo interessando le dinamiche organizzative degli apparati statali, ma toccando più nel profondo la tutela e la garanzia dei diritti fondamentali, i quali sempre più spesso si trovano esposti a rischi – come gli attacchi cibernetici – provenienti proprio dal mondo digitale e dal cibernspazio¹.

Viene così in evidenza la sicurezza cibernetica, la quale ha visto una rapida sostituzione semantica di espressioni più tecniche e legate alla natura informatica del tema quali “computer security” o “information security” da parte di quella, oggi sicuramente predominante, di “cybersecurity”² (o,

* Questo lavoro è stato finanziato dal progetto NextGenerationEU “Security and Rights in CyberSpace” (SERICS). L'articolo costituisce una versione ampliata e rivista della relazione presentata alla VI Conferenza italiana di ICON-S (Cagliari 3-4 ottobre 2025).

¹ Cfr. A. Venanzoni, *L'ordine costituzionale della cybersecurity*, in *Forum di Quaderni Costituzionali*, 4, 2024, 34; R. Ursi, *La sicurezza cibernetica come funzione pubblica*, in Id. (a cura di), *La sicurezza nel cibernspazio*, Milano, 2023, 9 ss.

² Su tale espansione cfr. R. Brighi - P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, in *Federalismi.it*, 21, 2021, spec. 20, i quali richiamano lo studio di M. Veale - I. Brown, *Cybersecurity*, in *Internet Policy Review*, 9, 2020, dal quale emerge come “cybersecurity” risulti essere il concetto più diffuso sia nelle pubblicazioni accademiche sia in diversi ambiti come l'ingegneria, le relazioni internazionali e la sicurezza pubblica, in ciò avendo superato termini decisamente più tecnici come “computer security”, “system security” o “information security”. R. Brighi - P.G. Chiara, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, cit., spec. 19, osservano inoltre come l'espressione “computer security” faccia riferimento «a una visione originaria

come nel prosieguo, cibersicurezza), nella quale il concetto di sicurezza informatica come protezione delle reti e dei sistemi informatici digitali allarga considerevolmente il proprio perimetro di significato. Sicché tale concetto si è evoluto – e continuerà a farlo in ragione della rapida mutabilità del contesto informatico-digitale – pur senza giungere ad una nozione condivisa dalle istituzioni e dalla dottrina giuridica³.

Un contributo fondamentale è stato quello dell'Unione europea, la quale, in diversi atti che vedremo nel prosieguo, ha fortemente determinato un ampliamento concettuale della definizione di cibersicurezza fino ad arrivare a ricomprendere le «attività necessarie per proteggere i sistemi di rete e di informazione, gli utenti di tali sistemi e le altre persone interessate dalle minacce informatiche»⁴. In questa direzione, quindi, parrebbe individuarsi un'evoluzione della stessa cibersicurezza da sicurezza informatica di reti e sistemi digitali a strumento di tutela dell'ordine costituzionale come preconditione essenziale per garantire non solo l'ordinata convivenza, e quindi la sopravvivenza di qualsiasi ordinamento giuridico⁵, proprio attraverso «la riaffermazione ordinamentale della sicurezza digitale»⁶, ma anche – così come vale in generale per tutto ciò che avviene nel ciberspazio – in qualità di elemento fondamentale per il godimento dei diritti fondamentali dell'uomo⁷.

di sicurezza informatica intesa come protezione del computer o, più in generale, del sistema informatico, dei suoi apparati, dei programmi informatici, delle infrastrutture e dei dati elaborati e trasmessi. Successivamente, nella “società dei dati”, si è approdati a un concetto di sicurezza maggiormente orientato alla protezione delle informazioni, la c.d. *information security*».

³ In dottrina v. *ex multis* G. D'Angelo - G. Giacomello, *Cybersicurezza*, Bologna, 2023; G. Ziccardi, *La cybersecurity nel quadro tecnologico (e politico) attuale*, in G. Ziccardi - P. Perri (a cura di), *Tecnologia e diritto*, Milano, 2019, 207 ss.; M.A. Rizzi - F. Serini, *Una proposta di studio dei concetti di cibersicurezza e cyberresilienza in senso giuridico tra ordinamento europeo e italiano*, in *Rivista italiana di informatica e diritto*, 2, 2024, 115-136; T. Stevens, *Global Cybersecurity: New Directions in Theory and Methods*, in *Politics and Governance*, 2, 2018; C. Lotta, *Governance della rete, accesso a Internet e cibersicurezza*, Napoli, 2024.

⁴ Art. 2, regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»). In maniera analoga il legislatore italiano con il decreto-legge 14 giugno 2021, n. 82 (Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale), come convertito dalla legge 4 agosto 2021, n. 109, il quale definisce la cibersicurezza come «l'insieme delle attività [...] necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico» (art. 1, c. 1, lett. a).

⁵ Cfr. M. Matassa, *La regolazione della cybersecurity in Italia*, in R. Ursi (a cura di), *La sicurezza nel ciberspazio*, cit., spec. 21.

⁶ Cfr. A. Venanzoni, *L'ordine costituzionale della cybersecurity*, cit., 35-36.

⁷ Cfr. L. Moroni, *La governance della cybersecurity a livello interno ed europeo: un quadro intricato*, in *Federalismi.it*, 14, 2024, 179, secondo il quale «tutelare la sicurezza nel ciberspazio è oramai indispensabile per garantire il pieno godimento dei diritti fondamentali nella realtà virtuale», come, ad esempio, la libertà di manifestazione del pensiero, l'identità personale,

La cibersecurity non riguarda più soltanto le minacce provenienti dalla dimensione fisica, ma allarga il proprio orizzonte di riferimento includendo quelle del mondo virtuale del ciber spazio⁸; in questo modo, viene meno la distinzione tra sicurezza esterna ed interna⁹, in ragione del fatto che le minacce alla cibersecurity possono provenire da un numero inesauribile di fonti diverse, quindi, per esempio, da attori pubblici come altri Stati ovvero da privati come imprese, società e finanche persone fisiche dotate degli strumenti e delle capacità tecniche adeguate indipendentemente dalla loro residenza fisica e territoriale¹⁰.

Proprio per queste ragioni la cibersecurity assume una portata trasversale, interessando i singoli individui, le imprese, la società nel suo complesso, ma anche gli Stati e gli organismi sovranazionali e internazionali¹¹. Ed è proprio a questi ultimi livelli che la cibersecurity richiede un'azione istituzionale e regolativa opportunamente in grado di rispondere alle sfide e alle minacce provenienti dallo spazio cibernetico e dal mondo digitale. Sebbene la risposta a tali nuovi elementi problematici dovrebbe partire proprio dagli Stati e dagli strumenti costituzionali a loro disposizione¹², non può non osservarsi come i singoli Stati siano difficilmente in grado di garantire le condizioni essenziali per la "sicurezza dei diritti"¹³ dei cittadini nella dimensione del ciber spazio, essendo invece necessario rispondere alle sfide globali derivanti per la cibersecurity con forme di cooperazione sovrastatali e altrettanto globali al fine di rendere consistente la sicurezza nello spazio cibernetico ed effettiva la tutela dei diritti fondamentali anche nel nuovo mondo digitale¹⁴. Sicché viene così in evidenza l'obiettivo che si intende perseguire in questa sede, vale a dire quello di fornire un contributo che indaghi la portata globale della cibersecurity, partendo dal livello eurounitario per muovere verso quello internazionale e globale, con particolare riguardo alle relative forme di regolazione e specialmente alla possibilità di sviluppare modelli di *governance* costituzionale della cibersecurity di portata globale, mantenendo tuttavia una prospettiva di analisi e un metodo di ricerca propri del diritto costituzionale e del costituzionalismo, in una sorta di rilettura della cibersecurity attraverso le lenti del

la libertà del voto ovvero la riservatezza e il diritto all'immagine.

⁸ Cfr. S. Savaş - S. Karataş, *Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance*, in *International Cybersecurity Law Review*, 3, 2022, 11-12; secondo S.A. Salvaggio - N. González, *The European framework for cybersecurity: strong assets, intricate history*, in *International Cybersecurity Law Review*, 4, 2023, 142, «[t]he realms of cybersecurity and traditional security have been merged into one».

⁹ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, in *Global Constitutionalism*, 1, 2018, 112 ss., spec. 117.

¹⁰ Cfr. L. Moroni, *La governance della cybersecurity a livello interno ed europeo: un quadro intricato*, cit., 182-183.

¹¹ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 117.

¹² Cfr. L. Moroni, *La governance della cybersecurity a livello interno ed europeo: un quadro intricato*, cit., 185-186.

¹³ Su questa particolare e condivisibile concezione v. per tutti M. Rutolo, *Sicurezza, dignità e lotta alla povertà. Dal "diritto alla sicurezza" alla "sicurezza dei diritti"*, Napoli, 2012.

¹⁴ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 117; L. Moroni, *La governance della cybersecurity a livello interno ed europeo: un quadro intricato*, cit., 186.

costituzionalismo globale.

2. Il ruolo dell'Unione europea nell'ambito della sicurezza digitale

Come si diceva poc'anzi, le sfide multidimensionali poste dalla cibersicurezza non possono essere affrontate dai singoli Stati, proprio per la natura globale e reticolare della sicurezza digitale e informatica (nonché delle minacce per la stessa), ma richiedono necessariamente il protagonismo degli organismi sovranazionali e, come vedremo, internazionali e globali.

Se vogliamo procedere in via incrementale, e anche secondo una modalità di analisi cronologicamente coerente, occorre muovere dalla posizione dell'Unione europea, che negli ultimi anni ha ricoperto un ruolo determinante nel panorama normativo¹⁵, di fatto occupandosi della sicurezza digitale nel suo essere «ambito trasversale»¹⁶ e coordinando la disciplina della cibersicurezza con la regolazione di altri ambiti che, in particolare, avendo come strumento comune quello della Rete, si collegano più o meno direttamente ad essa come la protezione dei dati personali, il mercato digitale o l'intelligenza artificiale¹⁷.

Proprio al fine di rendere effettiva la tutela dei diritti fondamentali anche nello spazio cibernetico attraverso forme adeguate di cibersicurezza, pare necessario indagare quali strumenti siano stati approntati dall'Unione europea e dagli Stati membri al fine di disegnare una *governance* della cibersicurezza in grado di assolvere a tali compiti; in questa direzione troviamo numerosi atti europei che verranno ora passati in rassegna con l'intento di meglio ricostruire l'architettura istituzionale europea della sicurezza informatica e digitale.

I primi atti europei strategici e di indirizzo, sostanzialmente di *soft law* e in qualche modo collegati con la cibersicurezza, fanno la loro comparsa all'inizio degli anni 2000¹⁸, laddove viene offerta una panoramica genera-

¹⁵ Secondo F. Pizzetti, *Introduzione alla regolazione europea della società digitale*, in Aa. Vv., *La regolazione europea della società digitale*, Torino, 2024, 4, ciò avrebbe determinato un'espansione globale dell'azione dell'Unione europea, in maniera analoga a quanto avvenuto in materia di dati personale con il GDPR o potrebbe avvenire, secondo alcuni, con l'AI Act, nella logica del cd. effetto Bruxelles (sul punto v. A. Bradford, *The Brussel Effect. How the European Union Rules the World*, Oxford, 2020). Sul punto v. anche Z. Bederna - Z. Rajnai, *Analysis of the cybersecurity ecosystem in the European Union*, in *International Cybersecurity Law Review*, 2, 2022, 35 ss.; G. Cassano - M. Iaselli - G. Spangher, *Cybersecurity: contesto normativo di riferimento a livello nazionale ed europeo*, in *Diritto di internet*, 4, 2022, 637 ss.

¹⁶ D. Marrani, *Il coordinamento delle politiche per la cybersecurity dell'UE nello spazio di libertà, sicurezza e giustizia*, in *Freedom, Security & Justice: European Legal Studies*, 1, 2021, spec. 80.

¹⁷ Cfr. G. Barozzi Reggiani, *La race for the cyberspace degli Stati e il tema della cybersecurity: tra sovranità e modelli di governance*, in *Rivista italiana di informatica e diritto*, 2, 2025, spec. 12. Si pensi quindi al GDPR, al Digital Markets Act, al Digital Services Act ovvero all'AI Act, collegati anche da un comune approccio di natura costituzionale come osservato da O. Caramaschi, *Il costituzionalismo al cospetto dell'intelligenza artificiale: nuove sfide, quali soluzioni?*, in *Rivista italiana di informatica e diritto*, 1, 2025, 29-51.

¹⁸ Si pensi alla Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni - Creare una società

le delle principali minacce provenienti dallo spazio cibernetico, tuttavia il termine cibernsicurezza – o meglio “cybersecurity” – verrà impiegato ufficialmente solo qualche anno più tardi nella relazione pubblicata nel 2008 sull’implementazione della “Strategia europea in materia di sicurezza” del 2003¹⁹.

In questa prima fase la legislazione europea si segnala per la creazione da parte del regolamento (CE) 2004/460 dell’Agenzia europea per la sicurezza delle reti e dell’informazione (meglio nota con l’acronimo “ENISA” da European Network and Information Security Agency)²⁰, con lo scopo di garantire un alto ed efficace livello di sicurezza delle reti e dell’informazione nell’ambito della Comunità europea²¹. Questa struttura – oggi ridenominata Agenzia dell’Unione europea per la cibernsicurezza – ha ricoperto un ruolo più formale che sostanziale, fino all’approvazione della Strategia europea per la cibernsicurezza del 7 febbraio 2013²², che ha dato

dell’informazione sicura migliorando la sicurezza delle infrastrutture dell’informazione e mediante la lotta alla criminalità informatica del 26 gennaio 2001, [COM\(2000\) 890 def.](#), nonché alla Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale e al Comitato delle regioni - Sicurezza delle reti e sicurezza dell’informazione: proposta di un approccio strategico europeo del 6 giugno 2001, [COM \(2001\) 298 def.](#), laddove la sicurezza delle reti e dell’informazione viene identificata «come la capacità di una rete o di un sistema d’informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisi o atti dolosi che compromettono la disponibilità, l’autenticità, l’integrità e la riservatezza dei dati conservati o trasmessi e dei servizi forniti o accessibili tramite la suddetta rete o sistema» (par. III).

¹⁹ Consiglio dell’Unione europea, Relazione sull’attuazione della strategia europea in materia di sicurezza. Garantire sicurezza in un mondo in piena evoluzione ([S407/08](#)), 11 dicembre 2008.

²⁰ Su questa prima fase anteriore al 2013 v. in particolare in dottrina B. Bruno, *Cybersecurity tra legislazioni, interessi nazionali e mercato: il complesso equilibrio tra velocità, competitività e diritti individuali*, in *Federalismi.it*, 14, 2020, 11-45; E. Longo, *La disciplina della cibernsicurezza nell’Unione europea e in Italia*, in Aa. Vv., *La regolazione europea della società digitale*, cit., 209 ss.

²¹ [Regolamento \(CE\) 2004/460](#) del Parlamento europeo e del Consiglio del 10 marzo 2004, che istituisce l’Agenzia europea per la sicurezza delle reti e dell’informazione; art. 1.1.

²² Comunicazione congiunta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Strategia dell’Unione europea per la cibernsicurezza: un ciberspazio aperto e sicuro, [JOIN/2013/01 final](#). Sulla Strategia il Parlamento europeo ha adottato la Risoluzione del 12 settembre 2013 sulla strategia dell’Unione europea per la cibernsicurezza: un ciberspazio aperto e sicuro ([2013/2606\(RSP\)](#)), nella quale il Parlamento europeo, condividendo il contenuto della Strategia, formula alcune indicazioni; in particolare «sottolinea la necessità di sviluppare una politica di comunicazione strategica in materia di cibernsicurezza nell’UE, situazioni di crisi cibernetica, revisioni strategiche, collaborazione pubblico-privato e segnalazioni, nonché raccomandazioni destinate al pubblico» (punto 3) e «invita nuovamente gli Stati membri ad adottare, senza indebito ritardo, strategie nazionali per la cibernsicurezza che coprano gli aspetti tecnici e quelli relativi al coordinamento, alle risorse umane e alla dotazione finanziaria e comprendano regole specifiche sui benefici e le responsabilità del settore privato, al fine di garantire la partecipazione di quest’ultimo, nonché a prevedere procedure complete per la gestione del rischio e a salvaguardare il quadro normativo» (punto 5).

In particolare, a seguito della Strategia per la cibernsicurezza, è stato approvato il [regolamento \(UE\) n. 526/2013](#) del Parlamento europeo e del Consiglio del 21 maggio 2013 relativo all’Agenzia dell’Unione europea per la sicurezza delle reti e dell’informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004.

nuovo impulso all'approccio europeo alla sicurezza digitale²³, delineando una visione europea in materia di cibersicurezza sempre più articolata, con una particolare e mirata attenzione alla tutela dei diritti fondamentali e della privacy da perseguirsi attraverso una nuova *governance* multilivello e *multistakeholder* in grado di coniugare democraticità, efficienza e responsabilità condivisa dei vari attori coinvolti, altresì proponendo alcuni strumenti pratici per poter raggiungere gli obiettivi posti in tema di sicurezza cibernetica²⁴.

Inizia così a prospettarsi l'impegno delle istituzioni europee quanto alla necessità di regolazione del ciberspazio al fine di tutelare i diritti fondamentali e i valori basilari per l'ordinamento giuridico europeo, non solo mostrandosi in ciò già ben consapevoli della pluralità di soggetti, pubblici e (sempre più) privati, coinvolti nel funzionamento dello spazio cibernetico, ma anche nell'evidenziare l'importanza della dimensione internazionale della cibersicurezza attraverso un nuovo ruolo per la diplomazia internazionale²⁵, la quale a sua volta contribuirebbe a formare una politica estera dell'Unione europea più coesa in materia di ciberspazio, volta a promuovere i valori europei fondamentali²⁶.

Sulla base di questa prima strategia europea sulla cibersicurezza viene approvata nel 2016 la Direttiva (UE) 2016/1148, cd. Direttiva NIS (Network and Information Security)²⁷ con la finalità di raggiungere un elevato livello comune di sicurezza delle reti e dei sistemi informativi, in particolare attraverso il conseguimento di un livello minimo di cibersicurezza in ciascuno

²³ Secondo G. Borriello - G. Fristachi, *Stato (d'assedio) digitale e strategia italiana di cibersicurezza*, in *Rivista di Digital Politics*, 1-2, 2022, 162, il 2013 rappresenta «l'anno spartiacque in termini di avanzamento cibernetico a livello comunitario».

²⁴ Cfr. C. Cencetti, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, in *Quaderni LAI*, 2014, 35 ss.

²⁵ Cfr. E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, in *Rivista AIC*, 4, 2022, 7.

²⁶ La Strategia prevede, a tal proposito, che l'Alto rappresentante si occupi, insieme agli Stati membri e all'Agenzia europea per la difesa, di «curare il dialogo con i partner internazionali, in particolare la NATO, con altre organizzazioni internazionali e centri di eccellenza multinazionali, per garantire capacità efficaci di difesa, individuare settori di cooperazione ed evitare duplicazioni degli sforzi» (punto 2.3); inoltre l'Unione europea è chiamata «ad elaborare una politica internazionale dell'UE in materia di ciberspazio coerente e mirante ad aumentare l'impegno e a intensificare le relazioni con i principali partner e le principali organizzazioni internazionali [...] come il Consiglio d'Europa, l'OCSE, le Nazioni Unite, l'OSCE, la NATO, l'UA, l'ASEAN e l'OSA» (punto 2.5).

Inoltre, come ricorda E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, cit., 7, lo studio della Commissione europea *International Cyber Capacity Building: Global Trends and Scenarios*, pubblicato il 23 settembre 2021 dallo EU Institute for Security Studies, avrebbe evidenziato come tra le capacità fondamentali di cui uno Stato necessita per godere di una discreta sicurezza cibernetica ci sia una tendenza favorevole verso quelle legate alle relazioni internazionali nel ciberspazio, inclusa «*the capacity to develop and act upon an understanding of how international law applies in cyberspace, norms of responsible state behaviour and confidence building measures*», nonché quella «*to engage in the international cyber diplomacy around these issues, for example in the UN Open-Ended Working Group and UN Group of Government Experts*» (sul punto v. *infra*).

²⁷ 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.

Stato membro. Come esplicitato anche dal successivo regolamento di esecuzione (UE) 2018/151²⁸, lo scopo era il coinvolgimento di tutti gli attori (sia pubblici sia privati) interessati all'elaborazione delle strategie europea e nazionali per la cibersicurezza, nonché, specialmente attraverso la cooperazione a livello nazionale, al conseguimento della “resilienza cibernetica” nell'intero territorio europeo, in modo da tutelare tanto il mercato unico europeo quanto i diritti fondamentali dei cittadini²⁹.

Tale prospettiva di risultato richiedeva il coinvolgimento dei principali soggetti destinatari della normativa europea, in particolar modo degli Stati ai quali venivano affidati diversi obblighi tra i quali quello di elaborare strategie nazionali in materia di cibersicurezza – sulla base di contenuti minimi indicati dalla Direttiva NIS, in una precisa logica di armonizzazione a livello europeo – le quali dovevano non solo determinare obiettivi e priorità della strategia nazionali, ma anche definire «un quadro di *governance* per conseguire gli obiettivi e le priorità della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi, inclusi i ruoli e le responsabilità degli organismi pubblici e degli altri attori pertinenti»³⁰; quello di designare una o più autorità nazionali responsabili della sicurezza delle reti e dei sistemi informativi (cd. Autorità NIS) al fine di controllare l'applicazione della Direttiva a livello nazionale³¹; nonché, infine, l'istituzione di gruppi di intervento per la sicurezza informatica in caso di incidenti informatici (cd. CSIRT, ossia *Computer Security Incident Response Team*)³².

Anche sulla base di questi sviluppi normativi si è giunti all'adozione della seconda Strategia in materia di cibersicurezza³³, nella quale si anticipava la necessità di riformare l'ENISA – che fino a quel momento aveva rappresentato uno dei principali sforzi dell'Unione europea per istituzionalizzare il processo legislativo in materia di cibersicurezza³⁴ – come poi effettiva-

²⁸ Regolamento di esecuzione (UE) 2018/151 della Commissione del 30 gennaio 2018 recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente.

²⁹ Cfr. E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, cit., 7-8.

³⁰ Direttiva (UE) 2016/1148, art. 7; si prevede inoltre che le strategie nazionali debbano individuare «misure di preparazione, risposta e recupero, inclusa la collaborazione tra settore pubblico e settore privato»; indicare «programmi di formazione, sensibilizzazione e istruzione relativi alla strategia in materia di sicurezza delle reti e dei sistemi informativi», «un piano di valutazione dei rischi per individuare i rischi», nonché «un elenco dei vari attori coinvolti nell'attuazione della strategia nazionale in materia di sicurezza delle reti e dei sistemi informativi».

³¹ Direttiva (UE) 2016/1148, art. 8; nonché la designazione di «un punto di contatto unico nazionale in materia di sicurezza delle reti e dei sistemi informativi» (coincidente con l'Autorità nel caso in cui questa fosse unica), entrambi da dotare «di risorse adeguate per svolgere in modo efficiente ed efficace i compiti loro assegnati e conseguire in questo modo gli obiettivi della presente direttiva».

³² Direttiva (UE) 2016/1148, art. 9.

³³ Comunicazione congiunta al Parlamento europeo e al Consiglio - Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE, JOIN(2017) 450 final.

³⁴ Sull'evoluzione della normativa europea sulla cibersicurezza e, contestualmente, del

mente avvenuto con il regolamento (UE) 2019/881³⁵ (cd. Cybersecurity Act o Regolamento sulla cibersicurezza), il quale ha, di fatto, rideterminato obiettivi, funzioni, poteri e aspetti organizzativi della ridenominata Agenzia dell'Unione europea per la cibersicurezza³⁶, nonché individuato un quadro comune europeo per l'introduzione di sistemi di certificazione non soltanto per garantire un livello adeguato della cibersicurezza di prodotti, servizi e processi legati alle tecnologie dell'informazione e della comunicazione, ma anche con la finalità dichiarata di evitare la frammentazione del mercato interno³⁷ con riguardo ai sistemi europei di certificazione della cibersicurezza³⁸. In particolare, quindi, l'Agenzia per la cibersicurezza viene resa permanente e ne vengono aumentate le funzioni, di natura tipicamente consultiva³⁹, specialmente in supporto agli Stati membri e alle istituzioni, agli organi e agli organismi dell'Unione europea, su tutti la Commissione europea, anche in funzione di coordinamento⁴⁰, principalmente nella defi-

ruolo svolto dell'Unione europea sul tema v. in dottrina E. Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity*, Oxford, 2022; A. Contaldo - L. Salandri, *La disciplina della cybersecurity nell'Unione europea*, in A. Contaldo - D. Mula (a cura di), *Cybersecurity Law. Disciplina italiana ed europea della sicurezza cibernetica anche alla luce delle norme tecniche*, Pisa, 2020, 1 ss.

³⁵ Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza»).

³⁶ Regolamento (UE) 2019/881, artt. 3 ss.

³⁷ Cfr. E. Fahey, *The EU as a Global Digital Actor: Institutionalising Global Data Protection, Trade, and Cybersecurity*, cit., 95, la quale osserva come la politica europea in materia di cibersicurezza si collochi storicamente in una logica legata al mercato interno, più da un punto di vista teorico che pratico. In questo senso è stato principalmente il Cybersecurity Act del 2019 ad orientare la sicurezza cibernetica europea verso il mercato interno, non solo dal momento che le politiche europee in tema di cibersicurezza sono rilevanti per il funzionamento del mercato interno, per la sicurezza dei consumatori e per il funzionamento delle imprese, ma anche, in particolare, perché tale regolamento è stato adottato in virtù dell'art. 114 TFUE che costituisce la base giuridica fondamentale per il ravvicinamento e l'armonizzazione delle legislazioni nazionali a tutela del mercato interno.

³⁸ Cfr. art. 1 del regolamento (UE) 2019/881. In questa direzione lo stesso regolamento prevede l'istituzione di un Quadro europeo di certificazione della cibersicurezza istituito proprio «al fine di migliorare le condizioni di funzionamento del mercato interno aumentando il livello di cibersicurezza all'interno dell'Unione e rendendo possibile, a livello di Unione, un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza allo scopo di creare un mercato unico digitale per i prodotti TIC, i servizi TIC e i processi TIC» (art. 46, par. 1).

³⁹ Alcuni in dottrina si sono mostrati critici rispetto alla natura meramente consultiva di tali attribuzioni, sostenendo che invece «sarebbe stato preferibile attribuire all'Agenzia funzioni maggiormente incisive, in considerazione della rilevanza del bene giuridico tutelato e della crescente esigenza di sicurezza informatica all'interno del mercato unico digitale» (L. Previti, *Pubblici poteri e cybersecurity: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*, in *Federalismi.it*, 25, 2022, 74).

⁴⁰ Sul punto in particolare v. la successiva Cybersecurity Strategy for the Digital Decade del dicembre 2020, nella Comunicazione congiunta al Parlamento europeo e al Consiglio - La strategia dell'UE in materia di cibersicurezza per il decennio digitale, [JOIN\(2020\) 18 final](#), la quale si segnala in questa sede per aver istituito la Joint Cyber Unit (o JCU) la quale

nizione e nell'attuazione delle politiche europee in materia di cibersicurezza, nonché del coordinamento delle stesse⁴¹, sebbene questo incremento delle funzioni attribuite all'ENISA non sia stato accompagnato da un (necessario) incremento dei poteri, i quali, invece, si limitano ad essere consultivi e di supporto, ciò rappresentando un elemento di forte restrizione dell'effettiva efficacia dell'attività dell'agenzia stessa⁴².

Tuttavia, l'impianto normativo europeo, specialmente con riguardo alla Direttiva NIS, ha mostrato alcune lacune e punti di debolezza, emersi particolarmente durante un periodo piuttosto intenso di attacchi informatici in concomitanza della pandemia e del conflitto russo-ucraino⁴³. Pertanto, per incrementare il livello di coordinamento delle politiche di cibersicurezza in grado di fornire agli Stati membri ulteriori strumenti di contrasto e tutela al fine di accrescere il livello generale della cibersicurezza europea si è giunti alla riforma della Direttiva NIS con la Direttiva (UE) 2022/2555 (meglio nota come Direttiva NIS 2⁴⁴).

Quest'ultima si segnala per il fatto di essere intervenuta sulle criticità relative al recepimento da parte degli Stati della precedente normativa, in particolare introducendo e rafforzando gli strumenti di cooperazione tra le autorità nazionali in una logica di armonizzazione europea⁴⁵, nonché rivedendo i settori e ampliando il novero degli operatori di servizi pubblici e privati sottoposti agli obblighi in tema di cibersicurezza⁴⁶. Per quanto

costituisce una «piattaforma virtuale e fisica per la cooperazione tra le varie comunità di cibersicurezza all'interno dell'Ue, ciò con particolare attenzione al coordinamento tecnico e operativo volto a contrastare gravi minacce e incidenti informatici di natura transfrontaliera» (G. Barozzi Reggiani, *La race for the cyberspace degli Stati e il tema della cibersicurezza: tra sovranità e modelli di governance*, cit., 15).

⁴¹ Art. 4 del regolamento (UE) 2019/881, laddove si asserisce, inoltre, che l'Agenzia «promuove la cooperazione, inclusa la condivisione di informazioni, e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione e i portatori di interessi del settore pubblico e privato su questioni relative alla cibersicurezza», nonché, tra le altre, «contribuisce a rafforzare le capacità di cibersicurezza a livello di Unione per sostenere le azioni degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri».

⁴² Cfr. F. Sanchini, *Sicurezza cibernetica e architettura istituzionale: verso una governance costituzionalmente orientata?*, in *Federalismi.it*, 26, 2025, 170-191, spec. 177-178.

⁴³ Cfr. E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional law*, cit., 8-9.

⁴⁴ 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).

⁴⁵ Direttiva (UE) 2022/2555, artt. 7-13.

⁴⁶ Direttiva (UE) 2022/2555, artt. 2-3 e allegati I e II. La direttiva, in particolare, superando la distinzione precedente tra operatori di servizi essenziali e fornitori di servizi digitali, individua criteri più precisi e definiti proprio al fine di individuare tali soggetti e contestualmente ridurre la discrezionalità statale nello svolgimento di questa rilevante operazione; inoltre, viene attivata una policy di “divulgazione coordinata delle vulnerabilità” (o “*coordinated vulnerability disclosure*”) affiancata dalla creazione di una banca dati europea delle vulnerabilità, prescrivendo altresì che in sede di attuazione ciascuno Stato adotti una propria regolazione interna relativa alle forme di rilevamento delle vulnerabilità dei sistemi informatici. Sul punto in dottrina v. almeno F.N. Ricotta,

più rileva in questa sede, la Direttiva NIS 2, al fine di accrescere la cibersecurity dell'Unione europea e ridurre le minacce ai sistemi di rete e informatici qualificati come essenziali e importanti dalla normativa stessa, si preoccupa di rafforzare notevolmente il sistema di *governance* della cibersecurity delineato con la Direttiva NIS. In particolare, troviamo al vertice del sistema l'autorità europea rappresentata dall'ENISA, mentre al livello inferiore vi sono le autorità e gli organismi degli Stati membri; in particolare la Direttiva NIS 2 ha previsto l'istituzione di alcuni organi quali le autorità nazionali competenti NIS, le autorità di gestione delle crisi informatiche e i team di risposta agli incidenti di sicurezza informatica (CSIRT)⁴⁷; inoltre, al fine di svolgere le funzioni di attuazione della Direttiva NIS 2 e della vigilanza quanto alla corretta applicazione delle disposizioni in essa contenute⁴⁸, alle autorità nazionali sono attribuiti importanti poteri di controllo⁴⁹. L'architettura istituzionale europea così delineata e il ruolo delle autorità nazionali competenti NIS con riguardo alla loro rilevanza quanto alle strategie europee in tema di cibersecurity dovrebbero richiedere un'attuazione uniforme a livello nazionale; tuttavia, già a seguito della Direttiva NIS, la quale all'art. 8 aveva previsto per prima l'istituzione delle autorità nazionali competenti, vi è stata un'applicazione delle disposizioni piuttosto eterogenea tra gli Stati membri⁵⁰.

Senza entrare nel merito di tale questione, si ritiene utile focalizzare soltan-

Vulnerability disclosure e penetration testing: profili giuridici rilevanti per l'adozione di una politica nazionale conforme alla Direttiva NIS 2, in *Rivista italiana di informatica e diritto*, 2, 2024, 82 ss.; F. Casarosa - G. Comandé, *Aspettando la NIS2: ovvero il diritto privato della cybersecurity*, in *Il Diritto dell'informazione e dell'informatica*, 1, 2024, 29 ss.; da ultimo G. Barozzi Reggiani, *La race for the cyberspace degli Stati e il tema della cybersecurity: tra sovranità e modelli di governance*, cit.

⁴⁷ Direttiva (UE) 2022/2555, art. 1, par. 2, lett. a).

⁴⁸ In questo senso v. direttiva (UE) 2022/2555, art. 1, laddove si prevede che «1. La presente direttiva stabilisce misure volte a garantire un livello comune elevato di cibersecurity nell'Unione in modo da migliorare il funzionamento del mercato interno. 2. A tal fine, la presente direttiva stabilisce: a) obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cibersecurity e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT); b) misure in materia di gestione dei rischi di cibersecurity e obblighi di segnalazione per i soggetti di un tipo di cui all'allegato I o II nonché per soggetti identificati come critici ai sensi della direttiva (UE) 2022/2557; c) d) norme e obblighi in materia di condivisione delle informazioni sulla cibersecurity; obblighi in materia di vigilanza ed esecuzione per gli Stati membri». Inoltre, l'art. 8, par. 2, della stessa direttiva stabilisce che le autorità nazionali competenti «controllano l'attuazione della presente direttiva a livello nazionale».

⁴⁹ Direttiva (UE) 2022/2555, art. 32, par. 2.

⁵⁰ In dottrina v. A. Lauro, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *Rivista del Gruppo di Pisa*, 3, 2021, 532 ss.; L. Moroni, *La governance della cybersecurity a livello interno ed europeo: un quadro intricato*, cit., 186 ss. Si possono individuare tre gruppi di Stati: un primo gruppo ha affidato il ruolo di autorità nazionale competente NIS a organismi tecnici di regolazione ovvero a svariate autorità amministrative indipendenti (ad es. Lussemburgo, Cipro); un secondo gruppo ha invece assegnato tale ruolo a Ministeri ovvero ad organismi collegati direttamente ad essi (ad es. Irlanda, Germania); un terzo gruppo, infine, ha conferito il ruolo di autorità nazionale competente direttamente al vertice del Governo ovvero a un'agenzia governativa dipendente da esso (ad es. Francia, Italia).

to brevemente l'attenzione quantomeno sull'architettura istituzionale derivata da tale normativa europea nell'ordinamento italiano, il quale rientra nel gruppo di Stati che hanno attribuito il ruolo di autorità nazionale competente NIS ai vertici dell'esecutivo ovvero a un'agenzia ad esso in qualche misura riconducibile. Inizialmente sono state attribuite al Presidente del Consiglio dei ministri importanti prerogative in tema di sicurezza cibernetica, in particolare quanto alla predisposizione della strategia nazionale in materia di cibersicurezza, ricoprendo un ruolo apicale anche in veste, almeno in un primo periodo, di autorità nazionale competente NIS⁵¹. Un tale impianto istituzionale è stato modificato con l'istituzione dell'Agenzia per la cibersicurezza nazionale (o cd. ACN)⁵² indicata come autorità nazionale competente NIS, la quale rappresenta uno degli elementi fondamentali della *governance* italiana della cibersicurezza proprio laddove è chiamata a dare attuazione alla strategia nazionale di sicurezza cibernetica adottata dal Presidente del Consiglio dei ministri⁵³, il quale esercita la propria influenza sull'Agenzia⁵⁴ già a partire dalla nomina – ed eventualmente revoca – dei vertici della stessa⁵⁵.

In sostanza, ciò che emerge dalla normativa interna e dall'architettura istituzionale che ne è derivata, anche a seguito delle più recenti modifiche normative intervenute con la legge 28 giugno 2024, n. 90 in materia di rafforzamento della cibersicurezza nazionale⁵⁶ e con il d. lgs. 4 settembre

⁵¹ Così è stato con l'approvazione della legge 7 agosto 2012, n. 133 “Modifiche alla legge 3 agosto 2007, n. 124, concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto” e con il d. lgs. 18 maggio 2018, n. 65 di recepimento della Direttiva NIS, rubricato “Attuazione della 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”, il quale agli artt. 6 e 7 affidava al Presidente del Consiglio dei ministri l'adozione della strategia nazionale di cibersicurezza mentre ad alcuni Ministeri il ruolo di autorità competente NIS in base al settore di riferimento (così al Ministero dello sviluppo economico per il settore energia; al Ministero delle infrastrutture e dei trasporti per il settore trasporti; al Ministero dell'economia e delle finanze per il settore bancario e per il settore infrastrutture dei mercati finanziari; al Ministero della salute per l'attività di assistenza sanitaria; al Ministero dell'ambiente e della tutela del territorio e del mare e alle Regioni e alle Province autonome di Trento e di Bolzano in merito al settore fornitura e distribuzione di acqua potabile).

⁵² Questo cambiamento è avvenuto con il d.l. 14 giugno 2021, n. 82, convertito con modificazioni dalla l. 4 agosto 2021, n. 109, recante “Disposizioni urgenti in materia di cibersicurezza, definizione dell'architettura nazionale di cibersicurezza e istituzione dell'Agenzia per la cibersicurezza nazionale”. Sul punto in dottrina v. almeno F. Serini, *La nuova architettura di cibersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in *Federalismi.it*, 12, 2022, 241 ss.; per quanto riguarda l'Agenzia v. per tutti I. Forgiione, *Il ruolo strategico dell'Agenzia nazionale per la cybersecurity nel contesto del Sistema di sicurezza nazionale: organizzazione e funzioni, tra regolazione europea e interna*, in R. Ursi (a cura di), *La sicurezza nel cyberspazio*, cit., 106 ss.

⁵³ Cfr. art. 2, c. 1, lett. b) del d.l. 14 giugno 2021, n. 82, laddove inoltre si prevede il parere del Comitato interministeriale per la cibersicurezza (v. art. 4, c. 2).

⁵⁴ Secondo T.F. Giupponi, *Il governo nazionale della cibersicurezza*, in *Quaderni costituzionali*, 2, 2024, 277-304, spec. 297, il ruolo dell'Agenzia per la cibersicurezza nazionale risulta «sostanzialmente strumentale» con riguardo «alle competenze della Presidenza del Consiglio in materia di cibersicurezza».

⁵⁵ Cfr. art. 2, c. 1, lett. c), del d.l. 14 giugno 2021, n. 82.

⁵⁶ In dottrina v. almeno A. Iannuzzi, *Considerazioni sul disegno di legge “Disposizioni in*

2024, n. 128 di recepimento della Direttiva NIS 2⁵⁷, è un significativo accentramento di poteri e attribuzioni attorno all'esecutivo e particolarmente al Presidente del Consiglio dei ministri, con ciò determinandosi una rilevante questione circa la portata del controllo parlamentare che viene esercitato in questo specifico ambito⁵⁸. La funzione parlamentare di controllo nei confronti del potere esecutivo è stata rafforzata – rispetto ai classici strumenti previsti in via ordinaria come interrogazioni, interpellanze, mozioni, inchieste, indagini conoscitive ovvero audizioni in sede di commissioni – dallo stesso legislatore italiano, il quale ha individuato nel Comitato parlamentare per la sicurezza della Repubblica (cd. COPASIR⁵⁹) l'organo di derivazione parlamentare in grado di svolgere la funzione di controllo sul Governo nell'esercizio dell'attività di indirizzo politico in tema di cibersicurezza, in modo particolare attraverso diverse attribuzioni ad esso appositamente assegnate⁶⁰. Tuttavia, un tale impianto presenta alcune criticità quanto all'effettiva capacità di questo organo di contro-

materia di rafforzamento della cibersicurezza nazionale e di reati informatici” (AC 1717), in Rivista italiana di informatica e diritto, 1, 2024, 59-63; E. Longo, Audizione informale per il disegno di legge in materia di “Disposizioni in materia di rafforzamento della cibersicurezza nazionale e di reati informatici” (AC 1717), ivi, 66-70.

⁵⁷ 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”. Inoltre, tra la principale normativa di attuazione si segnalano: DPCM 9 dicembre 2024, n. 221 “Regolamento per la definizione dei criteri per l'applicazione della clausola di salvaguardia di cui all'articolo 3, commi 4 e 12, del decreto legislativo del 4 settembre 2024, n. 138, di 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”; DPCM 30 aprile 2025 “Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale”; DPCM 2 ottobre 2025 “Modifica del decreto del Presidente del Consiglio dei ministri 30 aprile 2025, concernente la disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale”.

⁵⁸ Cfr. F. Sanchini, *Sicurezza cibernetica e architettura istituzionale: verso una governance costituzionalmente orientata?*, cit., 179-180; T.F. Giupponi, *Il governo nazionale della cibersicurezza*, cit., 287 ss. e 295 ss.; L. Moroni, *La governance della cibersicurezza a livello interno ed europeo: un quadro intricato*, cit., 191 ss.

⁵⁹ Su questi aspetti v. A. Lauro, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, cit., 541 ss.; O. Caramaschi, *La cibersicurezza nazionale ai tempi della guerra (cibernetica): il ruolo degli organi parlamentari*, in *Osservatorio costituzionale*, 4, 2022, 77 ss.

⁶⁰ Cfr. d.l. 14 giugno 2021, n. 82; tra queste troviamo il potere di chiedere l'audizione del Presidente dell'ACN (art. 5, c. 6) e di esprimere pareri sull'adozione di alcuni atti, quali i regolamenti che riguardano l'organizzazione dell'ACN (art. 6, c. 3); il regolamento di contabilità dell'ACN (art. 11, c. 3); le procedure per la stipula di contratti di appalti di lavori e forniture di beni e servizi per le attività dell'ACN (art. 11, c. 4); disciplina del contingente di personale addetto all'ACN (art. 12, c. 8). Inoltre, viene previsto che ogni anno entro il 30 giugno il Presidente del Consiglio dei ministri trasmetta al COPASIR una relazione annuale sulle attività svolta dall'ACN negli ambiti relativi alla tutela della sicurezza nazionale nello spazio cibernetico con riguardo ai profili di competenza del Comitato (art. 14, c. 2); contestualmente occorre notare, per completezza, che si prevede altresì che entro il 30 aprile di ogni anno il Presidente del Consiglio dei ministri debba trasmettere una analoga relazione in materia di cibersicurezza nazionale al Parlamento (art. 14, c. 1).

bilanciare adeguatamente l'accentramento di poteri in capo all'esecutivo attraverso un'opportuna ed efficace azione di controllo in tema di sicurezza digitale in grado di offrire maggiore trasparenza e democraticità alla complessiva *governance* della cibersicurezza⁶¹.

Tornando brevemente e conclusivamente al quadro giuridico e istituzionale europeo in tema di cibersicurezza – negli ultimi anni arricchito da ulteriori atti di rilievo⁶² – tra i vari elementi di interesse che emergono (come, ad esempio, la protezione dei diritti fondamentali ovvero il coinvolgimento degli attori fondamentali del settore sia pubblici sia privati⁶³),

⁶¹ Le principali criticità riguardano la composizione ristretta del COPASIR e la segretezza che ne contraddistinguono i lavori, nonché il fatto di operare secondo il principio di riservatezza, subendo in questo senso il ruolo del Presidente del Consiglio dei ministri che può rappresentare un limite all'azione dell'organo quanto ad efficacia e trasparenza, per esempio nell'accesso a documenti riservati per ragioni di sicurezza ovvero nell'esercizio di talune attività ispettive.

In dottrina cfr. E. Longo, *Il diritto costituzionale e la cibersicurezza. Analisi di un volto nuovo del potere*, in *Rassegna parlamentare*, 2, 2024, 340 ss., il quale osserva come a fronte di un aumento dei poteri del Presidente del Consiglio dei ministri il controllo svolto dal COPASIR non risulti «adeguato a garantire un sufficiente livello di trasparenza necessario in questi ambiti»; F. Sanchini, *Sicurezza cibernetica e architettura istituzionale: verso una governance costituzionalmente orientata?*, cit., 181-183; A. Lauro, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, cit., spec. 542, il quale ritiene che il ruolo del COPASIR sia «limitante rispetto alla vastità di ambiti cui ormai presiede e limitato tanto nella composizione che nelle forme di pubblicità»; L. Moroni, *La governance della cibersicurezza a livello interno ed europeo: un quadro intricato*, cit., 186 ss., 192-193, il quale individua alcuni interventi del legislatore che potrebbero ovviare alle criticità emerse, in particolare la «previsione di audizioni parlamentari pubbliche semestrali o trimestrali dell'ACN» ovvero «l'istituzione di nuova commissione parlamentare bicamerale ad hoc di controllo sull'attività del Governo, la cui maggiore rappresentatività della composizione e pubblicità dei lavori garantiscano una adeguata conoscenza delle decisioni assunte in materia di cibersicurezza».

⁶² Si pensi alla [direttiva \(UE\) 2022/2556](#) del Parlamento europeo e del Consiglio del 14 dicembre 2022 che modifica le direttive 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 per quanto riguarda la resilienza operativa digitale per il settore finanziario (sul punto v. anche il [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) ovvero alla [direttiva \(UE\) 2022/2557](#) del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, nonché al [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 (regolamento sulla ciberresilienza) e al [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 (regolamento sulla ciber-solidarietà).

Quanto al rapporto tra Cyber Resilience Act e Artificial Intelligence Act v. F. Bagni, *The Regulatory Sandbox and the Cybersecurity Challenge: from the Artificial Intelligence Act to the Cyber Resilience Act*, in *Rivista italiana di informatica e diritto*, 2, 2023, 201-217, mentre con riguardo agli altri atti europei in tema di cibersicurezza v. P.G. Chiara, *Il Cyber Resilience Act: la proposta di regolamento della Commissione europea relativa a misure orizzontali di cibersicurezza per prodotti con elementi digitali*, in *Rivista italiana di informatica e diritto*, 1, 2023, 143 ss.

⁶³ Cfr. E. Raffiotta, *Cybersecurity regulation in the European Union and the issues of constitutional*

quello che qui più rileva è il rapporto tra *governance-government* nella relazione tra Unione europea e Stati membri⁶⁴. Gli atti europei sulla cibersicurezza riaffermano più volte che, in molti ambiti e con riferimento a diversi profili, l'ordinamento dell'Unione europea rispetta la sovranità e la discrezionalità politica degli Stati membri⁶⁵, in maniera conforme ai Trattati, i quali stabiliscono, come è noto, che l'Unione europea rispetta le funzioni essenziali dello Stato, con particolare riguardo alle «funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro»⁶⁶. Si tratta quindi di un ambito competenziale nel quale gli Stati godono di una discreta autonomia nell'adottare le misure ritenute idonee per proteggere beni e valori essenziali dei propri ordinamenti giuridici e, contestualmente, nel definire le Strategie di sicurezza nazionali e le rispettive strutture amministrative dedicate. Di converso si determina come il ruolo dell'architettura istituzionale europea – su tutti si pensi all'Agenzia dell'Unione europea per la cibersicurezza (ENISA)⁶⁷ – sia quello di supporto e cooperazione con gli Stati membri e le autorità statali preposte al fine di un maggiore coordinamento e dell'attuazione della normativa europea. Sicché, più che di verticalizzazione dell'impianto normativo europeo, potrebbe parlarsi, più opportunamente, di orizzontalizzazione dovuta al processo di armonizzazione delle legislazioni nazionali, in una logica di *governance* europea⁶⁸ della

lam, cit., 9.

⁶⁴ Sul punto v. ampiamente G. Barozzi Reggiani, *La race for the cyberspace degli Stati e il tema della cibersicurezza: tra sovranità e modelli di governance*, cit., 16-17.

⁶⁵ In questo senso vanno si vedano, ad esempio, l'art. 1, par. 6, della Direttiva NIS, laddove si prevede che la «direttiva lascia impregiudicate le misure adottate dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare di tutela della sicurezza nazionale, comprese le misure volte a tutelare le informazioni, la cui divulgazione sia dagli Stati membri considerata contraria agli interessi essenziali della loro sicurezza, e di mantenimento dell'ordine pubblico, in particolare a fini di indagine, accertamento e perseguimento di reati», oppure l'art. 1, par. 6, della Direttiva NIS 2, dove si stabilisce che la «direttiva lascia impregiudicata la responsabilità degli Stati membri di tutelare la sicurezza nazionale e il loro potere di salvaguardare altre funzioni essenziali dello Stato, tra cui la garanzia dell'integrità territoriale dello Stato e il mantenimento dell'ordine pubblico», o, ancora, l'art. 1, par. 4 e 5, del regolamento (UE) 2025/38 i quali prevedono, rispettivamente, che «[l]e azioni intraprese a norma del presente regolamento sono realizzate nel debito rispetto delle competenze degli Stati membri e integrano le attività svolte dalla rete di CSIRT, da EU-CyCLONe e dal gruppo di cooperazione NIS» e che «[i]l presente regolamento lascia impregiudicate le funzioni statali essenziali degli Stati membri, tra cui la garanzia dell'integrità territoriale dello Stato, il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza nazionale. In particolare, la sicurezza nazionale resta una competenza esclusiva di ciascuno Stato membro».

⁶⁶ Art. 4, par. 2, Trattato sull'Unione europea (TUE).

⁶⁷ In questo senso sottolinea C. Cencetti, *Cybersecurity: Unione europea e Italia Prospettive a confronto*, cit., 26, che «l'attività principale dell'ENISA è quella di coordinare l'operato degli stati membri e favorire il dialogo intra-europeo, attraverso l'elaborazione di linee guida e l'individuazione di best practices. A questo scopo, l'agenzia pubblica molti documenti, disponibili online e liberamente consultabili, per cercare di tenere aggiornato lo stato dell'arte della cybersecurity in Europa e stimolare il confronto tra i vari stati, nell'intento che si affermino le pratiche più avanzate».

⁶⁸ Sul punto v. A. Kasper, *EU Cybersecurity Governance – Stakeholders and Normative Intentions*

cibersicurezza analogamente a quanto può (o potrebbe) realizzarsi anche a livello globale (v. *infra*).

3. La dimensione internazionale della cibersicurezza

Nel corso degli anni l'approccio europeo si è sempre più evoluto in quello che è stato definito “*geopolitical turn*” verso uno sviluppo estensivo internazionale e globale della cibersicurezza⁶⁹. Emblematica in questo senso è la Strategia in materia di cibersicurezza del 2020⁷⁰ nella quale si afferma esplicitamente che, per promuovere e difendere la propria visione del ciber spazio e della cibersicurezza, l'Unione europea «deve intensificare il suo impegno e la sua leadership nei processi di normazione internazionale, nonché rafforzare la sua rappresentanza negli organismi di normazione internazionali ed europei e in altre organizzazioni per lo sviluppo di norme», nonché continuare «a collaborare con i partner internazionali per far progredire e promuovere un ciber spazio globale, aperto, stabile e sicuro in cui il diritto internazionale, in particolare la Carta delle Nazioni Unite (ONU), sia rispettato» con la necessità che l'Unione europea e gli Stati membri «assumano una posizione maggiormente proattiva nelle discussioni in seno all'ONU e in altre sedi internazionali pertinenti»⁷¹.

Questa “propensione” internazionale e globale dell'Unione europea ci consente di allargare l'analisi anche (e soprattutto per quanto riguarda l'obiettivo di questo scritto) a tali dimensioni. L'Unione europea è ben rappresentata negli organismi internazionali⁷², svolgendo un ruolo significativo nella promozione del diritto internazionale e degli sviluppi in tema di cibersicurezza a livello globale⁷³.

Seguendo pertanto questa tendenza europea e spostandoci su un piano

Towards Integration, in M. Harwood - S. Moncada - R. Pace (eds.), *The future of the European Union: Demisting the Debate*, Institute for European Studies, 2020.

⁶⁹ Cfr. F. Delerue - A. Géry, *International Law and Cybersecurity Governance: The Way Forward*, in *Id.* (eds.), *International Law and Cybersecurity Governance*, Leiden, 2022, 10.

⁷⁰ Comunicazione congiunta al Parlamento europeo e al Consiglio - La strategia dell'UE in materia di cibersicurezza per il decennio digitale, [JOIN\(2020\) 18 final](#).

⁷¹ Cfr. par. 3 “Promuovere un ciber spazio globale e aperto” della Strategia in materia di cibersicurezza 2020.

⁷² Si pensi al Consiglio d'Europa, all'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE), all'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) e alle Nazioni Unite, nonché ad alcuni organismi a quest'ultima riferibili come l'Unione internazionale delle telecomunicazioni (ITU), il World Summit on the Information Society (WSIS) e l'Internet Governance Forum (IGF).

⁷³ Cfr. E. Fahey, *Developing EU Cybercrime and Cybersecurity: On Legal Challenges of EU Institutionalisation of Cyber Law-Making*, in T. Hoerber - G. Weber - I. Cabras (eds.), *The Routledge Handbook of European Integrations*, London, 2022, 82-84. Sul ruolo dell'Unione europea come attore internazionale di cibersicurezza v. anche J. Odermatt, *The European Union as a Cybersecurity Actor*, in S. Blockmans - P. Koutrakos (eds.), *Research Handbook on the EU's Common Foreign and Security Policy*, Cheltenham, 2018, 354-373; A. Verhelst - J. Wouters, *Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives*, in *International Organization*, 2, 2020.

pienamente internazionale, vengono in rilievo due principali “arene” dove in tema di cibersicurezza si è giunti alla previsione di convenzioni internazionali e forme di *governance* di portata assai rilevante: il Consiglio d’Europa e le Nazioni Unite.

Quanto al primo pare necessario annoverare fin da subito la Convenzione sulla criminalità informatica del Consiglio d’Europa, meglio nota come Convenzione di Budapest⁷⁴, la quale rappresenta (perlomeno finora) l’accordo internazionale più rilevante che affronta specificamente il tema della sicurezza informatica essendo un trattato di cd. *law enforcement* che si concentra su diversi tipi di azione e intervento – tra cui l’adozione di legislazioni appropriate e la promozione della cooperazione internazionale – per l’integrità dei sistemi informatici da crimini commessi attraverso la Rete, con particolare riguardo alla violazione del diritto d’autore, alla pornografia minorile, alle frodi informatiche e all’integrità stessa dei sistemi informatici⁷⁵.

Sebbene non manchino certamente altri strumenti a carattere pattizio sul tema della cibersicurezza e con una portata “regionale”⁷⁶, il caso della Convenzione di Budapest si segnala come particolarmente interessante in ragione della sua ratifica da parte di 81 Stati, quindi ben oltre il numero degli Stati membri del Consiglio d’Europa e pertanto con una presenza di Stati non solo europei, ma anche africani, americani e pacifico-asiatici⁷⁷,

⁷⁴ Convention on Cybercrime (*ETS No. 185*) del 23 novembre 2001, entrata in vigore il 1 luglio 2004. La Convenzione è stata successivamente integrata dai due protocolli addizionali: troviamo così il *First Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems* (*ETS No. 189*) del 28 gennaio 2003, entrato in vigore il 1 marzo 2006 (firmato da 47 Stati e ratificato da 38), seguito dal *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (*CETS No. 224*) del 12 maggio 2002 (firmato da 51 Stati, ma ratificato soltanto da 2 quindi non ancora entrato in vigore).

⁷⁵ Cfr. E. Fahey, *Developing EU Cybercrime and Cybersecurity: On Legal Challenges of EU Institutionalisation of Cyber Law-Making*, cit., 99-100; A. Gascón Marcén, *The Budapest Convention and the UN Cybercrime Convention negotiations*, in A. Segura Serrano (ed.), *Global Cybersecurity and International Law*, London, 2024, 175-176.

⁷⁶ Tra questi si vedano la cd. Convenzione di Minsk del 2001 della Comunità degli Stati Indipendenti (*Agreement on cooperation among the States members of the Commonwealth of Independent States in combating offences relating to computer information*); la cd. Convenzione di Ekaterinburg del 2009 (*Agreement on Cooperation in Ensuring International Information Security*) tra gli Stati membri dell’Organizzazione per la Cooperazione di Shanghai (tra cui Cina, Federazione russa e alcuni Stati dell’Asia centrale); la cd. Convenzione del Cairo nel 2010 della Lega degli Stati arabi (*Arab Convention on Combating Information Technology Offences*) sottoscritta da 18 Stati arabi; la cd. Convenzione di Malabo nel 2014 dell’Unione degli Stati africani (*African Union Convention on Cyber Security and Personal Data Protection*) ratificata al momento da 16 Stati su 55. Per un’analisi di dottrina sul punto v. M. Fidler, *Fragmentation of International Cybercrime Law*, in *Utah Law Review*, 3, 2025, 737 ss.; E. Tikk - M. Kerttunen (eds.), *Routledge Handbook of International Cybersecurity*, London, 2020.

Secondo I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 131-132, emerge così, almeno per il momento, un quadro complesso e di profonda frammentazione, tanto che secondo K. Bannelier - T. Christakis, *Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors*, in *Les Cahiers de la Revue Défense Nationale*, 2017, 82, il problema sarebbe che «*the proliferation of these initiatives in very diverse fora does not necessarily reflect good governance of cybersecurity*».

⁷⁷ Si tratta di 45 Stati membri del Consiglio d’Europa su 46 (l’Irlanda ha firmato la Convenzione, tuttavia senza ancora averla ratificata), oltre a Stati quali, tra gli altri,

in quello che potremmo definire “effetto Strasburgo”, sul modello del cd. effetto Bruxelles, dal momento che questa Convenzione ha continuato ad espandere la propria portata (anche indirettamente⁷⁸) nel corso degli anni, con un evidente influsso positivo per quanto riguarda l’azione globale in materia di cibersicurezza anche, e soprattutto, in seno alle Nazioni Unite, costituendo in tal senso una sorta di *transnational gold standard* per la regolazione nazionale della cibersicurezza a livello globale⁷⁹, altresì in ragione del fatto che contiene alcune importanti disposizioni a tutela dei diritti fondamentali⁸⁰.

Similmente interessanti risultano essere i recenti sviluppi nell’ambito delle Nazioni Unite che sembrano trovarsi ad un punto di svolta apprezzabile con specifico riferimento alla dimensione “globale” della cibersicurezza⁸¹. Sebbene l’impegno sul tema da parte delle Nazioni Unite sia ormai storicamente piuttosto risalente⁸², deve osservarsi come vi siano stati alcuni ten-

Argentina, Australia, Brasile, Canada, Cile, Colombia, Ghana, Giappone, Marocco, Nigeria, Paraguay, Perù, Senegal e Stati Uniti. Oltre a questi altri 16 Stati al momento risultano essere firmatari della Convenzione o essere stati invitati ad aderirvi. Cfr. Council of Europe, *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*, consultato il 16 ottobre 2025.

⁷⁸ Alcuni studiosi sostengono che diversi Stati dell’Oceano pacifico e del nordest asiatico abbiano allineato le proprie legislazioni nazionali alle disposizioni contenute nella Convenzione di Budapest pur non essendone parti; cfr. C. Le Nguyen - W. Golman, *Diffusion of the Budapest Convention on cyber-crime and the development of cybercrime legislation in Pacific Island countries: ‘Law on the books’ vs ‘law in action*, in *Computer Law & Security Review*, 2021; L. Chang, *Legislative Frameworks Against Cybercrime: The Budapest Convention and Asia*, in T.J. Holt - A.M. Bossler (eds.), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, London, 2020, 327 ss.

⁷⁹ Cfr. E. Fahey, *Developing EU Cybercrime and Cybersecurity: On Legal Challenges of EU Institutionalisation of Cyber Law-Making*, cit., 99-100.

⁸⁰ Si pensi all’art. 15 della Convenzione di Budapest: «1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure [...]».

⁸¹ Sebbene le Nazioni Unite siano centrali in questo contributo, non mancano altre importanti organizzazioni internazionali che si occupano della cibersicurezza a livello internazionale. Ad esempio, I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 129-130, evidenzia il ruolo dell’International Telecommunications Union (ITU) e di alcune rilevanti iniziative, tra le quali si segnalano la Global Cybersecurity Agenda (GCA) lanciata nel 2007 al fine di stabilire un «*framework for international cooperation aimed at enhancing confidence and security in the information society*» e il Global Cybersecurity Index (GCI) il quale rappresenta una rilevante iniziativa volta al monitoraggio dell’impegno sulla cibersicurezza da parte dei diversi Stati e che è giunto alla sua quinta pubblicazione (2014, 2017, 2018, 2020 e 2024).

⁸² In dottrina v. almeno A. Stiano, *Il cyberspazio nel diritto internazionale contemporaneo: tra frammentazione e patrimonio comune dell’umanità*, in *La Comunità Internazionale*, 4, 2018; A. Henriksen, *The end of the road for the UN GGE process: The future regulation of cyberspace*, in *Journal of Cybersecurity*, 1, 2019, 1 ss.; G.M. Farnelli, *Il contributo delle Nazioni Unite allo*

tativi recenti di affrontare il tema della sicurezza informatica nella forma più compiuta e articolata di un trattato internazionale, specialmente nella direzione più ambiziosa di individuare una cornice regolatoria di portata globale⁸³. Ciò è avvenuto segnatamente con riguardo al contrasto della criminalità digitale con la Risoluzione 74/247 del 27 dicembre 2019 dell'Assemblea generale delle Nazioni Unite, laddove è stato istituito un Comitato intergovernativo speciale di esperti (noto come “open-ended ad hoc intergovernmental committee of experts” o AHC), a composizione non limitata e volutamente rappresentativa di tutte le regioni, con il preciso compito di elaborare una convenzione internazionale concernente il contrasto all'uso delle tecnologie dell'informazione e della comunicazione per finalità criminali, capace di tenere debitamente conto sia degli strumenti internazionali esistenti sia degli sforzi a livello nazionale, regionale-sovrannazionale e internazionale⁸⁴. Muovendo rapidamente verso l'epilogo e tralasciando per motivi di opportunità le fasi intermedie, il 24 dicembre 2024 l'Assemblea generale delle Nazioni Unite, con la Risoluzione 79/243, ha ufficialmente adottato la nuova Convenzione contro il cybercrime⁸⁵, la quale è stata sottoscritta da settantadue Stati nel corso di una cerimonia formale ad Hanoi, in Vietnam, il 25-26 ottobre 2025 – restando aperta alla firma fino al 31 dicembre 2026 presso la sede delle Nazioni Unite a New York – ed entrerà in vigore novanta giorni dopo la ratifica da parte del quarantesimo firmatario⁸⁶. L'obiettivo primario di questa Convenzione è quello di rafforzare la cooperazione internazionale per accrescere la cibersicurezza e proteggere le società dai pericoli provenienti dal ciber spazio, in particolare aggiornando il quadro normativo globale previsto in larga parte dalla Convenzione di Budapest rispetto al nuovo contesto tecnologico-digitale e geopolitico⁸⁷. In questo senso vengono introdotti nuovi obblighi

sviluppo dell'International Cybersecurity Law, in *Osorin Working Paper*, 1, 2020; C. Henderson, *The United Nations and the Regulation of Cyber-Security*, in N. Tsagourias - R. Buchan (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, 2021, 582 ss.

⁸³ In dottrina A. Segura Serrano, *Cybersecurity and Cybercrime: Dynamic Application versus Norm-Development*, in *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 3, 2021, 718 ss., ha definito la Convenzione sul cybercrime come «*test case of norm-developments*».

⁸⁴ Assemblea generale delle Nazioni Unite, Risoluzione 74/247 del 27 dicembre 2019, *Countering the use of information and communications technologies for criminal purposes* (UN Doc A/RES/74/247). Si veda anche la Risoluzione 75/282 del 26 maggio 2021 per alcune questioni pratico-organizzative relative al Comitato intergovernativo speciale di esperti (UN Doc A/RES/75/282).

⁸⁵ Assemblea generale delle Nazioni Unite, Risoluzione 79/243 del 24 dicembre 2024, *United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes* (UN Doc A/RES/79/243).

⁸⁶ La Convenzione è stata firmata da 72 Stati durante la cerimonia dell'ottobre 2025, tra cui si segnalano Cina, Federazione russa, Unione europea (e 12 Stati membri europei, tra cui Francia, Spagna e Polonia), Regno Unito e Australia. Al momento risultano 74 Stati firmatari; il dato è aggiornato al 18 febbraio 2026.

⁸⁷ Come si legge nel Preambolo, tra gli obiettivi principali della Convenzione vi è «*to pursue, as a matter of priority, a global criminal justice policy aimed at the protection of society against cybercrime by, inter alia, adopting appropriate legislation, establishing common offences and procedural powers and fostering international cooperation to prevent and combat such activities more effectively at the national, regional and international levels*». Si insiste inoltre sulla necessità «*to enhance coordination and*

di incriminazione⁸⁸ e relative misure procedurali-applicative, sebbene, per quanto riguarda il contributo della Convenzione alla determinazione della legalità dello spazio cibernetico, questa non si occupa in alcun modo dei cd. attacchi cibernetici, vale a dire di quei tentativi intenzionali di ledere le infrastrutture, i sistemi informatici o le reti statali ovvero di rilevanza considerevole per i servizi strategici di portata nazionale che sono promossi direttamente da altri Stati o da gruppi che agiscono per conto di questi⁸⁹. Tale Convenzione rappresenta – o meglio, potrebbe rappresentare – un primo passo di regolazione della criminalità informatica nello spazio cibernetico, nella direzione di poter giungere a un quadro normativo globale soddisfacente in tema di regolazione del ciberspazio, specialmente per quanto riguarda i profili della cibersicurezza. Sarà fondamentale seguire il processo di applicazione della Convenzione a livello statale, in quanto essa coinvolge Stati che possono essere alquanto disomogenei tra di loro con riferimento alle strutture e ai principi costituzionali dei corrispondenti ordinamenti giuridici, con la conseguenza che le medesime disposizioni potrebbero trovare applicazione in maniera anche estremamente differen-

cooperation among States by, inter alia, providing technical assistance and capacity-building, including the transfer of technology on mutually agreed terms, to countries, in particular developing countries, upon their request, to improve national legislation and frameworks and enhance the capacity of national authorities to deal with cybercrime in all its forms, including its prevention, detection, investigation and prosecution, and emphasizing in this context the role that the United Nations plays».

⁸⁸ Come osserva M. Dimetto, *Convenzione delle Nazioni Unite contro il cybercrime e tutela dei diritti umani: influenze europee sullo scenario internazionale*, in *Freedom, Security & Justice: European Legal Studies*, 2, 2025, 109 ss., spec. 112-113, quanto agli obblighi di incriminazione, il testo finale della Convenzione prevede una serie limitata di crimini informatici tipici (cd. crimini “*cyber-dependent*”, vale a dire quelli che possono essere commessi soltanto attraverso sistemi informatici) e soltanto alcuni specifici reati che possono essere commessi “*offline*”, ma che le tecnologie digitali possono rendere più agevoli o efficaci (cd. crimini “*cyber-enabled*”); fra questi troviamo sia crimini che tutelano l’integrità dei sistemi tecnologici di informazione e comunicazione, come l’accesso illegale (art. 7), l’intercettazione illegale (art. 8), l’interferenza con dati elettronici attraverso il danneggiamento, l’alterazione o l’eliminazione degli stessi (art. 9), la creazione di interferenze al funzionamento dei sistemi di tecnologie della comunicazione e dell’informazione (art. 10), sia altri crimini i quali, diversamente, offrono tutela a beni diversi, come quelli relativi alla diffusione online di materiale attinente ad abusi o sfruttamento sessuale di minori (art. 16) o alla divulgazione non autorizzata di immagini intime (art. 17).

⁸⁹ Cfr. M. Dimetto, *Convenzione delle Nazioni Unite contro il cybercrime e tutela dei diritti umani: influenze europee sullo scenario internazionale*, cit., 127-129. Se per alcuni autori questa scelta rappresenta la volontà degli Stati di ritenere non necessaria una regolazione internazionale pattizia sul punto, potendo essere invece sufficiente il diritto internazionale generale, in particolare per quanto riguarda la responsabilità internazionale degli Stati (cfr. per tutti A. Stiano, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli, 2023, 260-261; in maniera più critica F. Delerue, *Cyber Operations and International Law*, Cambridge, 2020, 184 ss.), trattandosi quindi di una scelta di natura “politica”, per altri autori, invece, il diritto internazionale, specialmente nella sua configurazione di *jus ad bellum*, non sarebbe affatto idoneo a disciplinare gli attacchi informatici condotti dagli Stati in ragione delle caratteristiche tecniche di siffatti attacchi cibernetici (cfr. L. Baudin, *Cyberattaques et droit international public: de la négociation entre États à l’intégration des acteurs privés pour parvenir à la cyberpaix?*, Paris, 2023, 140: «[d]e nos observations sur le jus ad bellum, nous parvenons à la conclusion que celui-ci est, en l’état actuel, inadapté dans les cas d’attaques informatiques. [...] Déjà parce que les différentes notions liées à l’emploi du cyberspace n’ont pas été définies, ensuite parce que les particularités techniques des attaques informatiques n’ont pas été prises en considération»).

ziata nei vari ordinamenti⁹⁰; sotto questo profilo, risultano sostanziali e decisivi il ruolo svolto dai giudici nazionali – i quali potrebbero sviluppare un approccio comune in grado di tutelare i diritti fondamentali – e gli strumenti di cooperazione previsti dalla Convenzione per lo sviluppo delle capacità tecnico-organizzative anche degli Stati tecnologicamente meno avanzati⁹¹, con l’obiettivo un’armonizzazione di natura tecnica, ma soprattutto di applicazione uniforme della normativa a livello globale.

Parallelamente occorre soffermarsi anche sugli sviluppi per quanto concerne la *governance* internazionale della cibernsicurezza. Senza volersi addentrare nelle complicate e tortuose vicende che hanno caratterizzato gli ultimi trent’anni, basti qui ricordare che il tema della cibernsicurezza, in quel momento intesa come il rapporto tra le nuove tecnologie digitali e il contesto della sicurezza internazionale, viene affrontato per la prima volta dall’Assemblea generale delle Nazioni Unite verso la fine degli anni ‘90 tramite una proposta di risoluzione presentata dalla Federazione russa, poi approvata per *consensus* il 4 dicembre 1998 come Risoluzione 53/70⁹². L’effetto più significativo di tale risoluzione fu l’istituzione del Gruppo di esperti governativi, meglio noto semplicemente come *Group of Governmental Experts* (GGE)⁹³, creato attraverso la Risoluzione 58/32 del 18 dicembre 2003 dall’Assemblea generale quale gruppo di lavoro di esperti governativi in tema di cibernsicurezza, nominati dal Segretario generale sulla base di una distribuzione geografica equa e ponderata, con il compito specifico di valutare le questioni prioritarie e le strategie nazionali per la cibernsicurezza, nonché identificare le misure più adatte da adottare per rafforzare la sicurezza internazionale dei sistemi digitali globali di informazione e comunicazione. In questa direzione, l’Assemblea generale ha istituito dal 2004 in poi diversi GGE, con mandati biennali e una composizione variabile (oscillante tra 15 e 25 membri), i quali si sono focalizzati sull’esame delle principali minacce (anche potenziali) alla sicurezza provenienti dallo spazio cibernetico nel tentativo di individuare, nei report finali, strumenti e forme di cooperazione internazionali adeguati ad affrontarle⁹⁴. Sebber-

⁹⁰ Cfr. A. Balsamo, *Spazio virtuale e processo penale: la nuova Convenzione ONU sul cybercrime*, in *Diritto penale e processo*, 2, 2025, 246-247.

⁹¹ Cfr. M. Dimetto, *Convenzione delle Nazioni Unite contro il cybercrime e tutela dei diritti umani: influenze europee sullo scenario internazionale*, cit., 112-113. La Convenzione dedica al tema il Capitolo VII (Technical assistance and information exchange); in particolare v. gli artt. 54-56.

⁹² Assemblea generale delle Nazioni Unite, Risoluzione 53/70 del 4 dicembre 1998, *Developments in the field of information and telecommunications in the context of international security* (UN Doc A/RES/53/70). In dottrina v. P. Gargiulo, *The United Nations and Cybersecurity*, in *La Comunità internazionale*, Quaderno n. 29, P. Gargiulo - D. Giovannelli - A.L. Sciacovelli (eds.), *Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives*, Napoli, 2024, 205 ss.; I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 129-130.

⁹³ Nella denominazione ufficiale *United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UNGGE).

⁹⁴ L’Assemblea generale delle Nazioni Unite ha istituito sei GGE nel 2004, 2009, 2012, 2014, 2016 e 2019 attraverso sei Risoluzioni analoghe, le prime cinque aventi il medesimo oggetto, vale a dire “Developments in the field of information and telecommunications

ne queste relazioni contenessero importanti elementi sugli sviluppi della sicurezza digitale nel cberspazio che confermavano le necessità di applicare pienamente il diritto internazionale allo spazio cibernetico – rappresentando, di fatto, un importante sforzo di implementare quanto previsto dall’Assemblea generale in alcune risoluzioni circa la necessità che una solida cultura globale della cibersicurezza debba essere incoraggiata, promossa, sviluppata e attuata con vigore⁹⁵ – il lavoro dei GGE è contestabile non solo per uno scarsissimo impatto concreto, ma anche in ragione del fatto che forse il compito di raggiungere un accordo di rilevanza globale in relazione all’applicazione uniforme del diritto internazionale alla sicurezza informatica e ai mezzi di informazione e comunicazione nel cberspazio era troppo ambizioso, specialmente per un organismo – è bene ribadirlo, formato da esperti dei governi statali – non in grado di produrre impegni politici o giuridici di vasta portata da parte della comunità internazionale come sarebbe invece necessario se si vuole giungere ad una protezione efficace della cibersicurezza⁹⁶.

Nondimeno, l’emersione di profonde divergenze tra gli Stati membri delle Nazioni Unite portò nel 2018 ad una sorta di “opposizione istituzionale”, dal momento che furono istituiti due diversi “gruppi” di lavoro. Da un lato, il GGE per il periodo 2019-2021 composto da 25 esperti nazionali nominati sulla base di una distribuzione geografica equa, ma pur sempre un gruppo ristretto come previsto dalla Risoluzione 73/266⁹⁷. Dall’altro lato, invece, un nuovo gruppo denominato “*Open-Ended Working Group*” (OEWG)⁹⁸, individuato dalla Risoluzione 73/27⁹⁹ con il medesimo scopo

in the context of international security” (Risoluzione 58/32 dell’8 dicembre 2003 [UN Doc A/RES/58/32](#); Risoluzione 60/45 dell’8 dicembre 2005 [UN Doc A/RES/60/45](#); Risoluzione 66/24 del 2 dicembre 2011 [UN Doc A/RES/66/24](#); Risoluzione 68/243 del 27 dicembre 2013 [UN Doc A/RES/68/243](#); Risoluzione 70/237 del 23 dicembre 2015 [UN Doc A/RES/70/237](#)), e l’ultima avente come oggetto *Advancing responsible State behaviour in cyberspace in the context of international security* (Risoluzione 73/266 del 22 dicembre 2018 [UN Doc A/RES/73/266](#)). Quanto ai risultati di questi gruppi di esperti v. da ultimo il *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security* del 14 luglio 2021 ([UN Doc A/76/135](#)). In dottrina v. F. Delerue - A. Géry, *International Law and Cybersecurity Governance: The Way Forward*, cit., 9-10; P. Gargiulo, *The United Nations and Cybersecurity*, cit., 205 ss.; I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 129-130.

⁹⁵ Risoluzione 64/211 del 21 dicembre 2009, *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures* ([UN Doc A/RES/64/211](#)); analogamente v. anche la Risoluzione 58/199 del 23 dicembre 2003, *Creation of a global culture of cybersecurity and the protection of critical information infrastructures* ([UN Doc A/RES/58/199](#)).

⁹⁶ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 129-130.

⁹⁷ Risoluzione 73/266 del 22 dicembre 2018, *Advancing responsible State behaviour in cyberspace in the context of international security* ([UN Doc A/RES/73/266](#)); si tratta di una risoluzione proposta dagli Stati Uniti e approvata con 138 voti favorevoli, 12 contrari (tra cui Cina e Russia) e 16 astensioni.

⁹⁸ V. in dottrina almeno P. Gargiulo, *The United Nations and Cybersecurity*, cit., 211; F. Delerue - A. Géry, *International Law and Cybersecurity Governance: The Way Forward*, cit., 9-10.

⁹⁹ Risoluzione 73/27 del 5 dicembre 2018, *Developments in the field of information and telecommunications in the context of international security* ([UN Doc A/RES/73/27](#)); si tratta di una risoluzione proposta dalla Federazione russa e approvata con 119 voti favorevoli, 46

di studiare l'applicazione del diritto internazionale al cibernazio, anche con riguardo alla sicurezza, ma contraddistinto da una diversa composizione capace di rappresentare tutti gli Stati delle Nazioni Unite al fine di ricercare un processo negoziale più democratico e inclusivo. Sono stati istituiti due OEWG (2018 per il 2019-2020 e 2020 per il 2021-2025)¹⁰⁰, i quali hanno determinato, il secondo in modo particolare, rilevanti esiti per quanto concerne un possibile sviluppo in termini globali della *governance* della cibersicurezza (v. *infra*).

4. È possibile una *governance* (costituzionale) globale della cibersicurezza?

La rivoluzione digitale ha portato con sé numerosi benefici, ma anche diversi aspetti problematici, tra i quali sono stati evidenziati, anche in questa sede, quelli legati alla cibersicurezza quanto ai pericoli per sistemi informatici, reti e dispositivi digitali, nonché, in maniera conseguente, per i diritti fondamentali. La risposta a tale “lato oscuro” della digitalizzazione segue itinerari diversi, come la diffusione del concetto di “sovranità digitale”, spesso intesa come aspetto della più generale sovranità nazionale e quindi come forma di autonomia tecnologica nel mondo digitale e di controllo, specialmente da parte di uno Stato, su dati, tecnologie e infrastrutture digitali al fine di proteggerli da interferenze esterne¹⁰¹, ovvero, come è emerso nelle pagine precedenti, forme di cooperazione internazionale le quali procedono – lentamente, con numerose difficoltà e (al momento) parzialmente – nella direzione di un integrale quadro normativo del cibernazio¹⁰².

In un siffatto contesto sembra possibile immaginare un nuovo approccio globale, di natura anche costituzionale, alla *governance* e alla regolazione della cibersicurezza¹⁰³, in quella che è stata definita come “*digital constellation*”,

contrari (tra cui Stati Uniti e i Paesi membri dell'Unione europea) e 14 astensioni.

¹⁰⁰ L'Assemblea generale delle Nazioni Unite ha creato due OEWG successivi con un'agenda analoga, nel 2018 (2019-2020) e nel 2020 (2021-2025); Risoluzione 73/27, *Developments in the field of information and telecommunications in the context of international security* del 5 dicembre 2018 (UN Doc A/RES/73/27); Risoluzione 75/240, *Developments in the field of information and telecommunications in the context of international security* del 31 dicembre 2020 (UN Doc A/RES/75/240). Quanto agli esiti di questi due OEWG si vedano: United Nations General Assembly, *Report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* del 18 marzo 2021 (UN Doc A/75/816); United Nations General Assembly, *Final report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025* del 24 luglio 2025 (UN Doc A/80/257).

¹⁰¹ In dottrina v. almeno V. Bertola, *La sovranità digitale e il futuro di Internet*, in *Rivista italiana di informatica e diritto*, 1, 2022, 39-46; G. Finocchiaro, *La sovranità digitale*, in *Diritto pubblico*, 3, 2022, 809 ss.

¹⁰² Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 113-114, 116.

¹⁰³ Quanto al contesto generale della *governance* globale della cibersicurezza v. in dottrina, tra gli altri, V. Greiman, *Cybersecurity and Global Governance*, in *Journal of Information Warfare*, 4, 2015; P. Rosenzweig, *The International Governance Framework for Cybersecurity*, in *Canada-United States Law Journal*, 2, 2012, 405 ss.; S. Jayawardane - J.E. Larik - E. Jackson, *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance*, The Hague Institute for Global Justice Policy Brief, 2015; S. Savaş - S. Karataş, *Cyber governance studies*

vale a dire un modello in grado sia di ricomprendere un panorama complesso e interconnesso di attori (Stati, organismi internazionali, aziende digitali e società civile), sia di coinvolgere i vari livelli di governo interessati dall'evoluzione tecnologica (locale, statale, sovranazionale, internazionale e globale)¹⁰⁴. Sicché l'approccio teorico che meglio potrebbe informare tale formula globale di *governance* e di sviluppo di una cornice costituzionale (anche regolatoria) globale potrebbe essere quello del costituzionalismo globale, nella sua dimensione "verticale" di costituzionalizzazione del diritto internazionale¹⁰⁵; infatti, pur in assenza di un governo mondiale e di un potere costituente tradizionalmente inteso, si tratta di affrontare il tema della legittimazione democratica di decisioni che travalicano i confini delle politiche e della sovranità nazionali e, di conseguenza, costituzionalizzare in una logica democratica il frammentato sistema del diritto internazionale e della *governance* globale (v. *infra*)¹⁰⁶.

Restringendo il campo d'osservazione, almeno per il momento, alla *governance* (globale) della cibersicurezza, questa può essere delineata come un ambito specifico della più generale *governance* di Internet laddove diversi organismi internazionali si trovano coinvolti nel processo di normazione del settore, in una forte interconnessione tra soggetti pubblici e privati¹⁰⁷; alcuni sono specificamente interessati dalla *governance* della cibersicurezza da un punto di vista normativo di diritto internazionale pubblico come il Consiglio d'Europa o le Nazioni Unite, come in parte già osservato, altri svolgono, nell'ambito della *governance* della Rete, un ruolo più tecnico-normativo – come la Internet Engineering Task Force (IETF) o la International Organization for Standardization (ISO) – ovvero consultivo e di promozione del dialogo come l'Internet Governance Forum (IGF) vale a dire la piattaforma globale *multistakeholder* creata dalle Nazioni Unite nel 2006, come parte del World Summit on the Information Society (WSIS), al fine di promuovere la collaborazione tra governi, organizzazioni internazionali, aziende, società civile e accademia per discutere e affrontare le sfide derivanti dal ciber spazio nonché, sempre più, i temi legati alla sicurezza

in ensuring cybersecurity: an overview of cybersecurity governance, cit.

¹⁰⁴ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 116; I. Pernice, *Risk Management in the Digital Constellation – A Constitutional Perspective*, HIIG Discussion Paper Series, 7, 2017; e il chiaro rimando, quanto alla "postnational constellation", a J. Habermas, *The Postnational Constellation: Political Essays*, Cambridge, 2001.

¹⁰⁵ V. sul punto O. Caramaschi, *Il costituzionalismo globale: teorie e prospettive*, Torino, 2022, 119 ss.

¹⁰⁶ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 113. L'A. inoltre, 118, insiste sul ruolo di Internet a tal proposito, in quanto «*multilevel and, as an element of it, global constitutionalism is taken as a normative theory that informs and allows to frame a model of governance that includes legitimate rule-making at the global level as it would not be possible without the internet and, simultaneously, ensures that the internet itself is regulated and can be trusted as an communication infrastructure for not only economic but also democratic processes at all levels*».

¹⁰⁷ Cfr. T. Nascimento Heim, *Global governance and regulation of cybersecurity: Towards coherence or fragmentation?*, Twente, 2023, 19-22, secondo la quale, inoltre, il ruolo degli attori privati «*is related to the proper functioning of the system (confidentiality, integrity and availability), which aims to prevent/ combat cyber threats [or] to promote alternative norms processes opposing state cyber operations. The civil society groups, in turn, became interested in promoting privacy, human rights law and regulating the behaviour of the States and non-state actors in cyberspaces*».

cibernetica, nell'intento di favorire la definizione di taluni requisiti minimi come prima fase di un processo normativo orientato all'identificazione di norme applicabili a livello globale¹⁰⁸.

Eppure, di recente vi è stato un evento di portata significativa e, potenzialmente, rivoluzionaria per quanto riguarda il futuro della *governance* globale della cibersicurezza. Infatti, a luglio 2025 si sono conclusi i lavori dell'*Open-ended Working Group (OEWG) on security of and in the use of information and communications technologies (ICTs) 2021-2025* e nel report finale è stata prevista l'istituzione del *Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs*¹⁰⁹.

Questo "meccanismo globale" avrà carattere permanente, diversamente dai precedenti gruppi di lavoro, e rimarrà a guida statale, nel senso che i negoziati sulla sicurezza delle tecnologie della comunicazione e dell'informazione resteranno prerogativa esclusiva degli Stati, sebbene esso sarà aperto a tutti i membri delle Nazioni Unite con la possibilità di coinvolgere attori e *stakeholders* esterni interessati, quali, ad esempio, le imprese private, le organizzazioni non governative e il mondo accademico¹¹⁰. I lavori del meccanismo globale si svolgeranno con cicli quinquennali attraverso sessioni plenarie, gruppi tematici, riunioni intermedie appositamente dedicate, conferenze di revisione o qualsiasi altra riunione convocata in diversi formati, purché tali differenti modalità si rafforzino reciprocamente ed evitino discussioni duplicate¹¹¹. In particolare, il meccanismo globale si riunirà due volte all'anno, con una settimana di riunioni dei gruppi tematici e una settimana di riunioni in sessione plenaria¹¹², per svolgere alcune

¹⁰⁸ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 133-134.

¹⁰⁹ United Nations General Assembly, *Final report of the open-ended working group on security of and in the use of information and communications technologies 2021-2025* del 24 luglio 2025 (UN Doc A/80/257). La creazione del meccanismo globale si basa sulla proposta dell'OEWG contenuta nell'Allegato C del *Third Annual Report* del luglio 2024 (UN Doc A/79/214), a sua volta sostenuta dall'Assemblea generale nella Risoluzione 79/237 *Open-ended working group on security of and in the use of information and communications technologies 2021-2025 established pursuant to General Assembly resolution 75/240* del 24 dicembre 2024 (UN Doc A/RES/79/237). Come si legge nell'Allegato C, un meccanismo globale permanente e orientato all'azione che si baserà su «*the consensus agreements on the framework of responsible State behaviour in the use of ICTs from previous OEWG and GGE reports with the aim of continuing to promote an open, secure, stable, accessible, peaceful and interoperable ICT environment*» (par. 1) e su un «*open, inclusive transparent, sustainable and flexible process which would be able to evolve in accordance with States' needs and as well as in accordance with developments in the ICT environments*» (par. 4 b-c).

¹¹⁰ Cfr. l'apposita sezione *Additional Elements on Modalities on the Participation of Other Interested Parties and Stakeholders, including Businesses, Non-Governmental Organizations and Academia* prevista nell'*Annex I: Additional Elements for the Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs* (UN Doc A/80/257).

¹¹¹ Cfr. *Annex I*, cit., par. 4.

¹¹² Cfr. *Annex I*, cit., par. 14. Al par. 7 vengono delineati i *Dedicated Thematic Groups*, i quali «*will aim to build on and complement the discussions in the substantive plenary sessions*», in particolare offrendo «*the opportunity for more detailed and action-oriented discussions, allowing in particular the participation of experts*». Si tratta, nel dettaglio, dei seguenti gruppi tematici: «*An integrated, policy-oriented and cross-cutting dedicated thematic group drawing on the five pillars of the framework to address specific challenges in the sphere of ICT security in the context of international security in*

delle rilevanti funzioni che gli sono attribuite, come, ad esempio, l'esame delle cyberminacce esistenti e potenziali, il rafforzamento della sicurezza delle tecnologie della comunicazione e dell'informazione degli Stati, la predisposizione e l'attuazione di strumenti di soft law volontari e non vincolanti quanto al comportamento responsabile degli Stati nell'ecosistema cibernetico, ovvero l'applicazione del diritto internazionale al mondo digitale e della cibersicurezza anche con particolare riguardo alla possibilità di elaborare ulteriori norme vincolanti¹¹³.

Ora questo nuovo meccanismo globale, al momento delineatosi soltanto in maniera parziale e pertanto ancora da valutare nel suo concreto funzionamento, ben potrebbe rappresentare il punto di partenza di uno sforzo di individuazione (almeno teorico) di un nuovo modello – basato su organismi, strutture e politiche già presenti (o da sviluppare) – di «complementary normative process» per la governance della cibersicurezza a livello globale¹¹⁴. Questo si dovrebbe fondare su organismi globali *multistakeholder*, come l'IGF e l'appena menzionato meccanismo globale, deputati all'elaborazione di principi e norme in materia di cibersicurezza da trasporre in una fase successiva in normative applicabili a livello globale, rese giuridicamente vincolanti attraverso la combinazione di normazione e standardizzazione da parte di organismi tecnici – come i richiamati IETF o ISO – da un lato, e i processi legislativi nazionali e sovranazionali sul modello europeo dall'altro¹¹⁵. Contestualmente si renderà necessario procedere anche in maniera più generale e globale per il tramite di convenzioni internazionali elaborate, come nel recente caso della Convenzione sul cybercrime, dalle Nazioni Unite, le quali si troveranno impegnate in una doppia veste attraverso i propri organi appositamente dedicati, da un lato incaricandosi di coordinare e supervisionare l'adozione di tali norme vincolanti e applicabili globalmente nonché l'approvazione – sul modello della Convenzione di Budapest – delle strategie e delle legislazioni nazionali in tema di cibersicurezza, dall'altro assumendosi la responsabilità di supervisionare tali processi, ad esempio affidandola al Consiglio di sicurezza o, forse preferibilmente, al Segretario generale, ovvero di monitorare sull'applicazione di queste stesse norme, anche (e forse soprattutto) attraverso il contributo determinante di corti e tribunali di tutti i livelli nel vigilare sull'applicazio-

order to promote an open, secure, stable, accessible, peaceful, and interoperable ICT environment, with the participation of, inter alia, technical experts and other stakeholders. (DTG 1)»; «An integrated, policy-oriented and cross-cutting dedicated thematic group drawing on the five pillars of the framework to accelerate ICT security capacity-building, with the participation of, inter alia, capacity-building experts, practitioners, and other stakeholders. (DTG 2)».

¹¹³ Cfr. A. Insolia, *The impact of the practice of international organizations on the United Nations recent works on cybersecurity*, in *DPCE online*, 2, 2025, 966-967.

¹¹⁴ I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 136.

¹¹⁵ Ivi, 136-138. Secondo l'A. IETF e ISO «*have proved to be an excellent framework for setting technical standards as a basis for interoperability, and they should focus on privacy and cybersecurity engineering even more*». Inoltre, con riguardo alla cibersicurezza, una stretta interazione tra questi soggetti e i processi legislativi «*could lead to a burden-sharing between legislators on the one hand, who would be responsible for setting up, on the basis of the principles adopted by the bodies described, minimum security requirements for products and services, and standardisation bodies like IETF or ISO on the other, which would turn these requirements into technical norms to be met by products or terms of services before they are put on the markets*».

ne concreta e possibilmente uniforme di tali disposizioni¹¹⁶. Inoltre, se l'attuazione di tali norme sulla cibersicurezza negli ordinamenti giuridici resterà compito delle autorità nazionali, magari sotto la supervisione di organismi delle Nazioni Unite, come appunto il nuovo meccanismo globale, quest'ultimo potrebbe, infine, ricoprire un fondamentale compito di vigilanza sull'implementazione delle norme, nonché, contestualmente, quello di elaborazione di proposte di revisione delle stesse¹¹⁷.

Un così delineato modello di *governance* della cibersicurezza necessiterebbe, a questo punto, di una dimensione "costituzionale" di legittimazione democratica, nella misura in cui tali organismi, istituzioni e processi dovrebbero trovare una qualche forma di legame, più o meno diretto, con la volontà dei cittadini nella loro veste di "cittadini globali". L'elemento politico-democratico potrebbe essere contestualizzato nella cornice teorica del costituzionalismo globale, recuperando e declinando anche a livello globale l'approccio e gli strumenti propri del costituzionalismo multilivello, il quale consentirebbe di concettualizzare tale quadro "costituzionale" non tanto come un sistema centralizzato di potere a livello globale, ma piuttosto in quanto parte di un sistema costituzionale composito nel quale trovano collocazione elementi nazionali, sovranazionali e globali, in modo tale da collegare tra loro i cittadini e gli attori dei vari livelli¹¹⁸.

La produzione di normativa globale nel contesto della *governance* globale della cibersicurezza, necessiterebbe, a tal proposito, di essere accettata e legittimata democraticamente dai "cittadini globali", in particolare attraverso processi decisionali e di formazione della volontà che dovranno essere costruiti in maniera inclusiva e non sostitutiva dei processi politico-democratici e legislativi nazionali, ma che anzi saranno necessariamente basati proprio su questi nella dimensione costituzionale multilivello, pur nella consapevolezza che sarebbe opportuno integrarli con nuove e complementari forme globali di «action, control and judicial review»¹¹⁹. Proprio in questa direzione gli strumenti della democrazia digitale (o *e-democracy*)¹²⁰ costituiscono una delle possibili strade per sviluppare questa declinazione del costituzionalismo globale, peculiarmente perché potrebbero integrare le forme di democrazia tradizionale attualmente esistenti per quanto riguarda la legittimazione democratica della *governance* globale della ciber-

¹¹⁶ Ivi, 137-138.

¹¹⁷ Per un primissimo commento al nuovo meccanismo e alle sue prospettive future v. R. Payne, *The OEWG ends and a new UN cybersecurity permanent mechanism is born*, in *Global Partners Digital*, 24 luglio 2025; P. Pavlova - C. Painter, *The UN's Permanent Process on Cybersecurity Faces an Uphill Battle*, in *Lawfare*, 13 agosto 2025.

¹¹⁸ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 139-140. Sul punto in particolare v. Id., *The Global Dimension of Multilevel Constitutionalism: A Legal Response to the Challenges of Globalisation*, in P.-M. Dupuy - C. Tomuschat (eds.), *Völkerrecht als Wertordnung: Festschrift für Christian Tomuschat. Common values in international law: essays in honour of Christian Tomuschat*, Kehl am Rhein, 2006, 973 ss.

¹¹⁹ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 139-140.

¹²⁰ Per un inquadramento generale dell'*e-democracy* nel contesto dello spazio cibernetico v. almeno, da ultimo, O. Caramaschi, *La democrazia digitale (o e-democracy) nello spazio cibernetico: inquadramento teorico e profili applicativi*, in *Federalismi.it*, 33, 2025, 14-49.

sicurezza¹²¹; ciò dovrebbe avere luogo secondo una logica bidirezionale, perché se è vero che la democrazia digitale può svolgere un ruolo importante di partecipazione e legittimazione democratica nel ciberspazio anche con riguardo alla cibersicurezza, è altrettanto certo che lo sviluppo stesso dell'*e-democracy* richieda strumenti adeguati di tutela della sicurezza informatica dalle sempre più crescenti minacce provenienti dallo spazio cibernetico¹²².

Proprio quelle stesse minacce, come sfida posta dall'avvento della rivoluzione digitale, che richiedono di essere affrontate non tanto dagli Stati individualmente, ma a tutti i livelli da quello locale fino a quello globale, in una cornice costituzionale di *governance* della cibersicurezza che, nella logica del costituzionalismo globale, sia in grado di tutelare i diritti fondamentali e offrire adeguate forme di regolazione e controllo del potere digitale anche con specifico riguardo alla sicurezza cibernetica.

¹²¹ Cfr. I. Pernice, *Global cybersecurity governance: A constitutionalist analysis*, cit., 140-141, nonché Id., *E-Democracy, the Global Citizen, and Multilevel Constitutionalism*, in C. Prins - C. Cuijpers - P.L. Lindseth - M. Rosina (eds.), *Digital Democracy in a Globalised World*, Cheltenham, 2017, 27 ss.

¹²² Cfr. C.M. Codreanu, *Digital democracy in peril. Safeguarding e-democracy by boosting cybersecurity*, in *Proceedings of the Smart Cities International Conference*, 9, 2021, 471-472. Secondo l'A., infatti, «*liberal democracies should develop policies regarding cybersecurity, as cybersecurity should not be enhanced whilst democracy, individual freedoms and human rights deteriorated, but on the contrary cybersecurity should be strengthened alongside the promotion and consolidation of democratic processes, and this policy should also be promoted internationally. [...] Nevertheless, in order to develop e-democracy, governments should also take into consideration and seriously address cyber threats. The more democratic processes move (even partially) in cyberspace, the more vulnerabilities are created, which also means there will be more opportunities for malicious cyber operations, and hence cybersecurity should be a core element of every policy, programme, initiative or activity of anything digital done by governments, whether it is about e-democracy, e-government platforms or political parties campaigning on social media during elections*».

Abstract

Nel contesto della digitalizzazione globale e della sempre maggiore interconnessione digitale viene in evidenza il tema della sicurezza cibernetica o cibernsicurezza, la quale non riguarda soltanto le minacce provenienti dalla dimensione fisica, ma allarga il proprio orizzonte di riferimento includendo quelle del mondo virtuale del ciberspazio, assumendo una dimensione trasversale che interessa i singoli individui, le imprese, la società nel suo complesso, ma anche gli Stati e gli organismi sovranazionali e internazionali. Ed è proprio a questi ultimi livelli che la cibernsicurezza richiede un'azione istituzionale e regolativa opportunamente in grado di rispondere alle sfide e alle minacce provenienti dallo spazio cibernetico e dal mondo digitale. Sebbene la risposta a tali nuovi elementi problematici dovrebbe partire proprio dagli Stati e dagli strumenti costituzionali a loro disposizione, non può non osservarsi come i singoli Stati siano difficilmente in grado di garantire le condizioni essenziali per la sicurezza dei diritti dei cittadini nel ciberspazio, essendo invece necessario rispondere alle sfide globali derivanti per la cibernsicurezza con forme di cooperazione sovranazionali e altrettanto globali al fine di rendere consistente la sicurezza nello spazio cibernetico ed effettiva la tutela dei diritti fondamentali anche nel nuovo mondo digitale.

In the context of global digitalization and ever-increasing digital interconnection, the issue of cybersecurity comes to the fore. This concerns not only threats from the physical realm but also expands its scope to include those from the virtual world of cyberspace. This encompasses a transversal dimension that affects individuals, businesses, society as a whole, but also States and supranational and international organizations. It is precisely at these latter levels that cybersecurity requires appropriate institutional and regulatory action capable of responding to the challenges and threats posed by cyberspace and the digital world. While the response to these new challenges should begin with States and the constitutional instruments at their disposal, it is clear that individual States are unlikely to be able to guarantee the essential conditions for the security of citizens' rights in cyberspace. Instead, it is necessary to respond to the global challenges posed by cybersecurity with supranational and equally global forms of cooperation in order to ensure consistent cybersecurity and effective protection of fundamental rights in the new digital world.

Keywords

cibernsicurezza – spazio cibernetico – governance costituzionale globale – digitalizzazione – sicurezza digitale