ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

5 OTTOBRE 2022

Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico

di Luigi Previti
Ricercatore di Diritto amministrativo
Università degli Studi di Palermo

Pubblici poteri e cybersicurezza: il lungo cammino verso un approccio collaborativo alla gestione del rischio informatico*

di Luigi Previti
Ricercatore di Diritto amministrativo
Università degli Studi di Palermo

Abstract [It]: Il contributo mira ad analizzare l'attuale architettura istituzionale relativa alla cybersicurezza. Dopo aver richiamato i più significativi interventi legislativi adottati in materia a livello europeo e nazionale, il lavoro evidenzia come la migliore assicurazione possibile contro il rischio di attacchi informatici sia rappresentata dall'ampia partecipazione dei diversi protagonisti del cyberspazio al sistema di protezione della pubblica sicurezza cibernetica. Adottando una siffatta prospettiva, l'articolo sottolinea il ruolo strategico svolto dagli operatori economici del settore e dagli utenti delle reti e dei servizi digitali ai fini della definizione di una struttura più aperta e condivisa di prevenzione e di monitoraggio. Un ruolo che, tuttavia, non sembra essere ancora adeguatamente valorizzato all'interno dell'ordinamento giuridico italiano.

Title: Public authorities and cyber security: the long road to a collaborative approach to cyber risk management
Abstract [En]: The article aims to analyze the current institutional framework about cybersecurity. After having referred to the most significant legislative measures at European and national level, the work highlights that the best possible insurance against cyber risks is represented by the wide participation of the various protagonists of the cyberspace to the protection system of cyber public security. Moving from this perspective, the strategic role played by the economic operators and the users of the online infrastructures and services to the definition of a more shared system of prevention and monitoring is remarked. A role that, however, does not seem to be adequately valued within the Italian legal framework.

Parole chiave: transizione digitale; cyberspazio; sicurezza cibernetica; attacchi informatici; gestione del rischio; collaborazione pubblico-privato
Keywords: digital transformation; cyberspace; cybersecurity; cyber attacks; risk management; public-private partnership

1. Rischi informatici e transizione digitale

Negli ultimi anni il processo di digitalizzazione dei diversi settori dell'economia e della società ha raggiunto risultati alquanto sorprendenti, anche grazie allo sviluppo e alla diffusione di tecnologie e infrastrutture informatiche sempre più sofisticate e interconnesse[1]. L'obiettivo di sfruttare a pieno i

* Articolo sottoposto a referaggio.

[1] Com'è noto, si assiste oggi ad una moltiplicazione di sistemi informatici costantemente connessi ad *internet*, in grado di interagire tra di loro e con il mondo fisico in cui operano attraverso l'uso di appositi sensori. Si tratta di dispositivi che possono essere integrati all'interno degli oggetti fisici più diversi (*i.e.*, veicoli, edifici, elettrodomestici, lampioni stradali,

vantaggi ricavabili dall'uso dei predetti strumenti ha posto al centro del dibattito scientifico rilevanti questioni problematiche, come quelle inerenti alla creazione di un'architettura istituzionale in grado di affrontare l'emersione di nuove minacce per i diritti e le libertà fondamentali, rispetto alle quali le categorie giuridiche preesistenti risultano spesso inadeguate o inefficaci[2].

Un significativo segnale del cambiamento di prospettiva indotto dall'esigenza di gestire fenomeni e vulnerabilità ancora poco conosciuti può essere colto nei recenti atti normativi di matrice europea, ove la valutazione analitica della tipologia e dell'intensità dei diversi pericoli intrinsecamente legati alle moderne ICT viene indicata quale nuovo, necessario *modus operandi* per tutti i soggetti, pubblici e privati, che svolgono le proprie attività quotidiane all'interno del cyberspazio[3].

In questa direzione si inserisce, tra le altre, la proposta di regolamento europeo sull'intelligenza artificiale, pubblicata dalla Commissione europea il 21 aprile 2021 (c.d. *Artificial Intelligence Act*), con la quale sono state gettate le basi per la costruzione di un contesto di maggiore fiducia verso l'odierna rivoluzione digitale, di promozione degli investimenti finanziari nel settore e di salvaguardia dei principi e dei valori dell'Unione[4]. Con tale atto è stata suggerita, per la prima volta, l'introduzione di un quadro omogeneo di condizioni e di requisiti minimi ispirati ad una logica di tipo *risk-based*, ossia parametrati allo specifico livello di rischio che i singoli sistemi informatici presentano nei confronti della sicurezza, della salute e

ecc.) e che formano una rete di strumenti ormai nota con l'espressione *Internet of Things* (IoT). Per avere un'idea più chiara del fenomeno, si osservi che, secondo le stime di *International Data Corporation*, il principale fornitore globale di servizi di consulenza nel settore delle ICT, entro il 2025 il numero di macchine, di sensori e di telecamere connesse alla rete sarà pari a 41,6 miliardi. In materia, cfr. R.H. WEBER, E. STUDER, *Cybersecurity and the Internet of Things: Legal Aspect*, in *Computer Law & Security Review*, n. 36, 2016, p. 726 ss.; A. RAYES, S. SALAM, *Internet of Things: from Hype to Reality*, Springer, Cham, 2019; L. DE NARDIS, *The Internet in Everything. Freedom and Security in a World with No Off Switch*, New Haven, Yale University Press, 2020; G. NOTO LA DIEGA, *Internet of Things and the Law. Legal Strategies for Consumer-Centric Smart Technologies*, Routledge, Londra, 2022.

[2] Sulla capacità dell'innovazione tecnologica di mettere in crisi i preesistenti modelli e schemi concettuali, quali la sovranità statale, la spazialità dell'applicazione delle norme giuridiche, nonché il tradizionale ruolo degli attori pubblici e privati, cfr. J.L. BOWER, C.M. CHRISTENSEN, *Disruptive Technologies: Catching the Wave*, in *Harvard Business Review*, n. 73, 1995, p. 43 ss.

[3] Sulla necessità di affrontare i nuovi, inevitabili rischi connessi alla continua crescita della dimensione del cyberspazio, si vedano le recenti riflessioni di L. VIOLANTE, *Diritto e potere nell'era digitale. Cybersociety, cybercommunity, cyberstate, cyberspace: tredici tesi*, in *BioLaw Journal*, n. 1, 2022, p. 146, secondo il quale: «In termini di sicurezza il *cyberspace* costituisce il quarto dominio perché le problematiche della sicurezza, oltre a svilupparsi sulla terra, in mare e nello spazio, oggi si sviluppano anche nello spazio *cyber*»; con riferimento agli attuali rischi «da ignoto tecnologico», è doveroso, invece, il richiamo al lavoro di A. BARONE, *Il diritto del rischio*, Giuffrè, Milano, 2006, *passim*. Più in generale, sulla possibilità di qualificare la società contemporanea come "società del rischio", si vedano, per tutti, U. BECK, *La società del rischio. Verso una seconda modernità*, Carocci, Roma, 2000, spec. p. 25 ss., ove l'A. sottolinea che «nella modernità avanzata la produzione sociale di ricchezza va sistematicamente di pari passo con la produzione sociale di rischi» e, in particolare, quelli «prodotti dalla scienza e dalla tecnica», nonché F. FUKUYAMA, *L'uomo oltre l'uomo. Le conseguenze della rivoluzione biotecnologica*, Mondadori, Milano, 2002.

[4] Proposta di regolamento del Parlamento europeo e del Consiglio del 21 aprile 2021 che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale), COM/2021/206 final, in *www.eur-lex.europa.eu*. La proposta è stata accompagnata da due atti normativi adottati il medesimo giorno, ossia la comunicazione della Commissione europea, *Promuovere un approccio europeo all'intelligenza artificiale*, COM (2021) 205 final, nonché il Piano coordinato riveduto sull'intelligenza artificiale, COM (2021) 205 final, allegato alla predetta comunicazione, entrambi reperibili in *www.eur-lex.europa.eu*.

della sfera giuridica individuale. Un approccio metodologico che si fonda, in buona sostanza, sulla fissazione di limitazioni d'uso e di obblighi di progettazione chiari e proporzionati, sul contenimento dei costi di conformità alla normativa di settore da parte degli operatori economici e sulla previsione di oneri di monitoraggio e di segnalazione degli incidenti in capo agli stessi utenti[5].

Tra le principali criticità che interessano il processo di informatizzazione attualmente in corso, un posto di primario rilievo è certamente occupato dalle nuove insidie che si affacciano sulla dimensione della pubblica sicurezza cibernetica o della c.d. cybersicurezza[6]. Un tema che, pur costituendo, come pare evidente, la naturale precondizione per la crescita economica e lo sviluppo industriale degli Stati moderni, ha ricevuto soltanto di recente un'adeguata attenzione nelle agende politiche internazionali[7].

[5] Sull'impostazione seguita dalla suddetta proposta di regolamento europeo si vedano, quantomeno, G. MARCHIANÒ, *Proposta di regolamento della Commissione europea del 21 aprile 2021 sull'intelligenza artificiale con particolare riferimento alle IA ad alto rischio*, in *Ambientediritto.it*, n. 2, 2021; C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *Biolaw Journal*, n. 3, 2021, p. 415 ss.; G. DI GREGORIO, F. PAOLUCCI, O. POLLICINO, *L'intelligenza artificiale made in UE è davvero "umano-centrica"? I conflitti della proposta*, in *www.agendadigitale.eu*, 22 luglio 2021; F. LAMBERTI, *La proposta di regolamento UE sull'Intelligenza artificiale alla prova della privacy*, in *Federalismi.it*, 29 giugno 2022. In materia, cfr. anche A. BARONE, *Amministrazione del rischio e intelligenza artificiale*, in *European Review of Digital Administration Law*, n. 1-2, 2020, p. 65 ss., secondo il quale l'intera tematica dell'IA è dominata dalle esigenze di regolazione e di gestione dei rischi (sociali, economici, tecnici) che possono derivare dall'uso delle nuove tecnologie.

[6] Sul concetto di «sicurezza cibernetica», cfr. art. 2, comma 1, lett. *i*), DPCM 24 gennaio 2013, n. 66, ai sensi del quale la locuzione indica la «condizione per la quale lo spazio cibernetico risulti protetto grazie all'adozione di idonee misure di sicurezza fisica, logica, procedurale rispetto ad eventi, di natura volontaria o accidentale, consistenti nell'acquisizione e nel trasferimento indebiti di dati, nella loro modifica o distruzione illegittima, ovvero nel danneggiamento, distruzione o blocco del regolare funzionamento delle reti e dei sistemi informativi o dei loro elementi costitutivi», laddove per «spazio cibernetico» (o cyberspazio) deve intendersi, invece, «l'insieme delle infrastrutture informatiche interconnesse, comprensivo di *hardware*, *software*, dati ed utenti, nonché delle relazioni logiche, comunque stabilite, tra di essi». In dottrina, 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*, n. 21, 2021, pp. 20-21, i quali ricordano che limitare il concetto di sicurezza informatica alla sola protezione delle reti e dei sistemi informatici è oggi fuorviante e anacronistico; e ciò dal momento che un attacco *cyber* può causare non solo danni tecnologici, ma anche ledere diritti e libertà fondamentali, alterare gli equilibri politici di una nazione e, qualora vengano colpite infrastrutture critiche, determinare gravi conseguenze per comunità, istituzioni e imprese. In generale, per un'approfondita analisi dell'evoluzione del concetto di sicurezza pubblica nell'ordinamento giuridico italiano, si veda, da ultimo, il lavoro monografico di R. URSI, *La sicurezza pubblica*, Il Mulino, Bologna, 2022.

[7] Come si preciserà *infra*, infatti, un reale interessamento delle istituzioni pubbliche per le rilevanti questioni problematiche poste dalla tutela della cybersicurezza si è concretamente manifestato solo negli ultimi anni: dapprima, come conseguenza dell'accelerazione del processo di transizione digitale delle dinamiche economiche e sociali dovuta all'esperienza della pandemia da COVID-19 e, poi, come esigenza istituzionale indotta dall'esponenziale aumento di attacchi cibernetici riconducibili allo scoppio del drammatico conflitto tra Russia e Ucraina. Sui profili di diritto internazionale connessi alla tematica in esame, si vedano, tra gli altri, M.N. SCHMITT (a cura di), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge (UK), 2013; P. MARGULIES, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, in *Melbourne Journal of International Law*, n. 2, 2013, p. 496 ss.; J. MAOGOTO, *Technology and the Law on the Use of Force: New Security Challenges in the Twenty-First Century,* Routledge, Londra, 2014; N. TSAGOURIAS, R. BUCHAN (a cura di), *Research Handbook on International Law and Cyberspace,* Edward Elgar, Cheltenham, 2015; J. D'ASPREMONT, *Cyber Operations and International Law: An Interventionist Legal Thought*, in *Journal of Conflict & Security Law*, n. 3, 2016, p. 575 ss.; C. WHYTE, B.M. MAZANEC, *Understanding Cyber Warfare: Politics, Policy and Strategy*, Routledge, Londra, 2019.

Muovendosi nell'ambito delle suddette coordinate, il presente contributo mira ad analizzare l'attuale sistema istituzionale rivolto a contrastare l'impatto dirompente delle sempre più frequenti minacce cibernetiche, quali fattori in grado di pregiudicare l'effettivo raggiungimento degli obiettivi di transizione digitale stabiliti, da ultimo, nel Piano nazionale di ripresa e resilienza[8].

A tal proposito, dopo aver ricostruito, seppur brevemente, l'articolata architettura multilivello formatasi negli ultimi anni, l'analisi evidenzia il ruolo strategico del settore privato-imprenditoriale nella costruzione, all'interno del nostro ordinamento, di un meccanismo dinamico e partecipato di monitoraggio della rete informatica, anche nell'ottica dell'ulteriore affinamento delle recenti strategie di prevenzione e di protezione messe in campo *in subiecta materia*. Le considerazioni finali sottolineano il valore della collaborazione pubblico-privato non solo ai fini dell'accrescimento della resilienza delle infrastrutture e dei servizi digitali di fronte al verificarsi di crisi e di attacchi *cyber*, ma anche ai fini dell'affermazione di una solida cultura nazionale del rischio informatico per tutti i cittadini e le imprese.

2. Attori istituzionali e strumenti multilivello di tutela della cybersicurezza

La sensibilità dell'Unione per la salvaguardia della sicurezza delle reti e dei sistemi informatici emerge fin dai primi atti di indirizzo dedicati all'uso delle ICT, ove il perseguimento di tale obiettivo è posto in stretta correlazione alla creazione del mercato unico, quale spazio in cui i movimenti transfrontalieri di persone, beni e servizi vengono non solo agevolati, ma anche adeguatamente presidiati[9].

[8] Il rafforzamento della cybersicurezza nazionale costituisce, non a caso, uno degli ambiti di intervento del PNRR (Missione 1, Componente 1.1., Investimento 1.5), che riconosce il rapporto direttamente proporzionale tra la maggiore digitalizzazione del Paese e la sua maggiore esposizione alle minacce *cyber*. In tal senso, gli investimenti finanziari proposti in materia (0,62 Mld) riguardano quattro principali aree: *i*) il rafforzamento dei presidi di *front-line* per la gestione delle notifiche e degli eventi rischiosi che interessano le pubbliche amministrazioni e le imprese di interesse nazionale; *ii*) il consolidamento delle capacità tecniche di valutazione e di *audit* della sicurezza degli *hardware* e dei *software* utilizzati per l'erogazione di servizi critici da parte di soggetti, pubblici e privati, che svolgono una funzione essenziale; *iii*) l'assunzione e la formazione di personale competente nelle aree di pubblica sicurezza e di polizia giudiziaria dedicate alla prevenzione e investigazione del crimine informatico; *iv*) il rafforzamento degli *asset* e delle unità incaricate della protezione della sicurezza nazionale e della risposta alle minacce *cyber*.

[9] Sotto questa prospettiva, la predisposizione di un adeguato apparato di prevenzione e di contrasto nei confronti delle minacce cibernetiche rappresenta il naturale contraltare dell'impulso, impresso dalle stesse istituzioni dell'Unione, verso l'introduzione e l'utilizzo di sistemi e dispositivi tecnologici sempre più evoluti e interconnessi. Tra i primi interventi in materia occorre ricordare, tra gli altri, la comunicazione della Commissione europea del 6 giugno 2001, *Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo*, COM (2001) 298, par. 2.1, in *www.eur-lex.europa.eu*, in base alla quale: «La sicurezza delle reti e dell'informazione va intesa come la capacità di una rete o di un sistema d'informazione di resistere, ad un determinato livello di riservatezza, ad eventi imprevisti 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»; la direttiva 2002/21/CE del 7 marzo 2022, che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica e affida alle autorità nazionali di regolazione il compito di garantire il mantenimento dell'integrità e della sicurezza delle reti e delle comunicazioni pubbliche (art. 8, comma 4, lett. f); la comunicazione della Commissione europea del 26 settembre 2003, *Il ruolo dell'e-Government per il futuro dell'Europa*, COM (2003) 567, par. 2.1, in *www.eur-lex.europa.eu*, ove si riconosce che: «In futuro i cittadini esigeranno sempre più che le pubbliche autorità provvedano a tutelare la libertà, la giustizia e la sicurezza in tutta l'Unione europea. Occorre a tal fine garantire una cooperazione tra gli Stati membri e a livello internazionale e fare anche fronte a nuove forme di

Tuttavia, la consapevolezza di dover assicurare un più elevato livello di protezione degli enti e degli utenti che utilizzano le moderne tecnologie per le proprie attività economiche e istituzionali ha condotto negli ultimi anni all'introduzione di un quadro normativo maggiormente incisivo e coordinato in materia[10].

Sotto questa prospettiva, va rilevato come l'adozione e la successiva attuazione di una strategia europea per la cybersicurezza costituiscano un passaggio fondamentale per il successo delle recenti iniziative di

insicurezza generate dall'utilizzo di nuove tecnologie». In dottrina, sull'evoluzione della disciplina europea in tema di sicurezza informatica, cfr. C. CENCETTI, *Cybersecurity: Unione europea e Italia. Prospettive a confronto*, Nuova Cultura, Roma, 2014, p. 21 ss.; A. CONTALDO, D. MULA (a cura di), *Cybersecurity Law*, Pacini, Pisa, 2020, p. 7 ss.; C KOHLER, *The EU Cybersecurity Act and European standard: an introduction to the role of European standardization*, in *International Cybersecurity Law Review*, n. 1, 2020, p. 7 ss.

[10] A tal riguardo, cfr. il regolamento UE 2021/694 del 29 aprile 2021 che istituisce il programma "Europa digitale" (2021-2027), il quale, dopo aver indicato gli obiettivi principali del programma (calcolo ad alte prestazioni; intelligenza artificiale; cybersicurezza e fiducia; competenze digitali avanzate; implementazione e impiego ottimale delle capacità digitali e interoperabilità), sottolinea che: «La fiducia costituisce una condizione essenziale per il funzionamento del mercato unico digitale. Le tecnologie della cibersicurezza, come le identità digitali, la crittografia e il rilevamento delle intrusioni, e le loro applicazioni in ambiti quali il settore finanziario, l'industria 4.0, l'energia, i trasporti, la sanità e l'amministrazione elettronica sono essenziali per salvaguardare la sicurezza e la fiducia nelle attività e nelle operazioni online da parte dei cittadini, delle pubbliche amministrazioni e delle imprese» (Considerando 39).

innovazione tecnologica[11], finalizzate non solo a garantire servizi digitali efficienti e affidabili[12], ma anche a rafforzare la capacità dell'Unione di gestire il rischio di attacchi cibernetici[13].

Alla realizzazione di questi obiettivi è specificamente rivolta la direttiva UE 2016/1148, nota anche come "direttiva NIS" (*Network and Information Security*), che rappresenta il primo importante tentativo di armonizzazione delle legislazioni nazionali in tema di prevenzione e di risposta alle vulnerabilità informatiche nei settori più importanti[14].

---

[11] In materia si vedano, tra gli altri, la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 7 febbraio 2013, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, JOIN (2013) 1 final, in *www.eur-lex.europa.eu*; la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, JOIN (2017) 450 final, in *www.eur-lex.europa.eu*, ove l'Unione riconosce, per la prima volta, che: «sempre più spesso gli attori statali raggiungono i loro obiettivi geopolitici non solo attraverso strumenti tradizionali come la forza militare, ma anche attraverso strumenti cibernetici più discreti, volti anche ad interferire nei processi democratici interni. È ormai ampiamente noto l'utilizzo del ciberspazio come terreno di guerra, da solo o nell'ambito di un approccio ibrido. Le campagne di disinformazione, le notizie false e le operazioni cibernetiche mirate ad infrastrutture critiche sono sempre più comuni e richiedono una risposta. Per questo motivo, […] la Commissione ha sottolineato l'importanza della cooperazione nella ciberdifesa» (p. 2); la comunicazione della Commissione europea del 19 febbraio 2020, *Plasmare il futuro digitale dell'Europa*, COM (2020) 67 final, in *www.eur-lex.europa.eu*, ove si precisa che: «Una vera trasformazione digitale deve iniziare dalla fiducia di cittadini e imprese europei nella sicurezza di prodotti e applicazioni. Quanto più siamo interconnessi, tanto più siamo vulnerabili alle attività informatiche dolose. Per far fronte a questa minaccia crescente dobbiamo collaborare costantemente: stabilendo regole coerenti per le imprese e meccanismi più forti per la condivisione proattiva delle informazioni; garantendo la cooperazione operativa tra gli Stati membri e tra l'UE e gli Stati membri; stabilendo sinergie tra la ciberresilienza civile e le cibersicurezza; attività di contrasto e difesa nell'ambito della cibersicurezza; garantendo che le forze dell'ordine e la magistratura possano operare in modo efficace sviluppando nuovi strumenti da utilizzare contro i criminali informatici; e, non da ultimo, sensibilizzando i cittadini dell'UE alla cibersicurezza» (p. 5); nonché la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, JOIN (2020) 18 final, in *www.eur-lex.europa.eu*, che aggiorna la precedente strategia europea del settembre 2017 e che viene espressamente considerata come una componente essenziale per la piena realizzazione della transizione digitale dell'Europa e degli obiettivi indicati nel *Recovery plan*.

[12] In tal senso, cfr. la proposta di regolamento del Parlamento europeo e del Consiglio del 15 dicembre 2020, relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE, COM (2020) 825 final, in *www.eur-lex.europa.eu,* la quale intende migliorare il funzionamento del mercato interno e garantire un ambiente *online* sicuro e trasparente attraverso «una serie chiara ed equilibrata di obblighi armonizzati in materia di dovere di diligenza per i prestatori di servizi intermediari. Tali obblighi dovrebbero in particolare mirare a conseguire diversi obiettivi di interesse pubblico quali la sicurezza e la fiducia dei destinatari del servizio, compresi i minori e gli utenti vulnerabili, la tutela dei pertinenti diritti fondamentali sanciti dalla Carta, la garanzia di una significativa assunzione della responsabilità da parte di tali prestatori e il conferimento di maggiore potere ai destinatari e alle altre parti interessate, agevolando nel contempo la necessaria vigilanza da parte delle autorità competenti» (Considerando 34).

[13] Sulle nuove esigenze di sicurezza connesse all'avanzamento del processo di digitalizzazione dell'Unione, si veda la comunicazione della Commissione europea del 24 luglio 2020, *La strategia dell'UE per l'Unione della sicurezza*, COM (2020) 605 final, in *www.eur-lex.europa.eu,* ove si sottolinea che: «i benefici sempre più numerosi che le tecnologie digitali hanno apportato alla nostra vita hanno fatto della cibersicurezza delle tecnologie una questione di importanza strategica. I cittadini, le banche, i servizi finanziari e le imprese (in particolare le piccole e medie imprese) risentono pesantemente degli attacchi informatici. L'interdipendenza tra i sistemi fisici e quelli digitali aggrava ulteriormente i danni potenziali: qualsiasi impatto fisico è destinato a incidere sui sistemi digitali, mentre gli attacchi informatici ai sistemi di informazione e alle infrastrutture digitali possono bloccare i servizi essenziali. L'avvento dell'*internet* degli oggetti e il maggiore ricorso all'intelligenza artificiale comporteranno nuovi benefici ma anche una serie di nuovi rischi. […] La dipendenza da sistemi *online* ha dato il via a un'ondata di attacchi da parte della cibercriminalità. Il cosiddetto "*cybercrime-as-a-service*" (ossia l'offerta di servizi illegali) e l'economia "cibercriminale" sotterranea offrono un agevole accesso a prodotti e servizi informatici *online* offerti dalla criminalità informatica» (p. 3-4).

[14] Cfr. la direttiva UE 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, recepita nel nostro ordinamento dal d.lgs. 18 maggio 2018, n. 65. Sul punto, cfr. L. SALAMONE, *La disciplina del cyberspace alla luce della*

Nello specifico, pur seguendo un approccio regolatorio minimale[15], il legislatore europeo ha affidato, in primo luogo, ai singoli Stati membri il compito di: *i*) adottare una strategia nazionale sulla cybersicurezza, al fine di individuare priorità di intervento, piani di valutazione dei rischi, misure di risposta agli attacchi *cyber*, nonché di attivare programmi di formazione e di sensibilizzazione collettiva sulle diverse tematiche legate alla sicurezza delle reti e dei servizi *online*; *ii*) designare una o più autorità nazionali competenti in materia di sicurezza informatica (c.d. Autorità NIS), al fine di garantire la corretta attuazione dei principi e delle disposizioni della suddetta direttiva; *iii*) istituire un gruppo unico di intervento in caso di incidenti informatici (*Computer Security Incident Response Team,* di seguito CSIRT), al fine di trattare le situazioni di crisi secondo procedure predefinite, modalità di reazione proporzionate al tipo di evento e tempistiche il più possibile contenute[16]; *iv*) individuare un punto di contatto unico nazionale, al fine di assicurare un'effettiva cooperazione in materia tra le autorità europee e gli Stati membri[17].

Oltre all'introduzione dei suddetti organismi, la direttiva ha stabilito, in secondo luogo, una serie di rilevanti misure tecniche e organizzative per due determinate categorie di soggetti, ossia gli «operatori dei servizi essenziali» (OSE) e i «fornitori di servizi digitali» (FSD), la cui intensità è direttamente proporzionale alla strategicità e alle dimensioni dei singoli destinatari[18].

Si tratta di obblighi principalmente rivolti a rendere più affidabili le reti utilizzate, a prevedere e a minimizzare l'impatto delle minacce più significative sulla continuità delle operazioni e dei servizi svolti e ad assicurare la tempestiva comunicazione degli incidenti di sicurezza alle competenti autorità nazionali

direttiva europea delle reti e dell'informazione, in *Federalismi.it*., n. 23, 2017, spec. p. 7 ss., il quale nota che, senza la predetta iniziativa legislativa, sarebbe perdurata «una situazione in cui ogni Stato continuava ad agire da solo, senza tener conto delle interdipendenze tra le reti e i sistemi informativi in tutta l'Unione e attraverso strategie incoerenti e norme divergenti, con la naturale conseguenza […] di una protezione insufficiente dello spazio cibernetico dell'UE».

[15] Cfr. la clausola di armonizzazione minima di cui all'art. 3 della direttiva, ai sensi della quale gli Stati membri possono adottare o mantenere in vigore disposizioni volte a conseguire un livello più elevato di sicurezza cibernetica.

[16] Al fine di promuovere la cooperazione operativa tra i singoli Stati, la direttiva prevede altresì l'istituzione di una rete europea dei CSIRT.

[17] Lo scambio di informazioni e di migliori pratiche viene assicurato, inoltre, tramite l'istituzione di un apposito gruppo di cooperazione, composto dagli Stati membri, dalla Commissione europea e dall'ENISA (sulla quale si dirà meglio *infra*).

[18] In particolare, ai sensi della direttiva NIS gli «operatori dei settori essenziali» sono coloro che svolgono la propria attività economica nel settore della fornitura e distribuzione dell'acqua potabile, dell'energia, dei trasporti, della salute, delle infrastrutture digitali, dei servizi bancari e finanziari; al contrario, sono definiti come «fornitori di servizi digitali» coloro che operano nel settore dei motori di ricerca, dei servizi di *cloud computing* e delle piattaforme di commercio elettronico. L'applicazione del citato principio di proporzionalità – *rectius*, gradualità – impone che gli obblighi di sicurezza previsti per i primi siano più severi rispetto a quelli previsti per i secondi, atteso il più alto livello di rischio per la stabilità nazionale in caso di attacchi informatici nei confronti degli OSE. In merito al campo di applicazione della direttiva, occorre segnalare le rilevanti modifiche formulate sul punto nella proposta di revisione del 16 dicembre 2020, COM (2020) 823 final (c.d. "direttiva NIS 2"), in *www.eur-lex.europa.eu,* con la quale la Commissione europea ha manifestato l'intenzione di chiarire ed estendere la portata del precedente atto sia dal punto di vista soggettivo, ossia con riferimento all'individuazione dei soggetti coinvolti nella catena di gestione del rischio cibernetico (introducendo al riguardo una nuova classificazione dei destinatari degli obblighi di sicurezza, che si divideranno in "essenziali" e "importanti"), sia dal punto di vista oggettivo, ossia con riferimento alla razionalizzazione degli obblighi di comunicazione e degli *standard* minimi di sicurezza.

NIS. Comunicazioni, queste ultime, che possono anche provenire da enti o utenti che non sono formalmente identificabili come OSE o come FSD, sebbene in siffatta ipotesi il trattamento delle notifiche da parte delle autorità preposte sia consentito nella misura in cui non costituisce un onere eccessivo o sproporzionato[19].

Più di recente, l'incremento e la sofisticazione degli attacchi cibernetici a livello globale, che hanno assunto nel tempo forme più aggressive[20], nonché l'intenzione di affermare una più chiara visione europea del cyberspazio[21] hanno spinto le istituzioni sovranazionali a rivedere e ad aggiornare le prescrizioni normative precedentemente dettate. Al riguardo occorre richiamare, in particolare, le disposizioni introdotte dal regolamento UE 2019/881, c.d. *Cybersecurity Act*[22], il quale si caratterizza per la previsione di due significativi interventi.

Il primo riguarda l'istituzione di un sistema europeo di certificazione della cybersicurezza, ossia un insieme di regole e procedure volte ad assicurare, all'interno del territorio dell'Unione, la conformità di prodotti, servizi e processi ICT rispetto a determinati parametri minimi di sicurezza informatica.

---

[19] Art. 20 dir. UE 2016/1148.

[20] Oltre alle tipologie più note – come il *phishing*, ossia un tipo di frode informatica con la quale l'attaccante mira ad impadronirsi di informazioni preziose della vittima (quali numeri di carte di credito o di conti bancari, ID utente, *password*, ecc.), e le *botnets*, ossia applicazioni installate da un *hacker* sul computer della vittima al fine di prendere il controllo del dispositivo – la cronaca più recente ha registrato il diffondersi di attacchi c.d. "*DoS*" (*Denial of Service*), che si basano sull'invio di continue, automatizzate richieste di accesso ai sistemi informatici di un'infrastruttura digitale, con lo scopo di sovraccaricare quest'ultima e rendere così difficile, se non impossibile, eseguire l'accesso alla stessa, e di attacchi c.d. "*ransomware*", che mirano a bloccare l'accesso ad una rete e crittografare i dati ivi contenuti, salvo il pagamento di un riscatto in favore degli *hacker* da parte del gestore dell'infrastruttura bloccata. Per un'attenta analisi delle diverse minacce della dimensione cibernetica, si veda, tra gli altri, A. SAGLIOCCA, *La protezione dalle frodi, dal phishing e dalle estorsioni online*, in G. ZICCARDI, P. PERRI (a cura di), *Tecnologia e diritto*, III, Giuffrè, Milano, 2019, p. 211 ss.; P.L. MONTESSORO, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, in *Ist. del fed.*, n. 3, 2019, spec. p. 791 ss., il quale sottolinea che oggi gli strumenti tecnici per sferrare attacchi informatici sono in vendita nel c.d. *dark web* e, di conseguenza, il crimine informatico può essere perpetrato anche da soggetti non particolarmente esperti nell'uso delle tecnologie; W. STALLINGS, *Sicurezza dei computer e delle reti*, a cura di A. DE PAOLA e G. LO RE, Pearson, Milano-Torino, 2022, p. 8 ss.

[21] Come è agevole rilevare, l'interesse dell'Unione ad affermare la propria *leadership* in materia di cybersicurezza non risponde a mere esigenze di carattere giuridico-dogmatico, ma anche ad esigenze di carattere economico-culturale, dal momento che la sicurezza cibernetica può essere certamente considerato uno dei terreni principali sui quali gli Stati contemporanei intendono esercitare la propria sovranità (la c.d. sovranità tecnologica). In tal senso, si vedano le considerazioni espresse nella Risoluzione del Parlamento europeo del 12 marzo 2019 sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione e sulla possibile azione a livello di Unione per ridurre tali minacce, 2019/2575 (RSP), in *www.eur-lex.europa.eu,* ove si è chiarito come «l'Unione debba assumere un ruolo guida in materia di cibersicurezza, adottando un approccio comune basato su un utilizzo efficiente ed efficace delle competenze dell'Unione, degli Stati membri e dell'industria, dato che un mosaico di decisioni nazionali divergenti nuocerebbe al mercato unico digitale […]», si «invita la Commissione a sviluppare una strategia che ponga l'Europa all'avanguardia nel settore delle tecnologie di cibersicurezza, onde ridurre la dipendenza dell'Europa dalla tecnologia straniera in tale campo» e si «invita gli Stati membri a informare la Commissione in merito a qualsiasi misura nazionale intendano adottare al fine di coordinare la risposta dell'Unione, onde garantire le più elevate norme di cibersicurezza in tutta l'Unione».

[22] Regolamento UE 2019/881 del 17 aprile 2019 relativo all'Agenzia dell'Unione europea per la cybersicurezza e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione, che ha abrogato il precedente regolamento UE 526/2013 del 21 maggio 2013.

Attraverso un siffatto meccanismo, pertanto, viene promosso non solo il mutuo riconoscimento delle attestazioni e delle dichiarazioni di conformità rilasciate dagli enti di certificazione designati dai singoli Stati membri, ma anche l'acquisto e lo scambio di dispositivi e di sistemi tecnologici in Europa, il cui livello di affidabilità viene notevolmente incrementato[23].

Il secondo intervento di rilievo riguarda, invece, il rafforzamento dei poteri istituzionali dell'Agenzia dell'Unione europea per la cybersicurezza (*European Union Agency for Network and Information Security*, di seguito ENISA), autorità istituita, già nel 2004, con lo scopo di assistere le istituzioni europee e gli Stati membri nello sviluppo e nella revisione delle politiche e delle azioni strategiche in materia[24].

Nell'ambito del nuovo mandato, viene così attribuito all'Agenzia il compito di fornire pareri, consulenze e orientamenti, sostenere lo scambio di informazioni e di buone pratiche, promuovere il miglioramento delle tecniche di prevenzione, analisi e reazione nei confronti delle minacce più pericolose, stimolare l'aggiornamento della normativa europea di settore, supportare la rete europea dei CSIRT, incentivare l'uso del citato meccanismo di certificazione dei prodotti e dei servizi ICT e sensibilizzare l'opinione pubblica sui rischi informatici attualmente più diffusi. Si tratta, a ben vedere, di iniziative che perseguono chiari obiettivi di cooperazione interistituzionale, di coordinamento operativo e di incremento qualitativo delle misure organizzative e di risposta in situazioni di crisi di portata transfrontaliera aventi ad oggetto settori nevralgici dell'economia[25].

---

[23] In alcuni casi, peraltro, è consentito agli stessi produttori e fornitori di autovalutare la sicurezza dei propri prodotti e servizi ICT; un'ipotesi che viene contemplata, come è agevole intuire, unicamente per quei prodotti e servizi che presentano un basso rischio di incidenti e di malfunzionamenti (art. 53 del regolamento). In merito al richiamato sistema europeo di certificazione, cfr. anche la proposta di regolamento UE 2021/105 del 21 aprile 2021 sui prodotti macchina, COM (2021) 202 final, in *www.eur-lex.europa.eu,* la quale contempla (all'art. 17, comma 5) una presunzione di sicurezza per tutti i sistemi e i prodotti informatici certificati in base al citato regolamento UE 2019/881: «I prodotti macchina che sono stati certificati o per i quali è stata emessa una dichiarazione di conformità nel quadro di un sistema di certificazione di cibersicurezza adottato conformemente al regolamento (UE) 2019/881 e i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea sono considerati conformi ai requisiti essenziali di sicurezza e di tutela della salute di cui all'allegato III, sezioni 1.1.9 e 1.2.1, per quanto concerne la protezione contro la corruzione e la sicurezza e l'affidabilità dei sistemi di controllo nella misura in cui tali requisiti siano contemplati dal certificato di cibersicurezza o dalla dichiarazione di conformità o loro parti».

[24] Nello specifico, l'istituzione dell'Agenzia è avvenuta ad opera del regolamento CE 460/2004 del 10 marzo 2004, il quale ha affidato all'organismo europeo un mandato provvisorio (prorogato, di volta in volta, ad opera del regolamento CE 1007/2008, del regolamento CE 580/2011 e del regolamento 526/2013) e poteri istituzionali piuttosto contenuti (relativi, in buona sostanza, all'attività di consulenza tecnica nei confronti degli Stati membri in caso di attacchi o incidenti informatici). Quanto al livello organizzativo, ENISA è composta da: un consiglio di amministrazione, ove siedono i rappresentanti di ciascuno Stato membro dell'Unione e due membri nominati dalla Commissione, il quale stabilisce gli orientamenti generali del funzionamento dell'Agenzia; un comitato esecutivo, formato da cinque membri del citato consiglio di amministrazione, che assiste e prepara le decisioni di quest'ultimo; un direttore esecutivo, che provvede ad attuare le decisioni del consiglio di amministrazione sotto la sua responsabilità; un gruppo consultivo, composto da esperti riconosciuti a livello internazionale in rappresentanza dei portatori di interesse in materia di cybersicurezza. Con riferimento alla struttura e alle funzioni delle Agenzie nell'ordinamento amministrativo europeo si veda, per tutti, E. CHITI, *Le agenzie europee. Unità e decentramento nelle amministrazioni europee*, Cedam, Padova, 2002.

[25] Sul nuovo ruolo dell'Agenzia, cfr. A. CONTALDO, D. MULA (a cura di), *Cybersecurity Law*, *cit*., p. 71 ss. In tema di cooperazione interistituzionale, occorre richiamare il regolamento UE 2021/887 del 20 maggio 2021 che istituisce il Centro europeo di competenza per la cybersicurezza, con l'obiettivo di colmare, nel contesto della rete dei Centri

Invero, pur potendosi apprezzare le novità introdotte dai suddetti interventi, il quadro normativo vigente appare ancora piuttosto limitato, specie con riferimento alla previsione di un ruolo meramente consultivo e di indirizzo per l'ENISA, laddove 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[26]. Dal che pare possibile dedurre che l'effettiva affermazione della visione europea in tema di cybersicurezza dipenderà, in gran parte, dalla generale attività di vigilanza e di accertamento delle violazioni del diritto dell'Unione riconosciuta dai Trattati alla Commissione europea, così come dalla reale volontà politica degli Stati membri.

Volgendo lo sguardo al contesto giuridico italiano, è possibile osservare come il processo di definizione di un apposito sistema di prevenzione e di contrasto nei confronti delle minacce rivolte alla pubblica sicurezza cibernetica abbia avuto luogo, in un primo momento, tramite il coinvolgimento e il coordinamento di corpi amministrativi preesistenti, principalmente attivi nel c.d. «Sistema di informazione per la sicurezza della Repubblica» di cui alla l. 3 agosto 2007, n. 124[27].

In particolare, le prime significative disposizioni dedicate al tema della *cybersecurity* risalgono al periodo 2012-2013, a partire dal quale si è assistito alla progressiva creazione di una macchina amministrativa in grado di risolvere, attraverso l'attivazione di tre distinti livelli di intervento, le criticità sollevate dallo sviluppo e dalla diffusione delle moderne tecnologie[28].

---

nazionali di coordinamento, il profondo divario di capacità e di competenze esistente nel territorio dell'Unione e di diffondere il più possibile i risultati delle ricerche e delle attività finanziate.

[26] Sull'inadeguatezza della vigente disciplina europea rispetto alla complessità delle sfide e dei rischi connessi alla tutela della pubblica sicurezza cibernetica, si vedano i tre recenti e correlati documenti strategici, tutti adottati il 16 dicembre 2020: la proposta di revisione della direttiva NIS, *cit.*, ove si rimarca non solo che l'ambito di applicazione dell'attuale direttiva è troppo limitato e di portata ambigua, ma anche che l'applicazione della stessa è risultata sostanzialmente inefficace, dal momento che gli Stati membri si sono mostrati riluttanti ad irrogare le sanzioni ivi prescritte; la proposta di revisione della direttiva sulla resilienza dei soggetti critici, COM (2020) 829 final, in *www.eur-lex.europa.eu*, che mira a sostituire la direttiva 2008/114/CE dell'8 dicembre 2008 sull'individuazione e designazione delle infrastrutture critiche europee (c.d. direttiva ECI, *European Critical Infrastructure*, che riguarda ad oggi solamente i settori dell'energia e dei trasporti), estendendo il campo di applicazione degli obblighi e dei meccanismi di sorveglianza ivi previsti alle infrastrutture dei soggetti considerati «critici» dagli Stati membri e dei soggetti considerati «di particolare rilevanza a livello europeo», ossia che forniscono servizi essenziali a o in più di un terzo degli Stati membri; la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione, *La strategia dell'UE in materia di cybersicurezza per il decennio digitale*, *cit.*, che contiene proposte di intervento politico, normativo e finanziario in tre settori principali: *i*) resilienza, sovranità tecnologica e *leadership*; *ii*) sviluppo di capacità operative volte alla prevenzione, alla dissuasione e alla risposta; *iii*) promozione di un cyberspazio globale e aperto.

[27] Sull'impianto generale della suddetta legge, si vedano, tra gli altri, C. MOSCA, S. GAMBACURTA, G. SCANDONE, M. VALENTINI, *I servizi di informazione e il segreto di Stato*, Giuffrè, Milano, 2008; T.F. GIUPPONI, *Servizi di informazione e segreto di Stato nella legge n. 124/2007*, in AA.VV., *Studi in onore di Luigi Arcidiacono*, IV, Giappichelli, Torino, 2010, p. 1677 ss.; A. MASSERA, M. SIMONCINI, *La tutela amministrativa del segreto di Stato e delle informazioni classificate*, in *Giorn. dir. amm.*, n. 4, 2012, p. 362 ss.; M. FRANCHINI, *Il sistema nazionale delle informazioni per la sicurezza e l'Autorità delegata*, in *Giorn. dir. amm.*, n. 4, 2010, p. 431 ss.; Id., *Alcune considerazioni sulle nuove competenze del comitato parlamentare per la sicurezza della repubblica*, in *Rivista AIC*, n. 1, 2014.

[28] Sul punto, cfr. la l. 7 agosto 2012, n. 133, che ha modificato significativamente la citata l. n. 124/2007, nonché il DPCM 24 gennaio 2013, n. 66, rubricato "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale", adottato ai sensi dell'art. 1, comma 3-*bis*, l. n. 124/2007. Con riferimento alle attività di

All'interno di tale contesto, un ruolo di cruciale importanza viene affidato al Presidente del Consiglio dei ministri, nella qualità di vertice del citato Sistema di informazione per la sicurezza, al quale è attribuita la definizione degli indirizzi e degli obiettivi generali della politica di sicurezza cibernetica (primo livello di intervento). Tale funzione trova concreta manifestazione, segnatamente, nell'elaborazione di direttive[29] e di documenti programmatici, come il Quadro strategico nazionale e il Piano nazionale per la protezione cibernetica e la sicurezza informatica, che mirano a rafforzare la protezione delle infrastrutture critiche, materiali e immateriali, presenti sul territorio[30].

L'attuazione degli indirizzi e degli obiettivi fissati nei suddetti atti viene devoluta, invece, a una pluralità di organismi di supporto e di coordinamento operativo (secondo livello di intervento), tra i quali occupano una posizione di rilievo: il Comitato interministeriale per la sicurezza della Repubblica (CISR), con funzioni di consulenza rispetto agli atti di indirizzo di competenza del Presidente del Consiglio e di proposta rispetto alle misure normative e organizzative ritenute necessarie[31]; il Dipartimento delle informazioni per la sicurezza della Repubblica (di seguito, DIS), incaricato di presiedere tutte le attività di ricerca, di analisi e di elaborazione informativa relative alle minacce e agli attacchi cibernetici[32]; il Nucleo per la Sicurezza Cibernetica, istituito dal DPCM n. 66/2013 al fine di coordinare l'azione di tutti i soggetti coinvolti nella preparazione e nella gestione delle situazioni di crisi e di attivare le eventuali procedure di allerta e di risposta[33]; l'Agenzia per l'Italia digitale, alla quale è affidata l'individuazione delle soluzioni

prevenzione e di contrasto alla criminalità informatica, si segnala, inoltre, l'istituzione, ad opera del decreto del Ministero dell'interno del 9 gennaio 2008, del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC), quale unità specializzata interna al Servizio di Polizia postale e delle comunicazioni. A livello sovranazionale, invece, l'attività di contrasto è affidata principalmente ad Europol, che agisce in cooperazione con ENISA.

[29] Oltre che nei confronti del Dipartimento delle informazioni per la sicurezza (sul quale *infra*), il potere di direttiva del Presidente del Consiglio dei ministri è esercitato anche nei confronti dell'Agenzia informazioni e sicurezza esterna (AISE) e dell'Agenzia informazioni e sicurezza interna (AISI), le quali svolgono le rispettive attività di ricerca informativa sotto il coordinamento operativo del suddetto Dipartimento (art. 4, comma 3, lett. d-*bis*), l. n. 124/2007).

[30] In particolare, ai sensi dell'art. 3, comma 1, lett. a) e b), DPCM n. 66/2013, il Quadro strategico nazionale doveva contenere l'indicazione dei caratteri e delle tendenze evolutive delle minacce e delle vulnerabilità dei sistemi e delle reti di interesse nazionale, la definizione dei ruoli e dei compiti dei diversi soggetti, pubblici e privati, interessati alla gestione dei sistemi e delle reti di interesse strategico, l'individuazione di strumenti e di procedure tramite i quali migliorare le capacità nazionali di prevenzione e risposta rispetto alle minacce del cyberspazio; il Piano nazionale per la protezione cibernetica doveva indicare, invece, gli obiettivi e le linee di azione da porre in essere per realizzare il predetto Quadro strategico.

[31] Art. 4, comma 1, DPCM n. 66/2013. Il Comitato è presieduto dal Presidente del Consiglio ed è composto dall'Autorità delegata, ove istituita, dal Ministro degli affari esteri, dal Ministro dell'interno, dal Ministro della difesa, dal Ministro della giustizia, dal Ministro dell'economia e delle finanze, dal Ministro dello sviluppo economico (art. 5, comma 3, l. n. 124/2007).

[32] Cfr. art. 4, comma 3, lett. d-*bis*), l. n. 124/2007, introdotto dalla l. n. 133/2012, e art. 7 DPCM n. 66/2013, ai sensi del quale il DIS è chiamato, altresì, a trasmettere le informazioni e i dati rilevanti acquisiti al Nucleo per la sicurezza cibernetica, alle pubbliche amministrazioni e agli altri soggetti, pubblici e privati, interessati a ricevere tali informazioni.

[33] Art. 8 e 9 DPCM n. 66/2013. Sebbene le funzioni del Nucleo per la Sicurezza Cibernetica (oggi Nucleo per la cybersicurezza) siano rimaste sostanzialmente invariate nel tempo, la sua collocazione è cambiata più volte: nel 2013 esso è stato istituito presso l'Ufficio del Consigliere militare della Presidenza del Consiglio dei ministri, nel 2017 è stato

tecniche idonee a garantire la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati, dei sistemi e delle infrastrutture digitali delle pubbliche amministrazioni[34], nonché il coordinamento delle attività svolte dal CERT-PA (*Computer Emergency Response Team*)[35], istituito nel 2014, all'interno dell'Agenzia nazionale, per supportare il settore pubblico nelle iniziative di reazione e di ripristino (terzo livello di intervento)[36].

Seppur improntato ad un principio di razionale distribuzione delle funzioni tra i diversi attori istituzionali, il disegno normativo sopra descritto, tuttavia, si è rivelato presto alquanto complesso e inefficiente. E ciò sia per l'insufficiente attenzione rivolta alle problematiche connesse alla gestione delle situazioni di crisi, alle quali il successivo DPCM del 2017 dedica, non a caso, interventi più mirati[37], sia per il limitato coinvolgimento degli operatori economici del settore, i quali concorrono al funzionamento del sistema di sicurezza cibernetica solo in quanto gestori di infrastrutture o di servizi di rilievo nazionale[38].

Alle suddette lacune cercano di porre rimedio, sulla scia delle più recenti indicazioni europee, i successivi interventi legislativi in materia, ossia il d.lgs. 18 maggio 2018, n. 65, che recepisce la ricordata direttiva NIS, il d.l. 21 settembre 2019, n. 105, convertito dalla l. 18 novembre 2019, n. 133, che ha istituito il Perimetro di Sicurezza Nazionale Cibernetica (PSNC)[39], nonché il d.l. 14 giugno 2021, n. 82, convertito

posto alle dipendenze del DIS, mentre dal 2021 è inserito all'interno della nuova Agenzia nazionale per la cybersicurezza. Sull'importante ruolo di coordinamento svolto dal Nucleo nel quadro normativo attuale, si dirà meglio *infra*.

34 Artt. 51 e 71 d.lgs. 7 marzo 2005, n. 82 (c.d. Codice dell'amministrazione digitale, di seguito CAD). Com'è noto, l'Agenzia per l'Italia digitale è stata istituita dal d.l. 22 giugno 2012, n. 83, convertito dalla l. 7 agosto 2012, n. 134, al fine di attuare gli obiettivi strategici dell'Agenda digitale italiana.

35 La rete operativa dei CERT rappresenta, invero, un fenomeno mondiale, nato alla fine degli anni Ottanta, su iniziativa del governo statunitense, presso l'Istituto di Ingegneria della Carnegie Mellon University di Pittsburgh, al fine di coordinare le attività e favorire scambi di informazioni e di analisi tra i diversi gruppi di intervento. In tema si rinvia, per approfondimenti, a A. CONTALDO, F. PELUSO, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pacini, Pisa, 2018, p. 70 ss.

36 Accanto al citato CERT-PA è stata prevista, inoltre, l'istituzione di un CERT-Nazionale presso il Ministero dello sviluppo economico, al fine di assistere i cittadini e le imprese in situazioni di crisi cibernetiche. A partire da maggio 2020, con l'entrata in vigore del DPCM 8 agosto 2019, le funzioni dei predetti CERT sono state attribuite, invero, al neoistituito CSIRT Italia, mentre il CERT-PA è stato trasformato nel CERT-Agid, al fine di prestare supporto all'Agenzia per l'Italia digitale sugli aspetti riguardanti la cybersicurezza sui quali questa continua ad essere competente.

37 Cfr. DPCM 17 febbraio 2017. In particolare, il decreto ha rivisto le attribuzioni del Presidente del Consiglio dei ministri, del CISR e del Nucleo per la sicurezza cibernetica nelle situazioni di crisi informatica che coinvolgono aspetti di sicurezza nazionale, al fine di assicurare una risposta maggiormente unitaria e coordinata nella gestione e nella risoluzione delle predette ipotesi. Sulle novità introdotte dal DPCM, si rinvia a L. SALAMONE, *La disciplina del cyberspace alla luce della direttiva europea delle reti e dell'informazione*, *cit.*, p. 29 ss.; A. CONTALDO, D. MULA (a cura di), *Cybersecurity Law*, *cit.*, p. 119 ss.

38 Cfr. art. 11 DPCM n. 66/2013.

39 Com'è noto, l'istituzione del Perimetro nazionale risponde all'esigenza di assicurare un livello elevato di sicurezza delle reti, dei sistemi e dei servizi informatici utilizzati da quei soggetti (pubbliche amministrazioni, enti pubblici e privati) che esercitano «una funzione essenziale dello Stato» o che prestano «un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato», seppur non rientranti nell'ambito di applicazione della citata direttiva NIS. Si tratta di soggetti individuati in un apposito elenco, adottato con DPCM, su proposta del Comitato interministeriale per la cybersicurezza, non soggetto a pubblicazione o a istanze di accesso; sicché solo le amministrazioni e gli enti rientranti all'interno del suddetto Perimetro ricevono comunicazione dell'iscrizione (art. 1, comma 2-*bis*, d.l. n. 105/2019). Tra i decreti che hanno contribuito a dare attuazione alle disposizioni del d.l. n. 105/2019, occorre segnalare: il DPCM 30 luglio 2020, n. 131, che definisce le modalità e i criteri procedurali di individuazione dei soggetti pubblici e privati inclusi nel Perimetro nazionale (art. 1, comma 2, lett. a), nonché i criteri per la predisposizione

dalla l. 4 agosto 2021, n. 109, che ha istituito, con colpevole ritardo rispetto alle esperienze di altri Paesi europei e non solo, l'Agenzia per la cybersicurezza nazionale[40].

L'introduzione del nuovo assetto organizzativo risponde certamente all'esigenza di fronteggiare, in maniera più celere, coordinata ed organica, l'esponenziale aumento di attacchi informatici all'interno del nostro ordinamento[41]; esigenza alla quale va aggiunta la maturata consapevolezza dell'importanza della dimensione della sicurezza cibernetica per la buona riuscita del processo di digitalizzazione del Paese, come riconosciuto, da ultimo, nel citato Piano nazionale di ripresa e resilienza[42].

---

e l'aggiornamento degli elenchi delle reti, dei sistemi, dei servizi informatici da parte dei soggetti inclusi nel Perimetro (art. 1, comma 2, lett. b); il DPR 5 febbraio 2021, n. 54, che definisce le procedure e le modalità per le operazioni di valutazione spettanti al Centro di valutazione e certificazione nazionale (CVCN), attivo invero solo da luglio 2022, con riferimento alle forniture di beni e di servizi ICT richieste dai soggetti inclusi nel Perimetro (art. 1, comma 6, lett. a), b) e c); il DPCM 14 aprile 2021, n. 81, che definisce le procedure e le modalità per la notifica degli incidenti aventi impatto su reti, sistemi e servizi ICT al CSIRT Italia, nonché le misure di sicurezza relative alle reti, ai sistemi e ai servizi ICT adottate dai soggetti inclusi nel Perimetro (art 1, commi 2 e 3, lett. a) e b); il DPCM 15 giugno 2021, che individua le categorie di beni, sistemi e servizi ICT per la cui fornitura i soggetti inclusi nel Perimetro sono tenuti a seguire le procedure di valutazione spettanti al citato CVCN (art. 1, comma 6, lett. a); il DPCM 18 maggio 2022, n. 92, in vigore dal 30 luglio 2022, in materia di accreditamento degli istituendi laboratori accreditati di prova (LAP) e di raccordo tra i predetti laboratori, il suddetto CVCN e i Centri di valutazione (CV) del Ministero dell'Interno e del Ministero della Difesa (art. 1, comma 7, lett. b). Sull'istituzione del Perimetro di sicurezza nazionale cibernetica, cfr. B. CAROTTI, *Sicurezza cibernetica e Stato nazione*, in *Giorn. dir. amm.*, n. 5, 2020, p. 629 ss., secondo il quale l'espresso richiamo agli interessi dello Stato-Nazione da parte del d.l. n. 105/2019 potrebbe ben prestarsi a letture interpretative di stampo protezionistico, confliggenti con gli stessi obiettivi di armonizzazione legislativa e di collaborazione a livello internazionale che costituiscono la premessa teorica dei recenti interventi in tema di cybersicurezza; S. MELE, *Il Perimetro di sicurezza nazionale cibernetica e il nuovo "golden power"*, in G. CASSANO, S. PREVITI (a cura di), *Il diritto di internet nell'era digitale*, Giuffrè, Milano, 2020, p. 186 ss.

[40] Accanto alla menzionata Agenzia, il d.l. n. 82/2021 ha istituito, presso la Presidenza del Consiglio dei ministri, il Comitato Interministeriale per la cybersicurezza (CIC), chiamato a svolgere funzioni consultive, di proposta e di vigilanza in materia di politiche di cybersicurezza del tutto assimilabili a quelle in precedenza spettanti al CISR (il quale, nel nuovo assetto organizzativo, mantiene un ruolo importante nella gestione delle crisi cibernetiche, ai sensi degli artt. 4, comma 6, e 10 d.l. n. 82/2021). Al pari del CISR, il CIC è presieduto dal Presidente del Consiglio dei ministri ed è composto dall'Autorità delegata e dal Ministro degli affari esteri, dell'interno, della giustizia, della difesa, dell'economia e delle finanze, dello sviluppo economico, nonché dal Ministro della transizione ecologica, dell'università e della ricerca, dell'innovazione tecnologica e delle infrastrutture e della mobilità sostenibili, mentre il direttore generale dell'Agenzia nazionale per la cybersicurezza svolge le funzioni di segretario del Comitato. Per un'analisi comparata delle autorità di tutela della cybersicurezza previste negli altri ordinamenti, cfr. A. COLELLA, *Analisi comparata delle architetture decisionali in materia cibernetica dei paesi dell'area euro-occidentale*, in A. TORRE, *Costituzioni e sicurezza dello Stato*, Maggioli, Rimini, 2013, p. 439 ss.; A. RENZI, *La sicurezza cibernetica: lo stato dell'arte*, in *Giorn. dir. amm.*, n. 4, 2021, p. 546 ss., il quale osserva che un'analoga operazione di centralizzazione delle diverse funzioni amministrative di prevenzione e di gestione del rischio cibernetico è stata effettuata anche nel sistema statunitense e nel sistema francese.

[41] Sul punto, cfr. il report del 29 luglio 2022 pubblicato da ENISA, *Threat landscape for ransomware attacks*, reperibile in *www.enisa.europa.eu*, relativo al livello di rischio informatico legato ad attacchi *ransomware* in UE, Regno Unito e Stati Uniti, che evidenzia come, tra maggio 2021 e giugno 2022, l'Italia sia stato il quarto Paese più attaccato, dopo USA, Germania e Francia. Tra i casi più emblematici degli ultimi anni, sia consentito limitarsi a richiamare i noti attacchi al sistema di prenotazione vaccini della Regione Lazio dell'agosto 2021 e ai siti istituzionali del Senato, dell'ACI, dell'Istituto Superiore di Sanità e del Ministero della difesa del maggio 2022, episodio, quest'ultimo, riconducibile ad un gruppo di *hacker* criminali vicino alla Federazione russa. Al riguardo pare opportuno ricordare che, a seguito dello scoppio del conflitto tra Russia e Ucraina, il legislatore italiano ha adottato una serie di disposizioni volte alla diversificazione delle dotazioni informatiche delle nostre pubbliche amministrazioni, nell'ottica di prevenire eventuali pregiudizi per la sicurezza nazionale connessi all'accresciuta esposizione del Paese alle minacce cibernetiche. Sul punto, cfr. art. 29 d.l. 21 marzo 2022, n. 21.

[42] Sul punto, si rinvia a quanto osservato alla precedente nt. 8.

Nell'attuale architettura istituzionale, che tuttavia mantiene ferme le attribuzioni e la centralità del ruolo del Presidente del Consiglio dei ministri, così come l'impostazione di fondo della l. n. 124/2007[43], il riordino delle competenze amministrative distribuite dalla precedente normativa passa attraverso l'istituzione di un nuovo organismo, incaricato della «tutela degli interessi nazionali nel campo della cybersicurezza»[44].

Alla predetta autorità, che si differenzia dalle tradizionali agenzie amministrative per struttura e per funzioni[45], il d.l. n. 82/2021 ha affidato compiti e responsabilità significative, che riguardano,

[43] Diversi gli elementi normativi che confermano questa convinzione: in primo luogo, in virtù degli artt. 2 e 3 d.l. n. 82/2021, anche nella nuova architettura istituzionale il Presidente del Consiglio detiene in via esclusiva «l'alta direzione e la responsabilità generale delle politiche di cybersicurezza», «l'adozione della strategia nazionale di cybersicurezza», «la nomina e la revoca del direttore generale e del vicedirettore generale dell'Agenzia», l'adozione di «ogni disposizione necessaria per l'organizzazione e il funzionamento dell'Agenzia», nonché la scelta di delegare, analogamente a quanto già previsto dall'art. 3 l. n. 124/2007, ad un Ministro senza portafoglio o ad un Sottosegretario di Stato (c.d. Autorità delegata), l'esercizio delle funzioni attribuitegli in via non esclusiva; in secondo luogo, lo stesso d.l. n. 82/2021 riconosce espressamente la natura strumentale dell'attività dell'Agenzia nazionale rispetto alle competenze attribuite *ex lege* al Presidente del Consiglio in materia di cybersicurezza (art. 5, comma 2, ult. periodo), il quale ne determina, altresì, lo stanziamento annuale (art. 11, comma 1); infine, un'ulteriore conferma della centralità della posizione del PdCM nel nuovo disegno organizzativo si evince dai significativi poteri d'emergenza ad esso attribuiti dall'art. 5 d.l. n. 105/2019, ai sensi del quale: «il Presidente del Consiglio dei ministri, in presenza di un rischio grave e imminente per la sicurezza nazionale connesso alla vulnerabilità di reti, sistemi informativi e servizi informatici, su deliberazione del Comitato interministeriale per la sicurezza della Repubblica, può comunque disporre, ove indispensabile e per il tempo strettamente necessario alla eliminazione dello specifico fattore di rischio o alla sua mitigazione, in deroga ad ogni disposizione vigente, nel rispetto dei principi generali dell'ordinamento giuridico e secondo un criterio di proporzionalità, la disattivazione, totale o parziale, di uno o più apparati o prodotti impiegati nelle reti, nei sistemi o per l'espletamento dei servizi interessati». In dottrina, cfr. B. CAROTTI, *Sicurezza cibernetica e Stato-nazione*, *cit.*, p. 639 ss., il quale sottolinea la persistente centralità della posizione del Presidente del Consiglio nell'ambito del nuovo sistema nazionale *cyber*; A. RENZI, *La sicurezza cibernetica: lo stato dell'arte*, *cit.*, pp. 545-546, il quale evidenzia le chiare assonanze tra l'organizzazione amministrativa dell'Agenzia nazionale e quella delle agenzie del comparto *intelligence*; A. LAURO, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione*, in *La Rivista Gruppo di Pisa*, n. 3, 2021, p. 535.

[44] Art. 5, comma 1, d.l. n. 82/2021.

[45] In particolare, rispetto al modello generale di cui agli artt. 8 e 9 d.lgs. 30 luglio 1999, n. 300, è possibile osservare che: ai sensi dell'art. 7 d.l. n. 82/2021, sono organi dell'Agenzia unicamente il direttore generale, il vice direttore generale e il collegio dei revisori dei conti, non essendo previsto dunque un apposito comitato direttivo; ai sensi dell'art. 5, comma 2, d.l. n. 81/2021, l'Agenzia «ha personalità giuridica di diritto pubblico» e non è sottoposta ai poteri di vigilanza e controllo ministeriali, ma alle direttive del Presidente del Consiglio dei Ministri e, ove istituita, dell'Autorità delegata, che se ne avvalgono «per l'esercizio delle competenze di cui al presente decreto»; l'operato dell'Agenzia è sottoposto, inoltre, al controllo del COPASIR, il quale può chiedere l'audizione del direttore generale su questioni di propria competenza (art. 5, comma 6) ed esprime il proprio parere sull'adozione del regolamento di organizzazione e di funzionamento dell'Agenzia, sull'adozione del regolamento di contabilità e del regolamento sul reclutamento del personale, nonché sulla stipula di contratti di appalto e forniture di beni e servizi necessari per le attività istituzionali dell'Autorità. Sul modulo organizzativo delle agenzie amministrative, cfr., *ex multis*, D. SERRANI, *L'organizzazione per ministeri*, Officina editore, Roma, 1979; G. ARENA, voce *Agenzia amministrativa*, in *Enc. giur.*, I, Roma, 1998, p. 1 ss.; F. MERLONI, *Le agenzie nel sistema amministrativo italiano*, in *Dir. pubbl.*, n. 3, 1999, p. 717 ss.; L. CASINI, *Le agenzie amministrative*, in *Riv. trim. dir. pubbl.*, n. 2, 2003, p. 393 ss.; C. CORSI, *Agenzia e agenzie: una nuova categoria amministrativa?,* Giappichelli, Torino, 2005; N. BASSI, voce *Agenzie nazionali ed europee*, in *Enc. dir.*, II, Milano, 2009, p. 41 ss.; E. CHITI, voce *Agenzie amministrative*, in *www.treccani.it-Diritto on line*, 2014. In materia, cfr. anche L. PARONA, *L'istituzione dell'Agenzia per la cybersicurezza nazionale*, in *Giorn. dir. amm.*, n. 6, 2021, spec. p. 713 ss., secondo il quale i profili evidenziati inducono a ritenere che l'Agenzia presenti caratteri tipici sia dell'ente strumentale sia delle autorità operanti nell'ambito del Sistema di informazione per la sicurezza per la Repubblica di cui alla l. n. 124/2007.

principalmente, la prevenzione e la tutela della sicurezza nazionale nel cyberspazio[46], l'ispezione, l'accertamento e l'irrogazione delle sanzioni prescritte in caso di violazione della normativa di settore[47], la gestione delle vulnerabilità informatiche e le attività di contrasto in caso di attacco.

Nell'ambito di queste ultime attività, funzioni di grande rilevanza sono attribuite al CSIRT Italia, introdotto in sede di recepimento della direttiva NIS e incardinato, dapprima, presso il DIS e, oggi, trasferito presso l'Agenzia[48]. Spetta al predetto gruppo di intervento, in particolare, monitorare periodicamente il verificarsi di attacchi e di incidenti a livello nazionale, ricevere le segnalazioni obbligatorie provenienti dagli OSE e dai FSD di cui alla direttiva NIS[49] e le segnalazioni facoltative provenienti dagli altri soggetti, pubblici e privati, comunque interessati da una minaccia *cyber*, emettere preallarmi e allerte e offrire assistenza operativa in situazioni di crisi[50].

All'Agenzia nazionale spettano, inoltre, importanti compiti di promozione e di coordinamento delle iniziative e dei progetti rivolti alla formazione e alla sensibilizzazione collettiva sulle problematiche riguardanti la cybersicurezza[51]. Attività che vengono espletate sia tramite il supporto di un organo interno,

---

[46] Sotto questo profilo, si segnala il trasferimento del citato Centro di valutazione e di certificazione nazionale, originariamente istituito presso il MISE, in seno all'Agenzia nazionale per la cybersicurezza, al fine di consentire al Centro di attuare un controllo preventivo sulla sicurezza di tutti gli acquisti di beni e di sistemi ICT che supportano la fornitura di servizi e funzioni essenziali a livello nazionale. A tal proposito si noti che, a partire dal 30 giugno 2022, i soggetti inseriti nel Perimetro sono tenuti a comunicare tempestivamente al CVCN l'intenzione di procedere all'acquisto dei suddetti beni e servizi; in questo caso, i bandi di gara e i relativi contratti possono essere condizionati, sospensivamente o risolutivamente, al rispetto delle imposizioni e/o al superamento dei test di *hardware* e *software* disposti dal CVCN.

[47] In tal senso, l'Agenzia nazionale è competente all'accertamento e all'irrogazione delle sanzioni amministrative previste dal d.lgs. n. 65/2018, in tema di sicurezza delle reti e dei sistemi informatici, dal reg. UE 2021/887 e dal d.lgs. 3 agosto 2022, n. 123, in tema di sistema di certificazione della cybersicurezza, dal d.l. n. 105/2019, in tema di Perimetro di sicurezza nazionale cibernetica, e dal d.lgs. 1 agosto 2003, n. 259 (c.d. Codice delle comunicazioni elettroniche), in tema di protezione delle reti e dei servizi di comunicazione elettronica accessibili al pubblico.

[48] Cfr. art. 7, comma 3, d.l. n. 82/2021. Sulle funzioni del CSIRT Italia, cfr. art. 4 DPCM 8 agosto 2019.

[49] Come si è detto, infatti, gli OSE e FSD sono tenuti *ex lege* a comunicare tempestivamente eventuali incidenti o attacchi cibernetici considerati "rilevanti" all'autorità nazionale competente (*i.e.* CSIRT Italia) al fine di consentire l'intervento della stessa.

[50] Le suddette funzioni del CSIRT Italia vengono svolte a stretto contatto con il Nucleo per la cybersicurezza, incaricato di acquisire, anche tramite lo stesso gruppo di intervento, comunicazioni circa violazioni o tentativi di violazione della sicurezza delle reti e dei servizi digitali, nonché di ricevere dal CSIRT le notifiche rese ai sensi della direttiva NIS. In quanto centro di raccolta delle informazioni e segnalazioni, il Nucleo è chiamato a valutare, infatti, se i predetti eventi assumano dimensioni, intensità o natura tali da richiedere l'assunzione di decisioni coordinate in sede interministeriale (art. 9, comma 1, lett. e, f, g) e, nel caso in cui ciò sia necessario, assicurare che vengano espletate in maniera ottimale tutte le attività di reazione e di stabilizzazione di competenza delle diverse amministrazioni (art. 10, commi 4 e 5).

[51] In tal senso, l'Agenzia è incaricata di supportare lo sviluppo di competente e capacità industriali, tecnologiche e scientifiche nel settore (art. 7, comma 1, lett. r), di stipulare accordi bilaterali e multilaterali con istituzioni, enti ed organismi di altri Paesi per la partecipazione congiunta a programmi di cybersicurezza (art. 7, comma 1, lett. s), di sostenere e coordinare la partecipazione italiana a progetti e iniziative europei e internazionali (art. 7, comma 1, lett. t), di contribuire allo sviluppo di una cultura nazionale in materia di cybersicurezza (art. 7, comma 1, lett. u), di promuovere la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane, anche attraverso l'attivazione di percorsi formativi universitari e l'assegnazione di borse di studio, di dottorato e assegni di ricerca (art. 7, comma 1, lett. v).

ossia il Comitato tecnico-scientifico, sia tramite il coinvolgimento delle università, degli enti di ricerca, del sistema produttivo nazionale e delle altre istituzioni pubbliche competenti[52].

L'istituzione dell'autorità, che opera quale interlocutore unico per i soggetti ricompresi nel PSNC, pare conferire maggiore compattezza ad un disegno normativo inizialmente frammentato e complesso, che risulta oggi improntato all'accentramento delle competenze[53] e al coordinamento delle linee strategiche e delle azioni operative[54], nell'ottica della semplificazione delle procedure decisionali e dell'eliminazione delle sovrapposizioni funzionali preesistenti.

Anche le più recenti scelte legislative, seppur apprezzabili per i profili appena evidenziati, sembrano, tuttavia, prestare il fianco a due principali obiezioni.

La prima riguarda l'inadeguatezza di un'architettura istituzionale preposta alla salvaguardia della sicurezza cibernetica nazionale ma principalmente, se non esclusivamente, rivolta ad attenuare l'impatto delle minacce informatiche sulle reti e sui servizi ICT di maggiore rilevanza per il Paese[55].

Sotto questa prospettiva, infatti, appare criticabile la mancata previsione di analoghi strumenti di prevenzione e di reazione nei confronti di attacchi solo indirettamente rivolti contro obiettivi di importanza strategica, ossia che perseguono tale finalità soltanto dopo aver colpito *target* di rilevanza inferiore (si pensi, ad esempio, ai tentativi di intrusione e di manomissione informatica ai danni di PMI

[52] Art. 7, comma 1-*bis*, d.l. n. 82/2021.

[53] Nella qualità di «Autorità nazionale per la cybersicurezza», all'Agenzia vengono attribuiti compiti in precedenza spettanti ad altri organismi statali, come quelli relativi al Ministero dello sviluppo economico, incluse le funzioni inerenti alla certificazione della cybersicurezza di beni, sistemi e servizi ICT e al Perimetro nazionale (art. 7, comma 1, lett. f) e DPCM 15 giugno 2022), alla Presidenza del Consiglio dei ministri (art. 7, comma 1, lett. h), al Dipartimento delle informazioni e della sicurezza (art. 7, comma 1, lett. i) e all'Agenzia per l'Italia digitale, comprese le funzioni inerenti alla sicurezza e alla disponibilità dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni e all'adozione di linee guida contenenti regole tecniche in materia di cybersicurezza di cui agli artt. 51 e 71 del CAD (art. 7, comma 1, lett. m).

[54] In materia, va ricordato che la suddetta Agenzia: predispone la strategia nazionale di cybersicurezza (art. 7, comma 1, lett. b); è qualificata come «Autorità nazionale di certificazione della cybersicurezza» ai sensi dell'art. 58 del citato reg. UE 2019/881, con il compito di coordinare e di dirigere il sistema italiano di certificazione, qualificazione e valutazione della cybersicurezza dei prodotti, servizi e processi ICT (art. 7, comma 1, lett. e), come confermato, da ultimo, dal d.lgs. n. 123/2022); è designata quale «Centro nazionale di coordinamento» ai sensi dell'art. 6 del citato reg. UE 2021/887, con il compito di supportare il Centro europeo di competenza per la cybersicurezza nell'attività di rafforzamento delle capacità, delle conoscenze e della competitività dell'Unione nel settore (art. 7, comma 1, lett. aa). Per un quadro riassuntivo delle funzioni della nuova Agenzia, si veda S. ATERNO, *Sicurezza informatica. Aspetti giuridici e tecnici*, Pacini, Pisa, 2022, p. 234 ss.

[55] In materia, cfr. A. MONTI, *Internet e ordine pubblico*, in G. CASSANO, S. PREVITI, *Il diritto di internet nell'era digitale*, *cit*., p. 76-77. In particolare, dopo aver criticato la tendenza ad utilizzare in maniera impropria la locuzione "spazio cibernetico" (è noto, infatti, che il termine "cibernetica" identifica, più precisamente, quella disciplina scientifica introdotta dal matematico Nobert Wiener nel lavoro *Cybernetics or Control and Communication in the Animal and the Machine*, MIT Press, Cambridge (MA), 1948, che studia l'interazione fra l'uomo e la macchina), l'A. sottolinea come la c.d. "sicurezza cibernetica" ricomprenda ma non si possa esaurire nelle misure tecniche e organizzative previste per i gestori delle infrastrutture critiche dal citato d.lgs. n. 65/2018.

che hanno come fornitori enti inseriti nel PSNC o ai danni di persone fisiche che lavorano per società ed enti di grande rilevanza)[56].

La seconda principale obiezione riguarda, invece, la tuttora insoddisfacente valorizzazione del ruolo degli operatori economici del settore e degli utenti del cyberspazio, i quali potrebbero fornire un contributo decisivo allo sviluppo di un sistema più efficiente e resiliente di prevenzione e di monitoraggio delle nuove minacce. Un ruolo che, al contrario, risulta essere riconosciuto nei più recenti atti di indirizzo sovranazionali, come si passerà adesso a chiarire in dettaglio.

3. Pubblico e privato di fronte alle nuove minacce della rete: l'esigenza di un approccio collaborativo per la creazione di un cyberspazio più aperto e resiliente

Come si è detto, la gestione del rischio cibernetico perseguita negli ultimi anni nel nostro ordinamento risulta complessivamente più organica e più fluida rispetto a quella voluta nelle ricordate direttive del 2013 e del 2017 del Presidente del Consiglio dei ministri. Tuttavia, nonostante le significative modifiche introdotte, dapprima, con il d.l. n. 105/2019 e, poi, con il d.l. n. 82/2021, l'impianto normativo vigente sembra continuare a riflettere, in gran parte, le logiche e le dinamiche operative proprie della legge sul comparto *intelligence* (l. n. 124/2007).

Tale circostanza parrebbe trovare giustificazione nella considerazione per la quale i sempre più frequenti attacchi *cyber* ai settori strategici del Paese rappresentano una minaccia seria ed eccezionale per la sicurezza nazionale, tale da non poter essere fronteggiata con il ricorso agli ordinari strumenti di difesa dei confini territoriali[57]. Il che richiederebbe l'attivazione di quelle procedure di raccolta e di analisi delle

[56] Sul punto l'attuale sistema nazionale *cyber* pare presentare criticità analoghe a quelle della ricordata direttiva NIS. Sui limiti applicativi della suddetta direttiva, cfr. la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, *cit*., ove si chiarisce che «la direttiva riguarda unicamente i settori strategici chiave, ma per logica un approccio analogo sarebbe necessario da parte di tutti i portatori d'interessi colpiti da ciberattacchi, in modo da giungere a una valutazione sistematica delle vulnerabilità e dei punti di accesso sfruttati dagli autori di tali attacchi». Al riguardo, cfr. anche R. BRIGHI, P.G. CHIARA, *La cybersecurity come bene pubblico: alcune riflessioni normative a partire dai recenti sviluppi nel diritto dell'Unione Europea*, *cit*., p. 22, i quali rimarcano come «gli attacchi si basano sulle sempre nuove lacune di sicurezza dei sistemi informatici, ma trovano altresì la principale vulnerabilità nel fattore umano. La *cybersecurity* di un paese non dipende solo dalla sicurezza informatica delle organizzazioni del settore pubblico e privato, ma anche dalla sicurezza dei singoli utenti che possono fungere da vettori di attacco a istituzioni o infrastrutture critiche».

[57] Come nota attentamente R. URSI, *La difesa: tradizione e innovazione*, in *Diritto Costituzionale*, n. 1, 2022, pp. 17-18, nella dimensione del cyberspazio «le minacce all'integrità dello Stato da temere non sono l'invasione di un esercito nemico, come nella prima metà del Novecento, ovvero l'attacco missilistico, come nella seconda metà, e neanche più un attentato terroristico di vasta scala, all'inizio del nuovo millennio, bensì un attacco cibernetico, idoneo ad inibire il funzionamento dei sistemi informatici dei gangli vitali di un Paese». Attacchi che «[…] possono avere anche effetti potenzialmente distruttivi se impiegati per indurre il malfunzionamento delle infrastrutture critiche, generando danni materiali ingenti e la potenziale perdita di vite umane». Sul punto, cfr. anche L. MARTINO, *La quinta dimensione della conflittualità. L'ascesa del cyberspazio e i suoi effetti sulla politica internazionale*, in *Politica & Società*, n. 1, 2018, p. 62 ss.; G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della emergenza normalizzata*, in *Rivista AIC*, n. 4, 2019, p. 65 ss. Lo stretto legame tra la tutela della sicurezza nazionale e la tutela della sicurezza cibernetica costituisce, invero, la *ratio* delle recenti modifiche normative in tema di *golden power* introdotte dal citato d.l. n. 21/2022, all'interno del previgente art. 1-*bis* d.l.

informazioni, da un lato, e di assunzione delle decisioni e delle iniziative conseguenti, dall'altro, tipiche del Sistema di informazione per la sicurezza[58].

Invero, l'estensione indiscriminata, al settore della cybersicurezza, dei principi e dei caratteri che connotano l'attività amministrativa svolta dagli organismi inseriti nel Sistema (*i.e.*, riservatezza delle comunicazioni, centralizzazione delle funzioni e unilateralità dei processi decisionali) non sembrerebbe rappresentare l'impostazione metodologica più idonea a superare le sfide per la pubblica sicurezza lanciate dalla diffusione del cyberspazio.

Al riguardo è possibile affermare, infatti, come l'obiettivo di garantire un più elevato livello di sicurezza informatica non possa che richiedere la creazione di un'architettura istituzionale notevolmente più aperta all'esterno rispetto a quella dettata dalla l. n. 124/2007, nella quale gli operatori economici del settore e gli utenti della rete possano avere un ruolo più attivo e propulsivo [59]. E ciò, in particolare, in considerazione del fatto che la costante interazione tra attori pubblici e mondo privato-imprenditoriale consentirebbe non solo una maggiore condivisione di conoscenze, soluzioni tecniche e buone pratiche, ma anche un'auspicabile partecipazione "dal basso" al processo di determinazione delle linee guida e delle decisioni strategiche in materia, nel rispetto delle esigenze di segretezza eventualmente presenti nelle singole fattispecie[60].

---

15 marzo 2012, n. 21, con riferimento all'acquisto di beni e servizi relativi alla progettazione, realizzazione, manutenzione e gestione delle reti di comunicazione elettronica a banda larga basate sulla tecnologia 5G, nonché di ulteriori beni e servizi ICT rilevanti ai fini della sicurezza cibernetica nazionale. In materia, si vedano le analisi di R. CHIEPPA, *La nuova disciplina del golden power dopo le modifiche del decreto legge n. 21 del 2022 e della legge di conversione 20 maggio 2022, n. 51*, in *Federalismi.it*, 8 giugno 2022, p. 20 ss.; nonché di S. MELE, *Il Perimetro di sicurezza nazionale cibernetica e il nuovo "golden power"*, *cit.*, p. 196 ss.

[58] Al riguardo occorre notare come lo schema operativo seguito nel comparto *intelligence* sia stato riprodotto, da ultimo, all'interno del d.l. 9 agosto 2022, n. 115 (c.d. decreto aiuti-*bis*), il cui art. 37, rubricato "Disposizioni in materia di *intelligence* in ambito cibernetico", risponde all'esigenza di rafforzare le capacità di risposta del sistema nazionale *cyber* in caso di aggressione informatica (nei confronti del nostro Paese o di un Paese alleato). In tal senso, la norma prevede che il Presidente del Consiglio dei ministri, acquisito il parere del CISR e sentito il COPASIR, può autorizzare l'AISE e l'AISI, sotto il coordinamento del DIS, ad avviare un'attività offensiva «*in caso di crisi o di emergenza cibernetica a fronte di minacce che coinvolgono aspetti di sicurezza nazionale e non siano fronteggiabili solo con azioni di resilienza, anche in attuazione di obblighi assunti a livello internazionale*».

[59] Cfr. la comunicazione della Commissione europea del 24 luglio 2020, *La strategia dell'UE per l'Unione della sicurezza*, *cit.*, 24, ove si riconosce che: «Un'Unione della sicurezza autentica ed efficace deve essere basata sullo sforzo comune di tutte le componenti della società. I governi, le autorità di contrasto, il settore privato, l'istruzione e i cittadini stessi devono essere impegnati, attrezzati e adeguatamente interconnessi per costruire la preparazione e la resilienza per tutti, in particolare per le persone più vulnerabili, le vittime e i loro parenti e i testimoni».

[60] Sotto questa prospettiva, risulta apprezzabile l'impostazione seguita dalla recente strategia nazionale di cybersicurezza 2022-2026 del maggio 2022, reperibile in *www.acn.gov.it*, ove si rimarca che la piena e costante collaborazione pubblico-privato permea l'intera strategia, «improntata ad un approccio "*whole of society*", che vede il settore pubblico agire sinergicamente con quello privato, il mondo accademico e della ricerca, i media, le famiglie, gli individui per rafforzare la resilienza cibernetica della nazione e della società nel suo insieme». E ciò anche per l'evidente circostanza che lo spazio cibernetico è costituito da prodotti e servizi ICT realizzati o erogati principalmente da soggetti privati (p. 26 della strategia). Un interessante riconoscimento del ruolo del settore privato nel potenziamento delle difese cibernetiche nazionali è contenuto anche nell'*Executive Order on Improving the Nation's Cybersecurity* del 12 maggio 2021, reperibile in *www.cisa.gov,* adottato dal Presidente Biden a seguito dei duri attacchi informatici subiti dalla società *SolarWinds* e dal gruppo *Colonial Pipeline*, ove si ricorda che: «*cybersecurity requires more than government action. Protecting our Nation from malicious*

In altri termini, se è evidente che le autorità amministrative deputate *ex lege* alla prevenzione e alla gestione delle crisi cibernetiche costituiscono l'ossatura organizzativa necessaria per la tutela della pubblica sicurezza nel cyberspazio, allo stesso tempo l'attuale assetto burocratico difficilmente potrà raggiungere i desiderati obiettivi di efficienza e di resilienza in assenza di un coinvolgimento più diretto delle imprese e degli individui impegnati quotidianamente nell'uso dei servizi e dei sistemi informatici[61].

Alla luce di queste premesse, nei successivi paragrafi si cercherà di precisare quale specifico ruolo ciascuna delle predette categorie soggettive debba essere chiamata a svolgere all'interno della novellata architettura *cyber*, al fine di individuare le modalità di intervento necessarie per promuovere un approccio più collaborativo e orizzontale alla tematica in esame.

4. (Segue) Il ruolo degli operatori del settore…

Una delle manifestazioni più emblematiche della recente strategia italiana di contrasto agli attacchi informatici è certamente rappresentata dall'introduzione del Perimetro di sicurezza nazionale, ossia di uno spazio artificialmente delimitato nel quale concentrare l'esercizio delle funzioni di monitoraggio, di ispezione, di accertamento e di sanzione attribuite *ex lege* all'Agenzia nazionale per la cybersicurezza.

Ai diversi soggetti, pubblici e privati, inseriti nel suddetto Perimetro il nostro legislatore ha richiesto, in particolare, il rispetto di una serie di adempimenti organizzativi e comunicativi tutt'altro che irrilevanti, i quali riguardano, tra gli altri: *i*) la predisposizione e l'aggiornamento annuale degli elenchi delle reti, dei sistemi e dei servizi informatici concretamente utilizzati; *ii*) il compimento di analisi di valutazione del rischio di eventuali interruzioni o compromissioni della propria attività; *iii*) l'assolvimento di precisi oneri di comunicazione al Centro di valutazione e certificazione nazionale in caso di ricorso a forniture

cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace». In tema di compartecipazione dei privati alla definizione delle politiche pubbliche, si veda, per tutti, S. CASSESE, *La partecipazione dei privati alle decisioni pubbliche*, in *Riv. trim. dir. pubbl.*, n. 1, 2007, p. 13 ss.

[61] Sul valore della condivisione delle informazioni rilevanti in ambito *cyber*, cfr., da ultimo, la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, *cit.*, par. 2.1., la quale – dopo aver precisato che l'Unione europea è al momento priva di un'adeguata consapevolezza dell'importanza della tematica, dal momento che le diverse autorità nazionali non prevedono in maniera sistematica la raccolta e la condivisione delle informazioni necessarie per sviluppare un ambiente istituzionale sensibile alle problematiche relative alla sicurezza informatica – ha previsto l'istituzione di un'«unità congiunta per il ciberspazio» (*Joint Cyber Unit*), ossia di una piattaforma europea, virtuale e fisica, finalizzata a promuovere la cooperazione operativa tra comunità civili, diplomatiche, forze dell'ordine e della difesa e settore privato in caso di gravi minacce e incidenti di natura transfrontaliera. Al riguardo, il documento ha precisato che: «l'unità congiunta per il ciberspazio non sarà un organismo aggiuntivo e autonomo, né influirà sulle competenze e i poteri delle autorità nazionali di cibersicurezza o dei partecipanti dell'UE. L'unità agirebbe piuttosto come punto d'appoggio dove i partecipanti possono avvalersi del supporto e delle competenze reciproche, soprattutto nel caso in cui le varie cibercomunità debbano lavorare a stretto contatto».

esternalizzate di beni, sistemi e servizi ICT; *iv*) il tempestivo rispetto di obblighi di notifica al menzionato CSIRT Italia in caso di incidenti o attacchi[62].

Tuttavia, se la previsione di speciali misure burocratiche può ragionevolmente essere giustificata alla luce delle peculiari caratteristiche del pericolo da affrontare, non altrettanto ragionevole appare la logica unilaterale (di tipo *top-down*) posta alla base delle suddette modifiche normative.

Al riguardo è possibile notare che, analogamente a quanto si verificava nel precedente assetto istituzionale, le linee di indirizzo e le soluzioni operative volte ad assicurare la sicurezza informatica nel nostro ordinamento continuano ad essere stabilite dalle sole autorità pubbliche competenti, e cioè in assenza di adeguate forme di partecipazione dei portatori di interesse e degli operatori economici del settore[63].

La predetta circostanza suscita, a ben vedere, numerose perplessità. E ciò non solo per la nota situazione di dipendenza del comparto pubblico dalle abilità e dalle esperienze in ambito tecnologico-informatico possedute dal mondo imprenditoriale[64], ma anche per il significativo contributo che i destinatari delle suddette misure potrebbero dare al complessivo incremento del livello di resilienza cibernetica del Paese[65].

Nello specifico, la rilevanza di tale contributo può essere apprezzata sotto una duplice prospettiva.

---

[62] Sul punto, cfr. art. 1, commi 2, 3, 6, 7, 8, d.l. n. 105/2019.

[63] Sotto questa prospettiva va letta la previsione normativa che contempla la mera partecipazione senza diritto di voto alle riunioni del Nucleo per la cybersicurezza dei «soggetti pubblici o privati eventualmente interessati» in situazioni di crisi di natura cibernetica (art. 10, comma 3, d.l. n. 82/2021); disposizione che non appare idonea ad assicurare un effettivo coinvolgimento del settore imprenditoriale nel sistema di gestione delle suddette crisi. Non convincente è anche il contenuto precettivo del novellato art. 33-*septies*, comma 4, d.l. 18 ottobre 2012, n. 179, secondo il quale l'Agenzia nazionale «con proprio regolamento» e, dunque, senza alcuna forma di coinvolgimento esterno «stabilisce i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la pubblica amministrazione» e «definisce, inoltre, le caratteristiche di qualità, di sicurezza, di performance e scalabilità, interoperabilità, portabilità dei servizi *cloud* per la pubblica amministrazione». In materia appaiono interessanti le considerazioni di A. LAURO, *Sicurezza cibernetica e organizzazione dei poteri: spunti di comparazione, cit.*, p. 537, il quale ricorda che, mentre in Italia la collaborazione con i privati è stata finora prevalentemente di natura finanziaria e rivolta allo sviluppo di nuove tecnologie, in Germania e in Francia si è assistito, al contrario, alla creazione di appositi organismi, che raccolgono rappresentanti delle amministrazioni pubbliche e del mondo privato-imprenditoriale e che svolgono importanti compiti di analisi, pianificazione ed elaborazione di indirizzi normativi in materia di cybersicurezza.

[64] Com'è noto, la mancanza di adeguate competenze informatiche all'interno delle pubbliche amministrazioni ha rappresentato, e rappresenta ancora, uno dei principali motivi dei ritardi accumulati dal nostro ordinamento con riferimento al processo di informatizzazione del settore pubblico. Sul punto occorre ricordare, peraltro, che, ai sensi dell'art. 68 CAD, le pubbliche amministrazioni possono rivolgersi al mercato per l'acquisto di programmi e strumenti informatici soltanto all'esito di una valutazione comparativa di tipo tecnico ed economico delle diverse soluzioni disponibili (in termini di costo complessivo, di interoperabilità, di sicurezza, di conformità alla normativa sulla protezione dei dati personali e di servizio); valutazione dalla quale deve risultare motivatamente «l'impossibilità di accedere a soluzioni già disponibili all'interno della pubblica amministrazione, o a *software* liberi o a codice sorgente aperto, adeguati alle esigenze da soddisfare».

[65] Sul concetto di resilienza informatica nazionale, cfr. art. 1, comma 1, lett. b), d.l. n. 82/2021, che la definisce come un insieme di «attività volte a prevenire un pregiudizio per la sicurezza nazionale» di cui all'art. 1, comma 1, lett. f) del DPCM n. 131/2020, ossia «un danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale».

In primo luogo, un'adeguata valorizzazione dell'interlocuzione tra attori istituzionali e soggetti privati favorirebbe una più proficua condivisione di conoscenze e di capacità specialistiche.

Un risultato che risulta essere particolarmente apprezzabile nel delicato contesto della cybersicurezza, nel quale il grado di complessità delle soluzioni e degli strumenti adoperati rendono gli operatori economici del settore i soggetti più qualificati a suggerire alle autorità pubbliche le tecniche, i dispositivi e i servizi più sicuri e affidabili tra quelli disponibili sul mercato[66].

All'interno di un siffatto contesto, inoltre, i soggetti in questione potrebbero essere chiamati a svolgere un ruolo più incisivo in sede di elaborazione e di aggiornamento delle linee guida e degli *standard* di sicurezza rivolti alle reti, ai sistemi e ai servizi inclusi nel Perimetro.

Sotto questa prospettiva, il coinvolgimento delle imprese del settore nel processo di determinazione delle misure e dei requisiti minimi di sicurezza cibernetica non solo offrirebbe alle autorità competenti un valido supporto tecnico, ma rappresenterebbe anche un utile deterrente contro il rischio di imporre adempimenti inidonei o di portata eccessiva rispetto agli obiettivi di *policy* prefissati. Il che conduce a sottolineare come la maggiore partecipazione delle imprese al sistema nazionale di gestione delle criticità informatiche possa concretamente agevolare l'introduzione di rimedi ritagliati sull'effettivo grado di pericolosità delle minacce, in conformità ai principi di proporzionalità e di ragionevolezza dell'azione amministrativa esercitata in ambito *cyber*[67].

Sul punto è necessario osservare che la mancata previsione di adeguati momenti di interazione tra settore pubblico e privato contrasta anche con le indicazioni formulate in materia nei menzionati atti di indirizzo sovranazionali.

---

[66] In tal senso, il grado di complessità tecnica che caratterizza il fenomeno in esame giunge a rendere desiderabile ciò che, in altri contesti, potrebbe apparire paradossale, ovvero che siano gli stessi operatori economici del settore ad aiutare le autorità nazionali a comprendere la natura e la portata delle minacce da affrontare, oltre che a suggerire quali misure e accorgimenti concreti adottare per tutelare al meglio la pubblica sicurezza. Sul punto si vedano, *ex multis*, le osservazioni di A. BARONE, *Il diritto del rischio*, *cit*., p. 64 ss., secondo il quale: «Il diritto del rischio delinea modelli relazionali basati, piuttosto che su meccanismi di *command and control* o di integrale "autoamministrazione" privata, sull'integrazione e sulla cooperazione tra pubblico e privato». Quest'ultima, infatti, «[…] è senza dubbio in grado di ridurre le asimmetrie informative delle Amministrazioni, inevitabilmente dotate di minori informazioni sui rischi da incertezza scientifica rispetto a chi, con i propri processi di produzione, causa i medesimi rischi». Cfr. anche la comunicazione della Commissione europea del 31 maggio 2006, *Una strategia per una società dell'informazione sicura. Dialogo, partenariato e responsabilizzazione*, COM (2006) 251, par. 3.2.1., in *www.eur-lex.europa.eu,* ove si evidenzia che: «Per poter formulare efficacemente una politica, è necessario comprendere con chiarezza la natura e la portata delle sfide. Ciò richiede non solo dati statistici ed economici affidabili e aggiornati sugli incidenti a danno della sicurezza informatica e sui livelli di fiducia dei consumatori e degli utilizzatori, ma anche dati aggiornati sulle dimensioni e le tendenze in atto nell'industria della sicurezza delle TIC in Europa».

[67] Una declinazione concreta dei suddetti principi generali è ravvisabile nel d.l. n. 105/2019, laddove si prevede che l'individuazione dei soggetti da includere nel Perimetro debba seguire un criterio di gradualità, ossia debba tenere conto dell'entità del potenziale pregiudizio per la sicurezza nazionale derivante dal malfunzionamento, dall'interruzione o dall'uso improprio delle reti, dei sistemi e dei servizi informatici gestiti da tali soggetti.

Dall'analisi di questi atti emerge, infatti, come le imprese che offrono i propri prodotti nel cyberspazio debbano assumere un impegno più diretto e responsabile ai fini del mantenimento di un soddisfacente livello di sicurezza delle reti e dei sistemi informatici, come si ricava, in particolare, dall'affermazione di due significativi principi[68].

Da un lato, il principio di "sicurezza *by design*", in base al quale i produttori e i fornitori devono immettere sul mercato unicamente beni e/o servizi in grado di assicurare determinati livelli di resilienza contro il rischio di incidenti e attacchi. Un'obbligazione, quest'ultima, che non solo deve essere rispettata fin dal momento della progettazione dell'infrastruttura o del dispositivo tecnologico, ma che costituisce altresì una specifica parte della prestazione contrattuale assunta dal professionista nei confronti del consumatore[69].

Dall'altro, il c.d. "principio di responsabilità", in virtù del quale gli operatori economici del settore devono assumere, nei confronti degli utenti della rete, il ruolo di interlocutori privilegiati durante l'intero ciclo di vita dei prodotti ICT acquistati sul mercato. Una circostanza che determina per tali soggetti il sorgere di un particolare dovere di diligenza[70], che si esplica, ad esempio, nell'obbligo di curare i necessari aggiornamenti *software* dei prodotti, di risolvere con celerità le vulnerabilità segnalate dai consumatori, nonché di garantire un corretto utilizzo dei dati personali trattati nello svolgimento delle proprie attività imprenditoriali[71].

---

[68] Sul punto, si vedano la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 13 settembre 2017, *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE*, *cit.*, p. 6, ove si riconosce che: «Un approccio di "sicurezza fin dalla progettazione" adottato dai produttori di dispositivi connessi, *software* e attrezzature informatiche permetterebbe di definire la questione della cibersicurezza prima di immettere nuovi prodotti sul mercato. Questo potrebbe rientrare nel principio di "responsabilità", da elaborare ulteriormente insieme agli operatori del settore, che potrebbe ridurre le vulnerabilità dei prodotti/*software* applicando una serie di metodi che vanno dalla progettazione ai test e alla verifica, inclusa la verifica formale ove applicabile, la manutenzione a lungo termine e l'utilizzo di processi sicuri lungo il ciclo di sviluppo, così come lo sviluppo di aggiornamenti e correzioni atti a risolvere vulnerabilità precedentemente nascoste e rapidi interventi di aggiornamento e riparazione»; nonché la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, *cit.*, par. 3.2, ove si sottolinea che: «per sviluppare una cooperazione multipartecipata sulle questioni di cibersicurezza, la Commissione e l'alto rappresentante, in linea con le rispettive competenze, mirano a rafforzare gli scambi regolari e strutturati con i portatori di interessi, compreso il settore privato, il mondo accademico e la società civile, sottolineando che la natura interconnessa del ciberspazio richiede che tutti i portatori di interessi si scambino informazioni e si assumano le proprie responsabilità specifiche per mantenere un ciberspazio globale, aperto, stabile e sicuro».

[69] Si tratta, invero, di un'obbligazione di non semplice esecuzione, dal momento che, come nota P.L. MONTESSORO, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, *cit.*, p. 790, oggi gli *hacker* investono ingenti risorse nella ricerca degli errori di programmazione (*bug*), al fine di modificare ad arte il comportamento del calcolatore in cui è inserito il programma difettoso. Sicché «il progettista deve correggere tutte le vulnerabilità del suo sistema, mentre all'*hacker* basta scoprirne una […]».

[70] Cfr. ancora la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, *cit.*, par. 1.5., ove si precisa che il dovere di diligenza esigibile nei confronti dei produttori dovrà essere potenziato a livello normativo, proprio a causa della crescente diffusione del fenomeno dell'*Internet of things* di cui si è detto *supra*.

[71] Sui possibili conflitti tra tutela della cybersicurezza e tutela della *privacy*, si è espresso in più occasioni lo stesso Garante europeo per la protezione dei dati, secondo il quale le recenti iniziative legislative in tema di *cybersecurity* non dovrebbero

In considerazione di quanto appena rilevato, va accolta, dunque, con particolare favore l'introduzione di forme più strutturate, e meno occasionali, di confronto tra i soggetti interessati, anche tramite la creazione di veri e propri organismi *ad hoc,* volti a facilitare lo scambio reciproco di esperienze e conoscenze ed a incentivare la definizione di indirizzi condivisi[72].

Com'è noto, la realizzazione di un siffatto obiettivo non risulta affatto agevole nel contesto *cyber*, dal momento che i tentativi di instaurazione di un sincero dialogo tra i diversi portatori di interessi rischiano di essere pregiudicati da comprensibili timori di sovraesposizione.

In tal senso, se da una parte le autorità amministrative possono manifestare una certa riluttanza nel condividere dati riguardanti la propria sicurezza informatica, temendo di compromettere in tal modo la propria immagine istituzionale, dall'altra gli stessi operatori economici potrebbero non voler collaborare con il settore pubblico per non correre il rischio di confidare informazioni aziendali di natura riservata o personale, di ledere la propria reputazione sul mercato e di esporsi al rischio di azioni legali[73].

---

pregiudicare quanto già previsto dal GDPR, ma dovrebbero, al contrario, ispirarsi ai principi di quest'ultimo, come quelli del *privacy by design* e del *privacy by default* (art. 25 GDPR). Così, EDPS, *Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive*, 11 March 2021, par. 2.1, in *www.edps.europa.eu*: «*The EDPS is aware of the potential of artificial intelligence in developing advanced cybersecurity capabilities for the real-time detection, analysis, containment and response to cyber threats in a continuously enlarged digital landscape. However, these technologies generally require processing of large amounts of personal data (e.g. user log data) and come with their own risks that need to be identified and mitigated (e.g. lack of transparency or bias). Use of technologies for improving cybersecurity should not unduly interfere with the rights and freedoms of individuals. The first step to avoid or mitigate those risks is to apply the data protection by design and by default requirements laid down in Article 25 GDPR, which will assist in integrating the appropriate safeguards such as pseudonymisation, encryption, data accuracy, data minimization, in the design and use of these technologies and systems. […] Integrating the privacy and data protection perspective in the traditional cybersecurity management will ensure a holistic approach and enable synergies to public and private organizations when managing cybersecurity and protecting the information they process without useless multiplication of efforts*»; nonchè Id., *Opinion 8/2022 on the Proposal for a Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union*, 17 May 2022, par. 3.1, in *www.edps.europa.eu:* «*In order to comply with the Proposal, the EUIs, as well as CERT-EU, will have to deploy certain cybersecurity processes and measures, which are bound to imply additional processing of personal data and of electronic communications data, including traffic data. […] The EDPS therefore considers that it should be clarified, for the avoidance of any doubt, in a new recital that "All cybersecurity systems and services involved in the prevention, detection, and response to cyber threats should be compliant with the current data protection and privacy framework, and should take relevant technical and organizational safeguards to ensure this compliance in an accountable way"*».

[72] Sotto questa prospettiva va letta l'istituzione del Centro europeo di competenza industriale, tecnologica e di ricerca sulla cybersicurezza ad opera del regolamento UE 2021/887 del 20 maggio 2021, che risponde al precipuo scopo di sviluppare e sostenere le capacità, i mezzi e le competenze tecnologiche dell'Unione in materia di cybersicurezza, promuovendo e agevolando, anche tramite l'azione dei diversi centri nazionali di coordinamento – in Italia, tale ruolo spetta, come si è detto, all'Agenzia nazionale – la partecipazione della società civile, dell'industria, della comunità accademica e della ricerca. Il Centro e la rete europea gestiscono i fondi destinati alla cybersicurezza dal programma Europa digitale e dal programma Orizzonte Europa e possono beneficiare, inoltre, di contributi dei singoli Stati membri. Ad analoghe esigenze di cooperazione pubblico-privato parrebbe rispondere anche l'imminente istituzione dell'Unità congiunta per il cyberspazio, quale piattaforma strutturata di condivisione di informazioni e di competenze, in merito alla quale si è già detto *supra*.

[73] Al riguardo, cfr. R. BOSSONG, B. WAGNER, *A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union*, in *Crime, Law and Social Change*, n. 67, 2017, p. 273, i quali evidenziano come le suddette criticità giustificano una generale preferenza per l'utilizzo di strumenti di *governance* di tipo *top-down*, che si fondano, ad esempio, sulla previsione di specifici doveri di notifica in capo agli operatori privati in caso di rilevanti incidenti informatici. Sul punto, cfr. anche il report del Gruppo di coordinamento sulla sicurezza cibernetica della Banca d'Italia, *Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass*, agosto 2018, reperibile in *www.bancaditalia.it*, ove si sottolinea che, nonostante il valore strategico della condivisione delle informazioni sulle minacce informatiche, le imprese che hanno

Per cercare di non perdere i rilevanti benefici derivanti dalla creazione di preziose sinergie operative, una soluzione percorribile sembrerebbe essere rappresentata dal ricorso ad apposite forme, contrattuali o istituzionalizzate, di partenariato pubblico-privato, con il precipuo scopo di contribuire al perseguimento degli obiettivi di prevenzione e di contrasto nei confronti dei crescenti pericoli della dimensione cibernetica[74].

Attraverso queste specifiche forme di cooperazione diventerebbe più semplice, infatti, non solo, come si è detto *supra,* supportare lo sviluppo e la diffusione delle più avanzate tecniche di gestione delle situazioni di crisi, ma anche, e soprattutto, fornire incentivi concreti a coloro che condividono le proprie competenze professionali per offrire una migliore comprensione dei rischi informatici attuali e della loro possibile evoluzione[75].

Un esempio virtuoso di collaborazione pubblico-privato è offerto, ancora una volta, dal livello sovranazionale, dal momento che la recente strategia europea in tema di cybersicurezza prevede, tra le altre, l'istituzione di una rete di centri operativi di sicurezza (c.d. SOC, *Security Operations Center*), incaricati

subito attacchi sono spesso riluttanti a svelarli per timore di ricadute reputazionali e sono disposte a condividere i propri dati solo in contesti che garantiscono riservatezza e reciprocità. Sicché, se talvolta gruppi di operatori economici particolarmente sensibili al rischio cibernetico (ad esempio i gestori di infrastrutture critiche) si aggregano volontariamente, più spesso è necessario un intervento delle autorità pubbliche per garantire il necessario clima di fiducia tra operatori economici e autorità pubbliche.

[74] In ambito europeo, si veda la positiva esperienza del primo accordo di partenariato pubblico-privato sulla cybersicurezza del 5 luglio 2016, promossa dalla comunicazione della Commissione europea del 6 maggio 2015, *Strategia per il mercato unico digitale in Europa*, COM (2015) 192 final, par. 3.4., con il quale è stata instaurata una più stabile cooperazione tra diversi soggetti, pubblici e privati, interessati a stimolare la ricerca e l'innovazione in ambito cibernetico, rilanciare l'industria europea della sicurezza informatica e introdurre soluzioni innovative e affidabili (prodotti, servizi e *software* ICT) in alcuni settori strategici dell'Unione (*i.e.*, energia, sanità, trasporti, finanza). Nello specifico, l'accordo ha ricevuto un investimento da parte dell'Unione europea, nel quadro del programma Orizzonte 2020, di 450 milioni di euro, mentre gli investimenti degli operatori del mercato della cybersicurezza, rappresentati dall'Organizzazione europea per la sicurezza informatica (ECSO), sono stati tre volte maggiori, per un totale di circa 1,8 miliardi tra il 2016 e il 2020. In tema di partenariato pubblico-privato si vedano, *ex multis*, M.P. CHITI, voce *Partenariato pubblico privato*, in *Enc. giur.*, X, Milano, 2007, p. 690 ss.; Id. (a cura di), *Il partenariato pubblico-privato. Concessioni finanza di progetto società miste fondazioni*, Editoriale Scientifica, Napoli, 2009; R. DIPACE, *Partenariato pubblico privato e contratti atipici*, Giuffrè, Milano, 2006; F. MASTRAGOSTINO (a cura di), *La collaborazione pubblico-privato e l'ordinamento amministrativo*, Giappichelli, Torino, 2011; G. CERRINA FERONI (a cura di), *Il partenariato pubblico privato. Modelli e strumenti*, Giappichelli, Torino, 2011; A. DI GIOVANNI, *Il contratto di partenariato pubblico privato tra sussidiarietà e solidarietà*, Giappichelli, Torino, 2012; M. RICCHI, *L'architettura dei contratti di concessione e di partenariato pubblico privato nel nuovo codice dei contratti pubblici (d.lgs. n. 50/2016)*, in *Riv. giur. Mezz.*, n. 3, 2016, p. 811 ss.; A. FIORITTO (a cura di), *Nuove forme e nuove discipline del partenariato pubblico privato*, Giappichelli, Torino, 2017; G. MULAZZANI, *La collaborazione pubblico-privato e la sussidiarietà orizzontale*, Cacucci, Bari, 2020.

[75] In tema appaiono interessanti le proposte contenute nella citata strategia italiana sulla cybersicurezza 2022-2026, ove si fa riferimento al coinvolgimento di un gruppo di aziende qualificate e specializzate in materia di *incident response* e alla creazione di una rete di CERT settoriali, al fine di fornire un valido supporto tecnico al CSIRT Italia qualora dovesse verificarsi una serie di incidenti *cyber* di natura sistematica (cfr. Obiettivo 2.B della suddetta strategia).

di assicurare un monitoraggio costante, in tempo reale, delle intrusioni e delle anomalie informatiche nelle reti e nei sistemi di diversi portatori di interesse[76].

Nelle intenzioni della Commissione europea, la suddetta rete dovrebbe ricomprendere, grazie ad appositi investimenti sulla formazione professionale, anche le PMI, in modo tale da migliorare la velocità di rilevamento, di analisi e di condivisione dei dati relativi agli attacchi *cyber*. Sotto questa prospettiva, tramite lo sfruttamento dei vantaggi ricavabili dall'introduzione del *network*, nonché tramite l'utilizzo delle innovative capacità di previsione e di classificazione offerte dai moderni strumenti di intelligenza artificiale[77], il legislatore europeo intende sviluppare un vero e proprio scudo di sicurezza informatica all'interno dell'Unione, consentendo alle autorità pubbliche e ai soggetti privati di segnalare potenziali minacce prima che queste abbiano causato ingenti danni su larga scala.

Un esempio, quest'ultimo, che conferma le criticità in precedenza evidenziate nei confronti dell'attuale apparato nazionale, la cui impostazione di fondo, nonostante alcune recenti apprezzabili previsioni[78], continua a riprodurre la logica unilaterale e centralizzata tipica della disciplina del comparto *intelligence*. Il che conduce ad auspicare l'adozione di interventi normativi volti a correggere un siffatto approccio.

5. (Segue) …e degli utenti informatici

Nell'ottica di definire un'architettura *cyber* realmente efficiente e orizzontale, la promozione di un ruolo più attivo da parte degli operatori del settore non dovrebbe rappresentare l'unica strategia da seguire, ma occorrerebbe valorizzare anche i compiti e le responsabilità spettanti agli utenti della rete e dei servizi digitali.

Tale affermazione trova conferma nella circostanza per la quale, com'è noto, un certo, quand'anche limitato, rischio securitario è irrimediabilmente presente in ogni attività umana che si fonda sull'utilizzo di sistemi e di dispositivi informatici; sicché ogni iniziativa di contrasto alle attuali minacce cibernetiche

[76] Cfr. la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 16 dicembre 2020, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, *cit*., par. 1.2., ove si prevede lo stanziamento di oltre 300 milioni per l'istituzione dei predetti SOC, a sostegno della cooperazione pubblico-privato e transfrontaliera.

[77] Ci si riferisce, in particolare, a quelle tecniche di *machine learning* volte ad estrarre, tramite l'analisi dei dati inerenti agli episodi e agli autori delle minacce informatiche, informazioni significative sulle loro modalità di attuazione e sui possibili sviluppi del fenomeno, consentendo in tal modo alle autorità nazionali di predisporre misure e contromisure adeguate al livello di rischio *cyber*.

[78] Un esplicito, seppur generico, riferimento al valore strategico della dinamica collaborativa è rinvenibile all'art. 7, comma 1, lett. n), d.l. n. 81/2021, che affida all'Agenzia nazionale il compito di sviluppare e «rendere effettive» le capacità nazionali di prevenzione, di monitoraggio, di analisi e di risposta agli attacchi informatici, anche attraverso il ricorso a iniziative di partenariato pubblico-privato. Lo stesso decreto, inoltre, attribuisce all'Agenzia nazionale il potere di costituire e di partecipare a partenariati pubblico-privato, nell'ottica della migliore realizzazione delle sue finalità istituzionali (cfr. art. 7, comma 1, lett. z). Un significativo contributo alla costruzione di un'architettura nazionale *cyber* realmente partecipata e aperta sembrerebbe poter derivare dalla recentissima introduzione della rete dei laboratori accreditati di prova (c.d. LAP), quali soggetti, sia pubblici che privati, volti a supportare le procedure di valutazione e di analisi della qualità tecnica dei dispositivi tecnologici utilizzati dai soggetti inclusi nel Perimetro nazionale. In materia, si rinvia alle previsioni del DPCM n. 92/2022 e del d.lgs. n. 123/2022.

non può che cercare di ridurne l'impatto e gli effetti dannosi, senza potere, tuttavia, eliminarli definitivamente.

Per queste ragioni, una lungimirante e accurata strategia nazionale di mitigazione delle vulnerabilità informatiche non può esimersi dal dedicare una particolare attenzione al miglioramento del livello generale di alfabetizzazione digitale, dal momento che la previsione di apposite occasioni di formazione e di sensibilizzazione collettiva parrebbe rappresentare una formidabile arma di prevenzione nei confronti delle insidie del cyberspazio[79].

Il raggiungimento dell'obiettivo appena richiamato permetterebbe, in particolare, di conseguire una serie di rilevanti vantaggi pratici, che si apprezzano, quantomeno, sotto una triplice prospettiva.

In primo luogo, un'adeguata sensibilizzazione dell'opinione pubblica nei confronti delle tipologie di minacce e degli strumenti di tutela offerti dall'ordinamento sembrerebbe poter contribuire a ridurre l'efficacia degli attacchi meno sofisticati.

In tal senso, la promozione di momenti di formazione e di arricchimento culturale in materia di cybersicurezza risulterebbe importante per consentire la sedimentazione di opportune abitudini di "igiene informatica" all'interno della collettività[80]. Il che darebbe alle competenti autorità pubbliche la possibilità

[79] Sul valore dell'educazione dei cittadini nelle recenti politiche multilivello di sicurezza informatica, si vedano, tra gli altri, l'art. 7, comma 1, lett. d), direttiva NIS, che obbliga gli Stati membri a prevedere, all'interno delle rispettive strategie nazionali, appositi programmi di formazione, sensibilizzazione e istruzione; gli artt. 4, comma 7, e 10 reg. UE 2019/881, che attribuiscono ad ENISA il compito di promuovere un elevato livello di consapevolezza dei cittadini, delle organizzazioni pubbliche e delle imprese in materia di cybersicurezza, assistendo gli Stati membri nei loro sforzi di sensibilizzazione e di istruzione della collettività e incoraggiando un miglior coordinamento e scambio di buone pratiche a livello internazionale *in subiecta materia*; l'art. 7, comma 1, lett. v), d.l. n. 82/2021, che attribuisce all'Agenzia nazionale per la cybersicurezza il compito di promuovere «la formazione, la crescita tecnico-professionale e la qualificazione delle risorse umane nel campo della cybersicurezza, in particolare favorendo l'attivazione di percorsi formativi universitari in materia, anche attraverso l'assegnazione di borse di studio, di dottorato e assegni di ricerca, sulla base di apposite convenzioni con soggetti pubblici e privati». In generale, sull'importanza dell'istruzione e della formazione digitale quale strumento per affrontare al meglio le sfide poste dalla crescente diffusione delle *fake news*, del cyberbullismo, delle minacce *cyber* e delle frodi informatiche, cfr. anche la comunicazione della Commissione europea del 17 gennaio 2018, *Piano d'azione per l'istruzione digitale*, COM (2018) 22 final, in *www.eur-lex.europa.eu*. Al riguardo si vedano le interessanti osservazioni di G. ZICCARDI, *La cybersecurity nel quadro tecnologico (e politico) attuale*, in G. ZICCARDI, P. PERRI (a cura di), *Tecnologia e diritto*, *cit.*, p. 210, il quale nota che il seguire una serie di regole, spesso facili da comprendere anche per chi non abbia una preparazione tecnica, consentirebbe di disegnare un quadro, se non assolutamente sicuro, almeno di contrasto alle minacce più comuni e note. Ad esempio, «una cura nell'impostazione di un buon sistema di autenticazione, la configurazione di parametri di autorizzazione restrittivi, l'uso di un sistema di *backup* e di ripristino del sistema, l'installazione di *antivirus* e *firewall*, la diffusione della cifratura delle informazioni e una maniacale attenzione ai comportamenti (e alle relative vulnerabilità umane)».

[80] In materia, cfr. M. TADDEO, *Is Cybersecurity a Public Good?*, in *Minds & Machines*, n. 29, 2019, p. 352, secondo la quale l'idea di prevedere forme di responsabilità in capo agli utenti della rete e dei servizi digitali trova le proprie radici culturali nelle teorie economiche che considerano la robustezza dei sistemi informatici come un vero e proprio bene pubblico; P.L. MONTESSORO, *Cybersecurity: conoscenza e consapevolezza come prerequisiti per l'amministrazione digitale*, *cit.*, pp. 784-785, il quale nota che: «il normale utente finale, anche se elemento periferico e apparentemente poco importante nel complesso sistema dei servizi digitali, rappresenta un appetibile punto di accesso per gli attacchi informatici da parte degli *hacker,* proprio perché meno consapevole dei rischi e più indifeso in termini di sicurezza informatica. Anche per la *cybersecurity*, come per i vaccini, è necessaria la cosiddetta "immunità di gregge": solo una diffusa prevenzione basata sulla conoscenza può limitare significativamente la superficie di attacco e portare il rischio *cyber* al di sotto di livelli accettabili».

di concentrare le proprie risorse nei confronti dei soggetti più vulnerabili e immaturi, come gli anziani e i giovanissimi, spesso dotati di scarse competenze informatiche di base e, dunque, maggiormente esposti al rischio di cadere nelle trappole virtuali predisposte dai criminali professionisti.

In secondo luogo, una maggiore condivisione di *best practice* e di linee guida di comportamento *online* parrebbe poter determinare un auspicabile aumento del numero delle segnalazioni facoltative degli utenti della rete.

Una circostanza che consentirebbe non solo una migliore comprensione, da parte degli attori istituzionali, della capillarità e dell'evoluzione del fenomeno in esame, ma anche un complessivo incremento del senso di fiducia dei cittadini nei confronti delle applicazioni e dei sistemi tecnologici.

Infine, la previsione di nuove iniziative e di congrui investimenti finanziari nel campo della formazione costituirebbe uno strumento particolarmente utile per supportare la più ampia diffusione possibile di una vera e propria cultura della sicurezza e del rischio informatico, quale prerequisito fondamentale per la realizzazione di una giusta e sostenibile transizione digitale a livello nazionale[81].

Un risultato, quest'ultimo, che, come emerge anche dai ricordati atti di indirizzo europei, non pare poter essere raggiunto attraverso la mera imposizione di adempimenti burocratici nei confronti dei gestori delle infrastrutture e dei servizi ICT, ma solo attraverso la valorizzazione delle responsabilità condivise possedute da tutti i diversi protagonisti del cyberspazio, ciascuno dei quali è chiamato ad assumere condotte e precauzioni conformi alle regole organizzative e comportamentali stabilite in materia[82].

---

[81] A livello internazionale, il concetto in questione ha trovato esplicito riconoscimento nella risoluzione dell'Assemblea generale delle Nazioni Unite del 31 gennaio 2003, *Creation of a global culture of cybersecurity*, A/RES/57/239, in *www.digitallibrary.un.org* – ove sono stati indicati, per la prima volta, nove fondamentali principi in grado di diffondere una cultura globale della sicurezza informatica *(Awareness, Responsability, Response, Ethics, Democracy, Risk assessment, Security design and implementation, Security management, Reassessment*) – e nella risoluzione del Consiglio dell'Unione europea del 18 febbraio 2003, *Un approccio europeo per una cultura della sicurezza delle reti e dell'informazione*, 2003/C 48/01, in *www.eur-lex.europa.eu*. Peraltro, sebbene il compito di diffondere la predetta cultura della sicurezza informatica rappresenti, fin dalla sua istituzione, uno dei compiti principali dell'ENISA (art. 3, par. 1, lett. j), reg. CE 460/2004) e, da ultimo, dell'Agenzia nazionale per la cybersicurezza (art. 7, comma 1, lett. u), d.l. n. 82/2021), il recente rapporto Censis-*Deepcyber* del 22 aprile 2022, *Il valore della cybersecurity*, reperibile in *www.censis.it*, ha sottolineato che in Italia quattro persone su dieci sono indifferenti o non si tutelano contro gli attacchi informatici; il che non stupisce se si considera che, secondo il predetto rapporto, solo il 24,3% degli italiani dichiara di sapere precisamente cosa si intende per *cybersecurity*, mentre il 58,6% dichiara il conosce il tema a grandi linee e il 17,1% dichiara di non sapere cosa sia.

[82] Sul principio di responsabilità condivisa, quale elemento cardine per il corretto funzionamento della *governance* europea sulla cybersicurezza, cfr. la risoluzione del Consiglio del 18 dicembre 2009, *Un approccio cooperativo in materia di sicurezza delle reti e dell'informazione*, 2009/C 321/01, in *www.eur-lex.europa.eu*, ove si riconosce che: «la sicurezza delle reti e dell'informazione è di responsabilità comune di tutte le parti interessate, compresi gli operatori, i fornitori di servizi, i fornitori di *hardware* e di *software*, gli utenti finali, gli enti pubblici e i governi nazionali»; nonché la comunicazione congiunta della Commissione europea e dell'Alto rappresentante dell'Unione del 7 febbraio 2013, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, *cit*., par. 1.2, ove si riconosce che: «la crescente dipendenza dalle tecnologie dell'informazione e delle comunicazioni in tutti i campi della vita umana ha creato vulnerabilità che è necessario definire adeguatamente, analizzare in profondità, riparare o ridurre. Tutti gli attori implicati, siano essi autorità pubbliche, settore privato o singoli cittadini, devono riconoscere questa responsabilità condivisa, attivarsi per proteggersi e se necessario assicurare una risposta coordinata per rafforzare la cibersicurezza».

L'importanza di promuovere la suddetta cultura della sicurezza informatica viene apprezzabilmente riconosciuta, da ultimo, nella recente strategia italiana sulla cybersicurezza del maggio 2022, ove tale obiettivo viene espressamente qualificato come «fattore abilitante», necessario per la piena attuazione degli altri obiettivi di protezione, di risposta e di sviluppo indicati nello stesso documento.

Al riguardo la suddetta strategia sottolinea l'esigenza di prevedere un capillare programma di educazione digitale per tutti i livelli di istruzione scolastica, nel tentativo di stimolare l'adozione di comportamenti sicuri e virtuosi nel cyberspazio; programma al quale devono far seguito apposite iniziative culturali rivolte ad accrescere la percezione delle problematiche legate alla sicurezza cibernetica all'interno delle organizzazioni pubbliche e private. Un contesto in cui occorrerà prevedere peculiari responsabilità in capo ai livelli apicali, ai quali spetta definire efficaci piani di gestione interna del rischio *cyber*, anche tramite operazioni di autovalutazione del proprio livello di esposizione[83].

6. Considerazioni conclusive

Nei precedenti paragrafi si è evidenziato come, pur costituendo un presupposto indispensabile per la realizzazione della desiderata transizione digitale del Paese, il tema della pubblica sicurezza cibernetica è stato posto al centro del dibattito giuridico italiano solo negli ultimi anni, anche grazie alle recenti spinte evolutive provenienti dall'Unione europea.

Come si è detto, il processo di definizione dell'architettura nazionale *cyber* è stato affidato, in un primo momento, ad una serie di atti normativi di coordinamento delle attribuzioni precedentemente spettanti agli enti del Sistema di informazione per la sicurezza della Repubblica. Una circostanza che pare aver conferito complessità e frammentarietà all'impianto organizzativo e operativo di riferimento.

Nelle modifiche normative successive, al contrario, il legislatore italiano ha adottato una prospettiva di maggiore concentrazione delle funzioni e delle azioni finalizzate alla prevenzione e al contrasto delle sempre più frequenti minacce informatiche, culminata nell'istituzione di un'Agenzia nazionale *ad hoc*.

Il complessivo assetto istituzionale che si ricava dagli ultimi interventi sembra, tuttavia, continuare a suscitare alcune rilevanti criticità, che necessitano di ulteriori adeguamenti e rifiniture[84].

In tal senso, il pieno raggiungimento degli obiettivi fissati nelle strategie multilivello di sicurezza informatica parrebbe richiedere e stimolare una più ampia partecipazione degli operatori economici e

[83] Cfr. p. 25 della suddetta strategia.

[84] Si tratta di modifiche normative delle quali la stessa Agenzia nazionale potrebbe farsi promotrice, dato che, ai sensi dell'art. 7, comma 1, lett. p), d.l. n. 82/2021, l'Autorità «cura e promuove la definizione e il mantenimento di un quadro giuridico nazionale aggiornato e coerente nel dominio della cybersicurezza, tenendo anche conto degli orientamenti e degli sviluppi in ambito internazionale» ed «esprime pareri non vincolanti sulle iniziative legislative o regolamentari concernenti la cybersicurezza».

degli utenti interessati all'interno dell'articolato *risk management system*, finora sostanzialmente rimesso alle sole decisioni delle competenti autorità pubbliche.

Secondo le modalità *supra* illustrate, infatti, l'effettivo coinvolgimento dei diversi protagonisti del cyberspazio, ciascuno per la sua parte, permetterebbe non solo di implementare le conoscenze e le capacità nazionali di reazione alle situazioni di crisi, ma anche di accrescere, più in generale, il senso di fiducia dei cittadini e delle imprese nei confronti delle moderne tecnologie informatiche.

Sotto questa prospettiva, pare potersi affermare come, di fronte alle sfide poste dalla crescente diffusione della dimensione cibernetica, la migliore assicurazione possibile contro i rischi per la pubblica sicurezza sia rappresentata dallo sviluppo di adeguate forme di collaborazione pubblico-privato e dal conseguente abbandono delle dinamiche tipiche del comparto *intelligence,* improntate alla segretezza e all'unilateralità dell'azione.

Una circostanza che conduce a riflettere sull'effettiva portata delle novità legislative introdotte in materia, le quali intendono garantire, da un lato, il rispetto di determinati *standard* da parte dei gestori delle infrastrutture e dei servizi strategici, ma non prevedono, dall'altro, momenti di virtuosa interlocuzione con il mondo imprenditoriale circa l'adeguatezza delle misure di sicurezza stabilite dall'alto.

Da qui la consapevolezza del lungo cammino che attende l'architettura nazionale di cybersicurezza per allinearsi ai valori della condivisione e della cooperazione sui quali si fonda la visione europea di cyberspazio.