medialaws

Anticipazioni

Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?

Federico Serini

Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?

Abstract

La cooperazione informativa rappresenta una delle attività funzionali al processo di integrazione europea, ed in particolare lo scambio di informazioni di sicurezza è espressione della capacità di cooperazione degli Stati membri quale elemento fondante lo "Spazio di libertà, sicurezza e giustizia" dell'Unione europea. L'analisi che si propone in questo contributo vuole studiare l'organizzazione e le procedure di scambio delle informazioni per il contrasto delle minacce informatiche al fine di osservare il processo di integrazione della cybersicurezza europea in corso, avendo modo di affrontare il rapporto tra il settore pubblico e privato variamente coinvolti.

Information cooperation represents one of the functional activities in the process of European integration, and in particular, the exchange of security information is an expression of the member states' ability to cooperate as a founding element of the European Union's "Area of Freedom, Security and Justice". The analysis proposed in this contribution aims to study the organization and procedures of information exchange for countering cyber threats to observe the ongoing European cybersecurity integration process, having a way to address the relationship between the public and private sectors involved.

Sommario

Keywords

cyber situational awareness - cybersecurity threat information sharing – cybersicurezza europea - cooperazione pubblico privato – dati personali

1. Breve premessa di studio: insicurezza di rete, rischio informatico e la cooperazione tra pubblico e privato

Le risorse informatiche costituiscono un elemento essenziale per le democrazie. Tali strumenti non rappresentano solo il mezzo che consente agli individui di esprimere liberamente la propria personalità in nuove forme e modi tramite la rete[1] ma, a livello tecnico[2], sono anche i parametri di configurazione e di funzionamento di molte infrastrutture che erogano servizi e funzioni essenziali per la società e l'economia (c.d infrastrutture critiche). Si pensi agli apparati informatici in uso presso gli operatori attivi nei settori bancario e finanziario, energetico, dei trasporti, delle comunicazioni, quello sanitario nonché quelli in dotazione presso le pubbliche amministrazioni e le varie istituzioni statali.

Questi strumenti sono ormai indispensabili sia per lo Stato in sé (apparato), sia per le sue componenti, prime fra tutte gli individui e le imprese (collettività)[3]. Tuttavia, allo stesso tempo, sono anche responsabili di aver trasferito i rischi del cyberspazio nel mondo reale, tanto che nell'attuale contesto informatizzato qualcuno ha avvertito che «ogni società è tanto vulnerabile quanto è vulnerabile l'informatica di cui fa uso» e pertanto «più le società sono avanzate, più sono vulnerabili»[4].

Nonostante tale condizione - secondo cui "rischio informatico=rischio sociale" - porti in evidenza come la tutela e la garanzia dei diritti e delle libertà nell'attuale società tecnologica passi anche per la sicurezza delle reti e dei sistemi informatici[5], i poteri pubblici hanno volto l'attenzione verso questo fenomeno solo di recente (più o meno a partire dalla fine degli anni '90 del secolo scorso), a seguito della progressiva dipendenza degli Stati e delle infrastrutture all'informatica.

La pretesa di sicurezza nel cyberspazio da parte degli Stati si scontra oggi con gli effetti derivanti da questo ritardo. Il cyberspazio è infatti un fenomeno originariamente

[1] V. Frosini, *La democrazia nel XXI secolo* (1997), Macerata, 2010, 40-41.

[2] C. Gallotti, *I sistemi di gestione per la sicurezza delle informazioni. La norma ISO/IEC 27001:2022 I controlli della ISO/IEC 27002:2022*, Raleigh, 2022.

[3] G. De Vergottini, *Sicurezza e i diritti fondamentali*, in L.E.R. Vega - L. Scaffardi - I. Spigno, *I diritti fondamentali nell'era della digital mass surveillance*, Napoli, 2021, 28.

[4] M.G. Losano, *Guerre ibride, omicidi mirati, droni: conflitti senza frontiere e senza diritto*, in L. Forni - T. Vettor (a cura di), *Sicurezza e libertà in tempi di terrorismo globale*, Torino, 2017, 22. Sugli effetti delle forme di connettività non solo dovute alle tecnologie ICT v. A.L. Baràbasi, *Linked. How everything is connected to everything else and what it means for business, science, and everyday life*, New York, 2014. Analogamente v. anche P. Khanna, *Connectography. Le mappe del futuro ordine mondiale*, Roma, 2016.

[5] Cfr. M. Dunn Cavelty, *Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities*, in *Science and Engineering Ethics,* 20, 2014, 704.

pubblico, nato con il progetto Arpanet[6], successivamente sviluppato e diffuso per mezzo dei privati, fuori dal controllo degli Stati[7]. Non è un caso se le prime definizioni di cybersicurezza (*cybersecurity*), sicurezza informatica (*computer security*) e sicurezza delle informazioni (*information security*) hanno trovato formulazione all'interno del c.d. "diritto dei privati"[8], nello specifico in normative tecniche di settore[9].

Tuttavia, se «[n]ell'ambiente digitale sembra non esserci più Stato, territorio, sovranità e neppure popolo, ma produzione principalmente privata del diritto»[10], non è dovuto solo perché il potere pubblico è arrivato "dopo", ma soprattutto perché l'oggetto della pretesa normativa, il cyberspazio, è un fenomeno globale privo di territorialità, che rappresenta un limite all'azione del potere pubblico che invece vanta «un'originaria necessità dei luoghi»[11].

In realtà, come rilevato dalla letteratura sul punto[12], il cyberspazio è una dimensione caratterizzata dalla convivenza di componenti immateriali, quali le connessioni, spettri elettromagnetici e protocolli di funzionamento, certamente non riconducibili ad alcuno spazio fisico; e componenti materiali, ossia le tecnologie fisiche, come cavi, *routers* e *switch*, localizzate entro i confini degli Stati, e generalmente prodotti da attori privati attivi nel mercato delle telecomunicazioni[13].

---

6 M. O'Mara, *The Code: Silicon Valley and the Remaking of America,* Londra, 2019.

7 G. Bombelli, *Dal moderno all'"ultramoderno"? Intorno al nesso diritto-tecnica-sicurezza*, in F. Pizzolato - P. Costa (a cura di), *Sicurezza e tecnologia*, Milano, 2017, 26.

8 Con la Raccomandazione ITU-T X.1205, del 18 aprile 2008, l'*International Telecommunication Union* (ITU) ha definito la cybersecurity come l'insieme degli strumenti politici, giuridici e tecnologici che hanno la finalità di proteggere il cyber environment e gli asset degli utenti dai cyber rischi, ed in particolare di garantire le tre priorità della riservatezza (*confidentiality*), integrità (*integrity*) e disponibilità (*availability*) degli stessi. Altra definizione è invece contenuta nella norma tecnica ISO/IEC 27032 ove la cybersicurezza è considerata come azione volta alla «preservation of confidentiality, integrity and availability of information in the Cyberspace».

9 Cfr. O.W. Cesarini, *Il diritto dei privati*, Milano, 1963. Sul punto v. anche S. Romano, *L'ordinamento giuridico* (1918), Macerata, 2018. In particolare, sulla normativa tecnica e il relativo processo di "normalizzazione" v. P. Aandreini - G. Caia - G. Elias - F.A. Roversi-Monaco, *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industriali*, Bologna, 1995; F. Salmoni, *Le norme tecniche*, Milano, 2001, 147; E. Chiti, *La normalizzazione*, in S. Cassese (a cura di), *Trattato di diritto amministrativo*, vol. IV, Milano, 2003, 4027 ss.; H. Schepel, *The Constitution Of Private Governance: Product Standards In The Regulation Of Integrating Markets*, Londra, 2005; A. Zei, *Tecnica e diritto tra pubblico e privato*, Milano, 2008; A. Moscarini, *Fonti dei privati e globalizzazione*, Roma, 2015; O. Kanevskaia, *Governance within standards development organizations: WHO owns the game?*, in *ITU Kaleidoscope Academic Conference 2017*, Nanjing, 2017, 1-8; A. Iannuzzi, *Il diritto capovolto. Regolazione a contenuto tecnico-scientifico e Costituzione*, Napoli, 2018. In particolare, sull'evoluzione storica della normazione tecnica nei settori della *computer* e *information security*, v. D. Russell - G.T. Gangemi, *Computer security basics*, Sebastopol, 1991, 23.

10 E. Cremona, *I poteri privati nell'era digitale. Libertà costituzionali, regolazione del mercato, tutela dei diritti*, Napoli, 2023, 45.

11 N. Irti, *Norma e luoghi*, Roma-Bari, 2006, 4.

12 Secondo lo studioso F. D. Kramer esistono 28 differenti definizioni del termine cyberspace. Cfr. Id., *Cyberpower and National Security: Policy Recommendations for a Strategic Framework*, in F.D. Kramer - S. Starr - L.K. Wentz, *Cyberpower and National Security*, Washington (D.C.), National Defense University Press,, 2009. Su tutti, per quel che qui interessa, il riferimento è alla definzione di Martin C. Libicki definisce il cyberspazio individuando tre livelli: fisico, sintattico e semantico M.C. Libicki, *Cyberdeterrence e cyberwar*, Santa Monica, 2009, 11 ss.

13 G. Suffia, *Geografia delle cyberwars*, Milano, 2018.

La morfologia appena tratteggiata rende evidente come in entrambo i piani l'azione pubblica per fini di sicurezza del cyberspazio richieda la necessaria cooperazione con i soggetti privati: relativamente al profilo immateriale, per tentare di regolare ciò che avviene "nel" cyberspazio, ossia le condotte e i comportamenti degli utenti, tra i quali possiamo individuare anche le minacce informatiche (*security*); per quanto riguarda il lato materiale, per tentare di garantire la sicurezza "del" cyberspazio attraverso la creazione e lo sviluppo di prodotti e soluzioni sul mercato che siano *(cyber)security by design*, in modo da garantire la progressiva sicurezza dell'ambiente digitale (*safety*)[14].
Lo scambio delle informazioni per il contrasto alle minacce informatiche è una pratica utile sia per i fini di *security* che di *safety* del cyberspazio. Pertanto, lo studio che si propone nei prossimi paragrafi sulle procedure di *cyber threat information sharing* rappresenta una privilegiata prospettiva di analisi dei rapporti tra il settore pubblico e privato coinvolti nei recenti cambiamenti che stanno interessando le politiche di cybersicurezza europea.

2. La circolazione delle informazioni negli assetti europei di sicurezza in senso tradizionale

Tra le attività funzionali al processo di integrazione europeo[15] ha assunto sempre maggiore importanza lo scambio di informazioni tra i diversi Stati membri, nonché tra quest'ultimi e le istituzioni europee, al fine di favorire il coordinamento delle attività amministrative dell'Unione in virtù dei principi di leale cooperazione, di cui all'art. 4, par. 3, del Trattato sull'Unione europea (TUE)[16], e di sussidiarietà, riconosciuto all'art. 5 TUE.
Si faccia riferimento al sistema di scambio delle informazioni per la sicurezza stradale, attuato con la direttiva (UE) 2015/413[17], o all'*Electronic Exchange of Social Security Information* (EESSI), il sistema informatico volto a supportare gli enti previdenziali degli Stati membri nello scambio rapido e sicuro di informazioni previdenziali[18], nonché al

[14] Sulla distinzione tra *safety* e *security* si rinvia a M. Durante, *Safety and Security in the Digital Age. Trust, Algorithms, Standards, and Risks*, in D. Berkich - M. d'Alfonso (a cura di), *On the Cognitive, Ethical, and Scientific Dimensions of Artificial Intelligence. Philosophical Studies Series*, 134, Berlin, 2019.

[15] G. de Búrca, J.H.H. Weiler, *The worlds of European constitutionalism*, New York, 2012.

[16] Il principio di leale cooperazione viene in rilievo soprattutto quando la realizzazione di un obiettivo dei Trattati richiede un esercizio coordinato delle competenze nazionali e di quelle dell'Unione. Tuttavia, oltre alla accezione bilaterale, tale principio risulta essere stato invocato anche nel rapporto tra Stati membri al fine di una più corretta applicazione del diritto UE v. *ex multis*, CGUE C-372/02, *Adanez Vega* (2002); C-105/94, *Celestini* (1994), nonché in relazione al rapporto tra istituzioni e al rispetto delle relative competenze v. CGUE C-65/93, *Parlamento c. Consiglio* (1993).

[17] Direttiva (UE) 2015/413 del Parlamento europeo e del Consiglio, dell'11 marzo 2015, intesa ad agevolare lo scambio transfrontaliero di informazioni sulle infrazioni in materia di sicurezza stradale Testo rilevante ai fini del SEE, che ha sostituito la direttiva 2011/82/UE annullata dalla Corte di giustizia dell'Unione europea con sentenza del 6 maggio 2014. L'obiettivo della direttiva è quello di attivare meccanismi cooperativi operativi tra gli Stati con l'intento di porre fine all'anonimato dei conducenti non residenti e perseguire le infrazioni al codice della strada commesse in uno Stato membro diverso da quello in cui il veicolo è stato immatricolato.

[18] Il sistema *Electronic Exchange of Social Security Information* (EESSI) è stato implementato nell'ambito

sistema di cooperazione amministrativa sicura tra le autorità fiscali nazionali istituito con la direttiva 2011/16/CE, recentemente modificata con direttiva di modifica (UE) 2021/514 (comunemente nota come «DAC7»).

Tuttavia, nello specifico caso delle politiche di sicurezza, lo scambio di informazioni tra le autorità di polizia e di *intelligence* degli Stati membri, e tra questi e le istituzioni europee, è un'attività che assume particolare rilevanza in quanto espressione della capacità di cooperazione degli Stati membri quale elemento fondante lo "Spazio di libertà, sicurezza e giustizia" dell'Unione europea[19].

Il tema è stato oggetto di recente attenzione da parte dell'Unione come è possibile apprendere dalla nuovo politica europea sulla sicurezza in generale, la *Security Union Strategy 2020-2025*, ove, a nostro modo di vedere, si è prospettato un inedito processo integrativo in questo settore, dato il riferimento al fatto che:

[a]nche se la responsabilità primaria della sicurezza incombe ai singoli Stati membri, negli ultimi anni è emerso chiaramente che la sicurezza di uno Stato membro è la sicurezza di tutti. L'UE può apportare una risposta multidisciplinare e integrata, fornendo agli operatori della sicurezza negli Stati membri gli strumenti e le informazioni di cui hanno bisogno[20].

Come noto, il sistema di sicurezza europeo si è sviluppato nel tempo sulla logica della cooperazione intergovernativa, non trovando mai una piena comunitarizzazione. L'esclusiva competenza degli Stati membri in materia di sicurezza, vedi la presenza nei Trattati delle clausole di tutela della "sicurezza nazionale" o dell'"ordine pubblico e della sicurezza" quali condizioni legittimanti il regime eccezionale statale rispetto all'applicazione del diritto europeo, è uno dei tratti caratterizzanti la politica europea in questo ambito[21].

Tuttavia, nonostante tali prerogative che accentrano il ruolo degli Stati membri, tale indirizzo non ha precluso la successiva elaborazione di politiche e la creazione di istituzioni comuni che hanno inevitabilmente richiesto l'impegno coordinato e coopera-

delle politiche di coordinamento della sicurezza sociale dell'Unione europea ed entrato pienamente in funzione nel giugno 2022. Per maggiori approfondimenti si rinvia alla pagina dell'EESSI.

[19] Cfr. Titolo V del TFUE rubricato per l'appunto «Spazio di libertà, sicurezza e giustizia».

[20] The EU Security Union Strategy 2020-2025, COM(2020) 605 final, del 24 luglio 2020.

[21] Vale la pena richiamare il contenuto dell'art. 4, par. 2, del Trattato sull'Unione europea (TUE) ove è previsto che «L'Unione rispetta l'uguaglianza degli Stati membri davanti ai trattati e la loro identità nazionale insita nella loro struttura fondamentale, politica e costituzionale, compreso il sistema delle autonomie locali e regionali. Rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro». Tale clausola di competenza statale permanente, aggiunta su esplicita richiesta del Regno Unito, deve essere inoltre letta in combinato disposto con l'art. 276 del Trattato sul funzionamento dell'Unione europea (TFUE), che esclude il controllo da parte della Corte di Giustizia sulla «validità o la proporzionalità di operazioni condotte dalla polizia o da altri servizi incaricati dell'applicazione della legge di uno Stato membro o l'esercizio delle responsabilità incombenti agli Stati membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna».

tivo sia tra gli Stati membri[22], sia tra questi e le competenti autorità europee[23], al fine di garantire l'esigenza di sicurezza in tutto lo spazio europeo[24].

In particolare, ripercorrendo brevemente l'evoluzione storica della cooperazione tra gli Stati europei nel settore di polizia, ci si accorge che è proprio nella raccolta, archiviazione, trattamento e scambio di informazioni che trova concreta realizzazione il processo integrativo in questo settore[25].

Proponiamo pertanto alcune tappe salienti di questo processo in modo da porter svolgere le successive considerazioni relativamente alla materia della cybersicurezza.

Nel 1975 i Ministri degli Interni e della Giustizia dei Paesi allora membri della CEE decisero di riunirsi nel forum che prende il nome di Gruppo TREVI con l'intento di costruire formule più intense di cooperazione tra le forze di polizia al di fuori della precedente esperienza internazionale dell'Interpol. Come si apprende dal "Programma d'azione relativo al rafforzamento della cooperazione in materia di polizia e di lotta al terrorismo o altre forme di criminalità organizzata" del 1990, inizialmente il principale ruolo del Gruppo era stato quello di garantire il controllo delle frontiere esterne anche grazie alla installazione di linee di comunicazione dirette.

Non è un caso se pochi giorni dopo l'adozione del citato Programma, venne sottoscritta la Convenzione di applicazione dell'Accordo di Schengen del 1985 con il quale si addiveniva alla istituzione di un sistema avanzato di cooperazione transfrontaliera e di scambio delle informazioni attraverso l'istituzione del «Sistema di informazione

[22] Per una rapida ricostruzione dei rapporti tra gli Stati diretti alla realizzazione di un sistema di sicurezza cooperativo v. M.M. Winkler, *Attività europea di intelligence, cooperazione di polizia e diritti umani*, in U. Draetta - N. Parisi - D. Rinoldi (a cura di), *Lo «spazio di libertà sicurezza e giustizia» dell'Unione europea. Principi fondamentali e tutela dei diritti*, Napoli, 2007, 293 ss; C. Mosca, *La sicurezza come diritto di libertà. Teoria generale delle politiche di sicurezza*, Torino, 2012, 319 ss; R. Ursi, *La sicurezza pubblica*, Bologna, 2022, 219 ss.

[23] Sul punto v. E. Chiti, *Le sfide della sicurezza e gli assetti nazionali ed europei delle forze di polizia*, in L. Forni - T. Vettor (a cura di), *Sicurezza e libertà in tempi di terrorismo globale,* cit.*,* 73, ove l'A. paragonando il processo integrativo europeo in materia di sicurezza, rispetto all'integrazio diretta alla realizzazione del mercato comune, scrive «[...] l'integrazione procede con particolare cautela, sconta la riluttanza dei governi nazioanli a rinunciare a un controllo sostanziale su queste politiche, si realizza attraverso strumenti più leggeri di quelli utilizzati per la costruzione del mercato interno e lo svolgimento delle politiche di regolazione economica e sociale».

[24] Oltre al concetto di ordine pubblico proprio di ogni identità nazionale che compone l'Unione, sulla scorta della giurisprudenza della Corte di giustizia è andato formandosi anche il concetto di ordine pubblico europeo. Sul punto v. G. Calesini, *Diritto europeo di polizia*, Roma, 2007, 211 ss.; D. Rinoldi, *L'ordine pubblico europeo*, Napoli, 2005; I.d., *Ordine pubblico europeo e spazio giuridico continentale*, in U. Draetta - N. Parisi - D. Rinoldi, *Lo «spazio di libertà sicurezza e giustizia» dell'Unione europea,* cit.*,* 61 ss.

[25] Nella elencazione dei principali atti legislativi sulla cooperazione di polizia disponibile presso il sito del Parlamento europeo (consultato il 2 dicembre 2023) risulta che gran parte di questi siano volti a istituire meccanismi di comunicazione per favorire lo scambio di informazioni tra i Paesi membri, v. la direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi; il regolamento (UE) 2018/1862 sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale; il regolamento (UE) 2019/818 che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione; la direttiva (UE) 2019/1153 che reca disposizioni per agevolare l'uso di informazioni finanziarie e di altro tipo a fini di prevenzione, accertamento, indagine o perseguimento di determinati reati; il regolamento (UE) 2021/784 relativo al contrasto della diffusione di contenuti terroristici online, applicabile dal 7 giugno 2022.

Schengen» (SIS)[26].

Tuttavia, fino a questo momento la cooperazione intergovernativa era avvenuta al di fuori dell'ordinamento europeo, ma le due esperienze citate rappresentarono uno modello per la successiva inclusione della cooperazione di polizia nel diritto comunitario così come organizzata nel Trattato di Maastricht del 1992[27]. In particolare, per ciò che qui interessa, nella dichiarazione n. 32 allegata al Trattato, all'art. K.1, n. 9, venivano specificate le modalità concrete di cooperazione ove si prevedeva che gli Stati si impegnano alla realizzazione di forme di collaborazione incentrate sullo «scambio di informazioni e di esperienze» nell'ambito dell'assistenza alle autorità nazionali incaricate delle azioni penali in materia penale e della sicurezza.

Principio che ha poi trovato concreta applicazione con due decisioni quadro che hanno reso l'*information sharing* vincolante per gli Stati membri: la decisione quadro 2008/960/Gai, che impone, all'interno di un quadro giuridico definito, lo scambio rapido ed efficace di informazioni tra le autorità deputate alla sicurezza, e la decisione-quadro 2008/615/Gai che dispone l'accesso reciproco alle informazioni anche attraverso l'interoperabilità di basi di dati nazionali.

Sempre all'interno del Trattato di Maastricht, all'art. K.1, n. 9, si faceva riferimento al primo Ufficio di polizia europeo, l'Europol, che venne poi istituito nel 1993 e divenuto pienamente operativo nel 1999. Anche in questo caso, come è possibile dedurre dall'art. 88 del Trattato sul funzionamento dell'Unione europea (TFUE), tra i compiti dell'Ufficio troviamo: «a) la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle informazioni trasmesse, in particolare dalle autorità degli Stati membri o di paesi o organismi terzi; b) il coordinamento, l'organizzazione e lo svolgimento di indagini e di azioni operative, condotte congiuntamente con le autorità competenti degli Stati membri o nel quadro di squadre investigative comuni, eventualmente in collegamento con Eurojust».

Dal breve quadro descritto si evince come all'iniziale approccio intergovernativo, basato sullo scambio "diretto" o a "rete" delle informazioni tra le autorità dei singoli Stati membri, si sia progressivamente affiancato il modello di cooperazione informativa accentrato, imperniato su banche dati comuni europee o comunque sistemi informativi gestiti da organismi sovranazionali, che trova oggi riconoscimento all'art. 87, par. 2, lett. a) del TFUE[28].

In particolare, secondo Alcuni, il grande cambiamento che contraddistingue il nuovo approccio da quello precedente, non starebbe tanto negli strumenti e nelle modalità

[26] Dalla sua istituzione il sistema SIS è stato oggetto di diversi interventi di aggiornamento, di cui l'ultimo è avvenuto con il regolamento (UE) 2018/1862. Tuttavia, la sua architettura tecnica è rimasta invariata nel tempo: il SIS risulta composto da una struttura nazionale (N-SIS) presente in ciascuno Stato membro, e duna una unità centrale (C-SIS) con sede a Strasburgo, la quale si occupa di gestire ed elaborare i dati inviati alle banche dati nazionali. Il coordinamento tra i diversi Paesi è favorito dalla presenza negli uffici nazionali del sistema informativo di un ulteriore ufficio SIRENE (*Supplementary Information Request at the National Entry*) che svolge le funzioni di sala operativa nell'intero arco della giornata allo scopo di consentire alle autorità di polizia e giudiziaria dei vari Paesi Schengen di acquisire ulteriori informazioni non disponibili in base al sistema SIS.

[27] Cfr. R. Ursi, *La sicurezza pubblica*, cit., 227.

[28] F. Peroni - M. Gialuz (a cura di), *Cooperazione informativa e giustizia penale nell'Unione europea*, Trieste, 2009, 10.

impiegate, quanto piuttosto nel mutato «contesto» nel quale si articola questo tipo di cooperazione ispirata al «principio di disponibilità delle informazioni» e dal quale discende a livello pratico «l'accesso reciproco e l'interoperabilità delle banche dati-nazionali, nonché l'accesso diretto (*on-line*) alle banche-dati dell'Unione da parte di autorità nazionali ed europee»[29].

Da ultimo, alla luce delle discrepanze tra la decisione quadro 2006/960/GAI e l'ambito di applicazione della convenzione che attua l'Accordo di Schengen, il legislatore europeo ha recentemente introdotto la direttiva (EU) 2023/977, relativa allo scambio di informazioni tra le autorità di contrasto degli Stati membri e che abroga la suddetta decisione quadro[30].

Brevemente, è possibile notare come tale iniziativa sia volta da una parte, a potenziare i punti di contatto unici stabiliti presso gli Stati membri, dall'altra a favorire la convergenza verso l'utilizzo da parte di tutte le autorità di contrasto della rete *Secure Information Exchange Network Application* (SIENA), gestita e sviluppata da Europol conformemente al regolamento (UE) 2016/794, al fine di «porre rimedio al problema della proliferazione dei canali di comunicazione utilizzati per la trasmissione di informazioni sull'attività di contrasto tra gli Stati membri, poiché [tale pratica] ostacola lo scambio adeguato e rapido di tali informazioni e aumenta i rischi per la sicurezza dei dati personali»[31].

Fanno tuttavia eccezione i casi di cui all'art. 13, c. 2, della direttiva ove è previsto che gli Stati membri possono consentire al loro punto di contatto unico o alle loro autorità di contrasto competenti di non avvalersi di SIENA nei casi in cui:

a) lo scambio di informazioni richiede il coinvolgimento di paesi terzi od organizzazioni internazionali o vi sono ragioni obiettive per ritenere che tale coinvolgimento sarà necessario in una fase successiva, anche attraverso il canale di comunicazione Interpol;
b) l'urgenza della richiesta di informazioni richiede l'uso temporaneo di un altro canale di comunicazione;
c) un incidente tecnico od operativo imprevisto impedisce al loro punto di contatto unico o alle loro autorità di contrasto competenti di utilizzare SIENA per lo scambio di informazioni.

Merita inoltre osservare che l'attenzione posta dall'Unione verso la circolazione delle informazioni per la cooperazione di polizia - ulteriormente amplificata a seguito degli

[29] N. Parisi, *Cooperazione fra le autorità nazionali ed europee incaricate "dell'applicazione delle legge" nello spazio di libertà, sicurezza e giustizia. I principi fondanti la circolazione internazionale delle informazioni*, in R. Del Coco - E. Pistoria (a cura di), *Stranieri e giustizia penale. Problemi di perseguibilità e di garanzie nella normativa nazionale ed europea*, Bari, 2014, 122-123.

[30] Direttiva (UE) 2023/977, relativa allo scambio di informazioni tra le autorità di contrasto degli Stati membri e che abroga la decisione quadro 2006/960/GAI del Consiglio. In particolare, sui motivi che hanno portato a tale intervento legislativo a livello europeo si faccia riferimento ai considerando 7 e 8 della direttiva. Inoltre al considerando 13 è ribadito che «[p]oiché la presente direttiva non si applica al trattamento di informazioni nell'ambito di un'attività che non rientra nel campo di applicazione del diritto dell'Unione, le attività concernenti la sicurezza nazionale non rientrano nel campo di applicazione della presente direttiva».

[31] Cfr. considerando 26, direttiva (UE) 2023/977.

attacchi terroristici di inizio millennio[32] - non si è limitata solo alla promozione degli scambi informativi e alla creazione di reti e banche dati centralizzate, ma si è diretta anche verso il profilo, di non secondaria rilevanza, della protezione di dette infrastrutture informatiche preposte alla circolazione del materiale informativo[33].

3. *A problem shared is a problem halved*. Le origini della *cyber threat information sharing*

L'esigenza di una cooperazione e di un coordinamento delle attività di contrasto alle minacce informatiche su larga scala si è avvertita per la prima volta negli Stati Uniti il 2 novembre 1988, in occasione di uno dei primi attacchi informatici a vasto impatto: il "Morris Worm", creato da Robert Tappan Morris, studente della Cornell University con lo scopo di dimostrare le inadeguatezze delle misure di sicurezza delle reti informatiche[34].

Sebbene il *malware* venne creato da Morris a soli fini di studio, l'esperimento uscì fuori dal controllo del suo creatore riuscendo a contagiare circa il 10% dei computer del mondo[35].

La portata dell'incidente richiese un'intensa collaborazione internazionale che riscontrò pesanti limitazioni a causa della mancata implementazione di meccanismi di condivisione delle informazioni sulle minacce informatiche[36].

A pochi giorni dall'evento venne istituito negli Stati Uniti il primo Gruppo di intervento operativo in caso di attacco informatico - il *Computer Emergency Response Team*

---

[32] E. Chiti, *Le sfide della sicurezza e* …, in L. Forni - T. Vettor (a cura di), *Sicurezza e libertà in tempi di terrorismo globale,* cit., 77 ss. L'A. sottolinea come a seguito degli eventi dell'11 settembre vi sia stata una apertura globale delle amministrazioni di polizia e militari dell'Unione europea.

[33] Si faccia riferimento a: la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/Gai del Consiglio, nota come direttiva sulla criminalità informatica; la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, nota come direttiva NIS, oggi abrogata e sostituita dalla direttiva (UE) 2022/2555, c.d. NIS II; regolamento (UE) 2018/1726 relativo all'Agenzia dell'Unione europea - eu-LISA - per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia. Nonché, infine, la stessa rete SIENA che assicura la sicurezza delle trasmissioni.

[34] Le motivazioni che portarono il giovane studente a sviluppare il primo prototipo di "worm" possono essere ricostruire dalla lettura della sentenza della Corte d'appello US, v. United States Court of Appeals, No. 774, Docket 90-1336, Argued Dec. 4, 1990. Decided March 7, 1991, *United States of America, Appellee, v. Robert Tappan Morris, Defendant-Appellant*. In particolare, circa la il potere pervasivo del programma sviluppato da Morris, dalla ricostruzione dei fatti nella pronuncia si apprende che: «[t]he tactic he selected was release of a worm into network computers. Morris designed the program to spread across a national network of computers after being inserted at one computer location connected to the network. Morris released the worm into Internet, which is a group of national networks that connect university, governmental, and military computers around the country. The network permits communication and transfer of information between computers on the network».

[35] Dal sito della *Federal Bureau of Investigation* (FBI) statunitense, si apprende che «[w]ithin 24 hours, an estimated 6,000 of the approximately 60,000 computers that were then connected to the Internet had been hit. Computer worms, unlike viruses, do not need a software host but can exist and propagate on their own».

[36] A. Contaldo - F. Peluso, *Cybersecurity. La nuova disciplina italiana ed europea alla luce della direttiva NIS*, Pisa, 2018, 70 ss.

(CERT) - con l'obiettivo di diffondere le notifiche sugli incidenti e coordinare la comunicazione durante l'emergenza. Per quanto riguarda la natura di questo primo "centro di soccorso informatico", si precisa che si trattava di una iniziativa nata all'interno delle accademie e dei centri di ricerca, più nello specifico dall'agenzia statunitense DARPA (*Defence Advanced Research Projects Agency*), la quale istituì tale Gruppo presso la Carneige Mellon University di Pittsburgh, in Pennsylvania, che ne detiene ancora oggi la proprietà del marchio[37].

L'insegnamento tratto dalla drammatica esperienza evidenziò così come nel contesto della sicurezza informatica non sia solo necessario un approccio di tipo reattivo (*ex post*) legato all'emergenza in corso, ma anche un approccio di sicurezza preventivo (*ex ante*), attraverso il monitoraggio e l'analisi costante delle risorse informatiche in uso, al fine di rilevare intrusioni e anomalie in tempo reale (c.d. *cyber situational awareness*)[38].

Nel 1997, dopo i primi attacchi terroristici al World Trade Center (1993) e a Oklahoma City (1995), il Presidente Clinton nominò la Commissione per la protezione delle infrastrutture critiche al fine di individuare le possibilità di cooperazione tra il settore pubblico e quello privato per proteggere adeguatamente le infrastrutture critiche degli Stati Uniti. La Commissione si espresse con un rapporto finale, il "rapporto Marsh", che tra le principali raccomandazioni prevedeva l'istituzione dei *Information Sharing and Analysis Centres* (ISACs): partenariati pubblico-privati senza scopo di lucro, organizzati con lo scopo di raccogliere informazioni sulle minacce informatiche provenienti dai CERTs e SOCs (c.d. informazioni di cybersicurezza) - in un primo momento solo quelle veicolate ai danni delle infrastrutture critiche - al fine di condividerle all'interno di una rete di soggetti fidati che partecipano allo scambio informativo su base volontaria[39].

Nel 2015, sempre con lo scopo di promuovere e facilitare la condivisione delle informazioni di cybersicurezza, il Presidente Obama per mezzo di un *executive order* istituì le *Information Sharing and Analysis Organizations* (ISAOs): organizzazioni create per rac-

[37] I. Skierka - R. Morgus - M. Hohmann - T. Maurer, *CSIRT Basics for Policy-Makers. The History, Types & Culture of Computer Security Incident Response Teams*, New America and the Global Public Policy Institute (GPPi), maggio 2015, 9 ss. CERT, acronimo di *Computer Emergency Response Team*, è una sigla spesso utilizzata al posto di CSIRT (*Computer Security Incident Response Team*). In entrambo i casi si tratta di una denominazione volta a descrivere un gruppo di intervento incaricato di monitorare gli incidenti a livello nazionale; emettere preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; intervenire in caso di incidente; analizzare dinamicamente i rischi e gli incidenti; svolgere attività di sensibilizzazione situazionale. La distinzione tra i due acronimi è dovuta ad una questione di mero diritto dei marchi, in quanto il CERT nacque su iniziativa dell'agenzia statunitense DARPA (*Defence Advanced Research Projects Agency*), la quale istituì tale Gruppo presso la *Carneige Mellon University* di Pittsburgh in Pennsylvania che ne detiene ancora oggi la proprietà del marchio, diversamente dal nominativo CSIRT che invece è di libero utilizzo. Sul punto v. A. Contaldo - F. Peluso, *Cybersecurity,* cit.; L. Salandri - A. Contaldo, *La nuova disciplina giuridica c.d. "orizzontale" della cybersicurezza per le infrastrutture in un'ottica di sviluppo dei sistemi informativi*, in *Riv. amm.*, 2016, 567-595.

[38] Termine migrato dal linguaggio militare. Nel particolare contesto della sicurezza informatica, secondo l'Agenzia governativa statunitense che si occupa della gestione delle tecnologie, il *National Institute of Standards and Technology* (NIST), per "*cyber situational awareness"* deve intendersi «[p]erception of elements in the system and/or environment and a comprehension of their meaning, which could include a projection of the future status of perceived elements and the uncertainty associated with that status». Sul punto v. S. Jajodia - P. Liu - V. Swarup - C. Wang, *Cyber situational awareness*, New York, 2009.

[39] Sulle origini storiche delle ISACs v. ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models,* 2018.

cogliere, analizzare e diffondere informazioni sulle minacce informatiche non direttamente legate ai settori delle infrastrutture critiche, estendendo così il meccanismo di condivisione anche alle piccole e medie imprese operative in diversi settori (vi rientrano ad esempio studi legali, contabili e di consulenza che supportano clienti intersettoriali, ecc.)[40].

Lo stesso anno venne anche emanato il *Cybersecurity Information Sharing Act* (c.d. CISA bill), la legge federale con il quale gli Stati Uniti hanno inteso regolare e promuovere lo scambio di informazioni relative alle minacce informatiche tra il settore privato e le istituzioni governative[41].

I benefici riscontrati dall'introduzione di queste procedure di scambio evolute nell'esperienza statunitense hanno ben presto portato all'ingresso di altri Paesi in tali ecosistemi informativi, fino al suo recepimento all'interno degli accordi sovranazionali.

Difatti, il meccanismo di *cyber information sharing* costituisce ormai un principio fondamentale nei rapporti internazionali[42], quale corollario del concetto di sicurezza cooperativa[43].

Sul punto, vale la pena ricordare che nelle linee guida in materia di sicurezza dei sistemi e delle reti d'informazione elaborate dall'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) nel 2002[44], tra i nove principi prodromici all'instaurazione di una cultura della sicurezza, trova spazio anche il principio di "risposta" secondo il quale «[l]e parti interessate devono operare tempestivamente e in uno spirito di cooperazione per prevenire, rilevare e rispondere agli incidenti di sicurezza». Ed in particolare, queste sono chiamate a «scambiare, in maniera adeguata, le informazioni di cui dispongono sulle minacce e vulnerabilità e devono creare procedure per una rapida ed efficace cooperazione volta a prevenire e a rilevare gli incidenti di sicurezza e a rispondervi» tale che «[c]iò potrebbe comportare scambi d'informazioni e una cooperazione transfrontaliera, ove autorizzato».

Principio che ha ovviamente trovato ospitalità anche nelle politiche di cybersicurezza dell'Unione europea declinato sotto il profilo sia organizzativo, attraverso l'articolazione di una rete amministrativa *ad hoc*, sia normativo, attraverso l'imposizione di obblighi relativi alla gestione della sicurezza informatica che ricomprendono, tra i diversi, la notifica degli incidenti di sicurezza alle competenti autorità.

---

[40] Come emerge dal contenuto dell'*executive order* istitutivo delle *Information Sharing and Analysis Organizations* (ISAOs), si tratta di organizzazioni operative in diversi settori, quali «private companies, nonprofit organizations, executive departments and agencies (agencies), and other entities», istituite con il fine di condividere le informazioni relative ai rischi e agli incidenti di sicurezza informatica e collaborare per rispondere in maniera più vicina possibile e in tempo reale. Il funzionamento a livello tecnico di tali organizzazioni intersettoriali è supportato dalla *ISAO Standard organization* definita dall'*executive order* come «non-governmental organisation [...] to improve the US's cybersecurity posture by identifying standards and guidelines for robust and effective information sharing and analysis related to cybersecurity risks, incidents, and best practices».

[41] Cybersecurity Information Sharing Act of 2014, S. 2588.

[42] T. Hitchens - N. Goren, *International Cybersecurity Information Sharing Agreements*, in *Center for International & Security Studies*, U. Maryland, 2017.

[43] R. Cohen, *Cooperative Security: From individual Security to International Stability*, in *Marshall Center Papers*, 3, aprile 2001.

[44] OCSE, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, 2002.

4. La cooperazione europea di *cyber information sharing* tra soggetti pubblici e privati

La *cyber (trheat) information sharing* è il termine con il quale generalmente si indicano le attività consistenti nello «scambio di una varietà di informazioni relative alla sicurezza delle reti e delle informazioni, quali rischi, vulnerabilità, minacce e problemi di sicurezza interna, nonché buone prassi»[45].
Nel paragrafo precedente è stato evidenziato come questa pratica sia sorta da una obiettiva necessità di contrastare le minacce informatiche attraverso le azioni coordinate di Gruppi di intervento dislocati nel mondo e le infrastrutture critiche. In particolare, si è posto in luce come i primi ecosistemi di scambio informativo delle minacce informatiche siano sorti sulla scorta di iniziative autonome da parte degli stessi soggetti interessati (perlopiù infrastrutture critiche di natura privata). Nei successivi sottoparagrafi saranno analizzate l'architettura europea di cybersicurezza (par. 4.1), avendo modo di riflettere anche sul ruolo dei soggetti privati, particolarmente presenti in questo settore (par. 4.2), e il relativo rapporto tra questi e il settore pubblico, generalmente espresso attraverso l'istituzione di partenariati (par. 4.3).

4.1. L'organizzazione amministrativa delle istituzioni di cybersicurezza europea

Analogamente alle politiche europee di sicurezza brevemente evidenziate, anche il profilo organizzativo delle istituzioni di cybersicurezza europea si basa su una rete di amministrazioni aventi perlopiù funzioni organizzative e di coordinamento delle competenti autorità nazionali. Pertanto, anche in questo ambito l'azione europea non influisce sulle competenze e i poteri degli Stati membri ai quali resta sempre riservato l'esercizio dei poteri autoritativi di sicurezza.
L'articolazione amministrativa europea di cybersicurezza si è sviluppata nel tempo attraverso l'istituzione di diversi organismi di coordinamento decentrati, organizzati perlopiù sul modello delle agenzie dotate di personalità giuridica[46], che trovano nello scambio informativo l'elemento essenziale per lo svolgimento delle loro funzioni.
Dal 2004 è presente l'Agenzia Europea per la Cybersicurezza (ENISA), istituita con l'obiettivo di creare «un clima di fiducia grazie alla sua indipendenza, alla qualità della consulenza fornita e delle informazioni diffuse, alla trasparenza delle sue procedure e metodi di funzionamento e alla diligenza nello svolgere i compiti ad essa assegnati» ed inoltre «[p]oiché le reti elettroniche sono in larga misura private, l'Agenzia dovrebbe avvalersi delle informazioni del settore privato e cooperare con esso» (cons. 11). L'Agenzia venne inizialmente dotata di un mandato temporaneo, via via esteso con i regolamenti (UE) 1007/2008 e 580/2011. Tuttavia, solo con il regolamento (UE) 2019/881, il c.d. *Cybersecurity Act*, è stato conferito all'ENISA un mandato permanente,

[45] N. Robinson - E. Disley, *Incentives and Challenges on Information Sharing, Retrieved*, 2010, 9.

[46] Sulle agenzie amministrative europee v. E. Chiti, *Le agenzie europee. Unità e decentramento nelle amministrazioni europee*, Padova, 2002.

rafforzandone il ruolo, i compiti, le responsabilità, e predisponendo maggiori risorse al fine di contribuire al supporto degli Stati membri nel prevenire e rispondere efficacemente agli attacchi informatici.

In particolare, l'Agenzia ricopre la funzione di segretariato della rete composta dai gruppi di intervento nazionali (c.d. rete CSIRT), nonché sostiene la cooperazione operativa tra questi e il gruppo di intervento dell'Unione, il CERT-UE, che ha la funzione di rispondere in modo efficiente alle minacce informatiche dirette contro le reti e i sistemi istituzionali dell'Unione europea.

I CSIRT, *Computer Security Incident Response Teams* sono unità di intervento decentrate, istituite presso i singoli Stati membri (eventualmente anche all'interno di autorità competenti[47]), con l'incarico di svolgere attività reattive, come l'intervento in caso di incidente informatico, ed anche proattive, come il monitoraggio degli incidenti a livello nazionale, l'emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti e la relativa analisi di tali rischi e incidenti.

In entrambo i casi, questi soggetti rappresentano i nodi nevralgici dei processi di *cyber information sharing*. Difatti da una parte ricevono le informazioni sulle minacce informatiche in quanto ricettori delle notifiche degli incidenti di cybersicurezza da parte dei soggetti verso cui trova applicazione la disciplina NIS; dall'altra, partecipano alla più ampia cooperazione informativa a livello europeo per mezzo della rete che riunisce i rappresentanti dei gruppi di intervento di tutti gli Stati membri e la squadra CERT-UE, sotto il segretariato dell'ENISA (c.d. rete di CSIRT)[48].

---

[47] È ad esempio il caso del CSIRT Italia trasferito presso l'Agenzia Nazionale per la Cybersicurezza (ACN) con il decreto-legge n. 82 del 2022.

[48] In particolare, l'art. 15 Dir. (UE) 2022/2555, prevede che la rete svolge i seguenti compiti: «a) scambiare informazioni per quanto riguarda le capacità dei CSIRT; b) agevolare la condivisione, il trasferimento e lo scambio di tecnologia e delle misure, delle politiche, degli strumenti, dei processi, delle migliori pratiche e dei quadri pertinenti fra i CSIRT; c) scambiare informazioni pertinenti per quanto riguarda gli incidenti, i quasi incidenti, le minacce informatiche, i rischi e le vulnerabilità; d) scambiare informazioni in merito alle pubblicazioni e alle raccomandazioni in materia di cibersicurezza; e) garantire l'interoperabilità per quanto riguarda le specifiche e i protocolli per lo scambio di informazioni; f) su richiesta di un membro della rete di CSIRT potenzialmente interessato da un incidente, scambiare e discutere informazioni relative a tale incidente e alle minacce informatiche, ai rischi e alle vulnerabilità associati; g) su richiesta di un membro della rete di CSIRT, discutere e, ove possibile, attuare una risposta coordinata a un incidente identificato nella giurisdizione di tale Stato membro; h) fornire assistenza agli Stati membri nel far fronte a incidenti transfrontalieri a norma della presente direttiva; i) cooperare e scambiare migliori pratiche con i CSIRT designati in qualità di coordinatori di cui all'articolo 12, paragrafo 1, nonché fornire loro assistenza per quanto riguarda la gestione della divulgazione coordinata di vulnerabilità che potrebbero avere un impatto significativo su soggetti in più di uno Stato membro; j) discutere e individuare ulteriori forme di cooperazione operativa, anche in relazione a: i) categorie di minacce informatiche e incidenti; ii) preallarmi; iii) assistenza reciproca; iv) principi e modalità di coordinamento in risposta a rischi e incidenti transfrontalieri; v) contributi al piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala di cui all'articolo 9, paragrafo 4, su richiesta di uno Stato membro; k) informare il gruppo di cooperazione sulle proprie attività e sulle ulteriori forme di cooperazione operativa discusse a norma della lettera j) e, se necessario, chiedere orientamenti in merito; l) fare il punto sui risultati delle esercitazioni di cibersicurezza, comprese quelle organizzate dall'ENISA; m) su richiesta di un singolo CSIRT, discutere le capacità e lo stato di preparazione di tale CSIRT; n) cooperare e scambiare informazioni con i centri operativi di sicurezza regionali e a livello dell'UE al fine di migliorare la consapevolezza situazionale comune sugli incidenti e le minacce informatiche in tutta l'Unione; o) se del caso, discutere le relazioni sulle revisioni tra pari di cui all'articolo 19, paragrafo 9; p) fornire orientamenti volti ad agevolare la convergenza delle pratiche operative in relazione all'applicazione delle disposizioni del presente articolo in materia di cooperazione operativa».

Tale attività trova inoltre il supporto del "Gruppo di cooperazione", organismo composto dai rappresentanti degli Stati membri, dalla Commissione e dall'ENISA, la cui funzione è quella di agevolare la cooperazione strategica e lo scambio di informazioni tra gli Stati membri fornendo orientamenti e consulenza alle istituzioni europee nonché effettuando valutazioni coordinate dei rischi di cybersicurezza ed elaborando relazioni utili ai fini del riesame della disciplina NIS da parte della Commissione[49].

Nonostante gli sforzi diretti a istituire un quadro amministrativo e regolamentare in materia di scambio informativo, nella Strategia europea di cybersicurezza presentata nel dicembre 2020[50], si apprende che «[t]he EU lacks collective situational awareness of cyber threats». Secondo la Commissione il problema è dovuto, da una parte allo scarso coinvolgimento del settore privato nella cooperazione informativa, dall'altra alla resistenza degli Stati membri a condividere le informazioni in maniera sistematica e completa, rendendo così estremamente difficoltoso il funzionamento dei meccanismi di *cyber information sharing* tra gli Stati membri e le istituzioni dell'UE in caso di crisi o incidenti informatici transfrontalieri su larga scala[51].

La stessa Presidente della Commissione europea Ursula von der Leyen, nel "Discorso sullo stato dell'Unione 2021", ha ribadito la necessità di «gettare le basi per un processo decisionale collettivo» basato la scambio di «conoscenze provenienti da tutti i servizi e da tutte le fonti, dallo spazio ai formatori del personale di polizia, dall'*open source* alle agenzie di sviluppo».

È sulla scorta di tali considerazioni che la disciplina di cybersicurezza europea è stata recentemente aggiornata e potenziata proprio negli aspetti che interessano la cooperazione informativa.

A partire dal gennaio 2023 è entrata in vigore la direttiva (UE) 2022/2555 (Direttiva NIS II)[52], che ha abrogato la previgente direttiva (UE) 2016/1148 (Direttiva NIS I). Tra le diverse modifiche, la nuova disciplina ha istituito la "Rete europea delle organizzazioni di collegamento per le crisi informatiche" (*EU Cyber Crisis Liaison Organisation Network* - CyCLONe) con lo scopo di garantire una più stretta collaborazione e azione coordinata nei casi di incidenti di cyberisucrezza su larga scala. A tal fine la Rete sostiene la gestione coordinata a livello operativo degli incidenti e delle crisi di cybersicurezza su vasta scala e garantisce il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione[53].

Da giugno 2023 è inoltre operativo il *Joint Cyber Unit*: il cuore della nuova cooperazione operativa europea in materia di cybersicurezza. Si tratta di una piattaforma di raccordo ove i partecipanti, provenienti dalla comunità civile, diplomatica, dalle forze dell'ordine e dalla difesa, possono avvalersi del supporto e delle competenze reciproche, soprattutto nel caso in cui le varie comunità debbano lavorare a stretto contatto, in occasione

[49] Cfr. art. 14 Dir. (UE) 2022/2555.

[50] JOIN(2020) 18 final, *Comunicazione congiunta al parlamento europeo e al consiglio. La strategia dell'UE in materia di cibersicurezza per il decennio digitale*.

[51] *Ibidem*.

[52] Direttiva (UE) 2022/2555, *relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, che abroga la direttiva 2016/1148*.

[53] Cfr. art. 16 direttiva (UE) 2022/2555.

di incidenti su larga scala o crisi[54].

L'Unità non costituisce un organismo supplementare indipendente, ma è frutto della messa a disposizione di uno spazio comune fisico, situato a Bruxelles, e uno spazio virtuale composto da strumenti utili per una condivisione sicura e rapida delle informazioni.

Tra le amministrazioni europee che vi partecipano troviamo: relativamente alle politiche di polizia, lo *European Cybercrime Centre* (EC3), unità specializzata già istituita presso l'EUROPOL con funzioni di raccordo con le forze di polizia degli Stati europei[55]; sul piano diplomatico, lo *European External Action Service* (EEAS)[56] e il forum *Horizontal Working Party on Cyber Issues*[57]; infine, per quanto riguarda il settore difesa, il *framework Permanent Structured Cooperation* (PESCO)[58] e la *European Defence Agency* (EDA)[59].

Da ultimo, il 18 aprile 2023, la Commissione ha avanzato una proposta di regolamento che stabilisce una serie di misure per rafforzare la solidarietà e le capacità di individuare, prepararsi e rispondere alle minacce e agli incidenti di sicurezza informatica nel contesto europeo (c.d. *EU Cyber Solidarity Act*)[60].

Con questo strumento l'Unione intende incrementare la consapevolezza situazionale, la condivisione delle informazioni, nonché migliorare la preparazione e la risposta agli incidenti informatici a livello comune attraverso l'istituzione di tre nuovi meccanismi di raccordo: lo *European Cybersecurity Shield*, il *Cyber Emergency Mechanism* e il *Cybersecurity Incident Review Mechanism*.

Lo *European Cybersecurity Shield* avrà il compito di migliorare il rilevamento, l'analisi e la

---

[54] C(2021) 4520 *final*, *Sulla creazione di un'unità cibernetica congiunta*, 2021. A ben vedere il *Joint Cyber Unit* prende avvio dal precedente progetto "*Blueprint*" del 2017 istituito con la Raccomandazione (EU) 2017/1584 sulla risposta coordinata a incidenti e crisi di cybersicurezza su larga scala.

[55] Il Centro europeo per la criminalità informatica (*European Cybercrime Centre* - EC3) è un organismo istituito da Europol nel 2013, con sede all'Aia. La sua attività è quella di coordinare le attività transfrontaliere di contrasto alla criminalità informatica e funge da centro di competenza tecnica in materia. Per ulteriori si rinvia al sito ufficiale dell'EC3.

[56] Lo *European External Action Service* (EEAS), o anche Servizio europeo per l'azione esterna (SEAE), è il servizio diplomatico dell'UE, istituito per rendere più coerente ed efficace la politica estera dell'UE e rafforzare così l'influenza dell'Europa sulla scena mondiale. Per ulteriori si rinvia al sito ufficiale dell'EEAS.

[57] Il forum *Horizontal Working Party on Cyber Issues* è stato istituito nel 2016 ed è responsabile del coordinamento dei lavori del Consiglio sulle questioni informatiche, principalmente la politica informatica e le attività legislative. Il Gruppo collabora strettamente con la Commissione europea ed altre istituzioni quali il Servizio europeo per l'azione esterna, l'Europol, l'Eurojust, l'Agenzia europea dei diritti fondamentali (FRA), l'Agenzia europea per la difesa (EDA) ed infine l'Agenzia dell'Unione europea per la cybersicurezza (ENISA).

[58] Il *Permanent Structured Cooperation* (PESCO) nel settore della politica di sicurezza e di difesa è stato istituito l'11 dicembre 2017 con decisione 2017/2315 del Consiglio. Tale strumento offre un quadro giuridico per pianificare, sviluppare e investire congiuntamente in progetti di capacità condivisi e migliorare la prontezza operativa e il contributo delle forze armate.

[59] L'Agenzia europea per la difesa è stata istituita con un'azione comune del Consiglio dei ministri del 12 luglio 2004, «per sostenere gli Stati membri e il Consiglio nel loro sforzo di migliorare le capacità di difesa europee nel campo della gestione delle crisi e per sostenere la politica europea di sicurezza e di difesa nella sua forma attuale e in quella futura».

[60] COM(2023) 209 final, *Proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents*.

risposta alle minacce informatiche su larga scala attraverso l'istituzione di una nuova rete di piattaforme di *Security Operation Centres* SOC multinazionali. La prima fase del progetto è stata già avviata nel novembre 2022, e sono stati selezionati tre consorzi di centri operativi di sicurezza (SOC) transfrontalieri, che riuniscono enti pubblici di 17 Stati membri e dell'Islanda, nell'ambito del programma Europa digitale (si rinvia al par. 5.1 a proposito dei SOC).
Il *Cyber Emergency Mechanism* avrà il compito di migliorare la preparazione e la risposta agli incidenti di cybersicurezza attraverso: la valutazione dei meccanismi di risposta implementati presso i settori particolarmente critici selezionati al termine di una generale valutazione del rischio a livello europeo; la creazione dell'*EU Cybersecurity Reserve*, ossia servizi di risposta agli incidenti erogati da fornitori di servizi privati («trusted providers»), attivati su richiesta degli Stati membri o di istituzioni dell'Unione, per aiutarli ad affrontare problemi significativi o incidenti di sicurezza informatica su larga scala: ed infine, attraverso la promozione dell'assistenza reciproca tra gli Stati membri ove uno di questi sia stato interessato da un incidente di cybersicurezza[61].

4.2 Brevi cenni sulla privatizzazione della (cyber) sicurezza

Il paradigma weberiano che vede nello Stato l'unico detentore del legittimo uso della forza non è più coerente con l'attuale situazione. Il processo di globalizzazione ha portato ad una ri-articolazione dello Stato che ha di fatto trasferito alcune sue funzioni ad attori privati[62], tra cui, col tempo, anche quella della sicurezza[63]. Secondo Alcuni questo processo non ha visto una piena affermazione dei privati in questo settore, quanto piuttosto l'instaurazione di forme di *governance* ibrida, caratterizzate da una stretta collaborazione (*rectius* cooperazione) con il potere pubblico, il cui risultato ha portato alle cc.dd. *global security assemblages*, ossia la formazione di nuove strutture e pratiche di sicurezza che sono allo stesso tempo pubbliche e private, oltre che globali e locali[64].
Preme precisare che gran parte della letteratura in tema di "privatizzazione della sicurezza" è perlopiù concentrata sulle c.d. *Private Military or Security Companies services* - PM-

[61] Sul concetto di "assistenza reciproca", l'art. 10, lett. c) dell'*EU Cyber Solidarity Act* si limita a fare rinvio alla medesima nozione disposta nella Direttiva NIS II. Considerati i contrasti interpretativi della dottrina sulla qualificazione dell'attacco informatico come attacco armato (v. E. Corsi, *La Nato a difesa del cyber spazio? Il dilemma nel diritto internazionale*, in *Research Analysis del Center for Cyber Security and International Relations Studies*, 2018), nonché lo stato dell'arte circa la definizione di una politica di sicurezza e difesa europea (v. M. Frau, *I nodi irrisolti della difesa comune europea. Una prospettiva federalista*, in *federalismi.it*, 6, 2022), non è da escludersi che questo principio possa essere ricondotto all'omonimo principio di reciproca assistenza di cui all'art. 42 del TUE, ove è previsto che nel rispetto della politica e di sicurezza e di difesa «di taluni Stati membri» l'assistenza allo Stato aggredito sia subordinata al previo coinvolgimento della NATO, sul punto cfr. F. Pocar - M.C. Baruffi (a cura di), *Commentario breve ai Trattati dell'UE*, Padova, 2014, 42.

[62] S. Sassen, *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton, 2008.

[63] R. Abrahamsen - A. Leander, *Handbook of private security studies*, Londra, 2016.

[64] R. Abrahamsen - M. C. Williams, *Security Privatization and Global Security Assemblages*, in *The Brown Journal of World Affairs*, 18(1), 2011, 171.

SCs[65], mentre poca attenzione è stata dedicata all'analisi delle organizzazioni private che non hanno nulla a che fare con la sicurezza in senso tradizionale, pur essendone oramai largamente coinvolte: è il caso delle ricordate infrastrutture critiche operative in diversi settori di primaria rilevanza come quello sanitario, trasporti, finanziario, ecc.
A tal proposito l'analisi delle politiche di cybersicurezza europea può rappresentare un emblematico esempio di questo rapporto. Diversi documenti strategici, tra cui anche la strategia dell'Unione europea per la cybersicurezza del 2013[66], fanno riferimento alla collaborazione tra pubblico e soggetti privati operanti in diversi settori, senza tuttavia precisare come debba realizzarsi questa cooperazione nella pratica. Come si comprenderà il tema è particolarmente complesso in quanto non investe solo profili pratici, ma anche giuridici e politici. La domanda di fondo a cui la dottrina tenta di dare risposta è quella di trovare soluzioni che possano colmare il divario tra due opposte posizioni: la massimizzazione del profitto, ricercata dal settore privato, e la massimizzazione della sicurezza quale priorità dei governi.
Sebbene a nostro modo di vedere la ricerca di tali soluzioni da parte dell'Unione europea sia ancora *in fieri*, per il momento pare utile soffermarsi sul ruolo oggi ricoperto dagli attori privati nel processo di cybersicurezza europeo.
Benjamin Farrand ed Helena Carrapico in un recente studio hanno analizzato la progressiva rilevanza assunta dagli attori privati attivi nei settori della disciplina NIS[67] nel processo di regolazione della sicurezza delle reti e delle risorse informatiche. Dall'analisi delle politiche di cybersicurezza adottate a partire dagli anni 2000, i due Autori hanno individuato tre momenti fondamentali: una prima fase, dal 2001, in cui i soggetti privati sono considerati vittime delle azioni di *cybercrime*, e quindi ricoprono un «passive role as object of regulation»[68]; successivamente, a seguito dell'istituzione dell'ENISA nel 2004, il settore privato non viene considerato solo come obiettivo di potenziali attacchi informatici ma anche come «active stakeholder that sholud form part of the regulatory structure»[69]; ed infine, con la Strategia per una società dell'informazione sicura del 2006, la Commissione ha ritenuto che «private sector does not only act as an adopter of regulation, bur can also be actively involved in shaping policy responses and the resulting regulation»[70].
Lo studio dimostra quindi come il settore privato abbia assunto un ruolo sempre più influente all'interno dei processi di regolazione in questa particolare branca sicuritaria. Il riferimento è a un documento dell'ENISA del 2012 ove si dimostra che gli standard adottati nelle norme di cyberisucrezza europee per garantire la sicurezza e l'integrità

[65] *Ex multis*, R. Mandel, *The Privatization of Security*, in *Armed Forces & Society*, 2001, 129–151; V. Calderai, *The Privatization of Military and Security Services and the Limits of Contract Law*, in EUI MWP, 2010/31; P. W. Singer, *Corporate Warriors: The Rise of the Privatized Military Industry*, New York, 2008.

[66] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro*, del 7 febbraio 2013.

[67] B. Farrand - H. Carrapico, *Blurring public and private: cybersecurity in the age of regulatory capitalism*, in O. Bures - H. Carrapico (a cura di), *Security Privatization. How non-security-related Private Businesses Shape Security Governance*, Cham, 2018, 197 ss.

[68] Ivi, 202.

[69] Ivi, 205.

[70] Ivi, 207.

delle informazioni sono fortemente basati su alcuni standard industriali utilizzati nel mercato europeo delle telecomunicazioni[71]. Pertanto, come scrivono i due Autori «[t]hrough the identification of standards of best practice, as well as the perceived position of experts in the field of telecoms, although the Commission has imposed binding legislation upon them, they have nevertheless been able to influence the standards by which the legislation is applied and interpreted by feeding the multi-stakeholder process»[72].

Per quanto qui interessa, ci concentreremo sul secondo momento individuato nello studio che vede il settore privato responsabile della corretta applicazione della disciplina sulla sicurezza delle reti e delle risorse informatiche.

4.3 I partenariati pubblico-privati europei di cybersicurezza

Come anticipato (v. infra par. 3), l'esigenza di sicurezza delle reti e dei sistemi informatici ha richiesto da subito la collaborazione tra il settore pubblico e privato trovando concreta attuazione attraverso l'istituzione di partenariati *ad hoc*, soprattutto al fine di favorire la creazione di ecosistemi informativi volti a prevnire le minacce informatiche. Ne sono un esempio i citati ISACs, partenariati pubblico-privati non profit isituiti originariamente negli Stati Uniti per aiutare le infrastrutture critiche attravero la raccolta centralizzata, valutazione e diffusione delle informazioni di cybersicurezza fornite dai CERTs e SOCs[73].

Anche a livello europeo[74], il parteneriato pubblico-privato è risultato essere lo strumento più adadatto per garantire la sicurezza informatica dei settori qualificati come critici, soprattutto al fine sviluppare la prevenzione, la preparazione e la risposta europea agli atti di terrorismo informatico attraverso l'istituzione della rete di *information sharing* per la protezione delle infrastrutture critiche CIWIN (*Critical Infrastructure Warining Information Network*)[75].

La convenienza circa l'utilizzo di questo strumento nel particolare contesto della cybersicurezza, nonché della protezione delle infrastrutture critiche è stato individuata da Alcuni nei seguenti motivi: «(a) the private sector 'owns or controls' a large number of CIs [critical infrastructures]; (b) the implementation of security policies depends on the involvement of the private sector in the 'definition of strategic public policy objectives as well as operational priorities and measures'; (c) PPPs 'would bridge the

[71] ENISA, *Shortlisting network and information security standards and good practices*, 2012.

[72] B. Farrand - H. Carrapico, *Blurring public and private,* cit., 209.

[73] N. Choucri - S. Madnick - P. Koepke , *Institutions for cyber security: International responses and data sharing initiative*, Working Paper CISL# 2016–10, Cybersecurity Interdisciplinary Systems Laboratory, MIT, Cambridge, MA, 2016.

[74] O. Bures, *Contributions of Private Businesses to the Provision of Security in the EU: Beyond Public-Private Partnerships*, in O. Bures - H. Carrapico (a cura di), *Security Privatization,* cit., 32.

[75] Si rinvia al sito della Commissione europea a proposito dello CIWIN.

gap between national policy-making and operational reality on the ground'»[76].

Preme precisare che queste prime esperienze cooperative sono sorte su impulso dei governi ma la loro effettiva realizzazione e partecipazione è avvenuta in virtù della sola volontà dei soggetti che vi aderivano (c.d. approccio "*bottom-up*"). Auto-organizzati settorialmente secondo gli ambiti di operatività delle infrastrutture critiche (troviamo infatti ISACs nel settore finanziario, energetico, ecc.), la diffusione delle informazioni e degli allarmi sulle minacce informatiche avveniva sulla base di accordi di natura privata. La allora Comunità europea si è limitata in un primo momento a promuovere la creazione di detti Centri a livello nazionale (esigenza ancora attuale date le recenti sollecitazioni), riconoscendo «the importance of multi-stakeholder models such as Public Private Partnerships (PPPs), built on a long term, bottom-up model to mitigate identified risks where such an approach delivers added value in helping to ensure a high level of network resilience»[77]. Anche l'ENISA, sulla scorta dell'implementazione della disciplina NIS, ha prodotto documenti sui modelli cooperativi per la costituzione dei ISACs nazionali[78].

Tuttavia, considerata la sempre più avvertita necessità di coordinare le procedure di scambio delle informazioni e degli allarmi in modo uniforme, l'Unione si è anche attività per creare partenariati a livello europeo. È il caso dell'*European Information Sharing and Alerting System* (EISAS)[79], progetto avviato nel 2007 con il fine di «colmare la lacuna nella condivisione di informazioni [...]» attraverso lo studio di modelli di analisi e diffusione delle informazioni di cybersicurezza utili alla creazione di uno spazio di condivisione comune[80].

Come si apprende dal "*Deployment Feasibility Study*" del 2013, il programma EISAS si poneva l'obiettivo di creare un sistema di scambio informativo su larga scala rafforzando la cooperazione dei già esistenti ISACs settoriali degli Stati membri e semplificando il flusso informativo grazie alla consegna di «materiali pre-prodotti ai partecipanti»[81]. Tra le altre "migliori pratiche" si avvertiva infatti l'esigenza di processare le informazioni raccolte dai Centri nazionali, al fine di disseminare dati di alta qualità, oltreché evitare la duplicazione degli stessi.

Diversamente, l'*European Public-Private Partnership for Resilience* - EP3R, ha rappresentato il primo tentativo di istituire un partenariato comune a livello europeo per affrontare problemi di sicurezza e resilienza nel settore delle telecomunicazioni[82].

Il progetto, avviato nel 2009, è stato successivamente chiuso nel 2013. Alcuni studiosi hanno ricondotto i motivi che hanno portato al fallimento di questa esperienza alla

---

[76] F. Cappelletti - L. Martino, *Achieving Robust European Cybersecurity through Public–Private Partnerships: Approaches and Developments*, in *EU Policy Review,* 1, 2021, 62.

[77] Consiglio europeo, *Council Resolution on a collaborative European approach to network and information security*, 2009/C 321/01, 2009, sezione IV, 7.

[78] ENISA, *Information Sharing and Analysis Centres (ISACs) Cooperative models*, 2018.

[79] ENISA, *EISAS – European Information Sharing and Alerting System*, 2007; nonchè il report, *EISAS (enhanced) report on implementation*, pubblicato nel 2011.

[80] Sui diversi settori critici coinvolti nel circuito EISAS si rinvia al sito ufficiale.

[81] ENISA, *EISAS – European Information Sharing and Alerting System. Deployment Feasibility Study*, 2013.

[82] ENISA, *EP3R 2009-2013 Future of NIS Public Private Cooperation*, 2015.

scarsa partecipazione degli aderenti al progetto sotto diversi profili: la mancanza di impegno nella condivisione delle informazioni, la mancanza di trasparenza procedurale, nonché la scarsa partecipazione delle infrastrutture di piccola e media dimensione, diversamente da quelle maggiori coinvolte in prima persona dalla disciplina NIS[83].

La condivisione delle informazioni sulle minacce informatiche e gli allarmi attraverso l'istituzione di strutture cooperative come i partenariati resta tuttavia una priorità per le politiche europee di cybersicurezza. Nonostante il fallimento dell'EP3R, nella Strategia per la cybersicurezza europea del 2013 veniva ribadito che «il partenariato europeo pubblico-privato per la resilienza (EP3R) costituisce una valida piattaforma a livello dell'UE che dovrebbe essere ulteriormente sviluppata»[84]. A tal fine l'ENISA ha creato, all'interno del framework della piattaforma NIS, tre gruppi di lavoro, con un focus specifico sugli strumenti di co-regolamentazione e relative politiche pubbliche con riferimento alla gestione del rischio, alla condivisione delle informazioni e al coordinamento in caso di incidenti tra pubblico e attori privati, che hanno sostituito l'EP3R.

Nello stesso anno la Commissione europea accoglieva l'esigenza di istituire l'unità specializzata EC3 (*European Cybercrime Centre*) per il contrasto alla criminalità informatica presso l'Europol[85]. Si tratta di un caso di partenariato pubblico-privato ove tra le parti vi sono autorità che svolgono compiti di polizia. Nello specifico, come si apprende dal sito, l'EC3 si avvale di due gruppi di consultazione che includono attori del settore privato al fine di creare un ambiente cooperativo capace di cooperare sulle sfide legate alla criminalità informatica, promuovendo la collaborazione sia a livello strategico sia operativo[86].

Sulla scorta di tali gruppi, l'EC3 ha siglato diversi *Memoranda of Understanding* (MoU) con gli attori privati operanti in settori critici, come quello finanziario[87], ma soprattutto quelli attivi nel settore dei servizi di sicurezza informatica[88]. Tali accordi, sebbene siano espressione di una libera contrattazione privata, hanno avuto l'effetto di dirigere le parti verso fini pubblici e modelli comuni di condivisione delle informazioni di cybersicurezza che, da una parte hanno aiutato il settore privato ad innalzare i livelli di sicurezza, dall'altra hanno permesso all'EC3 di essere sempre aggiornato sulle ultime minacce informatiche[89].

---

[83] Cfr. K. Iron, *The Governance of Network and Information Security In the European Union: The European Public-Private Partnership for Resilience (EP3R)*, in S. Gaycken - J. Krueger - B. Nickolay (a cura di), *The Secure Information Society: Ethical, Legal and Political Challenges*, Berlino, Springer Publ., 2021, 83 ss.

[84] Commissione europea, *Strategia dell'Unione europea per la cibersicurezza …,* 2013, 7.

[85] Conclusioni 10603/12 del Consiglio sull'istituzione di un centro europeo per la criminalità informatica, 2012.

[86] Si rinvia alla pagina *The EC3 Advisory Groups – Law Enforcement and Private Sector Meetings to Discuss Latest Cybercrime Threats and Challenges*, del sito EUROPOL.

[87] Si rinvia alla pagina *Europol and the European ATM Security Team reaffirm their partnership in combating payment crimes*, del sito EUROPOL.

[88] Si faccia riferimento agli accordi con Karspersky, McAfee, Mnemonic, Microsoft, FireEye la cui documentazione è reperibile sul sito EUROPOL.

[89] R. Bossong - B. Wagner, *A typology of cybersecurity and Public-Private partnership in the context of the European union*, in O. Bures - H. Carrapico (a cura di), *Security Privatization,* cit., 236.

5. La *cyber information sharing* alla luce della Direttiva NIS II e delle linee guida ENISA

La natura transfrontaliera delle minacce informatiche ha caratterizzato l'organizzazione di cyberiscurezza per una più accentuata necessità di ricorrere a meccanismi di cooperazione informativa attraverso la costituzione di reti di scambio tra soggetti che nutrono fiducia vicendevolmente[90]

Oltre alle competenti autorità pubbliche di polizia, intelligence e difesa (come avviene per la sicurezza in senso tradizionale), tra i partecipanti allo scambio informativo in questo settore trovano spazio anche gli stessi beneficiari delle garanzie di cybersicurezza, perlopiù soggetti pubblici o privati operanti in settori critici.

Tali attori sono oggi disciplinati dalla ricordata direttiva (UE) 2022/2555 (Direttiva NIS II) che all'art. 1, par. 2 - diversamente dalla previgente normativa - prevede espressamente che la direttiva stabilisce «norme e obblighi in materia di condivisione delle informazioni sulla cybersicurezza».

Dal raffronto dei due testi è possibile anche intuire come l'Unione europea si stia sempre più dirigendo verso modelli di regolazione di tipo *risk-based* nelle politiche digitali[91]. Ne è prova l'introduzione dei concetti di «quasi incidente», «incidente» ed «incidente di cybersicurezza su vasta scala» che trovano definizione all'art. 6 della Direttiva NIS II, nonché quello di «incidente significativo» di cui all'art. 23, par. 3[92], i quali lasciano intendere i diversi gradi di intervento e gestione del rischio informatico da parte dei soggetti coinvolti nel processo di cybersicurezza europeo. Disciplina che deve inoltre essere interpretata alla luce del ricordato *EU Cyber Solidarity Act*, quale strumento volto a potenziare la gestione unica degli incidenti ad impatto diffuso nello spazio europeo.

Sinteticamente, è possibile notare che al variare di intensità di un incidente di cybersicurezza, da livello nazionale/locale a livello europeo o internazionale, il quadro di discipline vigenti fa corrispondere altrettante competenti strutture che favoriscono meccanismi di raccordo sempre più estesi.

Nello specifico, la recente disciplina NIS II ha integrato il sistema di risposta coordina-

---

[90] Sui meccanismi cooperativi e di coordinamento per fini di cybersicurezza v. F. Skopik - G. Settanni - R.Fiedler, *A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing*, in *Computers & Security*, 60, 2016, 154 ss.

[91] G. De Gregorio - P. Dunn, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *Common Market Law Review*, 59(2), 2022.

[92] Cfr. art. 6, nn. 5, 6, 7 della Direttiva NIS II ove per «quasi incidente» si intende «un evento che avrebbe potuto compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi, ma che è stato efficacemente evitato o non si è verificato»; per incidente, «un evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi»; ed infine per «incidente di cybersicurezza su vasta scala» si intende «un incidente che causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o che ha un impatto significativo su almeno due Stati membri». La nozione di «incidente significativo» è invece introdotta all'art. 23, par. 3 della direttiva rubricato "Obblighi di segnalazione", il quale lo definisce come un incidente che «a) ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato; b) si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli».

ta agli incidenti e alle crisi di cybersicurezza su vasta scala istituito con la Raccomandazione (UE) 2017/1584, del 13 settembre 2017, con la previsione dell'EU-CyCLONe, a cui si aggiungono il Gruppo di cooperazione e la Rete dei Gruppi di intervento, ribadendo tuttavia la necessità per tutti gli attori di «specificare ulteriormente i meccanismi di funzionamento della rete, compresi i ruoli, i mezzi di cooperazione, le interazioni con altri attori pertinenti e i modelli per la condivisione delle informazioni, nonché i mezzi di comunicazione»[93].

La scalarità degli incidenti di cybersicurezza ci permette quindi di distinguere le normali pratiche di condivisione delle informazioni per motivi di cybersicurezza rientranti nella definizione propria di *cyber information sharing*, dallo scambio informativo che si aziona in caso di emergenza a seguito di un incidente significativo su un soggetto "essenziale" o "importante", o a seguito di un incidente su larga scala. In particolare, per quanto riguarda la presente trattazione, l'interesse è di analizzare tali circuiti informativi ponendoci dalla prospettiva di coloro che alimentano e generano il traffico informativo a seguito dell'incidente, ossia i soggetti interessati dalla novellata disciplina NIS II. A tal proposito, nel caso si realizzino «incidenti significativi» nei confronti di soggetti qualificabili come come «essenziali» o «importanti» vige l'obbligo di segnalazione alle competenti autorità e/o ai CSIRT di cui all'art. 23. Diversamente, ove tale incidente abbia interessato «soggetti diversi» da quelli appena ricordati, l'adempimento informativo verso le competenti autorità consisterà in una «notifica volontaria di informazioni pertinenti» disciplinata all'art. 30, par. 1, lett. b).

Inoltre, oltre a tali procedure d'emergenza, vi sono anche altri circuiti informativi, che rientrano nelle attività di vera e propria *cyber information sharing*. Questa procedura si differenzia dalla prima per due caratteristiche: 1) il fatto che l'interlocuzione di tali soggetti non avviene solo con le preposte istituzioni europee, ma anche con altri attori NIS (perlopiù appartenenti allo stesso settore es. energetico, finanziario, ecc.), 2) per il fatto che non sussistono obblighi di partecipazione agli ecosistemi informativi. Tale circuito è alimentato dall'esclusiva volontà dei partecipanti, siano essi di rilevanza critica ai sensi della direttiva («essenziali» o «importanti») o diversi[94].

La condivisione (volontaria) delle informazioni avviene pertanto sulla scorta di accordi tra le parti. Sul punto la recente Direttiva NIS II ha introdotto l'art. 29, rubricato "Accordi di condivisione delle informazioni sulla cybersicurezza". Come si apprende dal disposto, il legislatore europeo ha indicato come obiettivo per gli Stati membri quello di mettere in condizione tutti i soggetti, critici e non, di «scambiarsi, su base volontaria, pertinenti informazioni sulla cybersicurezza, comprese informazioni relative a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli attori delle minacce, allarmi di cybersicurezza e raccomandazioni concernenti la configurazione degli strumenti di cybersicurezza per individuare le minacce informatiche». Al paragrafo secondo è precisato che tale scambio venga «attuato mediante accordi di condivisione delle informazioni sulla cybersicurezza che tengano conto della natura potenzialmente sensibile

[93] Cfr. considerando 68, della Direttiva NIS II.

[94] Si faccia riferimento al considerando 29 del Cybersecurity Act, ove è previsto che «l'ENISA dovrebbe sostenere la condivisione delle informazioni intra e intersettoriale [...]».

delle informazioni condivise» ed in particolare che gli Stati membri, nel facilitare la conclusione di simili accordi, «possono specificare gli elementi operativi, compreso l'uso di piattaforme TIC dedicate e di strumenti di automazione, i contenuti e le condizioni degli accordi di condivisione delle informazioni», e nel caso della partecipazione delle autorità pubbliche a tali accordi «possono imporre condizioni per le informazioni messe a disposizione dalle autorità competenti o dai CSIRT».

5.1. La progressiva europeizzazione degli strumenti di cooperazione informativa: SOC, Registri delle vulnerabilità, Standard di scambio e Piattaforme di *cyber threat sharing*

Appurati i soggetti segnalanti nel precedente paragrafo, è doveroso ora precisare di quali strumenti e processi, tali soggetti, siano essi di natura pubblica o privata, si servono per contribuire ad alimentare il traffico di informazioni di cybersicurezza alla luce della vigente disciplina europea.

a) I Security Operation Centres (SOCs)

Alla base del processo di condivisione delle informazioni relative alle minacce informatiche troviamo i *Security Operation Centers* (SOCs), centri operativi di sicurezza pubblici o privati che, attraverso il continuo monitoraggio delle reti e dei sistemi dell'organizzazione per il quale operano, evitano che gli attacchi informatici possano avere un impatto negativo sul funzionamento e l'economia dell'organizzazione limitandone i danni[95]. Tali centri sono in grado non solo di rilevare le minacce in corso, ma anche di estrapolarne informazioni particolarmente utili, sia per le attività di indagine condotte dalle forze di polizia (vedi la *digital forensics*), sia per le attività di prevenzione come i meccanismi di *information sharing*.
Nello specifico, questo patrimonio informativo è composta da: le vulnerabilità tecniche, ossia le debolezze del sistema o dei beni informatici che il criminale ha sfruttato per comprometterne la riservatezza, la disponibilità o l'integrità; gli *exploit*, ossia, il codice appositamente realizzato per sfruttare una determinata vulnerabilità e comprometterla, oppure altri tipi di infromazioni, come i c.d. indicatori di compromissione (IoC), termine con il quale si intende fare generalmente riferimento all'indirizzo del protocollo Internet (IP) del *server* eventualmente sfruttato per condurre l'attacco, il nome di dominio DNS (*Domain Name System*) o l'URL (*Uniform Resource Locator*) sospetti che rimandano a contenuti dannosi, ed infine l'identificativo di un file eseguibile dannoso o il testo dell'oggetto di un messaggio e-mail dannoso[96].

[95] Sulla definzione di SOC si rinvia alle linee guida ENISA, *How to set up CSIRT and SOC. Good practice guide*, dicembre 2020,.

[96] Sul punto si faccia riferimento alla scheda informativa pubblicata dal Centro nazionale per la sicurezza informatica olandese, il *National Cyber Security Centre* (NCSC), *Factsheet on Indicators of Compromise (IoCs)*,

Considerato che si tratta di Centri ad oggi perlopiù istituiti presso singoli enti e realtà industriali, sia di natura pubblica, sia privata, preme porre attenzione al citato *Cyber Solidarity Act*. Qualora la proposta di regolamento entri in vigore senza emendamenti, la realizzazione dell'*European Cybersecurity Shield* introdurrebbe due importanti novità nelle architetture di cybersicurezza nazionali e quella europea. Si prevede infatti che lo "Scudo" sarà costituito da SOC nazionali, di natura pubblica, designati da ciascuno Stato membro (art. 4), e dai «Cross-border SOCs», ossia Centri transfrontalieri costituiti da un consorzio di almeno tre Stati membri rappresentati dai SOC nazionali (c.d. *Hosting Consortium*), che si impegnano a lavorare insieme per coordinare il loro rilevamento informatico e le attività di monitoraggio delle minacce (artt. 6-7)[97].
Su quest'ultimo punto, si precisa che il Consorzi saranno costituito sulla base di accordi scritto in cui i membri dovranno anche dettagliare i requisiti e i pricincipi per la condivisione delle «relevant information» tra i partecipanti (art. 6)[98]. Inoltre, la proposta invita i singoli Consorzi a stringere accordi con altri Consorzi.

b) I Registri delle vulnerabilità e delle debolezze informatiche

Agli albori dell'informatica erano in uso le prime "liste" di vulnerabilità create ed alimentate dai primi utenti della "*Internet society*" (al tempo composta perlopiù ingegneri ed esperti di informatica)[99] per mezzo delle "*request for comments*" (o RfC)[100]. Si trattava di uno strumento di trasparenza che bene esprimeva l'autoregolamentazione che caratterizzava la Rete. È interessante notare come successivamente, sulla scorta della sempre maggiore rilevanza acquisita dagli attacchi informatici per le società e l'economia, gran parte di questi registri siano oggi perlopiù sviluppati e supervisionati da un connubio di enti privati e pubblici, soggetto al controllo dei governi[101].

2017.

[97] Sulla formazione del "*consortium*", la proposta di regolamento prevede che i membri del Consorzio ospitante stipulino un accordo consortile scritto che stabilisce le loro disposizioni interne, ove sono anche indicati in dettaglio i requisiti per la condivisione informazioni tra i partecipanti a un SOC transfrontaliero e per la condivisione di informazioni

[98] Sul contenuto delle "informazioni rilevanti" da trasferire, l'art. 6 della proposta prevede «information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding the configuration of cybersecurity tools to detect cyber-attacks».

[99] L'*Internet society* (ISOC) è un'organizzazione internazionale di diritto americano per la promozione dell'utilizzo e dell'accesso a Internet, oggi popolata da diverse sezioni locali (c.d. *chapters*) che vedono la partecipazione di gran parte dei paesi del mondo.

[100] La "*Repaired Security Bugs in Multics*", è stata la prima "lista" di vulnerabilità pubblicata pubblicata nel 1973 da Jerome H. Saltzer, con RfC n. 5. Le *request form comments* (RfC) sono «documents contain technical specifications and organizational notes for the Internet» così definiti dall'organismo internazionale che li prodoce, l'*Internet Engineering Task Force* (IETF), responsabile della standardizzazione dell'nternet e degli standard tecnici che ne consentono il funzionamento, primo fra tutti la suite di protocolli Internet (TCP/IP).

[101] Nonostante la scarsità di documenti ufficiali sul punto, da fonti Wiki si apprende che il primo (e forse anche unico) *database* di vulnerabilità sviluppato da un ente indipendente, quindi svincolato da

Negli Stati Uniti, sono attivi i *Common Vulnerabilities and Exposures* (CVE) e *Common Weakness Enumeration* (CWE)[102]: due indici che rientrano nella c.d. *vulnerability disclousure*, ossia la condivisione di informazioni sulle vulnerabilità e debolezze del *software* al fine di favorire la mitigazione degli effetti negativi di un accesso indesiderato da parte degli esperti di sicurezza. Si tratta di programmi di aggregazione e pubblicazione delle vulnerabilità e debolezze informatiche supervisionate da un ente privato non-profit, il *MITRE Corporation*[103], con il supporto dall'Agenzia per la sicurezza informatica e delle infrastrutture che fa capo al Dipartimento della sicurezza interna degli Stati Uniti. Inoltre, i *database* relativi ai CVE sono pubblicati in maniera sincrona su un altro registro, il *National Vulnerability Database* (NVE), gestito e fondato dall'agenzia pubblica *National Institute of Standards and Technology* (NIST)[104] a partire dal 2005.

Si comprenderà pertanto come l'origine geografica di tali banche dati sia una questione di rilevante interesse per i governi. Ne è prova il fatto che, oltre a quelle più comuni appena citate, di origine statunitense, sono stati istituiti ecosistemi informativi di questo tipo anche in altri Paesi, come ad esempio Giappone[105], Cina[106] e Russia[107].

Sul punto pare rilevante osservare che al considerando 63 della direttiva (UE) 2022/2555 è previsto che «sebbene simili registri o banche dati delle vulnerabilità esistano già [es. CVE e CWE], questi sono ospitati e mantenuti da soggetti non stabiliti nell'Unione». Con la Direttiva NIS II, l'Unione europea ha difatti promosso, per la prima volta, l'istituzione di un registro europeo delle vulnerabilità mantenuto dall'ENISA al fine di garantire «una maggiore trasparenza, per quanto riguarda la procedura di pubblicazione prima della divulgazione ufficiale della vulnerabilità, e resilienza in caso di perturbazioni o interruzioni nella fornitura di servizi analoghi»[108].

Tuttavia, se da un lato la divulgazione delle vulnerabilità e debolezze informatiche

controlli da parte di poteri pubblici, sia stato l'*Open Sourced Vulnerability Database* (OSVDB). Si trattava di un'iniziativa che ha preso avvio dalla nota *convention* per amanti dell'informatica, Def Con, nel 2002, per essere resa operativa con il primo *database open-source* nel 2004 (quindi svincolato anche da legami proprietari con le aziende di *software*) con il supporto della *Open Security Foundation* (OSF). Tuttavia, il 5 aprile 2016 il *database* è stato chiuso.

102 Si rinvia rispettivamente ai siti del *Common Vulnerabilities and Exposures* (CVE) e del *Common Weakness Enumeration* (CWE).

103 Come si apprende dal sito ufficiale dell'organizzazione, il MITRE si è costituito nel 1958 come società privata senza scopo di lucro per fornire consulenza ingegneristica e tecnica all'Aeronautica degli Stati Uniti. Il progetto fu utile per la creazione del primo centro di ricerca e sviluppo finanziato a livello federale (FFRDC), sponsorizzato dal Dipartimento della Difesa.

104 Il NIST è parte del Dipartimento del Commercio degli Stati Uniti.

105 v. *Japan Vulnerability Notes* (JVN).

106 v. *Chinese National Vulnerability Database* (CNNVD).

107 v. *Data Security Threats Database* (BDU), di cui non si hanno molte informazioni liberamente reperibili in rete se non alcuni articoli di stampo giornalistico, v. J. Leiden, *Russia's national vulnerability database is a bit like the Soviet Union – sparse and slow 7 comment bubble on white By design, though, not... er, general rubbishness*, in *The Register*, 17 luglio 2018.

108 Cfr. considerando 63, Direttiva NIS II. A ben vedere, l'art. 29 della direttiva, prevede che tra le «pertinenti informazioni sulla ciberiscurezza» rientrino, oltre alle vulnerabilità tecniche: informazioni relative a minacce informatiche, quasi incidenti, procedure, indicatori di compromissione (IoC), tattiche avversarie, informazioni specifiche suglia attori delle minacce, allarmi di cibersicurezza e raccomandazioni concernenti la configurazione degli strumenti di cibersicurezza per individuare le minacce informatiche.

all'interno di banche dati pubbliche coordinate e liberamente accessibili può certamente favorire la sicurezza informatica parte degli addetti, dall'altro può anche essere uno strumento di facile utilizzo da parte dei criminali aventi tutto l'interesse a sfruttarle per violare le reti e i sistemi informatici. Proprio per questo motivo al successivo considerando 58 della direttiva, il legislatore europeo ha previsto di «rafforzare il coordinamento» tra i segnalanti e i fabbricanti o fornitori dei beni e servizi ICT dal quale sono state rilevate tali vulnerabilità, in modo da velocizzare la comunicazione.
Si precisa inoltre che nel considerando viene fatto esplicito riferimento (c.d. rinvio fisso) alle norme internazionali ISO/IEC 30111 e ISO/IEC 29147 circa la gestione e divulgazione delle vulnerabilità anche a terzi soggetti.

c) Le piattaforme di *Cyber Information Sharing* e gli standards di condivisione

Generalmente la condivisione delle informazioni sulle minacce informatiche e gli allarmi avviene per il mezzo di piattaforme di *cyber information sharing*, di natura proprietaria od *open source* (come ad esempio *Malware Information Sharing Platform* - MISP)[109], che permettono di diffondere ed alimentare questo patrimonio informativo per mezzo di standard di linguaggio specifici (*rectius* standard sul formato dei dati[110]).
Tuttavia, da diverso tempo, il mercato della sicurezza ha visto la progressiva introduzione anche di piattaforme particolarmente evolute - le c.d. piattaforme di *Cyber Threat Intelligence* (CTI) - ossia strumenti capaci non solo di estrapolare e condividere le informazioni relative alle minacce informatiche e agli incidenti di sicurezza, ma anche di elaborarle attraverso l'incrocio con altre fonti esterne che permettono di restituire - per l'appunto - informazioni di *threat intelligence*[111].
Nello specifico la CTI è stata definita come «*systematic collection, analysis and dissemination of information pertaining to a company's operation in cyberspace and to an extent physical space. It is designed to inform all levels of decision makers. The analysis is designed to help keep situational awareness about current and arising threats*»[112].
L'aggregazione delle fonti che caratterizza le attività di *threat intelligence* permette infatti di avere un quadro generale sulle cc.dd. tattiche, tecniche e procedure (TTP), ossia: le descrizioni di alto livello del comportamento (tattiche); le descrizioni dettagliate del

[109] Si rinvia al sito del *Malware Information Sharing Platform* (MISP).

[110] I formati di dati maggiormente utilizzati per il funzionamento di queste piattaforme sono gli standard STIX/TAXII, CyBOX, OASIS. Per maggiori dettagli tecnici sul funzionamento delle piattaforme di *sharing* si rinvia alla citata guida del NIST di cui in nota 112.

[111] Preme distinguere la *cyber threat intelligence* dalla *cyber intelligence* quale autonoma branca dell'*intelligence* che consiste nel «complesso di attività programmate ed applicate per identificare, seguire, misurare e monitorare informazioni sulle minacce digitali, nonché dati sulle intenzioni e attività di entità avversarie» svolte con «strumenti cibernetici nel cyber spazio, cioè attraverso la rete, e hanno una particolarità, a differenza delle altre forme di intelligence, poiché non si può fare totale affidamento alle attrezzature elettroniche» v. U. Gori - L.S. Germani (a cura di), I*nformation Warfare 2011. La sfida della cyber intelligence al sistema Italia: dalla sicurezza delle imprese alla sicurezza nazionale*, Milano, 2012, 16 ss.; nonché M. Caligiuri, *Cyber Intelligence. Tra libertà e sicurezza*, Roma, 2016.

[112] Si rinvia alla pagina *Introduction to CTI as a General topic* presso il sito del FIRST.

comportamento nel contesto di una tattica (tecnica); descrizioni dettagliate nel contesto di una tecnica (procedure). Le TTP permettono quindi di descrivere la tendenza di un attore a utilizzare una specifica variante di *malware*, un ordine di operazioni, uno strumento di attacco, un meccanismo di consegna (ad esempio, un attacco di *phishing*) o un *exploit*[113].

Pertanto - per dirla con i termini della criminologia - le piattaforme di CTI permettono di ricostruire la "firma" e il "modus operandi" dell'attore malevolo[114], restituendo informazioni non solo di natura tecnica, utili per l'arricchimento dei bacini informativi tipici dell'*information sharing*, ma anche informazioni complesse e aggregate utili per eventuali attività di investigazione da parte degli addetti.

Il recente interesse degli Stati verso la sicurezza del cyeberspazio ha portato una parte della dottrina ad interrogarsi sui profili giuridici di dette piattaforme. Per molto tempo questi strumenti hanno trovato applicazione nel settore privato senza una vera e propria regolamentazione[115], soprattutto sotto il profilo del trattamento delle informazioni e della protezione dei dati personali che sarà approfondito nel prossimo paragrafo.

Per quel che qui interessa, ossia il profilo regolazione strettamente legato al legittimo utilizzo di questi strumenti, pare utile richiamare quanto disposto nella Direttiva NIS II, ove all'art. 29, par. 3 prevede che gli Stati membri «facilitano la conclusione degli accordi di condivisione delle informazioni sulla cybersicurezza [...]» e «possono specificare gli elementi operativi, compreso l'uso di piattaforme TIC dedicate e di strumenti di automazione, i contenuti e le condizioni degli accordi di condivisione delle informazioni». L'eventuale partecipazione a tali circuiti informativi dovrà inoltre essere notificata alle autorità competenti al momento di conclusione di tali accordi, così come il loro ritiro dagli stessi (par. 4).

L'ostacolo principale nello scambio di informazioni è la mancanza di standard comuni nella comunicazione. Sebbene la recente disciplina NIS sul punto non imponga il rispetto di requisiti comuni, pare utile rinviare ad uno studio "*work in progress*" condotto dall'ENISA relativamente allo scambio di informazioni tra i CSIRT e le autorità di polizia, ove si è proposta una tassonomia volta ad identificare quali informazioni possono essere condivise tra i due, e come ciò possa essere realizzato da una prospettiva tecnica e organizzativa[116].

---

113 C. Johnson - L. Badger - D. Waltermire - J. Snyder - C. Skorupka, *Guide to Cyber Threat Information Sharing*, NIST Special Publication 800-150, 2016.

114 R. Chiesa - S. Ciappi, *Profilo Hacker. La scienza del criminal profiling applicata al mondo dell'hacking*, Milano, Apogeo, 2007, 10 ss.

115 L. O. Nweke - S. Wolthusen, *Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection*, 2020 12th International Conference on Cyber Conflict (CyCon), Estonia, 2020, 63 ss.

116 ENISA, *Information sharing and common taxonomies between CSIRTs and Law Enforcement*, 2016.

6. La tutela dei diritti fondamentali e della sicurezza nel trattamento delle informazioni "sensibili e classificate" per lo Stato e dei dati personali contenuti nelle informazioni di cybersicurezza

Dal breve quadro sui soggetti segnalanti poc'anzi delineato emerge come il legislatore europeo abbia inteso distinguere i soggetti critici da quelli non rientranti in questa categoria in funzione dell'importanza per il settore in cui operano, o il tipo di servizi che forniscono, nonché delle loro dimensioni[117].

È bene precisare che le infrastrutture operanti in settori "critici" non rientrano solo nel campo d'applicazione della disciplina europea, ma anche nelle relative legislazioni nazionali degli Stati membri che, in alcuni casi, come in Italia, oltre ad aver recepito la disciplina NIS[118], hanno anche adottato legislazioni autonome in materia di cyberiscurezza nazionale.

La precisazione è d'obbligo poiché, se per la Direttiva NIS II le misure in essa disposte sono volte a garantire un livello comune elevato di cybersicurezza europea «in modo da migliorare il funzionamento del mercato comune» (art. 1), sul piano nazionale, vedi l'Italia, le misure contenute nel decreto decreto-legge del 21 settembre 2019, n. 105, istitutivo del Perimetro di Sicurezza Nazionale Cibernetica (PSNC), sono dirette ad assicurare la «tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico» (art. 1, par. 1, lett. a)[119].

L'intima connessione tra sicurezza nazionale e protezione delle infrastrutture critiche[120], porta a dover concludere che la circolazione nello spazio europeo delle informazioni di cybersicurezza - composte da elementi che possiamo immaginare come le "chiavi d'accesso" a reti e sistemi informatici critici - possa essere fortemente ostacolata da limiti dettati da prerogative statali sovrane, come la sicurezza interna[121], diversa rispetto al più ampio profilo della "sicurezza europea"[122].

---

[117] Cfr. considerando 15 della Direttiva NIS II.

[118] v. Decreto legislativo, 18 maggio 2018, n. 65, con il quale l'Italia ha recepito la disciplina NIS.

[119] Cfr. art. 1, c. 1, lett. a) del d.l. n. 105 del 2019, recante disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale.

[120] B. Valensise, *I settori strategici dopo la riforma*, in G. Della Cananea - L. Fiorentino (a cura di), *I "poteri speciali" del Governo nei settori strategici*, Napoli, 2020, 101 ss.

[121] Sul rapporto tra sovranità e sicurezza nell'ottica statuale v. C. Mortati, *Istituzioni di diritto pubblico*, Padova, 1962, 127 ss.; M.S. Giannini, *Sovranità (diritto vigente)*, in *Enciclopedia del diritto*, vol. XLIII, Milano, 1990, 224 ss.; G. de Vergottini, *Guerra e costituzione. Nuovi conflitti e sfide alla democrazia*, Bologna, 2004, 151 ss.; Id., *La difficile convivenza fra libertà e sicurezza. La risposta delle democrazie al terrorismo*, in *Rassegna Parlamentare,* 2, 2004 427 ss.; Id., *La persistente sovranità*, in *Recte sapere, Studi in onore di Giuseppe Dalla Torre*, Tomo II, Torino, 2014, 1373- 1392; A. Spadaro, *Dalla "sovranità" monistica all'"equilibrio" pluralistico di legittimazione del potere nello Stato costituzionale contemporaneo*, in *Rivista AIC*, 3, 2017, 1 ss.; E.A. Imparato, *Sovranità e sicurezza. Un connubio ancora vincente?* in *federalismi.it*, 1, 2019. Nonché sulla sovranità nell'era dell'informatizzazione v. A. Simoncini, *Sovranità e potere nell'era digitale*, in O. Pollicino - T.E. Frosini - E. Apa – M. Bassini (a cura di), *Diritti e libertà in internet*, Milano, 2017, 20 ss.; S. Mannoni - G. Stazi, *Sovranità. co. Potere pubblico e privato ai tempi del cyberspazio*, Napoli, 2021; V. Bertola - S. Quintarelli, *Internet fatta a pezzi. Sovranità digitale, nazionalismi e big tech*, Torino, 2023.

[122] V. S. Peers, *National Security and European Law*, in *Yearbook of European Law*, 16(1), 1996, 363 ss.; U.

Altro limite è certamente rappresentato dalla tutela dei diritti fondamentali dei singoli. Il materiale diffuso potrebbe infatti consentire di individuare le persone fisiche, trovando così applicazione il quadro di disciplina sulla protezione dei dati personali diversamente articolato in funzione della natura dei soggetti titolari del trattamento. In particolare la distinzione fondamentale è tra titolari del trattamento qualificabili come forze di polizia (o *law enforcement agencies* - LEAs) e soggetti che non rivestono tali incarichi.
Ulteriore considerazione riguarda la propagazione degli incidenti informatici che possono facilmente scalare da emergenza interna di una singola organizzazione, ad emergenza di livello nazionale o transnazionale. Motivo per cui il patrimonio informativo che caratterizza la *cyber information sharing* può essere utilizzato da diversi soggetti, per diverse finalità, che vanno dall'interesse degli enti alla salvaguardia dei propri affari, o delle pubbliche amministrazioni all'efficiente e continua fornitura dei servizi, fino alla difesa della sicurezza nazionale da parte dei governi e la sicurezza europea.
Nel presente paragrafo si tenterà pertanto di analizzare il differenziato regime di trattamento delle informazioni di cybersicurezza in considerazione del fatto: a) che tali informazioni possono essere utilizzate per la tutela della sicurezza interna degli Stati membri e quindi potrebbero esservi apposte classificazioni o potrebbero essere qualificate come "sensibili", limitandone di fatto la circolazione; b) che tali informazioni possono contenere dati personali rientranti nelle relative discipline di settore in funzione delle finalità e dei soggetti che le trattano: organizzazioni europee, forze di polizia, titolari "generici".

a) Lo scambio di informazioni "sensibili e classificate" di cybersicurezza e i limiti alla loro circolazione

Nel richiamato documento strategico del 2020, la Commissione osservava che «[l]'interoperabilità dei sistemi di informazioni classificate rimane tuttavia limitata, impedendo un trasferimento fluido delle informazioni tra le diverse entità» ravvisando così l'esigenza di un approccio interistituzionale al trattamento delle informazioni classificate a livello europeo, anche attraverso l'individuazione di «una base di riferimento per semplificare le procedure con gli Stati membri».
Come deducibile dalla citata proposta di Regolamento *EU Cyber Solidarity Act*, tali procedure sono ancora in fase di implementazione, e soprattutto non è stata individuata un'idonea base di legittimità. Il tema è estremamente sensibile poiché la cooperazione informativa, riconducibile al più ampio concetto di sicurezza collettiva[123], si scontra con le limitazioni poste per esigenze di sicurezza interna da parte degli Stati membri.
A tal proposito pare utile richiamare il contenuto dell'art. 346, lett. a) del Trattato sul

Draetta, *L'Unione europea tra processo costituente e sovranità nazionale*, in U. Draetta - N. Parisi - D. Rinoldi (a cura di), *Lo «spazio di libertà sicurezza e giustizia» dell'Unione europea,* cit., 17 ss; A. Alì, *Il diritto dell'Unione europea e la tutela della sicurezza nazionale degli Stati membri. Osservazioni a margine di alcuni casi esaminati dalla Corte di Giustizia dell'Unione europea*, in U. Gori - L. Martino, *Intelligence e interesse nazionale,* Aracne editrice, Roma, 2015, 593 ss.

[123] World Economic Forum, *Cyber Information Sharing: Building Collective Security. Insight Report*, ottobre 2020.

funzionamento dell'Unione europea (TFUE) già art. 296 del TCE. La norma rientra tra le disposizioni che autorizzano una deroga all'applicazione delle norme del TFUE in virtù di ragioni non economiche (c.d. clausola di salvaguardia), autorizzata in nome di esigenze di sicurezza e difesa nazionale con il fine di realizzare un delicato equilibrio tra le predette esigenze interne degli Stati e gli obiettivi fondamentali del mercato interno.

In particolare, con l'ipotesi di cui alla lett. a) del par. 1, si consente agli Stati membri di rifiutare di fornire informazioni a qualunque istituzione europea la cui divulgazione sia dagli stessi considerata «contraria agli interessi essenziali della propria sicurezza»[124], purché tale misura restrittiva sia ritenuta necessaria e mai per ragioni di carattere economico.

La dottrina si è variamente dibattuta sull'interpretazione del disposto tra approcci restrittivi ed estensivi[125]. Secondo la Commissione la disposizione «va oltre il settore della difesa, e mira in generale a proteggere le informazioni che gli Stati membri non possono divulgare senza mettere in pericolo i loro interessi essenziali della propria sicurezza»[126].

Pertanto, la deroga in questione esonera gli Stati dal più ampio obbligo derivante dal principio di leale collaborazione di cui all'art. 4, par. 3, del TUE, che impone agli Stati di fornire informazioni alle istituzioni dell'UE (compresa la Corte di giustizia) o ad altri Stati membri le informazioni che gli fossero richieste, al fine di mantenere segreto ciò che riguarda la propria sicurezza[127].

L'applicazione dell'art. 346 TFUE nel contesto della *cyber information sharing* trova riscontro nell'*EU Cyber Solidarity Act*, ove al considerando 23 è previsto che lo scambio informativo avvenga nel rispetto dei limiti del disposto ("*without prejudice*"), ed inoltre che tale disseminazione «*should be limited to that which is relevant and proportionate to the purpose of that exchange. The exchange of such information should preserve the confidentiality of the information and protect the security and commercial interests of the entities concerned, in full respect of trade and business secrets*».

A tal proposito, il considerando 9 della Direttiva NIS II prevede che la regolazione di tali traffici dovrebbe avvenire nel rispetto delle «norme dell'Unione o nazionali per la protezione delle informazioni classificate, gli accordi di non divulgazione o gli accordi

---

[124] Si tratta di una clausola di salvaguardia prevista dal Trattato che trova applicazione nelle sole ipotesi contemplate dal disposto. Introdotta con il fine di tutelare il segreto di Stato che riguarda la sicurezza nazionale dei Paesi membri, questo articolo rappresenta una deroga agli artt. 4, par. 3, del TUE e 337 del TFUE, rispettivamente dedicati, all'obbligo di fornire informazioni alle istituzioni europee in virtù del principio di leale collaborazione, il secondo, attributivo alla Commissione europea il potere di raccogliere tutte le necessarie informazioni e di procedere alle opportune verifiche per l'esecuzione dei suoi compiti. Sul punto v. F. Pocar - M.C. Baruffi (a cura di), *Commentario breve ai Trattati dell'UE*, cit., 1546 ss.

[125] Sull'approccio restrittivo v. P. Gori, *Art. 223*, in R. Monaco - R. Quadri - A. Trabucchi (diretto da), *Commentario CEE*, Milano, 1995, 1626 ss.; per altro orientamento, di interpretazione estensiva v. R. Smit,P. Herzog, *Article 223*, in P. Herzog - C. Campbell - G. Zagel (a cura di), *The Law of the European Union is the completely updated and revised edition of their Law of the European Community: A Commentary on the EC Treaty*, New York, 5.

[126] COM(2006)779 del 7 dicembre 2006 sull'applicazione dell'art. 296 del trattato CE agli appalti pubblici della difesa.

[127] V. F. Pocar - M.C. Baruffi (a cura di), *Commentario breve ai Trattati dell'UE,* cit., 1547.

di non divulgazione informali, quale il protocollo TLP» (su quest'ultimo torneremo a breve), e al successivo considerando 118 viene previsto che «l'ENISA dovrebbe predisporre l'infrastruttura, le procedure e le norme per il trattamento delle informazioni sensibili e classificate in conformità alle norme di sicurezza applicabili alla protezione delle informazioni classificate dell'UE».

Quella dello scambio e della protezione delle informazioni "sensibili e classificate" nel contesto europeo è una disciplina in evoluzione che è avanzata nel tempo per accordi e decisioni tra l'Unione europea e singoli Stati, anche non membri dell'UE[128]. Senza entrare nel dettaglio, brevemente, le parti concordano di sviluppare la cooperazione sulla sicurezza e sulla condivisione di informazioni classificate attenendosi ad alcune prerogative comuni: ciascuna delle parti deve proteggere le informazioni classificate fornite dall'altra, o scambiate con essa, a un livello almeno equivalente a quello offerto dalla parte che le fornisce; tutte le persone che hanno accesso alle informazioni classificate devono disporre di un adeguato nulla osta di sicurezza, basato sulla lealtà, sul carattere fidato e sull'affidabilità; Possono inoltre essere stabilite restrizioni sulla modalità di utilizzo e di divulgazione delle informazioni classificate, nonché di accesso alle stesse.

Sul punto è utile precisare che ai sensi dell'art. 2 della Decisione 2013/488/UE, per «informazioni classificate UE» (ICUE) si intende «qualsiasi informazione o qualsiasi materiale designati da una classifica di sicurezza UE, la cui divulgazione non autorizzata potrebbe recare in varia misura pregiudizio agli interessi dell'Unione europea o di uno o più Stati membri»[129].

Tuttavia, come precisato in dottrina, la clausola di cui al richiamato art. 346 lett. a) TFUE trova esclusiva applicazione verso gli Stati membri e non anche verso le imprese[130].

Principio che trova riscontro anche nel contesto degli scambi informativi di cybersicurezza atteso il contenuto del considerando 10 della citata Direttiva NIS II il quale, dopo aver evidenziato la connessione tra le infrastrutture critiche attive nel settore della produzione di energia elettrica da centrali nucleari e la sicurezza nazionale, prevede che «uno Stato membro dovrebbe poter esercitare la propria responsabilità per la salvaguardia della propria sicurezza nazionale in relazione a tali attività, comprese le attività all'interno della catena del valore nucleare, conformemente ai trattati».

Viene pertanto ribadita l'esclusiva competenza degli Stati nel dover adottare le misure necessarie a garantire la tutela degli interessi essenziali della sicurezza nazionale e salvaguardia dell'ordine pubblico e della pubblica sicurezza, promuovendo presso i soggetti

---

128 Per una panoramica sul punto si rinvia al sito Eur-Lex, v. anche E. De Capitani, *Unione europea e segreto di Stato*, in *www. astrid-online.it*, 2010.

129 Sono inoltre definiti al par. 2, quattro livelli di classificai: 1. Top Secret: informazioni e materiali la cui divulgazione non autorizzata potrebbe arrecare danni di eccezionale gravità agli interessi fondamentali dell'UE o di uno o più paesi dell'UE; 2. Secret: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gravemente gli interessi fondamentali dell'UE o di uno o più paesi dell'UE; 3. EU Confidential: informazioni e materiali la cui divulgazione non autorizzata potrebbe ledere gli interessi fondamentali dell'UE o di uno o più paesi dell'UE; 4. EU Restricted: informazioni e materiali la cui divulgazione non autorizzata potrebbe essere pregiudizievole per gli interessi dell'UE o di uno o più paesi dell'UE.

130 F. Sciaudone, *Art. 346 TFUE*, in A. Tizzano (a cura di), *Trattati dell'Unione europea, Le fonti del diritto italiano*, II ed., Milano, 2014, 2515 ss.

critici il ricorso ad accordi volontari per la condivisione delle informazioni sulla cybersicurezza «che tengono conto della natura potenzialmente sensibile delle informazioni condivise»[131].

Tra le basi legali menzionate dalla disciplina NIS è fatto riferimento anche agli «accordi di non divulgazione informali, quale il protocollo TLP»[132], acronimo di *Traffic Light Protocol*. Si tratta di uno standard internazionale elaborato dal FIRST (*Forum of Incident Response and Security Teams*) per facilitare la condivisione di informazioni potenzialmente sensibili e una più efficace collaborazione[133].

Difatti, salve le ipotesi in cui lo scambio informativo sia ritenuto contrario «agli interessi essenziali della propria sicurezza»[134] e quindi gli Stati possono rifiutarsi di fornire informazioni a qualsiasi organizzazione dell'Unione, a livello generale, il traffico delle informazioni di cyebersicurezza è solitamente gestito dal citato standard TLP, costituito da «un insieme di quattro etichette utilizzate per indicare i limiti di condivisione che i destinatari devono applicare»[135].

Nello specifico tali etichette sono rappresentate da quattro colori: il rosso, rappresenta la massima restrizione ed indica le informazioni non divulgabili al pubblico ma solo a singoli destinatari in quanto potrebbero compromettere la riservatezza delle persone fisiche, i segreti, la reputazione o il *business* dell'organizzazione; giallo, indica le informazioni la cui divulgazione è limitata all'organizzazione e ai suoi clienti con l'avvertenza che la loro circolazione debba essere soggetta a particolari garanzie quando il trasferimento di queste possa compromettere la riservatezza delle persone fisiche, i segreti, la reputazione o il *business* dell'organizzazione; verde, indica le informazioni che possono essere diffuse tra i membri del circuito informativo a cui appartiene la piattaforma di CTI, solitamente si tratta di informazioni utili ad aumentare la consapevolezza (*awareness*) all'interno della loro comunità. Non ci sono invece restrizioni per le informazioni che comportano un rischio minimo o nullo di uso improprio, in conformità alle norme e alle procedure applicabili per la divulgazione al pubblico.

b) La protezione europea dei dati personali contenuti nelle informazioni di cybersicurezza

È innanzitutto doveroso distinguere quando le informazioni oggetto di trasferimento per motivi di cybersicurezza possano o meno rientrare nelle discipline europee sul trattamento dei dati personali. Pare allora utile partire dalla definizione contenuta all'art. 4, par. 1, n. 1, del regolamento (UE) 2016/679 (anche noto come GDPR) secondo cui per «dato personale» deve intendersi «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")» che può essere «identificata, diretta-

131 Cfr. art. 29, par. 2, Direttiva NIS II.

132 Cfr. considerando 9, nonché art. 10, par. 7, della Direttiva NIS II.

133 Il FIRST è un forum globale che riunisce i team di risposta agli incidenti di sciurezza informatica, creato negli Stati Uniti nel 1989 a seguito della istituzione del primo CERT.

134 Cfr. art. 346, leet. a), del TFUE.

135 La definizione è stata tratta dal sito del FIRST.

mente o indirettamente» anche con riferimento a un «identificativo online»[136].

Nei precedenti paragrafi è stata evidenziata la natura perlopiù tecnica delle informazioni cybersicurezza. Tuttavia, nonostante tale "aspetto", non è da escludersi che queste informazioni possano identificare, o rendere identificabile, una persona fisica (nello specifico, l'attore malevolo che responsabile dell'incidente di sicurezza o anche la vittima dello stesso). E' ad esempio il caso dell'*Internet Protocol* (IP), qualificato come dato personale dalla costante giurisprudenza europea, sia esso dinamico o statico[137], gli indirizzi mail, l'*Uniform Resource Locator* (URL)[138], i nomi di dominio (DNS)[139], ma anche le informazioni bancarie come l'IBAN, nonché l'identificativo fornito per l'utilizzo dei *social networks*.

Appurata l'applicazione della disciplina europea dei dati personali sulle informazioni di cybersicurezza, pare ora opportuno riflettere sull'attività di trattamento che si caratterizza per tre elementi necessari: il titolare del trattamento, ossia «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali [...]» (art. 4, n. 7 GDPR); la, o le, finalità per il quale i dati personali raccolti sono trattati; ed infine il destinatario, ossia «la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi [...]» (art. 4, n. 9, GDPR).

Questa scansione tripartita ci è particolarmente utile per studiare la diversa applicazione delle discipline sul trattamento dei dati personali in riferimento al processo di *cyber information sharing* che, come abbiamo anticipato, vede la partecipazione di soggetti operanti in diversi settori (pubblico/privato, civile/autorità pubblica), e per diverse finalità che vanno dalla salvaguardia dei propri affari della singola organizzazione, fino alla difesa della sicurezza nazionale da parte dei governi, nonché la sicurezza europea e internazionale.

In considerazione di ciò, al fine di facilitarne lo studio, si propone l'analisi di quattro scenari, relativi a: 1) la diffusione di informazioni tra le organizzazioni per mezzo di piattaforme di *cyber information sharing* (o comunque all'interno dei circuiti ISACs); 2) lo scambio di informazioni dalle organizzazioni verso le autorità competenti, punti di contatto unici e i *Computer Security Incident Response Team* (CSIRT), 3) le informazioni acquisite da qualsiasi soggetto (critico e non) e poi trattate dalle autorità di polizia; 4) le informazioni trattate da soggetti diversi dalle forze di polizia ma per finalità di polizia. Precisiamo che le discipline sulla protezione dei dati personali a cui si farà riferimento

---

136 Cfr. art. 4, regolamento (UE) 2016/679.

137 *Ex multis*, si faccia riferimento alla nota sentenza Breyer, CGUE, C-582/14, del 19 ottobre 2016. Sul punto v. anche il parere 4/2007 del Working Party Article 29, sul concetto di dato personale ove viene precisato che «*some sorts of IP addresses which under certain circumstances indeed do not allow identification of the user, for various technical and organizational reasons. One example could be the IP addresses attributed to a computer in an internet café, where no identification of the customers is requested*».

138 v. M. Korse, *Personal Data in URLs*, in *privacywise*, 23 agosto 2017.

139 L'*Internet Corporation for Assigned Names and Numbers* (ICANN), che gestisce il *Domain Name System* (DNS), è responsabile anche della gestione del registro WHOIS, una banca dati pubblica secondo cui chiunque abbia un dominio web deve registrare non solo il proprio dominio, ma anche i propri nomi, indirizzi, indirizzi e-mail e numeri di telefono. Sul punto v. S. Vaughan-Nichols, *DNS is about to get into a world of trouble with GDPR*, in *Zdnet*, 18 aprile 2018.

sono pertanto: il già citato regolamento (UE) 2016/679; la direttiva (UE) 2016/680 (anche nota come "direttiva Polizia") relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali; ed infine, il regolamento (UE) 2018/1725 che stabilisce le norme applicabili al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione europea, ed infine il regolamento (UE) 2016/794, che disciplina il trattamento dei dati personali da parte dell'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol).

Sebbene ognuna di queste normative abbia un differente campo applicativo, sono tuttavia ispirate al medesimo corpo di principi sul trattamento dei dati personali ove, primo fra tutti, trova spazio il principio di «liceità, correttezza e trasparenza»[140], da cui discende la questione sulla selezione delle basi di legittimità, ossia le condizioni che rendono il trattamento di dati personali conforme alla legge e quindi lecito.

Partendo dallo scenario 1), i citati provvedimenti europei in materia di diritto dei dati personali non forniscono indicazioni precise al riguardo. Anche la proposta di Regolamento *EU Cyber Solidarity Act*, al considerando 22, fa un generico richiamo al rispetto delle «*existing legal requirements and in particular Union and national data protection law, as well as the Union rules on competition governing the exchange of information*».

L'esigua dottrina sul punto ha individuato la legittimità del trasferimento delle informazioni di cybersicurezza tra organizzazioni pubbliche e private nei circuiti di *cyber sharing* nella base contenuta all'art. 6, par. 1, lett. f) del GDPR relativa al «legittimo interesse del titolare del trattamento o di terzi»[141].

Come specificato dal vecchio gruppo dei Garanti, il *Working Party Article* 29, il ricorso alla base dell'interesse legittimo richiede la valutazione di tre elementi per determinare la liceità del trattamento: necessità, legittimità e bilanciamento degli interessi, al termine del quale potrebbe prevalere l'interesse dell'interessato, ossia il soggetto a cui si riferiscono i dati personali, piuttosto che quello del titolare che li tratta[142].

In tale occasione il Gruppo ha inoltre avuto modo di precisare che l'interesse legittimo dei terzi potrebbe essere pertinente quando «il responsabile del trattamento, talvolta incoraggiato dalle autorità pubbliche, persegue un interesse che corrisponde a un interesse pubblico generale o a un interesse dei terzi», come ad esempio nei casi in cui «il responsabile del trattamento va oltre gli obblighi giuridici specifici che è tenuto a rispettare conformemente a leggi e regolamenti al fine di contribuire all'impegno profuso dalle autorità di contrasto e dai soggetti privati per combattere le attività illegali, quali il riciclaggio di denaro, l'adescamento di minori o la condivisione illegale di file online».

---

[140] Cfr. art. 5, par. 1, lett. a) del regolamento (UE) 2016/679; art. 4, par. 1, lett. a) della direttiva (UE) 2016/680; art. 4, par. 1, lett. a) del regolamento (UE) 2018/1725.

[141] C. Sullivan - E.W. Burger, *"In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence*, in *Computer Law & Security Review*, 33(1), 2017, 14 ss. Vedi anche, L.O. Nweke - S. Wolthusen, *Legal Issues Related to Cyber Threat Information Sharing Among Private Entities for Critical Infrastructure Protection*, in *NATO CCDCOE 12th International Conference on Cyber Conflict*, 2020.

[142] Articolo 29 Working Group, *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE*.

Sul punto, pare utile richiamare la lettera del considerando 49 GDPR ove è previsto che «costituisce legittimo interesse del titolare del trattamento interessato trattare dati personali relativi al traffico, in misura strettamente necessaria e proporzionata per garantire la sicurezza delle reti e dell'informazione, vale a dire la capacità di una rete o di un sistema d'informazione di resistere, a un dato livello di sicurezza, a eventi imprevisti o atti illeciti o dolosi che compromettano la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali conservati o trasmessi e la sicurezza dei relativi servizi offerti o resi accessibili tramite tali reti e sistemi da autorità pubbliche, organismi di intervento in caso di emergenza informatica (CERTs), gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRTs), fornitori di reti e servizi di comunicazione elettronica e fornitori di tecnologie e servizi di sicurezza [...]». Nonché anche il considerando 50, ove è previsto che «l'indicazione da parte del titolare del trattamento di possibili reati o minacce alla sicurezza pubblica e la trasmissione dei dati personali pertinenti a un'autorità competente in singoli casi o in più casi riguardanti lo stesso reato o la stessa minaccia alla sicurezza pubblica dovrebbero essere considerate nell'interesse legittimo perseguito dal titolare del trattamento».

Tuttavia, pare opportuno distinguere il caso in cui lo *sharing* avvenga tra le sole organizzazioni partecipanti al circuito informativo, per il quale la base di legittimità del legittimo interesse pare certamente coerente, dal caso in cui lo scambio abbia ad oggetto informazioni tratte da minacce andate a buon fine (incidente). Come anticipato, a seguito dell'entrata in vigore della disciplina NIS, le organizzazioni rientranti nella qualifica di soggetto «essenziale o importante» che siano impattate da un incidente significativo, sono obbligate ad effettuare la notifica alle autorità competenti e/o ai CSIRTs.

In quest'ultimo caso la dottrina ha individuato la diversa base dell'art. 6, par. 1, lett. c) GDPR che legittima il trattamento qualora condotto in adempimento di un obbligo legale al quale è soggetto il titolare del trattamento[143].

Altri studiosi hanno inoltre individuato una ulteriore base di legittimità nella lett. e) dell'art. 6, par. 1, GDPR[144], ritenendo che la raccolta e disseminazione di informazioni cybersicurezza, aventi non necessariamente come destinatari le forze di polizia, costituisca «l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento»[145].

Tuttavia tale orientamento non pare trovare conforto nella lettera del considerando 121 della Direttiva NIS II, ove per il trattamento dei dati personali condotto al fine di garantire la sicurezza dei sistemi informatici e di rete da parte di «soggetti essenziali e importanti» contempla le sole due basi del legittimo interesse e dell'obbligo di legge, precisando che quest'ultima base interviene per legittimare il trattamento di dati personali contenuti nelle notifiche in caso di incidente rilevante. Diversamente per i dati personali contenuti in informazioni di cybersicurezza oggetto di scambio informativo

---

143 A. Albakri - E. Boiten - R. De Lemos., *Sharing Cyber Threat Intelligence Under the General Data Protection Regulation*, in M. Naldi - G.F. Italiano - K. Rannenberg - M. Medina - A. Bourka (eds.), *Privacy Technologies and Policy, 7th Annual Privacy Forum, APF 2019 Rome, Italy, June 13–14, Proceedings*, Berlin, 2019, 28 ss.

144 C. Sullivan - E.W. Burger, *"In the public interest"*, cit.

145 A. Albakri - E. Boiten - R. De Lemos, *Sharing Cyber Threat Intelligence Under the General Data Protection Regulation,* cit.

e notifica non obbligatoria di cui all'art. 30 della direttiva viene indicata la base dell'art. 6, lett. f).

Per quanto riguarda i casi riconducibili allo scenario 2), considerato il ruolo e la natura delle autorità competenti, dei punti di contatto unico e dei CSIRTs, ossia soggetti pubblici che non svolgono compiti e funzioni di polizia, si ritiene che il trattamento dei dati personali contenuti nelle informazioni di cybersicurezza trovi legittimità nell'art. 6, par. 1, lett. c) GDPR, per l'appunto relativo all'interesse pubblico. A titolo esemplificativo, si faccia riferimento alla *privacy policy* del CSIRT Italia ove è espressamente previsto che la «gestione delle segnalazioni inviate dagli utenti ai sensi degli articoli 12, 14 e 18 del Decreto Legislativo n. 65 del 18 maggio 2018 [avviene] sulla base giuridica dell'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento»[146].

Allo stesso modo, anche nel caso in cui la segnalazione provenga da parte delle istituzioni dell'Unione verso il Gruppo di intervento europeo, il CERT-UE, conformemente al regolamento (UE) 2018/1725, la *privacy policy* del Gruppo prevede che «il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri conferiti all'istituzione o all'organismo dell'Unione»[147].

Inoltre, il citato considerando 121 ricorda che, conformemente all'art 9 GDPR, gli Stati membri «potrebbe[ro] stabilire norme che consentano alle autorità competenti, ai punti di contatto unici e ai CSIRT, nella misura necessaria e proporzionata al fine di garantire la sicurezza dei sistemi informatici e di rete dei soggetti essenziali e importanti, di trattare categorie particolari di dati personali», prevedendo a tal fine di adottare misure adeguate e specifiche per tutelare i diritti e gli interessi fondamentali delle persone fisiche, comprese limitazioni tecniche al riutilizzo di tali dati e l'uso di misure all'avanguardia in materia di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita.

Relativamente lo scenario 3), nel caso in cui le autorità di pubblica sicurezza si trovino a dover trattare informazioni di cybersicurezza per fini di «prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica» (cfr. art. 1) trova applicazione la direttiva (UE) 2016/680 (anche nota come Direttiva di polizia)[148].

Precisiamo che sia il GDPR, sia la appena citata Direttiva di polizia, conformemente a quanto previsto dall'art. 16 del TFUE secondo cui l'Unione europea stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale «nell'pesercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione», non trovano applicazione verso quei trattamenti di dati personali svolti per finalità di tutela dell'interesse e della sicurezza nazionale (es. i trattamenti

[146] Si rinvia all'"Informativa sul trattamento dei dati personali" pubblicata sul sito del CSIRT Italia.

[147] Si rinvia alla "*Privacy policy*" pubblicata sul sito del CERT-UE di cui al link: *cert.europa.eu.*

[148] Cfr. art. 2 della direttiva (UE) 2016/680. In particolare, sulla protezione dei dati personali nelle procedure di information sharing da parte delle forze di polizia v. F. Boehm, *Information sharing and data protection in the Area of Freedom, Security and Justice. Towards harmonised data protection principles for EU-internal information exchange*, Springer, 2012.

di dati svolti da parte degli organismi di intelligence per tali fini)[149].

Altra considerazione deve esser fatta per le attività svolte dalle autorità di polizia fuori dai fini indicati dall'art. 1 delle Direttiva di polizia, tra cui vi rientrano «quelle di archiviazione nel pubblico interesse, di ricerca scientifica o storica o per finalità statistiche, a meno che il trattamento non sia effettuato nel contesto di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione» ove trova applicazione il GDPR (art. 9, par. 2).

Si ritiene pertanto necessario approfondire quando le attività di cybersicurezza possano rientrare nel campo applicativo della direttiva, ovvero in quello del regolamento generale.

A tal proposito, il considerando n. 12 della direttiva prevede che le attività di polizia «comprendono anche il mantenimento dell'ordine pubblico quale compito conferito alla polizia o ad altre autorità incaricate dell'applicazione della legge ove necessario per la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati». Mentre, il considerando 27 prevede che il perseguimento dei fini di polizia anzi descritti, renda «necessario che le autorità competenti trattino i dati personali raccolti a fini di prevenzione, indagine, accertamento o perseguimento di specifici reati al di là di tale contesto per sviluppare conoscenze delle attività criminali e mettere in collegamento i diversi reati accertati».

Secondo Nadezhda Purtova, le attività investigative di cybersicurezza, come il tracciamento di una *botnet* o l'individuazione della dimensione e il livello di minaccia di un incidente di sicurezza informatica reale o potenziale, possono certamente rientrare - in linea di principio - negli ambiti appena descritti e quindi nel capo applicativo della Direttiva di polizia[150].

Per quanto riguarda la legittimità dei trattamenti svolti per tali finalità, l'art. 8 prevede che siano gli Stati membri a disporre se il trattamento sia lecito, specificando anche gli obiettivi del trattamento, i dati personali da trattare e le finalità dello stesso[151]. Pertanto, deve ritenersi che tale condizione sia alla base dei trattamenti di dati personali interessati dalla *cyber information sharing* tra le autorità di polizia degli Stati membri.

Tuttavia, a tale scambio informativo non partecipano solo le competenti autorità nazionali, ma anche organismi di polizia sovranazionali, come l'Europol, ed in particolare l'unità specializzata contro la criminalità informatica EC3 attiva dal 2013.

Considerato che l'Unità opera presso l'Europol, il trattamento dei dati personali con-

---

149 Tuttavia, come rilevano J. Sajfert, T Quintel, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*, in *SSRN*, 2017, le agenzie di intelligence possono trovarsi a trattare dati personali anche per le finalità coperte dal campo applicativo della Direttiva di polizia che quindi ne troverebbe applicazione. Questo problema diventa ancora più rilevante nel contesto della condivisione delle informazioni tra le agenzie di intelligence nazionali e le forze di polizia.

150 N. Purtova, *Between the GDPR and the Police Directive: Navigating Through the Maze of Information Sharing in Public-Private Partnerships*, in *International Data Privacy Law*, 2018; D. Drewer - V. Miladinova, *The BIG DATA Challenge: Impact and opportunity of large quantities of information under the Europol Regulation*, in *Computer Law & Security Review*, 33, 2017, 298 ss.; T. Quintel, *Interoperable Data Exchanges Within Different Data Protection Regimes: The Case of Europol and the European Border and Coast Guard Agency*, in *European Public Law,* 2020, 205 ss.

151 Cfr. art. 8, direttiva (UE) 2016/680.

tenuti nelle informazioni di cybersicurezza da parte dell'Unità trova solida disciplina nel regolamento istitutivo l'Agenzia, il n. 794 del 2016[152], che cita il contrasto alla criminalità informatica tra gli obbiettivi dell'Europl[153]. Pertanto è al regolamento di quest'ultimo che faremo riferimento per analizzare la disciplina relativa al trattamento dei dati personali da parte di EC3.

Come si apprende dal testo di legge, un elemento importante nella lotta contro la criminalità informatica è l'applicazione SIENA (*Secure Information Exchange Network Application*), la rete sicura per lo scambio di informazioni e dati personali dell'Europol, finalizzata a garantire la protezione e i requisiti di sicurezza i tali informazioni scambiate tra Stati membri, Europol, altri organismi dell'Unione (art. 24), paesi terzi e organizzazioni internazionali (art. 25)[154].

Trattandosi di un sistema di scambio che vede Europol nel ruolo di intermediario, è bene distinguere i trasferimenti di dati personali in entrata, da parte di soggetti segnalanti, dai trasferimenti in uscita, verso i soggetti che potrebbero essere interessati dall'evento di sicurezza in questione.

Relativamente ai primi, tali dati possono essere forniti dagli Stati membri, e successivamente trasferiti dall'Europol sull'esclusiva base del loro consenso, liberamente revocabile in qualsiasi momento (art. 23, par. 6), ovvero, da parti private e pervenuti all'Europol per mezzo di un'unità nazionale, punto di contatto di un paese terzo o un'organizzazione internazionale con cui Europol ha concluso un accordo di cooperazione, nonché un'autorità di un paese terzo o un'organizzazione internazionale che forma oggetto di una decisione di adeguatezza (art. 26).

Una volta raccolti, al fine di raggiungere i suoi obiettivi, Europol può trattare dati personali per sole finalità «determinate, esplicite e legittime» (art. 28) consistenti in:

a) controlli incrociati diretti a identificare collegamenti o altri nessi pertinenti tra informazioni concernenti: i) persone sospettate di aver commesso un reato di competenza di Europol o di avervi partecipato, o che sono state condannate per un siffatto reato; ii) persone riguardo alle quali vi siano indicazioni concrete o ragionevoli motivi per ritenere che possano commettere reati di competenza di Europol; b) analisi strategiche o tematiche; c) analisi operative; d) facilitazione dello scambio d'informazioni tra Stati membri, Europol, altri organismi dell'Unione, paesi terzi e organizzazioni internazionali.

Per quanto riguarda la disseminazione presso i destinatari, l'Agenzia può trasferire i dati personali a: un organismo dell'Unione, nella misura in cui tale trasferimento sia necessario allo svolgimento dei suoi compiti o dei compiti dell'organismo dell'Unione destinatario (art. 24); a un'autorità di un paese terzo o a un'organizzazione internazionale, purché vi sia una decisione di adeguatezza adottata dalla Commissione ai sensi

[152] Regolamento (UE) 2016/794, che istituisce l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (EUROPOL) e sostituisce e abroga le decisioni del Consiglio 2009/371/GAI, 2009/934/GAI, 2009/935/GAI.

[153] Cfr. art. 3, regolamento (UE) 2016/794. Si faccia inoltre riferimento al rapporto EC3, *First year report*, 2013, 6, ove è espressamente previsto che «[f]ortunately the existing Europol framework, including its legal basis, corporate structure and information processing tools, offered a solid basis», nonché D. Drewer - J. Ellermann, *Europol's data protection framework as an asset in the fight against cybercrime*, 2012.

[154] Cfr. considerando 24, regolamento (UE) 2016/794.

dell'art. 36 della Direttiva di polizia, un accordo internazionale concluso tra l'Unione e tale paese terzo o organizzazione internazionale ai sensi dell'articolo 218 TFUE, un accordo di cooperazione che consenta lo scambio di dati personali (art. 25); nonché alle parti private, «se non in singoli casi, ove sia strettamente necessario» (art. 26, par. 5).

L'ultimo scenario (4), riguarda i soggetti tenuti a collaborare con le forze di polizia, o svolgere compiti di polizia, i quali quindi si trovano a dover trattare dati personali per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica.

A tal proposito, la Direttiva di polizia, all'art. 3, par. 7, contempla nella definizione di «autorità competente» non solo le forze pubbliche di polizia (lett. a), ma anche «qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica e i poteri pubblici» per i fini anzidetti (lett. b)[155].

Sul regime d'applicazione, il considerando 11 della direttiva è chiaro: «[q]ualora tale organismo o entità trattino dati personali per finalità diverse da quelle della presente direttiva, si applica il regolamento (UE) 2016/679». Invece, nei casi rientranti nell'ambito applicativo della direttiva (UE) 2016/680 tali soggetti «dovrebbero essere vincolati da un contratto o altro atto giuridico e dalle disposizioni applicabili ai responsabili del trattamento» in modo da vincolarli al rispetto degli obblighi e garanzie contemplati dalla stessa[156].

In quest'ultima ipotesi, il considerando 11 fa quindi un implicito riferimento ai trattamenti di dati personali che trovano base legale nell'esecuzione di contratti di cui all'art. 6, par. 1, lett. b), del GDPR. Condizione che porta ad una necessaria co-titolarità del trattamento tra parte privata e autorità di polizia in cui entrambe le parti decidono congiuntamente sulla necessità del trasferimento: l'autorità competente determina che ha bisogno dei dati e l'ente privato decide di rispettare la richiesta.

Come già osservato in precedenza (infra 4.3), nel particolare caso degli scambi di informazioni di cybersicurezza, tali rapporti tra parti private e autorità di polizia trova espressione all'interno di appositi partenariati pubblico-privati. Secondo Nadezhda Purtova, il quadro legislativo europeo sul punto non pare fornire certezza sulla disciplina da applicare nel caso di trattamento congiunto dei dati personali sia da parti private, sia da parte di forze di polizia[157]. Salvo concludere poi che: «*[w]hile GDPR lays down general data protection rules, the Police Directive operates as lex specialis. This means that when it comes to processing for the law enforcement purposes, GDPR forms a 'safety net' that in principle should*

[155] Cfr. art. 3, par. 7, lett. b), direttiva (UE) 2016/680.

[156] A tal proposito il considerando 11 prevede che ad esempio, «a fini di indagine, accertamento o perseguimento di reati, gli istituti finanziari conservano determinati dati personali da essi trattati, e li trasmettono solo alle autorità nazionali competenti in casi specifici e conformemente al diritto dello Stato membro». Ulteriore esempio di «altro organismo o entità» che tratta dati personali per conto delle autorità di polizia è il laboratorio privato forense che svolge analisi delle prove nei procedimenti penali su incarico di un tribunale, pubblico ministero o della polizia. Anche il fornitore di servizi *cloud* che fornisce in base a un contratto un servizio di archiviazione dei tribunali archivi digitali è un altro esempio, e avrebbe lo stato di un elaboratore sotto la direttiva.

[157] N. Purtova, *Between the GDPR and the Police Directive,* cit., 34.

'catch' all data processing for law enforcement purposes when the Police Directive does not apply»[158].

7. Considerazioni conclusive sul processo di integrazione della cybersicurezza europea

Sebbene per molto tempo il tema della sicurezza, così come anche quello della difesa ad essa collegato, siano rimasti fuori dal processo di integrazione europea, ciò non impedisce di considerare la questione della sicurezza come rilevante per l'avvio del processo di integrazione[159].

L'argomento ha assunto considerevole importanza a seguito del progressivo impatto delle politiche europee a livello internazionale, nonché dei recenti risvolti geopolitici. Tuttavia, nonostante il tema sia avvertito come una «impellente necessità»[160], neppure l'accelerazione delle politiche di difesa e sicurezza comune a seguito della Brexit del 2016 si sono rivelate col tempo idonee alla costruzione di un adeguato apparato difensivo[161].

Le difficoltà di mettere a punto una politica estera in senso tradizionale nel contesto europeo si accompagnano infatti alla difficoltà di definire la sicurezza interna dell'Unione. Le differenze culturali, le questioni politiche e le divergenze di interessi tra gli Stati membri hanno spesso rappresentato un ostacolo ad una collaborazione partecipata in questi ambiti.

La cooperazione per fini di cybersicurezza rappresenta uno dei fondamentali principi per la prevenzione e miglior gestione degli incidenti informatici e, come evidenziato nel corso della trattazione, necessita non solo del pieno coinvolgimento degli Stati membri, e quindi dei poteri pubblici, ma anche del settore privato, particolarmente presente nel cyberspazio.

Precedentemente, si è introdotto il tema della privatizzazione della sicurezza quale effetto della "crisi" del paradigma weberiano, secondo cui è il solo Stato ad essere titolare del legittimo uso della forza. Tuttavia, si è anche mostrato come questo fenomeno non abbia portato alla totale scomparsa dei poteri pubblici nella soddisfazione di pretese securitarie quanto piuttosto alla formazione di rapporti cooperativi di quest'ultimi con il settore privato.

L'analisi della *cyber information sharing* nel contesto delle politiche europee di cybersicurezza ha posto in evidenza il recente orientamento di "europeizzazione" di metodi e strumenti di natura generalmente privata. Si faccia riferimento ai citati esempi relativi alla creazione del SOC europeo, l'istituzione dei registri di vulnerabilità e debolezze, nonché, più in generale, la previsione di processi di gestione del rischio di ispirazione tecnica, incorporati all'interno di fonti di diritto derivato che ne impongono l'obbliga-

158 *Ivi*, 41.

159 A ben vedere dal Trattato di Schuman deduciamo che fosse stato proprio il porre rimedio alla rivalità franco-tedesca ad aver stimolato l'avvio del processo di integrazione.

160 B. Caravita, *Difesa europea, quali prospettive*, in *federalismi.it*, 1, 2019. V. anche M. Vellano - A. Miglio (a cura di), *Sicurezza e difesa comune dell'Unione europea*, Milano, 2022.

161 Cfr. M. Frau, *I nodi irrisolti della difesa comune europea. Una prospettiva federalista*, in *federalismi.it*, 6, 2022.

toria osservanza per una determinata categoria di soggetti[162].

Elementi questi che lascerebbero intravedere una nuova tendenza, certamente evolutiva dei rapporti tra pubblico e privato in questo settore, ove l'Unione europea non solo coopera, e co-regola, con il settore privato ma, da una parte, inizia ad occupare spazi prima appartenenti a questi, dall'altra ne funzionalizza l'operato al perseguimento di interessi pubblici[163].

Emblematico esempio di questo processo può essere colto sul piano normativo dalla definizione di "cybersicurezza europea", introdotta al culmine di un lungo processo che ha preso avvio con la disciplina sulla protezione delle infrastrutture critiche.

Ripercorrendo brevemente le tappe più significative di questo percorso[164], già nel 2001 la Commissione europea adottava una Comunicazione sulla criminalità "informativa" ove veniva data la definizione di «sicurezza dei sistemi informatici e di rete» facendo riferimento alla «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»[165].

Nel 2004, anno in cui veniva istituita l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), il Consiglio europeo lanciava lo *European Program for Criminal Infrastructure Protection* (EPCIP) con lo scopo di incrementare la prevenzione, la preparazione e la risposta europea agli atti di terrorismo informatico attraverso l'istituzione di una rete di *information sharing* per la protezione delle infrastrutture critiche (la *Critical Infrastructure Warining Information Network* - CIWIN), nonché per l'erogazione di finanziamenti per la realizzazione di progetti sulla protezione delle infrastrutture critiche e il varo di una normativa riguardante le infrastrutture critiche europee che avverrà poi nel 2008 con la direttiva 2008/114/CE relativa all'individuazione e designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la loro protezione[166].

---

[162] Sull'incorporazione v. D. Siclari, *Contributo allo studio della sussunzione legislativa di regole formate dai privati*, in *Studi in onore di Vincenzo Atripaldi*, Vol. I, 2010, 275 ss.

[163] Sul punto si faccia riferimento alla recente proposta di modifica del regolamento (UE) 1025/2012 relativo alle decisioni delle organizzazioni europee di normazione relative alle norme europee e ai prodotti, avanzata dalla Commissione europea il 2 febbraio 2022, ove è espressamente previsto che «nei casi in cui le organizzazioni europee di normazione [quali organizzazioni private] si concentrano sul sostegno alla legislazione e alle politiche dell'UE, sono necessarie garanzie per assicurare una procedura corretta e una rappresentanza equilibrata degli interessi delle parti, coerentemente con le priorità strategiche e le esigenze legislative [...]. Questo aspetto è ancora più importante in quanto alcune organizzazioni europee di normazione sono composte principalmente da operatori economici che hanno diritto di voto e la partecipazione delle organizzazioni della società civile e delle autorità pubbliche è limitata in alcuni casi».

[164] Sul punto v. A. Rotondo, *Cyber security e protezione delle infrastrutture critiche: l'efficacia del modello europeo*, in S. Marchisio - U. Montuoro (a cura di), *Lo spazio cyber e cosmico. Risorse dual use per il sistema Italia in Europa*, Torino, 2019, 125.

[165] Cfr. art. 2, c. 1. COM(2000)890 del 26 gennaio 2001, Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione mediante la lotta alla criminalità informativa.

[166] In particolare, all'art. 2, lett. e), direttiva 2008/114/CE viene fornita la definizione di «protezione» come «tutte le attività volte ad assicurare funzionalità, continuità e integrità delle infrastrutture critiche per evitare, mitigare e neutralizzare una minaccia, un rischio o una vulnerabilità».

Nella Comunicazione sulla protezione delle infrastrutture critiche informatizzate del 2011[167], la Commissione constatava l'insufficienza delle strategie nazionali di cybersicurezza e della resilienza dei loro sistemi e invitava gli Stati ad adottare una serie di misure basate sulla cooperazione transfrontaliera portando così all'esigenza di adottare uno specifico intervento armonizzato relativamente alla protezione delle infrastrutture critiche informatizzate.

Nel 2016 viene adottata la prima normativa sullo specifico tema della «sicurezza delle reti e dei sistemi informativi» con la direttiva (UE) 2016/1148, per l'appunto anche nota come direttiva *Network and Information Security*- NIS, oggi abrogata dalla richiamata direttiva (UE) 2022/2555 (Direttiva NIS II) entrata in vigore il 17 gennaio 2023.

Tuttavia, nonostante la rubricazione, dall'analisi dei testi emerge come il legislatore europeo abbia inteso coniugare ancora una volta la sicurezza informatica con la protezione delle infrastrutture critiche. Difatti, parte delle prescrizioni volte a «garantire un livello comune elevato di cybersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno» (art. 1), consistono perlopiù in una serie di obblighi gravanti sui soggetti individuati nella direttiva come "critici", che dovranno adempierli a pena di ingenti sanzioni amministrative[168].

Solo con il successivo regolamento (UE) 2019/881, relativo all'ENISA e alla certificazione della cybersicurezza per le tecnologie dell'informazione e della comunicazione (c.d. *Cybersecurity Act*), l'Unione ha introdotto - per la prima volta all'interno di un atto normativo giuridico - la nozione di cybersicurezza, definendola all'art. 2, n. 1, come «insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche»: nozione che è stato poi declinata negli ordinamenti dei diversi Stati membri[169].

Dal breve quadro tracciato emerge innanzitutto la distinzione fondamentale tra i due concetti di «cybersicurezza» e di «sicurezza dei sistemi informatici e di rete»[170]: mentre

---

[167] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa alla Protezione delle infrastrutture critiche informatizzate. Realizzazioni e prossime tappe: verso una sicurezza informatica mondiale, Bruxelles, 31 gennaio 2011.

[168] Sulla "delega" della sicurezza dal potere pubblico agli amministrati seppur nell'ottica della cybersicurezza nazionale italiana v. A. Monti, *Internet e ordine pubblico*, in G. Cassano - S. Previti (a cura di), *Il diritto di internet nell'era digitale*, Milano, 2020, 79, ove l'A. scrive «[...] chi è responsabile del funzionamento dei servizi essenziali deve farsi carico in proprio della loro difesa, sopportando le conseguenze del mancato rispetto di complessi obblighi tecnici e organizzativi in termini di sanzioni amministrative particolarmente afflittive».

[169] Cfr. con la nozione di "cybersicurezza nazionale" introdotta in Italia per la prima volta con il decreto-legge n. 82/2021, all'art. 1, c. 1, lett. a) come «insieme delle attività, fermi restando le attribuzioni di cui alla legge 3 agosto 2007, n. 124, e gli obblighi derivanti da trattati internazionali, necessarie per proteggere dalle minacce informatiche reti, sistemi informativi, servizi informatici e comunicazioni elettroniche, assicurandone la disponibilità, la confidenzialità e l'integrità e garantendone la resilienza, anche ai fini della tutela della sicurezza nazionale e dell'interesse nazionale nello spazio cibernetico». Sul punto sia concesso rinviare F. Serini, *La nuova architettura di cybersicurezza nazionale: note a prima lettura del decreto-legge n. 82 del 2021*, in f*ederalismi.it,* 12, 2022.

[170] Cfr. art. 6, c. 1, n. 2 della Direttiva NIS II, che definisce la sicurezza dei sistemi informatici e di rete come «la capacità dei sistemi informatici e di rete di resistere, con un determinato livello di confidenza, agli eventi che potrebbero compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o elaborati o dei servizi offerti da tali sistemi informatici e di rete o accessibili

con quest'ultimo concetto, originariamente, sorto nel contesto delle norme tecniche, si intende garantire la continuità del servizio erogato e la protezione delle informazioni trattate dal soggetto fornitore (tra cui possono rientrare anche i dati personali) al fine di «migliorare il funzionamento del mercato interno»; le attività di cybersicurezza, che comprendono anche la sicurezza delle reti e dei sistemi informatici, sono invece dirette alla più ampia «sicurezza degli individui nel cyberspazio»[171].

A nostro parere, con questa formulazione il legislatore europeo, oltre ad aver inserito la definizione la cybersicurezza all'interno di un atto normativo vincolante, è andato al di là del mero significato tecnico della materia (ossia la tutela della riservatezza, integrità e disponibilità delle risorse informatiche e delle informazioni), giungendo al concetto di sicurezza dell'umano, secondo Alcuni riconducibile alla sicurezza dello Stato[172].

Tale definizione può pertanto essere intesa come la proclamazione di un impegno politico dell'Unione e degli Stati membri «ad assicurare una disciplina della tecnologia informatica che assicuri il rispetto delle regole democratiche necessarie alla sopravvivenza della democrazia rappresentativa propria dello Stato costituzionale»[173]. Ricostruzione che appare coerente con l'indirizzo dettato a livello internazionale dal Consiglio d'Europa con l'*Internet Governance Strategy 2016-2019* ove, a proposito della definizione di principi e regole per la *governance* di Internet, si propone di «to ensure that public policy for the Internet is people-centred, meaning that it should respect the core values of democracy, human rights and the rule of law»[174].

Tuttavia, questo processo implica una ulteriore richiesta di sovranità da parte dell'Unione europea, oltre quella già conferita dagli Stati membri nei Trattati. Come intuibile dall'analisi del concetto giuridico di cybersicurezza europea, pare che il citato processo di europeizzazione vada oltre l'obiettivo di «migliorare il funzionamento del mercato interno», non interessando quindi solo l'occupazione da parte dell'Unione di spazi prima di competenza dei privati, ma anche di spazi presidiati dagli Stati per decenni.

Il progressivo accentramento dei poteri in seno all'Unione a cui stiamo assistendo deve essere interpretato alla luce del dibattuto obiettivo sul raggiungimento della "sovranità digitale europea"[175]: concetto che, sebbene dai documenti di natura politica in cui viene

---

attraverso di essi». E' opportuno notare che tale definizione richiama alcuni concetti fondamentali della *computer* e *information security* relativi alle tre proprietà fondamentali delle risorse informatiche e delle informazioni affinché queste possano essere considerate sicure, ossia, la loro riservatezza (*confidentiality*), integrità (*integrity*) e disponibilità (*availability*), spesso indicate con l'acronimo R.I.D (o C.I.A. in lingua inglese).

171 G. Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy,* Londra, 2019, 187.

172 L. Axworthy, *La sécurité humaine: la sécurité des individus dans un monde en mutation*, in *Politique étrangére*, 64(2), 1999, n 333 ss., ove l'A. scrive «*La sécurité humaine ne supplante pas la sécurité nationale [...]. Dan cette prospective, la sécurité humaine et la sécurité de l'État se complènt l'une l'autre*».

173 G. de Vergottini, *Sicurezza e diritti fondamentali,* in L.E.R. Vega - L. Scaffardi - I. Spigno, *I diritti fondamentali nell'era della digital mass surveillance*, cit., 28.

174 Consiglio d'Europa, *Internet governance - Strategy 2016-2019. Democracy, human rights and the rule of law in the digital world*, adottato dal *Committee of Ministers Deputies Meeting,* del 30 marzo 2016.

175 L. Floridi, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Philos. Technol*, 2020, 369 ss.; H. Roberts - J. Cowls - F. Casolari - J. Morley - M. Taddeo - L. Floridi, *Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies*, in *Internet Policy Review*, 6, 2021, G. Finocchiaro, *La sovranità digitale*, in *Dir. pubbl.*, numero tematico, 3, 2022.

utilizzato coincide con la capacità dell'Unione di eliminare la dipendenza tecnologica e usare la tecnologia europea per far funzionare il mercato interno, dall'analisi delle fonti di diritto derivato proiettate verso tale fine sembrano emergere mete ulteriori.
È il caso della citata Direttiva NIS II, e del regolamento istitutivo l'ENISA, le cui basi di legittimità sono state individuate nell'art. 114 TFUE, relativo al ravvicinamento delle legislazioni degli Stati membri «al fine di migliorare il funzionamento del mercato interno». Secondo Alcuni un simile fondamento giuridico potrebbe sollevare criticità dato che «il centro di gravità di queste misure è costituito dal rafforzamento della sicurezza»[176], piuttosto che dal rafforzamento del mercato interno.
In conclusione, ci si chiede se il processo d'integrazione della sicurezza europea, che vede ancora forti resistenze nell'attuazione di pratiche di scambio informativo da parte dalle autorità pubbliche di contrasto e soprattutto da parte del settore privato variamente coinvolti nei processi di cybersicurezza, possa far fronte alle attuali esigenze dettate dal rapporto sempre più stretto tra le società europee e l'informatica..

[176] Cfr. S. Poli, *Il rafforzamento della sovranità tecnologica europea e il problema delle basi giuridiche*, in *I Post di AISDUE, III, 2021, Sezione Atti Convegni AISDUE*, 5, 20 dicembre 2021, 78-79.