Freedom, Security & Justice: European Legal Studies

Rivista quadrimestrale on line
sullo Spazio europeo di libertà, sicurezza e giustizia

2021, n. 1

EDITORIALE SCIENTIFICA
ES

Rivista scientifica on line "Freedom, Security & Justice: European Legal Studies"
www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario
2021, n. 1

FOCUS

20 años de la Carta de derechos fundamentales de la UE. Su aplicación por los Tribunales Españoles

Il Focus contiene i testi rivisti di alcune delle relazioni tenute in occasione del Convegno internazionale organizzato presso l'Universidad Pompeu Fabru di Barcellona (28/29 settembre 2020)

IL COORDINAMENTO DELLE POLITICHE PER LA *CYBERSECURITY* DELL'UE NELLO SPAZIO DI LIBERTÀ, SICUREZZA E GIUSTIZIA

Daniela Marrani*

SOMMARIO: 1. Considerazioni introduttive. – 2. Le politiche per la *cybersecurity* dell'UE. – 3. Il nuovo quadro giuridico sulla *cybersecurity* europea. – 4. Le misure restrittive nell'ambito della PESC. – 5. Il coordinamento delle politiche per la *cybersecurity* dell'UE. – 6. Conclusioni.

1. Considerazioni introduttive

Il susseguirsi di minacce di varia natura alla vita e al benessere dei cittadini europei, alle imprese e alle istituzioni, mette in crisi i sistemi di risposta degli Stati membri e dell'UE e non si limita più da qualche anno al terrorismo internazionale o alla criminalità organizzata, per citare solo i fenomeni più rilevanti, ma abbraccia un ventaglio molto esteso di rischi che riguardano, tra l'altro, l'ambiente e i cambiamenti climatici, gli attacchi e gli incidenti informatici e da ultimo la salute, nell'attuale dilagare della pandemia da COVID-19.

La nozione di sicurezza dell'Unione europea quale emerge dagli orientamenti recenti, in linea con la prassi internazionale in tema di "sicurezza cooperativa" e di "sicurezza umana"[1], è molto ampia e non coincide con il perseguimento della pace e sicurezza internazionali nell'ambito della PESC. Come è stato delineato dalla Strategia globale per politica estera e di sicurezza dell'UE nel 2016[2], e ribadito nei successivi orientamenti dalla Commissione europea e dall'Alto Rappresentante per gli affari esteri e la politica di sicurezza, la dimensione interna ed esterna della sicurezza sono interconnesse. Di conseguenza, la *sicurezza* è disciplinata in maniera unitaria negli orientamenti generali delle Istituzioni, salvo trovare attuazione in strumenti giuridici

Articolo sottoposto a doppio referaggio anonimo.

* Ricercatore di Diritto internazionale e Docente di Diritto dell'Unione europea, Università degli Studi di Salerno. Indirizzo e-mail: dmarrani@unisa.it.

[1] In argomento, si vedano, tra gli altri, R. COHEN, *Cooperative Security: From Individual Security to International Stability*, *Marshall Center Papers*, n. 3, aprile 2001, reperibile *on-line* e L. AXWORTHY, *La sécurité humaine: la sécurité des individus dans un monde en mutation*, in *Politique étrangère*, 1999, n. 64-2, p. 337.

[2] Consiglio dell'Unione europea, *Una strategia globale per la politica estera e di sicurezza dell'Unione europea*, Bruxelles, 28 giugno 2016, https://eeas.europa.eu/topics/eu-global-strategy_en.

specifici per ogni diversa politica. In particolare, il nuovo approccio della Commissione europea alle crisi che riguardano la "sicurezza" è fondato sul concetto di "resilienza" trasversale a diverse politiche[3].

Un esempio recente è costituito dalla *strategia dell'UE in materia di cibersicurezza per il decennio digitale* del 16 dicembre 2020[4] la quale, nel suggerire una serie di azioni e di strumenti per fronteggiare le minacce informatiche, mira al contempo alla salvaguardia dei diritti e delle libertà fondamentali. Se, da un lato, l'obiettivo consiste nello sviluppare la resilienza delle infrastrutture, capacità operative volte alla prevenzione, alla dissuasione, e alla risposta nonché forme di cooperazione strategica al livello internazionale per favorire un ciberspazio aperto e sicuro, dall'altro lato, la strategia è integrata ad altri strumenti di diversa natura e finalità coerenti con i suoi obiettivi. Questi ultimi riguardano, in particolare, il documento *Plasmare il futuro digitale dell'Europa*[5], il *piano per la ripresa europea* della Commissione[6], la *strategia dell'UE per l'Unione della sicurezza*[7], la *strategia globale per la politica estera e di sicurezza dell'Unione europea*[8] e l'*Agenda strategica del Consiglio europeo 2019-2024*[9].

Dalla varietà degli obiettivi e delle competenze esercitate dall'Unione europea al fine di perseguire la *cybersecurity*, intesa come «*l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche*»[10], emerge un'esigenza primaria di coerenza (artt. 13, par. 1 TUE e 7 TFUE)[11] che si riflette nella necessità di un coordinamento tra politiche diverse al fine di perseguire un'efficace azione dell'UE[12]. In questo senso la

[3] Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Relazione 2020 in materia di previsione. Previsione strategica: tracciare la rotta verso un'Europa più resiliente*, Bruxelles, 9 settembre 2020, COM(2020) 493 final.
[4] Comunicazione congiunta al Parlamento europeo e al Consiglio, *La strategia dell'UE in materia di cibersicurezza per il decennio digitale*, Bruxelles, 16 dicembre 2020, JOIN(2020) 18 final.
[5] Comunicazione della Commissione, *Plasmare il futuro digitale dell'Europa*, del 19 febbraio 2020, COM(2020) 67 final.
[6] Comunicazione della Commissione, *Il momento dell'Europa: riparare i danni e preparare il futuro per la prossima generazione*, Bruxelles, del 27 maggio 2020, COM(2020) 456 final.
[7] COM(2020) 605 final. Cfr. nota 25.
[8] Cfr. nota 2.
[9] ttps://www.consilium.europa.eu/it/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/.
[10] Art. 2 (Definizioni), n. 1, Regolamento (EU) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013, in *GUUE* L 151 del 7 giugno 2019, p. 32.
[11] L'art. 7 TFUE recita: "*L'Unione assicura la coerenza tra le sue varie politiche e azioni, tenendo conto dell'insieme dei suoi obiettivi e conformandosi al principio di attribuzione delle competenze*".
[12] Come ha sottolineato di recente la Commissione nella Comunicazione della Commissione al Parlamento europeo e al Consiglio *Prima relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza*, COM(2020)797 final del 9 dicembre 2020: "La minaccia rappresentata dalle reti terroristiche transnazionali dimostra chiaramente che un'azione coordinata dell'UE è indispensabile per un intervento che protegga efficacemente gli europei, sostenendo i nostri valori comuni e lo stile di vita europeo. La situazione attuale indica la comparsa di minacce alla sicurezza transfrontaliere e intersettoriali sempre più complesse, che rendono ancora più essenziale una maggiore cooperazione in materia di sicurezza a tutti i livelli. Questo vale per la criminalità organizzata o il traffico di droga, ma

cybersecurity costituisce, secondo alcuni, un nuovo settore d'intervento (o una nuova "disciplina")[13], che tuttavia non è fondata su una distinta e specifica competenza attribuita dai Trattati[14]. Considerata la varietà di iniziative, anche normative, che compongono un quadro giuridico frammentario e in rapida evoluzione, il presente contributo si propone di esaminare il coordinamento tra le politiche dei Trattati con l'obiettivo di realizzare la *cybersecurity* nello spazio di libertà, sicurezza e giustizia.

2. Le politiche per la *cybersecurity* dell'UE

L'interesse collettivo degli Stati, più volte ribadito al livello internazionale, di un *cyberspace* aperto, progettato per dare a tutti la possibilità di esprimersi liberamente e di scambiarsi idee e informazioni, si scontra con le possibilità di *dual use* della Rete[15] e con l'emergere di minacce sempre più complesse alla sicurezza (c.d. minacce ibride) e al sistema dei diritti e delle libertà fondamentali, quali valori dell'Unione europea. Il problema dell'utilizzo malevolo della Rete richiede una intensa cooperazione in materia penale tra le autorità nazionali, di polizia e giudiziarie degli Stati membri dell'UE. Si tratta di una minaccia per la sicurezza nello spazio di libertà, sicurezza e giustizia (art. 67, par. 3 TFUE), resa più problematica dall'accelerazione dell'utilizzo delle tecnologie digitali in ragione delle limitazioni alla libertà di circolazione e di movimento delle persone imposte dalla pandemia da COVID-19.

La cooperazione a livello regionale europeo (a differenza dei risultati ottenuti in questa materia a livello globale)[16] ha portato all'adozione della convenzione del Consiglio d'Europa sulla cybercriminalità (Convenzione di Budapest)[17], cui hanno fatto

anche per il mondo digitale, in cui gli attacchi informatici e la cibercriminalità continuano ad aumentare", p. 1.

[13] I termini "cybersecurity" e in italiano "cybersicurezza" o "cibersicurezza", considerati equivalenti, saranno utilizzati alternativamente nel presente lavoro. Lo stesso vale per i termini "cybercriminalità" e "cibercriminalità" e per i termini "cyberspace" e "ciberspazio".

[14] È noto che nei nuovi settori d'intervento dell'UE, prima dell'inserimento di una base giuridica nei Trattati, le Istituzioni hanno utilizzato competenze già esistenti. Ad esempio, l'adozione di una disciplina sulla *privacy* è avvenuta sulla base dell'art. 95 TCE.

[15] Il concetto di *dual use*, inerente a varie tecnologie tra cui l'*Information and Communication Technology* (ICT), è riferito agli usi pacifici e quindi ai benefici che derivano dalla società dell'informazione, da un lato, e agli usi militari o bellici, dall'altro lato. Tale concetto è stato ripreso dal vertice del G7 di Taormina (26- 27 maggio 2017) nell'ambito del quale si è sottolineato l'impegno a difendere il cyberspazio come spazio aperto…. che promuove il benessere della società, e allo stesso tempo si è stabilito di combattere il terrorismo nelle sue manifestazioni in rete ("the rise of terrorism and violent extremism, including its manifestation online", così G7 Taormina *Leaders' Communiqué*, al punto 4).

[16] Va ricordato anche il tentativo di adottare una Convenzione globale sulla criminalità informatica (proposta presentata al XII Congresso delle Nazioni Unite, tenutosi dal 12 al 19 aprile 2010) che però è fallito a causa del disaccordo tra gli Stati.

[17] Convenzione sulla criminalità informatica, aperta alla firma a Budapest il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004. Al 22 febbraio 2021 sono 65 gli Stati parte, inclusi alcuni Paesi non europei. Per ulteriori informazioni si veda la pagina del Consiglio d'Europa: https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/185.

seguito alcune ulteriori iniziative volte a colmare le lacune della disciplina in parola[18]. Invero, il contrasto alla cybercriminalità presenta continue sfide in ragione dell'evolversi delle tecnologie. Si consideri, ad esempio, l'esigenza di disciplinare il *QR code*, utilizzato di recente (e con maggiore frequenza in tempi di pandemia da COVID-19) da criminali informatici al fine di veicolare *malware* o di commettere il furto di dati personali[19].

Le iniziative dell'Unione europea[20] non si sono concentrate soltanto sulla criminalità informatica ma hanno riguardato l'ambito trasversale a diverse politiche dell'UE della "sicurezza delle reti e sicurezza dell'informazione"[21]. In questa prospettiva, il Regolamento n. 460/2004 ha istituito l'Agenzia europea di sicurezza delle reti e dell'informazione (ENISA) ed ha invitato gli Stati membri a definire strategie nazionali per la *cybersecurity*. Successivamente, il Regolamento 2019/881 (c.d. "*Cybersecurity Act*") ha provveduto ad estendere e a rafforzare il mandato dell'ENISA[22]. La sicurezza informatica è quindi un obiettivo che continua ad essere centrale per l'Unione europea nella prospettiva della realizzazione del mercato e del perseguimento di *trade values*.

---

[18] In tema di cooperazione transfrontaliera ai fini di acquisizione della prova digitale all'estero occorre menzionare i lavori preparatori in vista dell'adozione del secondo Protocollo addizionale alla Convenzione di Budapest. In argomento, si veda F. GRAZIANI, *L'acquisizione della prova digitale all'estero: verso un secondo Protocollo addizionale alla Convenzione di Budapest sul* cybercrime, in S. MARCHISIO, U. MONTUORO (a cura di), *Lo spazio* cyber *e cosmico. Risorse* dual use *per il sistema Italia in Europa*, Torino, 2019, pp. 55-88; F. GRAZIANI, *La ricerca della prova digitale mediante captatore informatico nella prassi degli Stati e nell'ordinamento italiano: il difficile equilibrio tra prevenzione dei reati e tutela della riservatezza informatica*, in *La Comunità internazionale*, 2019, pp. 389- 418.

[19] Cfr. F. BUSSOLETTI*, Security, nuova vita per il QR Code e per il cybercrime*, in *Difesa & Sicurezza*, 18 settembre 2020, reperibile *on-line*.

[20] Per una ricostruzione delle azioni e degli interventi dell'Unione europea in materia di *cybersecurity*, si veda C. CENCETTI, Cybersecurity*, Unione europea e Italia. Prospettive a confronto*, in *Quaderni IAI*, Roma, 2014, pp. 21 ss.

[21] La Comunicazione sulla criminalità informatica , cui è seguita la Decisione quadro 2005/222 GAI del Consiglio del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione che aveva l'obiettivo di "far sì che gli attacchi ai danni di sistemi di informazione siano puniti in tutti gli Stati membri con sanzioni penali effettive, proporzionate e dissuasive, e migliorare ed incoraggiare la cooperazione giudiziaria". Nella comunicazione Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo del 6 giugno 2001, COM(2001)298 definitivo, la Commissione europea illustra un primo approccio strategico e delinea una disciplina specifica per determinati settori. In quest'ottica, vale la pena di ricordare la direttiva n. 2008/114 relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione dell'8 dicembre 2008 (*GUUE* L 345 del 23 dicembre 2008, p. 75 ss.) e la direttiva n. 2011/93 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile del 13 dicembre 2011 (*GUUE* L 335 del 17 dicembre 2011, p. 1 ss.). Non meno importante è la direttiva n. 2009/140, c.d. *framework* per le reti ed i servizi di comunicazione elettronica che, all'articolo 13, recante misure concernenti la sicurezza delle reti, invita gli Stati membri a creare «autorità nazionali di regolamentazione».

[22] Si veda il regolamento (UE) 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004, in *GUUE* L 165 del 18 giugno 2013, p. 41 ss. In seguito, l'esigenza di coerenza del mandato dell'ENISA con la disciplina introdotta dalla direttiva NIS, ha portato all'adozione del Regolamento (UE) 2019/881, cit. nota 10.

Per quanto riguarda gli strumenti operativi, occorre ricordare che gli stessi sono funzionali alle esigenze già evidenziate nella *Strategia di sicurezza interna dell'UE* del 2010[23], di perseguire una maggiore sicurezza interna dell'UE mediante cinque obiettivi strategici[24], aggiornata da ultimo con la Comunicazione della Commissione *sulla strategia dell'UE per l'Unione della sicurezza* del 24 luglio 2020[25]. Si segnala, in particolare, l'istituzione di organi cui vengono affidati la gestione dei rischi nel *cyberspace* e il coordinamento delle attività dei singoli Stati membri: il Centro europeo per la lotta alla criminalità informatica (EC3) istituito presso l'Europol e la squadra di risposta alle emergenze informatiche (CERT-UE), affiancati dal sistema europeo di condivisione delle informazioni e di allarme (EISAS). Tali strumenti sono in costante evoluzione alla luce dei più recenti sviluppi[26], che hanno portato, tra l'altro, al rafforzamento del Centro europeo per la lotta alla criminalità informatica con l'adozione dell'*EU Law Enforcement Emergency Response Protocol*[27], in attuazione della raccomandazione della Commissione n. 2017/1584 *relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala* del 13 settembre 2017[28]. Inoltre, nel 2019 è stata istituita una rete europea delle organizzazioni di collegamento per le crisi informatiche (EU- CyCLONe, acronimo di *Cyber Crisis Liaison Organisation Network*) per sostenere la gestione coordinata di incidenti e crisi di cibersicurezza su vasta scala e garantire il regolare scambio di informazioni tra gli Stati membri e le istituzioni dell'UE[29].

Va appena ricordato che il Parlamento europeo nella Risoluzione del 12 giugno 2012 sulla *Protezione delle infrastrutture critiche informatizzate – realizzazioni e*

[23] Comunicazione della Commissione al Parlamento europeo e al Consiglio *La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura*, del 22.11.2010, COM(2010) 673 def., adottata per il periodo 2011-2014.

[24] I cinque obiettivi strategici erano i seguenti: smantellare le reti criminali internazionali, prevenire il terrorismo e contrastare la radicalizzazione e il reclutamento, aumentare i livelli di sicurezza per i cittadini e le imprese nel ciberspazio, rafforzare la sicurezza attraverso la gestione delle frontiere e aumentare la resilienza dell'Europa alle crisi e alle calamità.

[25] La recente strategia aggiorna anche la precedente Comunicazione della Commissione *Agenda europea sulla sicurezza*, del 28 aprile 2015, COM (2015)185 final, adottata per il periodo 2015-2020. Nella *Strategia dell'UE per l'Unione della sicurezza*, COM(2020) 605 final, adottata per il periodo 2020- 2025, la Commissione prende atto delle nuove minacce alla sicurezza dei cittadini europei, tra cui la pandemia da COVID-19, e del massiccio utilizzo delle tecnologie digitali nella società, di cui tuttavia si sono avvalsi anche i cybercriminali per fini malevoli.

[26] Su cui, si veda da ultimo R. FLOR, Cybersecurity *ed il contrasto ai* cyber-attacks *a livello europeo: dalla CIA-Triad Protection ai più recenti sviluppi*, in *Diritto di Internet*, n. 3, 2019, pp. 453- 467.

[27] Per un approfondimento si veda la pagina: www.europol.europa.eu/newsroom/news/law-enforcement-agencies-across-eu-prepare-for-major-cross-border-cyber-attacks

[28] *GUUE* C239 del 19 settembre 2017, pp. 36- 58.

[29] Come è riportato dall'ENISA: "The CyCLONe's aim is to contribute to the implementation of the European Commission's Blueprint for rapid emergency response in case of a large-scale cross-border cyber incident or crisis and complements the existing cybersecurity structures at EU level by linking the cooperation at technical (e.g. Computer Security Incident Response Team - CSIRTs) and political levels (e.g. Integrated Political Crisis Response - IPCR)". https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone

prossime tappe: verso una sicurezza informatica mondiale[30] raccomandava alla Commissione «di proporre misure vincolanti volte a imporre norme minime in materia di sicurezza e resilienza e a migliorare il coordinamento tra i CERT nazionali» (n. 22) e la invitava a proporre, entro la fine del 2012, «una strategia globale dell'UE per la sicurezza di Internet basata su una terminologia chiara», che prevedesse di «stabilire norme minime di resilienza tra gli Stati membri, al fine di garantire un servizio sicuro, continuo, solido e resiliente, con riferimento sia alle infrastrutture critiche sia a un uso generico di Internet» garantendo al contempo «il libero flusso di informazioni» e «una solida protezione della vita privata e delle altre libertà civili» (n. 32).

Nella direzione indicata, la Commissione europea ha adottato la *Strategia dell'Unione europea per la cibersicurezza: Un ciberspazio aperto e sicuro* del 7 febbraio 2013[31] la quale ha iniziato a trovare attuazione nella direttiva del Parlamento europeo e del Consiglio recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione del 6 luglio 2016 (direttiva NIS), che ne costituisce il pilastro portante e la cui disciplina è attualmente in fase di revisione (si veda *infra* al par. 2)[32]. La *Strategia*, adottata congiuntamente dalla Commissione e dall'Alto rappresentante dell'Unione europea per gli affari esteri e la politica di sicurezza, è uno strumento di ampia portata sulla *cybersecurity*[33], che estende gli interventi dell'Unione ai tre principali settori di competenza: il mercato interno, lo spazio di libertà sicurezza e giustizia e la politica europea di sicurezza e difesa. Gli interventi sono articolati intorno a cinque priorità strategiche: raggiungere la ciberresilienza[34]; ridurre drasticamente il cibercrimine; sviluppare una politica e

[30] *GUUE* C 332 E del 15 novembre 2013, p. 22.

[31] Per un commento alla stessa cfr. *Editorial*, *A Regional Strategy for Cybersecurity*, in *Int'l J. Info. Sec. & Cybercrime*, n. 1, 2015, p. 5 ss. Per un'analisi critica, cfr. N. ARPAGIAN, *L'Europe de la sécurité numérique: très juridique, mais guère technologique, et encore insuffisamment économique*, in *F.F.E. «Annales des Mines – Réalités industrielles»*, 2016/3, pp. 51 -54, www.cairn.info/revue-realites-industrielles-2016-3-page-51.htm

[32] La Commissione ha adottato dal 2017 ad oggi una serie coordinata di atti con lo scopo di dare piena ed effettiva attuazione alla Strategia del 2013. Si veda la Comunicazione congiunta della Commissione al Parlamento europeo e al Consiglio del 13 settembre 2017, *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN(2017) 450 final; Racommandazione della Commissione del 13 settembre 2017 *on Coordinated Response to Large Scale Cybersecurity Incidents and Crises*, C(2017) 6100 final; Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), che ha portato all'adozione del Regolamento 2019/881, cit.

[33] Come è indicato: "La cibersicurezza si riferisce comunemente alle precauzioni e agli interventi che si possono prendere per proteggere il ciberdominio, in campo sia civile che militare, nei confronti delle minacce associate o che possono nuocere alle loro reti e infrastrutture di informazione interdipendenti. La cibersicurezza si propone di salvaguardare la disponibilità e l'integrità delle reti e dell'infrastruttura e la riservatezza delle informazioni che esse contengono". Cfr. Strategia, 1.1 *Contesto*, nota 4, p. 3.

[34] Si tratta di un concetto chiave dell'intera strategia europea, che racchiude l'insieme delle azioni finalizzate sia alla prevenzione degli incidenti informatici sia alla gestione e all'attenuazione del loro impatto. Nell'ambito di tali attività si possono menzionare le iniziative di formazione e le esercitazioni in materia di *cybersecurity*. Come si legge sulla pagina web della Banca Centrale Europea: "Cyber resilience refers to the ability to protect electronic data and systems from cyberattacks, as well as to resume business operations quickly in case of a successful attack". Allo scopo indicato, particolare rilievo assumono la

capacità di ciberdifesa connesse alla Politica di sicurezza e di difesa comune (PSDC)[35]; sviluppare le risorse industriali e tecnologiche per la cibersicurezza; creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costitutivi dell'UE[36]. Le priorità strategiche indicate continuano ad essere sviluppate alla luce dei continui e rapidi progressi realizzati negli ultimi anni come emerge dalla già menzionata *strategia dell'UE in materia di cibersicurezza per il decennio digitale* del 16 dicembre 2020.

La *cybersecurity* è quindi un obiettivo trasversale, e strategico, dell'Unione europea che concorre alla realizzazione delle finalità indicate all'art. 3 (commi 1, 2, e 3) del TUE sulla base del sistema delle competenze d'attribuzione relative a: mercato interno, spazio di libertà, sicurezza e giustizia, politica di sicurezza e difesa comune. Va appena ricordato che il Trattato di Lisbona ha dato un forte impulso allo sviluppo dello spazio di libertà, sicurezza e giustizia e che è proprio rispetto a tale settore che "si profila oggi, in un quadro legislativo generale assai stagnante, il più concreto ed interessante dinamismo legislativo dell'Unione"[37]. In questo ambito, peraltro, la legislazione dell'Unione europea dovrà svilupparsi conformemente alla Convenzione di Budapest. D'altro canto, i settori relativi al mantenimento dell'ordine pubblico e della sicurezza interna restano di competenza degli Stati membri, anche rispetto alle attività di *cyber espionnage* (e più in generale ai servizi di intelligence)[38]. Sviluppi interessanti si profilano anche nel contesto della politica di sicurezza e difesa comune con riguardo, in particolare, alla possibilità di far valere la clausola di solidarietà[39]. Ma è soprattutto nel settore del mercato interno (come si accennava) che si stanno articolando gli interventi legislativi dell'Unione europea finalizzati alla sicurezza delle reti informatiche nonché

Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza, del 5 luglio 2016, COM(2016) 410 final; e la Decisione della Commissione relativa all'istituzione di un partenariato pubblico-privato contrattuale per la sicurezza informatica (PPP contrattuale), del 5 luglio 2016, C(2016) 4400 final.

[35] Vale la pena di evidenziare che al fine di dare attuazione alla Strategia, su richiesta del Consiglio europeo del dicembre 2013 e su proposta dell'Alto rappresentante ed in collaborazione con la Commissione e con l'Agenzia di difesa europea, il Consiglio ha adottato il quadro strategico *EU Cyber Defence Policy Framework* il 18 novembre 2014.

[36] Con riguardo a tali priorità strategiche, l'Unione europea promuove un approccio *multi-stakeholder* che fa leva sulla sinergia con partner ed organizzazioni internazionali, con il settore privato e con la società civile.

[37] Così R. ADAM, A. TIZZANO, *Manuale di Diritto dell'Unione europea*, II ed., Torino, 2017, p. 531. Sul dinamismo dello Spazio di libertà, sicurezza e giustizia con riguardo all'evoluzione del quadro normativo e giudiziario e alle prospettive future si veda, di recente, A. DI STASI, L.S. ROSSI (a cura di), *Lo Spazio di libertà sicurezza e giustizia a vent'anni dal Consiglio europeo di Tampere*, Napoli, 2020, e in particolare la *Presentazione* di A. DI STASI e L.S. ROSSI, pp. 9-13.

[38] L'art. 4, par. 2 del TUE prevede espressamente che "la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro".

[39] Risoluzione del Parlamento europeo del 12 settembre 2013 sulla strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro, in *GUUE* C 93 del 9 marzo 2016, p. 112 ss. in cui il Parlamento invita la Commissione a «tenere conto del rischio di attacchi informatici contro gli Stati membri» nella definizione delle future modalità di attuazione della clausola di solidarietà (articolo 222 del TFUE). Cfr. punto 17.

allo sviluppo del mercato dei prodotti e dei servizi per la *cybersecurity* informatica[40]. Di recente, è emerso, in particolare, che la *cybersecurity* dei prodotti tecnologici è un aspetto di rilevanza strategica, come sottolinea la *strategia dell'UE per l'Unione della sicurezza*[41]. Il riferimento alla sicurezza delle reti 5G non è casuale[42], e l'esigenza di introdurre, senza ritardi, una disciplina europea risponde alle preoccupazioni emerse al livello globale con riferimento agli appalti per la realizzazione delle reti 5G negli Stati membri (e all'eventuale partecipazione di Stati extra-europei, ad esempio la Cina). La questione, che rischia di sollevare controversie commerciali al livello multilaterale, non può evidentemente essere esaminata nell'ambito del presente lavoro per la complessità e l'ampiezza degli approfondimenti che richiederebbe.

3. Il nuovo quadro giuridico sulla *cybersecurity* europea

L'esigenza di rispondere efficacemente alle "crisi di *cybersecurity*", come evidenziato sopra, ha portato all'adozione di un quadro normativo frammentario la cui revisione, di recente, si è proposta di migliorare la coerenza e l'efficacia degli atti normativi adottati, anche alla luce delle problematiche emerse in fase applicativa.

La direttiva 2016/1148, nota come "direttiva NIS" (*Network and Information Security*)[43], ha lo scopo di creare "una capacità minima comune" ed "obblighi comuni di sicurezza per gli operatori dei servizi essenziali e i fornitori di servizi digitali" nell'UE mediante interventi specifici che possano rafforzare l'efficienza complessiva dell'UE.

---

[40] Si veda la Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni *Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza*, del 5 luglio 2016, COM(2016) 410 final e la Decisione della Commissione relativa all'istituzione di un partenariato pubblico-privato contrattuale per la sicurezza informatica (PPP contrattuale), del 5 luglio 2016, C(2016) 4400 final.

[41] Cfr. nota 31.

[42] Si vedano in proposito la Raccomandazione (Ue) 2019/534 della Commissione europea del 26 marzo 2019, *Cibersicurezza delle reti 5G*, C(2019) 2335 final, e la Comunicazione della Commissione europea *Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE*, del 29 gennaio 2020, COM(2020) 50 final.

[43] Direttiva 2016/1148/UE del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione, in *GUUE* L 194/2016, p. 1 ss. In Italia, la Direttiva NIS è stata recepita con Decreto Legislativo 18 maggio 2018, n. 65 *Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione*, in GU Serie Generale n.132 del 9 giugno 2018, in vigore dal 24 giugno 2018. Sono stati adottati, a seguire, alcuni ulteriori provvedimenti, tra cui il Decreto legge 21 settembre 2019, n. 15 che istituisce il "perimetro di sicurezza nazionale cibernetica» al fine «di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato…" (art. 1). Cfr. *infra* nota 53.

A tal fine, la direttiva NIS prevede un livello minimo di sicurezza delle reti e dei sistemi informativi ("adeguato al rischio esistente")[44] e introduce l'obbligo a carico degli Stati membri di provvedere affinché determinati soggetti (operatori di servizi essenziali e fornitori di servizi digitali) notifichino senza indebito ritardo all'autorità competente o al gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) gli incidenti "che abbiano un impatto rilevante" rispettivamente sulla continuità dei servizi essenziali prestati o sulla fornitura di un servizio digitale (di cui si trova un elenco all'allegato III) [45]. Si tratta, quindi, di una direttiva di *armonizzazione minima* che lascia agli Stati membri un margine di apprezzamento più o meno ampio con riguardo al livello di sicurezza da perseguire e alle misure di prevenzione degli incidenti informatici da adottare[46]. Al fine di definire le modalità di applicazione della disciplina in parola e di indicare, tra l'altro, i criteri per determinare l'eventuale impatto rilevante di un incidente, è stato in seguito adottato il Regolamento di esecuzione n. 2018/151 della Commissione, del 30 gennaio 2018[47].

Nell'ottica di favorire lo scambio di informazioni sui rischi e sugli incidenti, ogni Stato membro designa uno o più gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) e partecipa al Gruppo di cooperazione[48]. Una sottile differenza distingue la nozione di *incidente* (che può essere causato anche da attività

[44] La direttiva prevede quindi analoghi obblighi di adottare misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi, tenuto conto "delle conoscenze più aggiornate in materia", cfr. rispettivamente l'art. 14, comma 1 (per gli operatori di servizi essenziali) e l'art. 16 comma 1 (per i fornitori di servizi digitali).

[45] Mercato online, motore di ricerca online, servizi nella nuvola (*cloud computing*). È altresì previsto un meccanismo di «notifica volontaria» (art. 20) per soggetti non appartenenti alle categorie di operatori di servizi essenziali e fornitori di servizi digitali per i quali è previsto invece l'obbligo di notifica.

[46] Ciò comporta, ai sensi dell'art. 3 della direttiva NIS, che gli Stati, fatto salvo l'articolo 16, par. 10 (che vieta agli Stati di imporre ulteriori obblighi in materia di sicurezza o di notifica ai fornitori di servizi digitali, che non siano giustificati da esigenze di sicurezza nazionale indicate all'art. 1, comma 6) possono "adottare o mantenere in vigore disposizioni atte a conseguire un livello di sicurezza più elevato della rete e dei sistemi informativi". In generale, sul concetto di armonizzazione minima, v. R. ADAM – A. TIZZANO, *op. cit.*, p. 650.

[47] Regolamento di esecuzione (UE) 2018/151 della Commissione, del 30 gennaio 2018, recante modalità di applicazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio per quanto riguarda l'ulteriore specificazione degli elementi che i fornitori di servizi digitali devono prendere in considerazione ai fini della gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi e dei parametri per determinare l'eventuale impatto rilevante di un incidente, in GUUE L 26 del 31 gennaio 2018, pp. 48- 51. In particolare, ai sensi dell'Articolo 4: "Un incidente è considerato come avente un impatto rilevante se si verifica almeno una delle seguenti situazioni: a) il servizio fornito da un fornitore di servizi digitali non è stato disponibile per oltre 5 000 000 di ore utente, dove per ore utente si intende il numero di utenti interessati nell'Unione per una durata di sessanta minuti; b) l'incidente ha provocato una perdita di integrità, autenticità o riservatezza dei dati conservati, trasmessi o trattati o dei relativi servizi offerti o accessibili tramite una rete e un sistema informativo del fornitore di servizi digitali che ha interessato oltre 100 000 utenti nell'Unione; c) l'incidente ha generato un rischio per la sicurezza pubblica, l'incolumità pubblica o in termini di perdite di vite umane; d) l'incidente ha provocato danni materiali superiori a 1 000 000 di EUR per almeno un utente nell'Unione".

[48] Il Gruppo di cooperazione è composto da rappresentanti degli Stati membri, dalla Commissione e dall'ENISA (art. 11, comma 2). L'attività di cooperazione per la *cybersecurity* si traduce tra l'altro nell'analisi dei rischi e nell'adozione di rapporti, si veda da ultimo il *NIS Cooperation Group Report* del 9 ottobre 2019, *EU coordinated risk assessment of the cybersecurity of 5G networks*, reperibile *on-line.* I CSIRT sono designati dagli Stati membri conformemente all'art. 9.

criminali) ai sensi della direttiva NIS ("ogni evento con un reale effetto pregiudizievole per la sicurezza della rete e dei sistemi informativi")[49], da quella di *attacco* ai sensi della direttiva n. 2013/40 relativa agli attacchi contro i sistemi di informazione (adottata sulla base dell'art. 83, par. 1). Quest'ultima intende armonizzare le norme penali degli Stati membri, relativamente a cinque fattispecie di reato elencate agli articoli da 3 a 7 (*Accesso illecito a sistemi di informazione*; *Interferenza illecita relativamente ai sistemi*; *Interferenza illecita relativamente ai dati*; *Intercettazione illecita*; *Strumenti utilizzati per commettere i reati*)[50]. Di particolare rilievo appare la definizione del reato di "Interferenza illecita relativamente ai sistemi" definito come: "l'atto di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione di dati informatici, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di tali dati o rendendo tali dati inaccessibili, compiuto intenzionalmente e senza diritto". La definizione sembra compatibile con la nozione di incidente ai sensi della direttiva NIS[51] la quale, peraltro, nel definire il proprio ambito di applicazione (v. art. 1, n. 4) fa salva la direttiva 2013/40, nonché altri atti vincolanti dell'Unione adottati in settori specifici (ad esempio nel settore bancario e in quello delle infrastrutture dei mercati finanziari)[52]. La diversa base giuridica delle due direttive indicate (relative l'una al mercato interno e l'altra allo spazio di libertà, sicurezza e giustizia) sollecita l'applicazione di un criterio di coerenza nell'ottica di una interpretazione sistematica delle norme in materia di *cybersecurity*. Va considerato, inoltre, che le attività per individuare eventuali rischi di incidenti, per prevenire, rilevare e affrontare incidenti nonché per attenuarne l'impatto (c.d. misure di "gestione del rischio") rientrano tra gli obblighi a carico degli Stati membri previsti dalla direttiva NIS nell'ambito dei "Quadri nazionali per la sicurezza della rete e dei sistemi informativi" (Capo II).

In fase applicativa è emersa una disomogeneità negli Stati membri con riguardo all'individuazione dei soggetti vincolati dalle disposizioni della direttiva e in particolare alla nozione di "operatori di servizi essenziali"[53]. La Commissione ha predisposto una

[49] Art. 4, n. 7.

[50] La direttiva mira anche ad introdurre sanzioni penali "per la creazione delle «botnet», ossia per l'azione con cui si stabilisce il controllo a distanza di un numero rilevante di computer infettandoli con software maligni per mezzo di attacchi informatici mirati. Una volta creata, la rete infettata di computer che costituiscono la «botnet» può essere attivata a insaputa degli utenti per lanciare un attacco informatico su larga scala" (considerando 5).

[51] La nozione di "incidente" definita all'art. 4, n. 7 è coerente con la descrizione contenuta nella Strategia al punto 1.1. secondo cui gli incidenti a carico della cibersicurezza possono essere «intenzionali o fortuiti» e le minacce possono avere origini diverse, ad esempio «attacchi criminali, di natura politica o terroristica, o commissionati da uno stato, oppure essere causate da calamità naturali e errori non intenzionali».

[52] La cui regolamentazione copre tutte le operazioni comprese la sicurezza, l'integrità e la resilienza delle reti e dei sistemi informativi.

[53] Per quanto riguarda l'Italia, in particolare, vale la pena di ricordare l'adozione di una disciplina finalizzata alla realizzazione di un'architettura strategica nazionale per la sicurezza e la difesa cibernetica, mediante due significative normative di recente adozione: il decreto legislativo n. 63 del 18 maggio 2018 (in attuazione della c.d. direttiva NIS) e il decreto legge n. 105 del 21 settembre 2019 sul perimetro di sicurezza nazionale cibernetica. Cfr. Camera dei Deputati, Dominio cibernetico, nuove tecnologie e

relazione ed ha avviato una consultazione pubblica (dal 7 luglio al 2 ottobre 2020) e visite presso gli Stati membri al fine di verificare l'attuazione della direttiva mediante incontri con gli operatori e le autorità nazionali[54]. All'esito della consultazione, a poco più di due anni dal termine di recepimento della direttiva in parola (9 maggio 2018), la Commissione ha presentato una nuova *proposta di direttiva del Parlamento europeo e del Consiglio relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148*, Bruxelles, 16 dicembre 2020 (c.d. NIS 2)[55].

La direttiva NIS, peraltro, impone agli Stati membri di adottare le cautele necessarie ai fini del trattamento di dati personali nell'ambito delle attività di prevenzione e di ripristino dei sistemi informatici a seguito di incidenti informatici[56]. I progressi compiuti negli ultimi vent'anni nella disciplina della protezione dei dati personali nell'Unione europea, al punto di ritenere che il diritto alla protezione dei dati personali è, tra i diritti umani, quello che beneficia di una regolamentazione più consistente e dettagliata nell'UE sono avvenuti superando qualche perplessità sollevata dalla dottrina. In particolare, si è discusso in merito alla base giuridica cui fa riferimento la direttiva 95/46: l'art.114 TFUE che stabilisce la competenza in materia di armonizzazione al fine di garantire il corretto funzionamento del mercato interno[57]. Non si tratta di una base giuridica che, in linea di principio, può essere utilizzata al fine di legiferare in materia di protezione dei diritti umani, benché il legislatore comunitario abbia moltiplicato le ipotesi di questo tipo (e la questione sia stata più volte oggetto di esame da parte della Corte di giustizia UE)[58]. Tale prassi ha trovato di recente una giustificazione: "there is an internal market competence to harmonize fundamental rights protection if certain conditions… are met. The precondition is that there are divergent national laws, which

---

politiche di sicurezza e difesa cyber, Documentazione e ricerche n. 83, 24 settembre 2019. Si veda anche la Relazione del Comitato Parlamentare per la Sicurezza della Repubblica (Copasir) sulle politiche e gli strumenti per la protezione cibernetica e la sicurezza informatica, a tutela dei cittadini, delle istituzioni, delle infrastrutture critiche e delle imprese di interesse strategico nazionale, Doc. XXXIV n. 1, dell'11 dicembre 2019, reperibile all'indirizzo: https://documenti.camera.it/_dati/leg18/lavori/documentiparlamentari/IndiceETesti/034/001/intero.pdf

[54] Relazione della Commissione al Parlamento europeo e al Consiglio di valutazione della coerenza degli approcci adottati dagli Stati membri per l'identificazione degli operatori di servizi essenziali conformemente all'articolo 23, paragrafo 1, della direttiva 2016/1148/UE sulla sicurezza delle reti e dei sistemi informativi, del 28 ottobre 2019, COM(2019)546 final.

[55] COM(2020) 823 final.

[56] Con riguardo alla protezione dei dati personali, va considerato il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, in GUUE L 119 del 4 maggio 2016, p. 1 ss. In tema di riservatezza dei dati e *cybersecurity*, sia consentito rinviare a D. MARRANI, *Cybersicurezza e tutela della riservatezza dei dati personali: le decisioni Breyer e Tele2 Sverige/Watson della Corte di giustizia UE*, in *Il Diritto dell'Unione europea*, 2017, n. 4, pp. 791- 828.

[57] Si veda, tra gli altri, F. BALDUCCI ROMANO, *La protezione dei dati personali nell'Unione europea tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Rivista italiana di diritto pubblico comunitario*, 2015, p. 1625 s.

[58] Vedi Corte giust. 10 dicembre 2002, C 491/01, *British American Tobacco (Investments) e Imperial Tobacco*; 8 giugno 2010, C 58/08, *Vodafone e a.*; 3 settembre 2015, C-398/13, *Inuit Tapiriit Kanatami e a. c. Commissione europea*.

are liable to put the establishment and functioning of the internal market at risk or to distort competition"[59]. Con l'entrata in vigore del Trattato di Lisbona, il problema dell'assenza di una base giuridica nei Trattati è stato risolto: è inserita una norma sulla protezione dei dati personali (art. 16 del TFUE) e la Carta di Nizza assume lo stesso valore giuridico dei Trattati. Tali cambiamenti (alla base del Regolamento 2016/679) riflettono una visione dinamica e integrata dei diritti e delle politiche dell'UE.

Nell'ottica di rafforzare il quadro istituzionale e normativo vigente, va menzionato anche il più ampio mandato conferito all'Agenzia dell'Unione europea per la cibersicurezza (ENISA) con il Regolamento n. 2019/881del 17 aprile 2019 (c.d. "Cybersecurity Act"). Il regolamento, la cui base giuridica è l'art. 114 TFUE, si propone di "*conseguire un elevato livello comune di cibersicurezza in tutta l'Unione, anche sostenendo attivamente gli Stati membri, le istituzioni, gli organi e gli organismi dell'Unione nel miglioramento della cibersicurezza*" (art. 3, par. 1). A tal fine, l'ENISA è dotata di ampie competenze e la sua azione è completata dal " quadro europeo di certificazione della cibersicurezza" con lo scopo di introdurre un modello di certificazione dei prodotti dell'ICT unificato e di superare eventuali conflitti e incongruenze tra modelli di certificazione nazionali differenti e, allo stesso tempo, di rafforzare la fiducia dei consumatori e dei cittadini europei nei prodotti ICT nell'ottica della piena realizzazione e del buon funzionamento del mercato unico digitale.

Il quadro giuridico sulla *cybersecurity* europea si va articolando in maniera sempre più complessa ed emerge un rafforzamento non solo delle competenze tecniche e operative dei rispettivi organismi coinvolti ma anche della collaborazione tra gli stessi: si pensi ad esempio alla cooperazione tra ENISA ed Europol ai fini di contrasto della cybercriminalità.

Con riguardo alla cybercriminalità è emerso un significativo ritardo degli Stati membri nel recepimento di alcune direttive dell'UE. In particolare, allo scopo di promuovere una disciplina penale armonizzata, la Commissione sta monitorando il recepimento e l'attuazione della direttiva relativa agli attacchi contro i sistemi di informazione[60]. Sono emersi altresì ritardi nell'attuazione della direttiva del 2011 relativa alla lotta contro l'abuso sessuale dei minori. In tale ambito, la Commissione ha adottato una strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori[61].

[59] Così V. KOSTA, *Fundamental Rights in EU Internal Market Legislation*, Oxford, 2015, p. 8.
[60] In riferimento alla situazione in Bulgaria, Italia, Portogallo e Slovenia a seguito dell'avvio di alcune procedure di infrazione nel 2019.
[61] Al riguardo, è emerso un problema specifico in merito ad alcuni servizi di comunicazione on- line, in specie i servizi di posta elettronica o di messaggistica, i quali dal 21 dicembre 2020 rientrano nell'ambito di applicazione della direttiva e-privacy e nelle definizioni rivedute del codice europeo delle comunicazioni elettroniche. Considerato che i fornitori di detti servizi svolgono importanti attività volontarie al fine di individuare, contrastare e denunciare gli abusi sessuali su minori on-line, attività che non sarebbero più consentite dalla disciplina in parola, la Commissione ha proposto un regolamento che autorizza il proseguimento di tali attività volontarie, a determinate condizioni, in attesa di presentare una iniziativa legislativa mirata.

Un altro profilo di particolare rilievo riguarda l'accesso transfrontaliero alle prove elettroniche nelle indagini penali[62]. Occorre ricordare che a seguito delle proposte della Commissione sull'accesso transfrontaliero alle prove elettroniche dell'aprile 2018, il Parlamento europeo non ha ancora definito la propria posizione e pertanto la procedura legislativa non si è ancora conclusa[63]. La questione è altresì oggetto di negoziati internazionali sia in sede ONU, sia in seno al Consiglio d'Europa per l'adozione di un secondo protocollo aggiuntivo alla Convenzione sulla cybercriminalità, sia a livello bilaterale in vista della conclusione di un accordo UE-USA sull'accesso transfrontaliero alle prove elettroniche.

Appare evidente che l'assenza di volontà politica degli Stati membri nel dare seguito all'attività delle Istituzioni limita in maniera determinante l'efficacia dell'azione dell'UE in un ambito molto delicato per la sicurezza dei cittadini europei e costituisce un grave ostacolo all'attività degli organi giudiziari, e quindi alla realizzazione dello spazio di libertà, sicurezza e giustizia[64].

4. Le misure restrittive nell'ambito della PESC

L'Unione europea, a partire dalla Strategia del 2013 ("*Strategia dell'Unione europea per la cibersicurezza: Un ciberspazio aperto e sicuro*")[65], fa propria la nozione di «*cyberspace*» elaborata dalla NATO[66]. Non a caso il termine è utilizzato prevalentemente negli atti adottati nell'ambito della Politica estera e di sicurezza comune (PESC) e più in particolare della PSDC, con riferimento all'obiettivo di realizzare progressivamente la «cyberdifesa» dell'UE, mediante un *Quadro strategico dell'UE in materia di ciberdifesa*, adottato nel 2014 e aggiornato nel 2018[67]. In

[62] Sulla delicata questione il 1º dicembre 2020 Europol, Eurojust e la rete giudiziaria europea hanno pubblicato la seconda edizione del "SIRIUS EU Digital Evidence Situation Report".

[63] COM/2018/226 e COM/2018/225.

[64] Come è noto, la realizzazione dello Spazio di libertà, sicurezza e giustizia richiede un bilanciamento costante tra i diritti e i valori fondamentali di libertà e sicurezza i quali, nello spazio digitale (*cyberspace*), assumono una dimensione del tutto particolare che riguarda alcuni diritti umani (ad esempio il diritto al rispetto della vita privata e la *privacy*, la libertà di espressione). Tale delicato bilanciamento non può prescindere dall'attività giudiziaria essenziale ad assicurare l'effettività delle soluzioni adottate nel bilanciamento in parola, soprattutto in un ambito delicato e in forte espansione al livello europeo quale è quello penale sia sostanziale che processuale. Per un approfondimento su tali problematiche si veda, A. DI STASI, L.S. ROSSI (a cura di), *op. cit*., pp. 9- 556. In generale, sui profili penali dello Spazio di libertà, sicurezza e giustizia si veda D. RINOLDI, *Lo spazio di libertà, sicurezza e giustizia*, in U. DRAETTA, N. PARISI (a cura di), *Elementi di diritto dell'Unione europea. Parte speciale. Il diritto sostanziale*, Milano 2014, pp. 1-93. In chiave storico-evolutiva si veda, inoltre, L. SALAZAR, *La costruzione di uno spazio penale comune europeo*, in G. GRASSO, R. SICURELLA (a cura di), *Lezioni di diritto penale europeo*, Milano, 2007, pp. 395- 466.

[65] Cfr. nota 39.

[66] In tale contesto, il *cyberspace* è descritto "as the fifth domain of military activity, equally critical to European Union (EU) Common Security and Defence Policy (CSDP) implementation as the domains of land, sea, air, and space".

[67] CONSIGLIO DELL'UNIONE EUROPEA, *Quadro strategico dell'UE in materia di ciberdifesa*, Bruxelles, 18 novembre 2014 e, a seguire, *Quadro strategico dell'UE in materia di ciberdifesa (aggiornato al 2018)*,

particolare, è stabilito un collegamento funzionale molto forte tra la disponibilità e l'accesso ad un cyberspazio sicuro, mediante lo sviluppo di capacità di difesa informatica solide e resilienti, e la realizzazione delle missioni e delle operazioni PSDC e, più in generale, degli obiettivi della PSDC.

L'Unione, in effetti, si propone anzitutto di sviluppare le capacità di cyberdifesa degli Stati membri e di proteggere le "proprie" infrastrutture di sicurezza e difesa, nell'ottica di una Unione europea di difesa più integrata che superi progressivamente i limiti dell'attuale metodo intergovernativo[68]. Altri obiettivi specifici dell'UE consistono nel promuovere la cooperazione civile-militare e le sinergie con altre politiche *cyber* dell'UE, con le pertinenti istituzioni e le agenzie dell'UE, nonché con il settore privato; migliorare la formazione, l'istruzione e le opportunità di collaborazione; e rafforzare la cooperazione con i partner internazionali, in particolare la NATO.

Dal 2014 ad oggi, significativi sviluppi hanno consentito all'Unione di realizzare progressi considerevoli nella cyberdifesa e nelle altre politiche dell'UE relative al *cyberspace* sopra richiamate.

Nell'ambito della cyberdifesa, il Consiglio ha adottato il 19 giugno 2017 un quadro relativo a una risposta diplomatica comune dell'UE alle attività informatiche dolose (noto anche come "*Cyber Diplomacy Toolbox*")[69]. In particolare, il Consiglio sottolinea come: "un approccio comune e globale dell'UE alla diplomazia informatica potrebbe contribuire a prevenire i conflitti, ridurre le minacce alla cibersicurezza e incrementare la stabilità nelle relazioni internazionali"[70]. In piena sintonia con le conclusioni del Consiglio del 2017 e i relativi seguiti[71], sono state introdotte «misure restrittive contro gli attacchi informatici», con la specifica finalità di prevenire e contrastare i *cyber-attacks* nell'ambito della PSDC. Ci si riferisce, in particolare, alla Decisione (PESC) n. 2019/797 del Consiglio del 17 maggio 2019 *concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri* e al Regolamento n.

Bruxelles, 19 novembre 2018 ("Obiettivo dell'aggiornato quadro strategico in materia di ciberdifesa è sviluppare ulteriormente la politica di ciberdifesa dell'UE tenendo conto degli opportuni sviluppi in altre sedi e settori pertinenti nonché dell'attuazione del suddetto quadro dal 2014", *ivi*, p. 2).

[68] A tal fine: "*The EU Cyber Defence Policy Framework (CDPF) supports the development of cyber defence capabilities of EU Member States as well as the strengthening of the cyber protection of the EU security and defence infrastructure, without prejudice to national legislation of Member States and EU legislation, including, when it is defined, the scope of cyber defence*", *ivi,* p. 2.

[69] Cfr. *Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica")*, del 19 giugno 2017, reperibili all'indirizzo: https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/it/pdf. Per ulteriori approfondimenti sull'evoluzione delle azioni in questo ambito si vedano anche le precedenti *Conclusioni del Consiglio sulla diplomazia informatica* dell'11 febbraio 2015, reperibili all'indirizzo: https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/it/pdf.

[70] *Ivi,* p. 2.

[71] Ci si riferisce, in particolare, alle conclusioni del Consiglio del 16 aprile 2018 sulle attività informatiche dolose e alle conclusioni del Consiglio europeo del 28 giugno 2018 e del 18 ottobre 2018 che hanno sottolineato, rispettivamente, l'esigenza di rafforzare le capacità nei confronti delle minacce alla *cybersecurity* provenienti dall'esterno dell'Unione e di migliorare la capacità di rispondere e di prevenire i *cyber attacks* mediante misure restrittive da adottare come seguiti di quanto stabilito nelle conclusioni del Consiglio del 19 giugno 2017.

2019/796 del Consiglio del 17 maggio 2019 *concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri*.

Si tratta di misure aventi ad oggetto limitazioni all'ingresso o al transito nel territorio degli Stati membri nonché di misure di congelamento di fondi e risorse economiche di persone fisiche o giuridiche, di gruppi o di entità non statali ritenute responsabili di *cyber* attacchi, o che abbiano fornito sostegno o agevolato tali attacchi informatici. Le condizioni stabilite dall'art. 1 della Decisione per l'applicazione delle misure restrittive richiedono che i *cyber attacks* producano o siano idonei anche potenzialmente a produrre a «effetti significativi» sui sistemi informativi, e in particolare (ma non solo) sulle infrastrutture critiche degli Stati membri, e che costituiscano «una minaccia esterna per l'Unione o i suoi Stati membri». L'art. 3 della Decisione chiarisce cosa si intenda per «effetti significativi» sulla base di una serie di parametri riguardanti, tra l'altro, la portata, l'entità, l'impatto o la gravità delle turbative causate, il numero di persone fisiche o giuridiche, o di Stati membri interessati. A prescindere dalla natura internazionalistica di siffatti rimedi, le misure sembrano criticabili sul piano della loro efficacia in ragione della natura stessa del *cyberspace* per il fatto che attività criminali o terroristiche possano essere condotte senza la necessità di alcuna presenza fisica sul territorio dello Stato della persona che opera in rete o mediante la rete informatica. Sembra, invece, che un qualche effetto possa essere riconosciuto alle medesime almeno sul piano politico[72].

In applicazione della nuova disciplina, il Consiglio ha adottato per la prima volta misure restrittive nei confronti di alcune persone fisiche e giuridiche con *Decisione del Consiglio concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri* del 30 luglio 2020[73] e *Regolamento di esecuzione (UE) 2020/1125 del Consiglio, del 30 luglio 2020, che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione*

[72] Ad esempio, un risultato significativo potrebbe essere quello di "push forward the conversation about similar measures within the UN context". Così E. MORET, P. PAWLAK, *The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?*, in *European Union Institute for Security Studies*, 2017, p. 3, reperibile *on-line*.

[73] Si tratta di due cittadini cinesi e di quattro cittadini russi (uno dei quali ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi), nonché di una persona giuridica con sede in Cina (la quale ha fornito sostegno finanziario, tecnico o materiale e ha agevolato la campagna "*Operation Cloud Hopper*", una serie di attacchi informatici con effetti significativi, che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi), una residente in Corea (ha fornito sostegno finanziario, tecnico o materiale e ha agevolato una serie di attacchi informatici con effetti significativi, che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi, compresi gli attacchi informatici pubblicamente noti come "*WannaCry*" e gli attacchi informatici contro l'autorità di vigilanza finanziaria polacca e *Sony Pictures Entertainment*, nonché il furto informatico alla *Bangladesh Bank* e il tentativo di furto informatico alla *Vietnam Tien Phong Bank*), e una residente nella Federazione russa (all'origine dell'attacco alla rete elettrica ucraina, nonché responsabile dei noti attacchi conosciuti con il nome di "NotPetya" o "EternalPetya"). Cfr. GUUE L246, 30 luglio 2020, p. 12.

o i suoi Stati membri[74]. Da ultimo la decisione (PESC) 2020/1537 del Consiglio de 22 ottobre 2020 che modifica la decisione (PESC) 2019/797 ha inserito altri due soggetti ed un organismo nell'elenco stabilito dalle decisioni precedenti[75].

Anche la Commissione europea e l'Alto Rappresentante dell'Unione per gli affari esteri e la politica di sicurezza sono intervenuti nell'ambito delle loro competenze al fine di promuovere la "resilienza", la "deterrenza" e la "difesa" dell'UE nei confronti dei cyberattacchi, come emerge dalla Comunicazione congiunta al Parlamento europeo e al Consiglio *Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE* del 13 settembre 2017[76]. La Comunicazione ricostruisce lo stato dell'arte in materia di *cybersecurity* nell'Unione europea e illustra un insieme articolato di possibili azioni dell'Unione in tutti i settori di interesse che riguardano il *cyberspace*: dal mercato digitale alla protezione dei dati personali, alla lotta alla *cyber* criminalità, alla politica estera e di difesa dell'UE, alle relazioni esterne. Nell'ambito dell'ampia analisi effettuata si evince (incidentalmente alla nota 82) una interessante e articolata definizione di "*cyberspace*": "L'UE considera il ciberspazio un campo di operazioni come la terra, l'aria e il mare. Gli interventi di ciberdifesa includono altresì la protezione e la resilienza dei sistemi spaziali e dell'infrastruttura terrestre correlata"[77].

Nella medesima prospettiva, improntata alla "cyberresilienza"[78], va menzionata la Dichiarazione dell'Alto rappresentante Josep Borrell, a nome dell'Unione europea, sulle attività informatiche malevole che sfruttano la pandemia di coronavirus del 30 aprile 2020[79].

Il Parlamento europeo nella Risoluzione del 13 giugno 2018 sulla cyberdifesa sottolinea lo stretto collegamento tra il settore civile e militare, considerato anche che molti prodotti dell'industria UE, immessi sul mercato, sono prodotti *dual use*[80]. Con l'obiettivo di migliorare l'efficienza dell'Unione e degli Stati membri in materia di investimenti e spese per la difesa, e di favorire l'autonomia strategica dell'UE in questo ambito, è stata avviata una cooperazione strutturata permanente (PESCO, secondo l'acronimo inglese) che si propone, tra l'altro, con l'ausilio di diversi progetti approvati[81], di rafforzare la cyberdifesa dell'UE[82].

---

[74] GUUE L246, del 30 luglio 2020, p. 4.
[75] GUUE L 351I del 22 ottobre 2020, p. 5.
[76] Bruxelles, 13 settembre 2017, JOIN(2017) 450 final.
[77] *Ivi*, p. 19.
[78] Come sottolinea la Commissione nella *Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro* del 2013: "Per promuovere la ciberresilienza nell'UE le autorità pubbliche e il settore privato devono sviluppare capacità e cooperare efficacemente. Basandosi sui risultati positivi ottenuti grazie alle attività realizzate finora, gli ulteriori interventi dell'UE possono contribuire in particolare a contrastare i rischi e le minacce cibernetiche aventi dimensione transfrontaliera e a preparare a una risposta coordinata in situazioni di emergenza. In questo modo si sosterrà concretamente il corretto funzionamento del mercato interno e si rafforzerà la sicurezza interna dell'UE", cfr. *Strategia*, p. 5.
[79] https://www.consilium.europa.eu/it/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.
[80] 2018/2004(INI).
[81] Per un elenco aggiornato dei progetti PESCO si rimanda alla tabella pubblicata sulla pagina del Consiglio: https://www.consilium.europa.eu/media/39664/table-pesco-projects.pdf.

Le iniziative sinteticamente descritte si inseriscono nell'ambito della Strategia globale per la politica estera e di sicurezza dell'Unione europea (c.d. Strategia globale)[83] che, nell'ottica sopra illustrata, si propone di integrare diverse politiche dell'UE e di collegare la dimensione interna e la dimensione esterna dell'Unione al fine di conseguire obiettivi di più ampia portata riconducibili alle finalità generali dei Trattati.

5. Il coordinamento delle politiche per la *cybersecurity* dell'UE

Le iniziative dell'UE con riguardo alla *cybersecurity* sopra descritte evidenziano il carattere frammentario degli interventi che riguardano diverse competenze e politiche dell'Unione e atti aventi diversa natura giuridica (atti vincolanti, quali regolamenti e direttive, orientamenti generali contenuti in comunicazioni della Commissione, risoluzioni del Parlamento europeo, decisioni PESC, ecc.)[84].

Come accennato, l'esigenza di coerenza tra le politiche dell'Unione europea contemplate dai Trattati impone un coordinamento tra le iniziative adottate sulla base delle competenze attribuite dal TFUE (politiche materiali non limitate alla Parte V relativa all'azione esterna dell'Unione) e dal TUE (ci si riferisce in particolare alla politica estera e di sicurezza comune). Va appena evidenziato che l'interpretazione delle norme dei Trattati nella prassi *post* Lisbona mette in luce alcune contraddizioni in merito al suddetto coordinamento con riferimento in particolare all'art. 40 TUE e all'art. 21, par. 3 TUE. Al riguardo, si ritiene che il coordinamento delle politiche per la *cybersecurity* richieda una interpretazione teleologica e sistematica delle norme in parola a pena di vanificare la realizzazione degli stessi obiettivi di *cybersecurity* evidenziati dagli orientamenti della Commissione europea e dell'Alto rappresentante per gli affari esteri e la politica di sicurezza.

Attiene infatti ad una esigenza di coerenza raccordare le misure restrittive adottate ai sensi dell'art. 215 TFUE nei confronti di persone fisiche identificate come responsabili di azioni malevole nel *cyberspace* (ad esempio di *cyber* attacchi o atti di cybercriminalità) e le altre politiche del TFUE, nel rispetto e ai fini della costruzione dello spazio di libertà, sicurezza e giustizia. Si tratta, tra l'altro, di tutelare i cittadini

---

[82] Per quanto concerne i profili istituzionali e alcune considerazioni in chiave evolutiva in merito alla PESCO, sia consentito rinviare a D. MARRANI, *La cooperazione strutturata permanente (PESCO): quadro giuridico-istituzionale per l'integrazione "flessibile" in materia di difesa europea*, in *Studi sull'integrazione europea,* 2019, n. 3, p. 719 ss.

[83] CONSIGLIO DELL'UNIONE EUROPEA, *Una strategia globale per la politica estera e di sicurezza dell'Unione europea,* del 28 giugno 2016, CFSP/PESC 543, CSDP/PSDC 395, reperibile *online*. Per una prima riflessione in argomento si veda *Editorial Comments*, in *Common Market Law Review*, 2016, pp. 1199-1208. L'attuazione della Strategia globale è stata avviata a partire dal *Piano d'attuazione in materia di sicurezza e difesa* presentato dall'Alto rappresentante il 14 novembre 2016, cui hanno fatto seguito ulteriori sviluppi.

[84] Come si è avuto modo di evidenziare: «…l'interesse alla stabilità e alla sicurezza del cyberspace appare trasversale alle diverse politiche dell'UE e si condensa nel concetto di cybersecurity dai contorni altrettanto vaghi e indefiniti se non declinati in senso funzionale nei diversi settori di attività», cfr. D. MARRANI, *La cooperazione internazionale per la sicurezza e la stabilità nel cyberspace*, Napoli, 2020, p. 79.

europei da reati penali o da violazioni della loro *privacy* mediante l'utilizzo della Rete e di garantire, nel contempo, il rispetto dei diritti fondamentali delle persone sottoposte a tali misure restrittive nello spazio di libertà, sicurezza e giustizia.

Ciò comporta, in pratica, che l'Unione eserciti in una certa misura un ruolo politico come attore globale in tema di *cybersecurity* nelle relazioni esterne con gli Stati terzi e con le organizzazioni internazionali. Si pensi, in particolare, ai rapporti bilaterali con i Paesi terzi (in merito, ad esempio, allo sviluppo delle reti con tecnologia 5G che dovrà tenere conto degli *standard* di sicurezza stabiliti per le tecnologie digitali nel mercato interno, al rispetto delle certificazioni introdotte dal regolamento n. 2019/88 e della disciplina sulla *privacy*) o alla partecipazione ai gruppi di lavoro delle Nazioni Unite per la definizione di norme di comportamento responsabile degli Stati nel *cyberspace*[85]. Va inoltre considerata la cooperazione transfrontaliera tra autorità nazionali al fine della raccolta delle prove digitali dei reati e la lotta alla cybercriminalità o la prevenzione degli attacchi informatici e la gestione degli incidenti su vasta scala.

Al fine di inquadrare meglio la problematica in esame, vale la pena di richiamare alcune riflessioni della dottrina sulle modalità di tale coordinamento su un piano generale, non avente ad oggetto la *cybersecurity* nello specifico, e riguardanti in particolare la prassi in materia di contrasto al terrorismo internazionale. Si tratta, come è noto, delle decisioni del Tribunale di primo grado del 2005 e della Corte di giustizia in appello del 2008 nel caso *Kadi I*, con riferimento alla legittimità delle misure restrittive adottate sulla base delle sanzioni decise dal Consiglio di sicurezza delle Nazioni Unite, e delle successive decisioni nel caso *Kadi II* e in altri casi simili[86]. La prassi ha evidenziato un ruolo determinante, anche se non sempre condiviso, della Corte di giustizia nel controllo di legittimità delle misure restrittive ex art. 215 TFUE in applicazione di decisioni PESC[87].

Si deve, in particolare, al contributo di alcuni eminenti studiosi aver messo in evidenza come a seguito dell'entrata in vigore del Trattato di Lisbona sia venuta meno la stretta corrispondenza tra obiettivi e competenze dell'UE[88]. Ciò ha comportato che le competenze attribuite nell'ambito di una specifica politica potessero essere utilizzate per

---

[85] Cfr. i lavori del *Group of Governmental Experts* (GGE) e dell'*Open-Ended Working Group* (OEWG) dell'ONU, su cui sia consentito rinviare a D. MARRANI, *La cooperazione internazionale per la sicurezza e la stabilità nel cyberspace*, cit., p 131 ss.

[86] Per un commento sul punto, si veda A. ROSAS, *EU Restrictive Measures against Third States: Value Imperialism, Futile Gesture Politics or Extravaganza of Judicial Control?*, in *Il Diritto dell'Unione europea*, 2016, n. 4, pp. 637- 651.

[87] Atteso che il controllo effettuato dalla Corte di giustizia in conformità con i principi dello stato di diritto, di proporzionalità, con il rispetto dei diritti umani e più in generale dei valori dell'UE è improntato a criteri di legittimità della politica sanzionatoria dell'Unione, la dottrina ha ipotizzato che in futuro questa materia non sia più compresa nell'ambito delle relazioni esterne dell'UE. Cfr. A. ROSAS, *op. cit.*, p. 650.

[88] E. CANNIZZARO, *L'intéraction entre objectifs politiques et compétences matérielles dans le système normatif de l'Union européenne*, in E. NEFRAMI (sous la direction de), *Objectifs et compétences dans l'Union européenne*, Bruxelles, 2013, pp. 211- 228; E. NEFRAMI, *L'action extérieure de l'Union européenne: Fondements, moyens, principes*, Paris, 2010; P. ELSUWEGE, *EU external action after the collapse of the pillar structure: in search of a new balance between delimitation and consistency*, in *Common Market Law Review*, vol. 47, 2010, pp. 987- 1019.

il raggiungimento di obiettivi collegati a finalità generali dell'UE piuttosto che circoscrivere il loro esercizio ad una determinata politica. Il ragionamento si articola in funzione dell'unitarietà dell'ordinamento dell'Unione europea e apre la strada a forme diverse di coordinamento tra politiche, in particolare la PESC e le politiche materiali disciplinate dal TFUE.

Vi è tuttavia un ostacolo al coordinamento in parola che riguarda la diversa natura delle competenze di cui trattasi: le prime eminentemente politiche in quanto espressione del metodo intergovernativo; le altre di natura economica e sociale (in ogni caso riconducibili alle materie proprie dell'integrazione) espressione del metodo comunitario. A salvaguardia delle rispettive prerogative, l'art. 40 TUE, a seguito della riforma introdotta dal Trattato di Lisbona (e già in precedenza ai sensi dell'art. 47 TUE) stabilisce una rigida separazione tra i due ambiti sopra considerati, con la conseguenza "d'entraver l'action coordonnée de l'Union et finalement de compromettre son ambition de se présenter comme un acteur politique global"[89]. Diversamente, l'art. 21, par. 3 TUE stabilisce: "L'Unione assicura la coerenza tra i vari settori dell'azione esterna e tra questi e le altre politiche. Il Consiglio e la Commissione, assistiti dall'alto rappresentante dell'unione per gli affari esteri e la politica di sicurezza, garantiscono tale coerenza e cooperano a questo fine".

Un esempio di coordinamento tra politiche del TFUE e la PESC riguarda, come accennato, le misure restrittive nei confronti di persone che hanno commesso reati nell'area dell'Unione. Le misure restrittive ai sensi dell'art. 215 TFUE sono il risultato di un atto politico nell'ambito della PESC che è coordinato con un atto vincolante (ad esempio un regolamento) della politica materiale disciplinata dal TFUE. La riflessione è volta inoltre a sondare la possibilità di un coordinamento delle Istituzioni al di là delle ipotesi stabilite dall'art. 215 TFUE. Non è possibile soffermarsi in maniera approfondita sul punto, basti osservare come il tema dell'attribuzione della condotta criminosa di privati a Stati terzi rivesta un'importanza fondamentale come è emerso anche nel caso di *cyber attacks*[90].

Una tesi che sembra poter essere condivisa è orientata a considerare in maniera flessibile il coordinamento tra politiche dell'UE, senza propendere né per una rigida divisione ai sensi dell'art. 40 TUE, né per una integrazione in ogni caso come lascerebbe intendere l'art. 21, par. 3 TUE. In tale prospettiva, è stata suggerita una "terza via" che farebbe leva: "sul negoziato informale e sulla ricerca del mutuo consenso fra Stati e Istituzioni sovrannazionali"[91]. La soluzione proposta, mediante "l'attenuazione del rigoroso principio delle competenze attribuite"[92], offrirebbe i vantaggi della coerenza e dell'efficienza delle iniziative per la *cybersecurity* dell'UE. È

[89] Così E. CANNIZZARO, *L'intéraction entre objectifs politiques et compétences matérielles dans le système normatif de l'Union européenne*, cit., p. 217.
[90] In argomento, sia consentito rinviare a D. MARRANI, *La cooperazione internazionale per la sicurezza e la stabilità nel cyberspace*, cit., p. 108 ss.
[91] Così E. CANNIZZARO, E. BARTOLONI, *Unitarietà e frammentazione nel sistema dell'azione esterna dell'Unione*, in *Il Diritto dell'Unione europea,* 2013, n. 3, p. 545.
[92] *Ivi*, p. 548.

proprio dello spazio di libertà, sicurezza e giustizia nella conformazione attuale il coordinamento dell'azione di attori e soggetti diversi secondo una logica intergovernativa indirizzato peraltro da posizioni forti delle Istituzioni: l'efficacia di un simile modello in settori che si trovano in una fase iniziale di regolamentazione quali la *cybersecurity* sembra pacifica.

6. Conclusioni

La costruzione progressiva di un quadro giuridico per la *cybersecurity* dell'UE è all'origine della frammentarietà degli interventi e dell'esigenza di coerenza tra diverse politiche funzionali alla realizzazione dell'obiettivo indicato. In tale contesto, l'assenza di una competenza attribuita è parzialmente compensata dagli orientamenti delle Istituzioni e dal ricorso all'art. 114 del TFUE. Sul piano pratico, la prassi in tema di coordinamento tra politiche del TFUE e PESC si rivela di particolare utilità nel definire l'azione dell'Unione in termini di *complementarietà* tra una serie di iniziative per la *cybersecurity*.

Come si è illustrato nell'ambito del presente lavoro, al di là della prevista armonizzazione delle discipline nazionali su profili attinenti i prodotti digitali, la certificazione della *cybersecurity* e i meccanismi di gestione dei rischi, gli Stati membri continuano a svolgere un importante ruolo di cooperazione intergovernativa al livello di istituzioni nazionali, di polizia e giudiziarie, supportati da una architettura istituzionale dell'UE che si definisce in maniera sempre più articolata e complessa.

L'insieme delle iniziative nello spazio di libertà, sicurezza e giustizia è in costante evoluzione, come dimostrano, ad esempio, i progressi compiuti nei lavori preparatori in vista dell'adozione del secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica in tema di acquisizione delle prove digitali all'estero[93]. Si ritiene che esista inoltre un ambito ancora in gran parte inesplorato relativo alla c.d. cyberdifesa attiva che riguarda, tra l'altro, l'attività di professionisti coadiuvati da strategie di *intelligence* capaci di individuare i mercati specializzati nell'offerta di prodotti e servizi digitali personalizzati (inclusi *malware* o *ransomware*) destinati ad alimentare attività illecite e/o criminose, e a prevenire eventuali *cyber* attacchi o incidenti informatici[94]. Occorre quindi che le autorità di polizia e giudiziarie degli Stati membri siano preparate anche in via preventiva a contrastare fenomeni nuovi e

[93] Una versione del testo in fase avanzata di redazione (al 20 novembre 2020) è disponibile all'indirizzo: https://rm.coe.int/provisional-text-of-provisions-2nd-protocol/1680a0522b. Per un primo commento sul negoziato in corso si veda F. GRAZIANI, *op. cit.*, p. 64 ss.

[94] Sulle nuove frontiere della difesa "attiva" che consiste nel prevenire e "correggere" determinate minacce prima che producano i loro effetti si veda, di recente, il dossier consultabile all'indirizzo: https://roma.repubblica.it/dossier-adv/eccellenze-lazio/2021/02/09/news/certego_tecnologie_processi_e_risorse_la_difesa_attiva_contro_il_cyber_crime-286701778/

complessi ed agiscano in maniera coordinata e sincronica anche con gli organismi dell'UE.

Specifiche raccomandazioni sulla *cybersecurity* nella transizione verso un'Europa digitale, quale obiettivo centrale dell'UE e priorità strategica del programma attuale della Commissione europea, sono contenute nella già menzionata *strategia dell'UE in materia di cibersicurezza per il decennio digitale*[95]. La strategia rispecchia l'approccio trasversale a diverse politiche dell'UE relative a mercato interno, spazio di libertà, sicurezza e giustizia e PESC. In aggiunta agli orientamenti in materia di sicurezza delle reti e dei sistemi informativi (NIS) e alla promozione di forme di strutturate di cooperazione tra diversi soggetti coinvolti, inclusa l'istituenda *unità congiunta per il ciberspazio*[96], che costituiscono il c.d. "scudo di cibersicurezza per l'UE", la strategia individua strumenti concreti di contrasto alla criminalità informatica. Ciò si traduce nel rafforzamento della cooperazione tra Europol e ENISA, nell'ampliamento e miglioramento della capacità delle forze dell'ordine di indagare sulla criminalità informatica, con particolare riferimento alla lotta contro l'abuso sessuale *on-line* dei minori e alle indagini digitali, compresa la criminalità nella *dark net*, nonché nell'elaborazione di norme processuali comuni che saranno definite con il supporto del laboratorio e del polo per l'innovazione di Europol.

Un importante complemento agli strumenti e alle politiche adottati sul piano interno è costituito dal pacchetto di strumenti della diplomazia informatica dell'UE, di cui si è illustrato il quadro delle misure restrittive attualmente in vigore. Al riguardo, la strategia suggerisce alcune interessanti modifiche al quadro giuridico esistente che hanno la finalità di potenziare e per alcuni aspetti di superare il (mero) coordinamento tra politiche dell'UE illustrato nel presente lavoro. In primo luogo è indicato un possibile ampliamento (o riforma) delle misure restrittive attualmente previste, mediante la valutazione di "ulteriori opzioni". In secondo luogo, la strategia ipotizza l'adozione del voto a maggioranza qualificata per l'inserimento di ulteriori persone negli elenchi allegati alla decisione PESC nell'ambito del regime di *sanzioni orizzontali* contro gli attacchi informatici[97]. La regola dell'unanimità per la decisione del Consiglio in merito alla redazione e alla modifica dei suddetti elenchi, stabilita dal regolamento 2019/796, costituisce un'evidente manifestazione del metodo intergovernativo che tende ad essere mitigato in futuro. Questo aspetto, unitamente all'evoluzione del regime sanzionatorio dell'UE (da sanzioni nei confronti di Stati terzi a sanzioni nei confronti di soggetti individuali, ovunque essi si trovino, per violazioni collegate a determinate tematiche: es. *cyber* attacchi) delinea un nuovo approccio alla sicurezza dell'UE non differenziato a seconda della politica (spazio di libertà, sicurezza e giustizia e PESC). Infine, la strategia suggerisce di integrare gli strumenti di diplomazia informatica nei meccanismi

[95] La strategia si propone di intervenire mediante strumenti normativi, di investimento e politici in tre settori principali: 1. resilienza, sovranità tecnologica e leadership; 2. Sviluppo delle capacità operative volte alla prevenzione, alla dissuasione e alla risposta e 3. Promozione di un ciberspazio globale e aperto.
[96] *Ivi*, p. 15.
[97] *Ivi*, p. 19.

di crisi dell'UE e di coordinare le azioni con gli obiettivi e gli strumenti volti a contrastare le minacce ibride e con il piano d'azione per la democrazia europea[98].

L'attuazione degli obiettivi delineati in materia di *cybersecurity* dell'UE necessita di un sistematico coordinamento tra politiche diverse. L'efficacia del processo, ancora *in itinere*, dipenderà dal livello di coerenza che le Istituzioni dell'UE e gli Stati membri riusciranno ad imprimere alla loro azione. Il risultato potrà essere misurato sia in termini di sicurezza interna nello spazio di libertà, sicurezza e giustizia, sia nella dimensione internazionale a cui l'Unione potrà portare un contributo rilevante quale attore globale.

ABSTRACT: La progressiva costruzione di un quadro giuridico dell'Unione europea sulla *cybersecurity* è all'origine di un certo grado di frammentazione. Pertanto, la coerenza tra le diverse politiche per la *cybersecurity* è fondamentale nella prospettiva della realizzazione dello spazio di libertà, sicurezza e giustizia dell'Unione europea. In questo contesto, la prassi del coordinamento tra le politiche del TFUE e PESC è un buon esempio di efficacia di azione dell'UE che fa leva sulla complementarità tra diverse iniziative. Il modello analizzato sembra applicabile alle politiche di *cybersecurity* nell'attuale sviluppo del processo di integrazione e la sua applicazione appare decisiva per l'ulteriore affermazione dell'UE quale attore globale.

KEYWORDS: cibersicurezza – competenze – politiche – misure restrittive – sicurezza dell'UE.

IN SEARCH OF CONSISTENCY BETWEEN CYBERSECURITY POLICIES IN THE EU AREA OF FREEDOM SECURITY AND JUSTICE

ABSTRACT: The ongoing construction of the EU cybersecurity legal framework is at the origin of a certain degree of fragmentation. Therefore, consistency between various cybersecurity policies is crucial in the perspective of the EU area of freedom, security and justice. In this context, the practice of coordination between TFEU and CFSP policies is a good example of effective EU action in terms of complementarity between different initiatives. This model seems applicable to cybersecurity policies at the current stage of development of the EU integration process and seems crucial in the further affirmation of the EU as a global actor.

KEYWORDS: cybersecurity – competences – policies – restrictive measures – EU security.

[98] Comunicazione della Commissione *sul piano d'azione per la democrazia europea*, Bruxelles, 3 dicembre 2020, COM/2020/790 final.