COMMISSIONE
EUROPEA

Bruxelles, 24.7.2020
COM(2020) 605 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

sulla strategia dell'UE per l'Unione della sicurezza

I. INTRODUZIONE

Nei suoi orientamenti politici la Commissione ha indicato chiaramente che occorre fare tutto il possibile per proteggere i nostri cittadini. La sicurezza non solo è fondamentale a livello personale, ma protegge anche i diritti fondamentali e costituisce il fondamento per la fiducia e il dinamismo nella nostra economia, nella nostra società e nella nostra democrazia. Il panorama della sicurezza in Europa è in costante evoluzione, oggetto di minacce mutevoli e di altri rischi tra cui i cambiamenti climatici, l'evoluzione demografica e l'instabilità politica al di fuori delle nostre frontiere. La globalizzazione, la libera circolazione e la trasformazione digitale continuano ad apportare prosperità, a renderci la vita più facile e a incentivare l'innovazione e la crescita; ma parallelamente a questi benefici, comportano rischi e costi intrinseci. Possono infatti essere manipolati da gruppi terroristici, dalla criminalità organizzata, ai fini di traffico di stupefacenti e di tratta di esseri umani, tutte minacce dirette ai cittadini e allo stile di vita europeo. Gli attacchi informatici e la criminalità informatica continuano ad aumentare. Le minacce alla sicurezza diventano inoltre sempre più complesse: si propagano grazie alla capacità di operare a livello transfrontaliero e all'interconnettività; traggono vantaggio dai labili confini tra il mondo fisico e quello digitale, sfruttano i gruppi vulnerabili e le disparità sociali ed economiche. Gli attacchi possono verificarsi senza preavviso e lasciare dietro di sé poche o nessuna traccia; soggetti statali e non statali possono mettere in atto una serie di minacce ibride[1]; e ciò che accade al di fuori dell'UE può avere un impatto determinante sulla sicurezza all'interno dell'UE.

La crisi della COVID-19 ha anche modificato il nostro concetto di minacce alla sicurezza e alla protezione e le politiche corrispondenti. Ha evidenziato la necessità di garantire la sicurezza sia negli ambienti fisici che in quelli digitali. Ha messo in luce l'importanza di un'autonomia strategica aperta per le nostre catene di approvvigionamento in termini di prodotti, servizi, infrastrutture e tecnologie critici. Ha rafforzato la necessità di coinvolgere tutti i settori e tutti gli individui in uno sforzo comune per garantire che l'UE sia, prima di tutto, più preparata e resiliente e disponga di strumenti migliori per reagire quando necessario.

I cittadini non possono essere protetti solo dagli Stati membri che agiscono singolarmente. Oggi più che mai dobbiamo far leva sui nostri punti di forza per lavorare insieme e l'UE è in una posizione privilegiata che le consentirà di fare la differenza. Può dare l'esempio, rafforzando il suo sistema generale di gestione delle crisi e lavorando all'interno e all'esterno delle sue frontiere per contribuire alla stabilità mondiale. Anche 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[2].

---

[1] Esistono molteplici definizioni di "minacce ibride", ma il concetto indica la combinazione di attività coercitive e sovversive, di metodi convenzionali e non convenzionali (cioè diplomatici, militari, economici e tecnologici), che possono essere usati in modo coordinato da soggetti statali o non statali per raggiungere determinati obiettivi (pur rimanendo sempre al di sotto della soglia di una guerra ufficialmente dichiarata). Cfr. JOIN(2016) 18 final.

[2] Ad esempio mediante i servizi forniti dai programmi spaziali dell'UE, come Copernicus, che forniscono dati di osservazione della Terra e applicazioni per la sorveglianza delle frontiere, la sicurezza marittima, le attività di contrasto, la lotta alla pirateria, la dissuasione del traffico di stupefacenti e la gestione delle emergenze.

L'UE può inoltre garantire che la politica di sicurezza resti fondata sui nostri valori europei comuni – rispettare e sostenere lo Stato di diritto, l'uguaglianza[3] e i diritti fondamentali e garantire la trasparenza, la responsabilità e il controllo democratico – per creare la fiducia su cui deve necessariamente basarsi. Può costruire un'autentica ed efficace Unione della sicurezza in cui i diritti e le libertà delle persone siano adeguatamente tutelati. La sicurezza e il rispetto dei diritti fondamentali non sono obiettivi contrastanti, bensì coerenti e complementari. Le politiche di sicurezza si devono fondare sui nostri valori e i diritti fondamentali, nel rispetto dei principi di necessità, proporzionalità e legalità, con salvaguardie appropriate che garantiscano l'assunzione di responsabilità e il ricorso giurisdizionale, consentendo nel contempo una risposta efficace per proteggere le persone, in particolare quelle più vulnerabili.

Esistono già importanti strumenti giuridici, pratici e di sostegno, che però devono essere rafforzati e attuati più adeguatamente. Sono stati compiuti molti progressi per migliorare lo scambio di informazioni e la cooperazione in materia di intelligence con gli Stati membri e per restringere lo spazio in cui i terroristi e i criminali operano. Permane tuttavia il problema della frammentazione.

Dobbiamo intervenire anche al di fuori delle frontiere dell'UE. Proteggere l'Unione e i suoi cittadini non significa più garantire solo la sicurezza all'interno delle frontiere dell'UE, ma anche affrontare la dimensione esterna della sicurezza. L'approccio dell'UE alla sicurezza esterna nel quadro della politica estera e di sicurezza comune (PESC) e della politica di sicurezza e di difesa comune (PSDC) rimarrà un elemento essenziale dell'attività dell'UE volta a rafforzare la sicurezza all'interno dell'UE. La cooperazione con i paesi terzi e a livello mondiale per affrontare le sfide comuni è fondamentale per una risposta efficace e esaustiva, dato che la stabilità e la sicurezza nei paesi vicini all'UE è fondamentale per la sicurezza dell'UE.

Sulla base dei precedenti lavori del Parlamento europeo[4], del Consiglio[5] e della Commissione[6], questa nuova strategia indica che un'autentica ed efficace Unione della sicurezza deve combinare un solido nucleo di strumenti e politiche per garantire la sicurezza nella pratica, riconoscendo nel contempo che la sicurezza ha implicazioni per tutte le componenti della società e per tutte le politiche pubbliche. L'UE deve garantire un ambiente sicuro a tutti i cittadini, indipendentemente da razza o origine etnica, religione, convinzioni personali, genere, età o orientamento sessuale.

La presente strategia copre il periodo 2020-2025 e si incentra sulla creazione di competenze e capacità per garantire un ambiente di sicurezza adeguato alle esigenze future. Definisce un approccio esteso a tutta la società in materia di sicurezza, in grado di rispondere in modo efficace e coordinato a minacce in rapida evoluzione. Definisce le priorità strategiche e gli interventi corrispondenti per affrontare i rischi fisici e digitali in modo integrato nell'intero ecosistema dell'Unione della sicurezza, concentrandosi sui settori in cui l'UE può apportare

[3] Un'Unione dell'uguaglianza: la strategia per la parità di genere 2020-2025, COM(2020) 152 final.

[4] Ad esempio i lavori della commissione TERR del Parlamento europeo, che ha riferito in materia nel novembre 2018.

[5] Dalle conclusioni del Consiglio del giugno 2015 su una "rinnovata strategia di sicurezza interna" ai più recenti risultati del Consiglio del dicembre 2019.

[6] "Attuare l'Agenda europea sulla sicurezza per combattere il terrorismo e preparare il terreno per l'Unione della sicurezza" (COM(2016) 230 final del 20.4.2016). Cfr. la recente valutazione dell'attuazione della legislazione nel settore della sicurezza interna: *Implementation of Home Affairs legislation in the field of internal security* - 2017-2020 (SWD(2020) 135).

un contributo effettivo. L'obiettivo è offrire un vero valore aggiunto in termini di sicurezza per proteggere tutti i cittadini dell'UE.

II. Un panorama europeo delle minacce per la sicurezza in rapida evoluzione

La sicurezza, la prosperità e il benessere dei cittadini dipendono dalla sicurezza. Le minacce a questa sicurezza dipendono dalla misura in cui le loro vite e i loro mezzi di sussistenza sono vulnerabili. Quanto maggiore è la vulnerabilità, tanto maggiore sarà il rischio che possa essere sfruttata. Sia le vulnerabilità sia le minacce sono in costante evoluzione e l'UE deve adattarsi.

La nostra vita quotidiana dipende da un'ampia gamma di servizi, ad esempio nei settori dell'energia, dei trasporti, della finanza e della salute. Questi servizi si fondano su infrastrutture, sia fisiche che digitali, e questo aspetto ne aumenta la vulnerabilità e la possibilità che possano subire perturbazioni. Durante la pandemia della COVID-19, le nuove tecnologie hanno consentito a molte imprese e servizi pubblici di continuare a operare, sia consentendoci di rimanere collegati nell'ambito del telelavoro sia mantenendo la logistica delle catene di approvvigionamento. Tuttavia, ciò ha anche dato il via a un aumento impressionante di attacchi dolosi, ad opera di coloro che hanno tentato di sfruttare per finalità criminali le perturbazioni dovute alla pandemia e il passaggio al telelavoro grazie alle tecnologie informatiche[7]. La carenza di beni ha creato nuove opportunità per la criminalità organizzata. Le conseguenze avrebbero potuto essere disastrose, mettendo a repentaglio i servizi sanitari essenziali nel periodo in cui sono stati sottoposti alle pressioni più intense.

I benefici sempre più numerosi che le tecnologie digitali hanno apportato alla nostra vita hanno fatto della **cibersicurezza** delle tecnologie una questione di importanza strategica[8]. I cittadini, le banche, i servizi finanziari e le imprese (in particolare le piccole e medie imprese) risentono pesantemente degli attacchi informatici. L'interdipendenza tra i sistemi fisici e quelli digitali aggrava ulteriormente i danni potenziali: qualsiasi impatto fisico è destinato a incidere sui sistemi digitali, mentre gli attacchi informatici ai sistemi di informazione e alle infrastrutture digitali possono bloccare i servizi essenziali[9]. L'avvento dell'Internet degli oggetti e il maggiore ricorso all'intelligenza artificiale comporteranno nuovi benefici ma anche una serie di nuovi rischi.

Il nostro mondo si fonda su infrastrutture e tecnologie digitali e sistemi online che ci consentono di creare attività imprenditoriali, consumare prodotti e usufruire di servizi: Tutte queste infrastrutture e tecnologie si basano sulla comunicazione e l'interazione. La dipendenza da sistemi online ha dato il via a un'ondata di attacchi da parte della

---

[7] Europol: *Beyond the pandemic*. *How COVID-19 will shape the serious and organised crime landscape in the EU* (Al di là della pandemia - In che modo la COVID-19 modificherà il panorama della criminalità organizzata e delle forme gravi di criminalità) (aprile 2020).

[8] Raccomandazione della Commissione sulla cibersicurezza delle reti 5G, C(2019) 2335; Comunicazione "Dispiegamento del 5G sicuro - Attuazione del pacchetto di strumenti dell'UE", COM(2020) 50 final.

[9] Nel marzo 2020 l'ospedale universitario di Brno nella Repubblica ceca ha subito un attacco informatico che l'ha costretto a reindirizzare i pazienti e a rinviare gli interventi chirurgici (Europol: *Pandemic Profiteering*. *How criminals exploit the COVID-19 crisis)* (Trarre vantaggio dalla pandemia: il modo in cui la criminalità sfrutta la crisi della COVID-19). L'intelligenza artificiale può essere utilizzata impropriamente per attacchi digitali, politici e fisici nonché a fini di sorveglianza. I dati raccolti dall'Internet delle cose possono essere utilizzati per sorvegliare le persone (smartwatch, assistenti virtuali, ecc.).

cibercriminalità[10]. Il cosiddetto "cybercrime as-a-service" (ossia l'offerta di servizi illegali) e l'economia "cibercriminale" sotterranea offrono un agevole accesso a prodotti e servizi informatici online offerti dalla criminalità informatica. I criminali si adattano rapidamente all'uso delle nuove tecnologie per scopi personali. Ad esempio, nella filiera farmaceutica legale sono stati inseriti medicinali contraffatti e falsificati[11]. L'aumento esponenziale di materiale pedopornografico online[12] ha messo in luce le conseguenze sociali dell'evoluzione dei modelli di criminalità. Da una recente indagine è emerso che la maggior parte delle persone nell'UE (55 %) è preoccupata dal fatto che criminali e truffatori possano avere accesso ai loro dati[13].

Il **contesto mondiale** inoltre aggrava tali minacce. Le politiche industriali aggressive di alcuni paesi terzi, in combinazione con gli incessanti furti di proprietà intellettuale favoriti dall'informatica, stanno modificando il paradigma strategico della protezione e della promozione degli interessi europei. Questo fenomeno è accentuato dall'aumento delle applicazioni a duplice uso che fa di un settore della tecnologia civile forte una risorsa importante per la difesa e la sicurezza. Lo spionaggio industriale ha un impatto significativo sull'economia, l'occupazione e la crescita dell'UE: si stima che il furto informatico di segreti commerciali costi all'UE 60 miliardi di EUR[14]. Ciò richiede una riflessione approfondita sul modo in cui le dipendenze e la maggiore esposizione alle minacce informatiche incidono sulla capacità dell'UE di proteggere in ugual misura i cittadini e le imprese.

La crisi dovuta alla COVID-19 ha altresì posto in evidenza in che modo le divisioni e le incertezze sociali creino vulnerabilità sul piano della sicurezza. Ciò aumenta la possibilità che si verifichino **attacchi** più sofisticati e **ibridi** da parte di soggetti statali e non statali, che sfruttano i punti deboli ricorrendo a una combinazione di attacchi informatici, danni alle infrastrutture critiche[15], campagne di disinformazione e radicalizzazione del discorso politico[16].

Allo stesso tempo le minacce più consolidate continuano ad evolversi. Nel 2019 si è registrata una diminuzione degli **attentati terroristici**. Ciononostante il rischio per i cittadini UE di un attacco jihadista effettuato o ispirato da Da'esh e al-Qaeda e i loro affiliati rimane elevato[17]. D'altro canto sta aumentando anche la minaccia dell'estremismo di destra

---

[10] Secondo alcune proiezioni, i costi delle violazioni di dati raggiungeranno 5 000 miliardi di USD l'anno entro il 2024, con un aumento di 3 000 miliardi di USD nel 2015 (*Juniper Research, The Future of Cybercrime & Security*).

[11] Uno studio del 2016 (Legiscript) ha stimato che, a livello globale, solo il 4 % delle farmacie online opera in modo legale, e le 30 000/35 000 farmacie illegali online mirano in particolare alla clientela dell'UE.

[12] Strategia dell'UE per una lotta più efficace contro l'abuso sessuale dei minori, COM (2020) 607.

[13] Agenzia dell'Unione europea per i diritti fondamentali (2020), *Your rights matter*: *Security concerns and experiences*, (I vostri diritti contano: preoccupazioni ed esperienze in materia di sicurezza), Indagine sui diritti fondamentali, Lussemburgo, Ufficio delle pubblicazioni.

[14] *The scale and impact of industrial espionage and theft of trade secrets through cyber* (Studio sulla portata e l'impatto dello spionaggio industriale e il furto di segreti commerciali nella rete), 2018.

[15] Le infrastrutture critiche sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini e il loro danneggiamento o distruzione avrebbe un impatto significativo (Direttiva 2008/114/CE del Consiglio).

[16] Il 97 % dei cittadini dell'UE si è imbattuto in notizie false, il 38 % su base giornaliera. Cfr. JOIN(2020) 8 final.

[17] In totale 13 Stati membri dell'UE hanno segnalato 119 attentati terroristici completati, falliti e sventati, con dieci morti e 27 feriti (Europol, Relazione sulla situazione e sulle tendenze del terrorismo nell'Unione europea, 2020).

violento[18]. Gli attacchi razzisti devono preoccuparci: gli attentati terroristici anti-semiti mortali di Halle hanno ricordato la necessità di rafforzare la reazione in linea con la dichiarazione del Consiglio del 2018[19]. Una persona su cinque nell'UE teme molto un attacco terroristico nei prossimi 12 mesi[20]. La grande maggioranza degli attentati terroristici recenti è costituita da attacchi a "tecnologia bassa", eseguiti da soggetti che agiscono da soli in spazi pubblici, mentre la propaganda terroristica online ha assunto un nuovo significato con la diretta streaming degli attacchi di Christchurch[21]. La minaccia rappresentata dalle persone radicalizzate resta elevata ed è potenzialmente rafforzata dai combattenti terroristi stranieri di ritorno e dagli estremisti che escono di prigione[22].

La crisi ha inoltre dimostrato che in nuove circostanze le minacce esistenti possono evolversi. Gruppi della **criminalità organizzata** hanno approfittato della carenza di alcuni beni per creare nuovi mercati illegali. Nell'Unione europea il traffico di sostanze stupefacenti illecite è ancora il più grande mercato criminale, il cui valore minimo al dettaglio è stimato a 30 miliardi di EUR[23]. La tratta di esseri umani continua: le stime calcolano per tutte le forme di sfruttamento un profitto annuale a livello mondiale pari a 30 miliardi di EUR[24]. Il commercio internazionale di farmaci contraffatti ha raggiunto 38,9 miliardi di EUR[25]. Allo stesso tempo, il numero limitato di confische consente ai criminali di continuare a espandere le proprie attività criminali e di infiltrarsi nell'economia legale[26]. Per i criminali e i terroristi è più facile avere accesso ad armi da fuoco, sul mercato online o grazie alle nuove tecnologie come la stampa 3-D[27]. L'uso dell'intelligenza artificiale, delle nuove tecnologie e della robotica aumenterà ulteriormente il rischio che i criminali sfruttino i vantaggi dell'innovazione per scopi dolosi[28].

Queste minacce pesano su varie categorie e colpiscono parti diverse della società in modi diversi. Comportano tutte seri rischi per le persone e le imprese e richiedono una risposta globale e coerente a livello dell'UE. Quando le vulnerabilità della sicurezza sono causate persino da piccoli oggetti domestici interconnessi, come un frigorifero o una caffettiera

---

18 Nel 2019 ci sono stati sei attacchi terroristici ad opera di gruppi di destra (uno è stato portato a termine, uno è fallito, quattro sono stati sventati: in tre Stati membri), rispetto ad uno solo nel 2018, e vi sono stati altri morti in casi non classificati come terrorismo (Europol, 2020).

19 Cfr. anche la dichiarazione del Consiglio relativa alla lotta contro l'antisemitismo e allo sviluppo di un approccio comune in materia di sicurezza per una migliore protezione delle comunità e delle istituzioni ebraiche in Europa.

20 Agenzia dell'UE per i diritti fondamentali: *Your rights matter*: *Security concerns and experiences* (I vostri diritti contano: preoccupazioni ed esperienze in materia di sicurezza), 2020.

21 Nel periodo che va da luglio 2015 alla fine del 2019 Europol ha reperito contenuti terroristici in 361 piattaforme (Europol, 2020).

22 Europol: *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism* (Esame delle migliori pratiche transatlantiche per contrastare la radicalizzazione nelle prigioni e le recidive dei terroristi), 2019.

23 Relazione 2019 dell'OEDT e di Europol sul mercato degli stupefacenti nell'UE.

24 Relazione di Europol *Trafficking in Human Beings, Financial Business Model* (Aspetto finanziario del modello operativo della tratta degli esseri umani) (2015).

25 Ufficio dell'UE per la proprietà intellettuale e relazione dell'OCSE sul commercio di prodotti farmaceutici contraffatti.

26 Relazione "Recupero e confisca dei beni: garantire che il crimine non paghi", COM(2020) 217 final.

27 Nel 2017 sono state utilizzate armi da fuoco nel 41 % dell'insieme degli attentati terroristici (Europol, 2018).

28 Nel luglio 2020 le autorità di contrasto e giudiziarie francesi e neerlandesi, insieme a Europol e Eurojust, hanno presentato l'indagine congiunta destinata a smantellare Encrochat, una rete telefonica cifrata utilizzata dalle reti criminali coinvolte in attacchi violenti, atti di corruzione, tentati omicidi e trasporti di stupefacenti su larga scala.

collegati ad Internet, non possiamo più contare esclusivamente sugli attori statali tradizionali per garantire la nostra sicurezza. Gli operatori economici devono assumersi maggiori responsabilità per quanto riguarda la cibersicurezza dei prodotti e servizi che immettono sul mercato; ma anche le singole persone devono avere almeno qualche nozione di base in materia di cibersicurezza per essere in grado di proteggersi.

III. Una risposta coordinata dell'UE per l'intera società

L'UE ha già dimostrato in che modo può apportare un reale valore aggiunto. Dal 2015 l'Unione della sicurezza ha creato nuovi collegamenti nel modo in cui le politiche di sicurezza sono affrontate a livello dell'UE. Ma occorre fare di più per coinvolgere l'intera società, comprese le autorità pubbliche a tutti i livelli, le imprese di tutti i settori e le persone in tutti gli Stati membri. La crescente consapevolezza dei rischi di dipendenza[29] e l'esigenza di una strategia industriale europea forte[30] richiedono un'UE dotata di una massa critica di produzione industriale tecnologica e di una catena di approvvigionamento resiliente. La forza presuppone anche il pieno rispetto dei diritti fondamentali e dei valori dell'UE: si tratta di una condizione preliminare per politiche di sicurezza legittime, efficaci e sostenibili. La presente strategia sull'Unione della sicurezza stabilisce assi di intervento concreti. Si articola intorno agli obiettivi comuni seguenti:

- ***Sviluppare competenze e capacità in materia di individuazione tempestiva, prevenzione e reazione rapida alle crisi:*** l'Europa deve essere più resiliente per prevenire, proteggere e resistere agli shock futuri. Dobbiamo sviluppare competenze e capacità anche per l'individuazione tempestiva e la risposta rapida alle crisi in materia di sicurezza attraverso un approccio integrato e coordinato, sia a livello globale che attraverso iniziative settoriali (ad esempio nei settori della finanza, dell'energia, della giustizia, delle autorità di contrasto, dell'assistenza sanitaria, della sicurezza marittima e dei trasporti) avvalendoci degli strumenti e delle iniziative esistenti[31]. La Commissione presenterà inoltre proposte per un sistema di gestione delle crisi di più ampia portata all'interno dell'UE, che potrebbe essere rilevante anche per la sicurezza.
- ***Priorità ai risultati***: una strategia orientata ai risultati deve basarsi su un un'attenta valutazione delle minacce e dei rischi in modo che il nostro impegno sia più efficace possibile. Deve definire e applicare le norme e gli strumenti adeguati e richiede una intelligence strategica alla base delle politiche di sicurezza dell'UE. Laddove occorra un intervento normativo dell'UE, è necessario effettuare un follow-up degli atti legislativi per accertarsi che siano pienamente attuati e per evitare frammentazioni e lacune che qualcuno potrebbe sfruttare. L'effettiva attuazione di questa strategia dipenderà anche dall'ottenimento di un finanziamento adeguato nel prossimo periodo di programmazione 2021-2027, anche per le agenzie dell'UE collegate.

---

[29] I rischi di dipendenza da paesi terzi comportano una maggiore esposizione alle minacce potenziali, che vanno dallo sfruttamento della vulnerabilità delle infrastrutture informatiche per compromettere infrastrutture critiche (ad esempio nel settore dell'energia, dei trasporti, delle banche o della sanità) all'assunzione del controllo di sistemi di controllo industriale e all'aumento delle possibilità di furto di dati o di spionaggio.

[30] Comunicazione della Commissione "Una nuova strategia industriale per l'Europa" COM(2020) 102 final.

[31] Tra cui i dispositivi integrati dell'UE per la risposta politica alle crisi (IPCR), il Centro di coordinamento della risposta alle emergenze, la raccomandazione della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (C(2017) 6100), e il documento di lavoro su un protocollo operativo per contrastare le minacce ibride (*EU Playbook)* SWD(2016) 227.

- ***Associare tutti gli operatori del settore pubblico e del settore privato in uno sforzo comune:*** i principali operatori sia del settore pubblico che di quello privato sono stati finora poco propensi a condividere informazioni in materia di sicurezza per timore di compromettere la sicurezza nazionale o la competitività[32]. Eppure, la massima efficacia la otteniamo quando siamo tutti pronti a sostenerci l'un altro. In primo luogo, ciò significa una cooperazione più intensa tra Stati membri, con il coinvolgimento delle autorità di contrasto e giudiziarie e di altre autorità pubbliche, e con la partecipazione delle istituzioni e delle agenzie dell'UE, al fine di giungere alla comprensione e allo scambio necessari per soluzioni comuni. Anche la cooperazione con il settore privato è fondamentale, tanto più che l'industria possiede una parte importante dell'infrastruttura digitale e non digitale indispensabile per lottare efficacemente contro la criminalità e il terrorismo. Anche i singoli individui possono apportare il loro contributo, ad esempio creando competenze e consapevolezza per combattere la criminalità informatica o la disinformazione. Infine, questo sforzo comune deve estendersi al di là delle nostre frontiere, instaurando legami più stretti con i partner che condividono gli stessi principi.

IV. Proteggere tutti nell'UE: priorità strategiche per l'Unione della sicurezza

L'UE si trova in una posizione privilegiata per rispondere a queste nuove sfide e minacce globali. L'analisi della minaccia menzionata evidenzia quattro priorità strategiche interdipendenti su cui occorre lavorare a livello unionale, nel pieno rispetto dei diritti fondamentali: i) un ambiente della sicurezza adeguato alle esigenze future, ii) affrontare le minacce in evoluzione, iii) proteggere i cittadini europei dal terrorismo e dalla criminalità organizzata, iv) un ecosistema europeo forte in materia di sicurezza.

1. Un ambiente della sicurezza adeguato alle esigenze del futuro

Protezione e resilienza delle infrastrutture critiche

Nella vita quotidiana gli individui dipendono da infrastrutture chiave, per viaggiare, lavorare o beneficiare di servizi pubblici essenziali come gli ospedali, i trasporti, l'approvvigionamento energetico, o per esercitare i loro diritti democratici. Se queste infrastrutture non sono sufficientemente protette e resilienti, gli attacchi possono causare enormi perturbazioni – fisiche o digitali – sia nei singoli Stati membri che potenzialmente in tutta l'UE.

L'attuale quadro dell'UE in materia di protezione e resilienza delle infrastrutture critiche[33] non è al passo con l'evoluzione dei rischi. L'aumento delle interdipendenze implica che le perturbazioni in un settore possono avere un impatto immediato sulle operazioni in altri settori: un attacco contro la produzione di energia elettrica potrebbe interrompere il funzionamento delle telecomunicazioni, degli ospedali, delle banche o degli aeroporti, mentre un attacco alle infrastrutture digitali potrebbe causare perturbazioni nelle reti energetiche o della finanza. Con l'aumento della dipendenza della nostra economia e della nostra società dalle tecnologie online, i rischi di questo tipo non fanno che aumentare. Il

[32] Comunicazione congiunta "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE", JOIN(2017) 450 final.

[33] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016). Direttiva 2008/114/CE del Consiglio, relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione.

quadro legislativo deve far fronte all'aumento dell'interconnessione e dell'interdipendenza, con misure rigorose in materia di protezione e resilienza delle infrastrutture critiche, sia informatiche che fisiche. I servizi essenziali, compresi quelli basati sulle infrastrutture spaziali, devono essere adeguatamente protetti contro le minacce attuali e previste, ma devono anche essere resilienti. I sistemi devono pertanto essere in grado di prepararsi agli eventi avversi, di pianificare la loro risposta, di farvi fronte e di riprendersi da questi eventi, adattandosi in maniera più adeguata.

Al tempo stesso, gli Stati membri hanno esercitato il loro potere discrezionale attuando la legislazione esistente in modi diversi. La frammentazione che ne deriva può compromettere il mercato interno e rendere il coordinamento transfrontaliero più difficile, ovviamente in misura maggiore nelle regioni frontaliere. Gli operatori che forniscono servizi essenziali in diversi Stati membri devono conformarsi a diversi regimi di comunicazione. La Commissione sta valutando se **nuovi quadri per le infrastrutture fisiche e digitali** potrebbero comportare una maggiore coerenza e un approccio più omogeneo in modo da garantire l'affidabilità della fornitura di servizi essenziali. Questo quadro deve essere accompagnato da **iniziative settoriali specifiche** per affrontare i rischi specifici cui devono far fronte le infrastrutture critiche, ad esempio nei settori dei trasporti, dell'energia, della finanza e della sanità[34]. Data l'elevata dipendenza del settore finanziario dai servizi informatici e la sua grande vulnerabilità ai ciberattacchi, un primo passo sarà un'iniziativa sulla resilienza operativa digitale per i settori finanziari. A causa della particolare sensibilità e dell'impatto del sistema energetico, un'iniziativa specifica mirerà a rafforzare la resilienza delle infrastrutture energetiche critiche alle minacce fisiche, informatiche e ibride, garantendo parità di condizioni per gli operatori del settore energetico al di là delle frontiere.

Gli effetti sulla sicurezza degli investimenti diretti esteri che rischiano di incidere sulle infrastrutture o le tecnologie critiche saranno anch'essi oggetto delle valutazioni effettuate dagli Stati membri e dalla Commissione nell'ambito del nuovo quadro europeo per il controllo degli investimenti diretti esteri[35].

L'UE può anche mettere a punto strumenti nuovi per sostenere la resilienza delle infrastrutture critiche. L'Internet mondiale ha dimostrato finora un elevato livello di resilienza, in particolare per quanto riguarda la capacità di sostenere un aumento dei volumi di traffico. Tuttavia, dobbiamo essere pronti ad affrontare eventuali crisi future che minacciano la sicurezza, la stabilità e la resilienza di Internet. Assicurare che Internet continui a funzionare significa garantire che resista agli incidenti informatici e alle attività online dolose e limitare la dipendenza da infrastrutture e servizi situati al di fuori dell'Europa. Ciò richiederà una serie di atti legislativi, rivedendo le norme esistenti per garantire un livello comune elevato di sicurezza delle reti e dei sistemi informatici nell'UE; sarà inoltre necessario aumentare gli investimenti nella ricerca e nell'innovazione e

[34] Tenuto conto del fatto che il settore sanitario è stato sotto pressione, in particolare durante la crisi dovuta alla COVID-19, la Commissione prenderà in considerazione anche iniziative volte a rafforzare il quadro di sicurezza sanitaria dell'UE e le agenzie UE competenti al fine di rispondere alle gravi minacce sanitarie transfrontaliere.

[35] Con la sua piena entrata in vigore l'11 ottobre 2020, il regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione, doterà l'UE di un nuovo meccanismo di cooperazione in relazione agli investimenti diretti provenienti da paesi terzi che potrebbero incidere sulla sicurezza o sull'ordine pubblico. Nel quadro del regolamento, gli Stati membri e la Commissione valuteranno i potenziali rischi connessi agli IDE e, se opportuno e pertinente per più di uno Stato membro, proporranno mezzi adeguati per attenuare tali rischi.

prevedere la diffusione o il rafforzamento delle infrastrutture e delle risorse Internet di base, in particolare il sistema dei nomi di dominio[36].

Un elemento fondamentale per proteggere le principali risorse digitali dell'UE e nazionali consiste nel dotare le infrastrutture critiche di un canale sicuro per le comunicazioni. La Commissione sta collaborando con gli Stati membri per istituire un'infrastruttura quantistica da punto a punto sicura, terrestre e spaziale, associata al sistema di comunicazioni satellitari governative sicure previsto dal regolamento relativo al programma spaziale[37].

Cibersicurezza

Il numero di attacchi informatici continua ad aumentare[38]. Questi attacchi sono più sofisticati che mai, provengono da un'ampia gamma di fonti all'interno e all'esterno dell'UE e si incentrano sulle aree di massima vulnerabilità. Spesso sono coinvolti soggetti statali o sostenuti dallo Stato e gli attacchi sono diretti a infrastrutture digitali chiave come i principali fornitori di servizi cloud[39]. I rischi informatici si stanno dimostrando una grave minaccia anche per il sistema finanziario. Il Fondo monetario internazionale ha stimato la perdita annua dovuta agli attacchi informatici al 9 % del reddito netto delle banche a livello mondiale, pari a circa 100 miliardi di USD[40]. Il passaggio a dispositivi connessi comporterà grandi vantaggi per gli utenti: tuttavia, con una quantità inferiore di dati conservati e trattati nei centri di dati e una quantità superiore trattata più vicino all'utente "ai margini della rete"[41], la cibersicurezza non sarà più in grado di concentrarsi sulla protezione di punti centrali[42]

Nel 2017 l'UE ha presentato un approccio alla cibersicurezza fondata sullo sviluppo della resilienza, su una risposta rapida e un'azione efficace di dissuasione[43]. L'UE adesso deve garantire che le sue capacità in materia di cibersicurezza siano al passo con la realtà, al fine di garantire resilienza e risposte adeguate. Ciò presuppone un approccio che coinvolge tutta la società, in cui le istituzioni, le agenzie e gli organismi dell'UE, gli Stati membri, l'industria, il mondo accademico e gli individui danno alla cibersicurezza la priorità che richiede[44]. Anche questo approccio orizzontale deve essere integrato da approcci di cibersicurezza settoriali in funzione delle diverse aree quali l'energia, i servizi finanziari, i trasporti o la sanità. La prossima fase del lavoro dell'UE dovrebbe essere messa a punto in una strategia europea per la cibersicurezza riveduta.

---

[36] Il sistema dei nomi di dominio (DNS) è un sistema di nomi gerarchico e decentrato per computer, servizi, o altre risorse collegati a Internet o ad una rete privata. Traduce nomi di dominio negli indirizzi IP necessari per localizzare e individuare servizi e dispositivi informatici.

[37] Proposta di regolamento che istituisce il programma spaziale dell'Unione e l'Agenzia dell'Unione europea per il programma spaziale, COM(2018) 447 final.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Gli attacchi distribuiti di negazione del servizio (DDoS) rimangono una minaccia permanente: nel febbraio 2020 i fornitori principali hanno dovuto far fronte a massicci attacchi di tipo DDoS, come gli attacchi contro i servizi web di Amazon.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

[41] L'*edge computing* è un'architettura informatica distribuita e aperta dotata di un potere di trattamento decentrato, su cui si fondano l'informatica mobile e le tecnologie dell'Internet delle cose. Nell'*edge computing*, i dati sono trattati dal dispositivo stesso o da un computer o un server locale, anziché essere trasmessi a un centro dati.

[42] Comunicazione su una strategia europea per i dati, COM(2020) 66 final.

[43] Comunicazione congiunta "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE", JOIN(2017) 450 final.

[44] La relazione "*Cybersecurity – our digital Anchor*" (Cibersicurezza – il nostro ancoraggio digitale) del Centro comune di ricerca offre una panoramica multidimensionale della crescita della cibersicurezza negli ultimi 40 anni.

Esplorare forme di cooperazione nuove e più efficaci tra i servizi di intelligence, il SITCEN dell'UE e altre organizzazioni preposte alla sicurezza dovrebbe rientrare tra gli interventi volti a rafforzare la cibersicurezza e a combattere il terrorismo, l'estremismo, la radicalizzazione e le minacce ibride.

Dato il dispiegamento in corso dell'**infrastruttura 5G** nell'UE e la potenziale dipendenza di molti servizi critici dalle reti 5G, le conseguenze di una perturbazione sistemica e generalizzata sarebbero particolarmente gravi. Il processo avviato dalla raccomandazione della Commissione del 2019 sulla cibersicurezza delle reti 5G[45] ha portato adesso a interventi specifici degli Stati membri in relazione alle misure chiave stabilite nel pacchetto di strumenti per il 5G[46].

Una delle principali esigenze a lungo termine è lo sviluppo di una cultura della **cibersicurezza fin dalla progettazione**, in cui l'elemento della sicurezza è integrato nei prodotti e nei servizi. Un importante contributo in tal senso sarà il nuovo quadro di certificazione della cibersicurezza di cui al regolamento sulla cibersicurezza[47]. Il quadro è già in fase di elaborazione: due sistemi di certificazione sono già in preparazione e le priorità per gli ulteriori regimi saranno definite più avanti nel corso dell'anno. La cooperazione tra l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), le autorità preposte alla protezione dei dati e il comitato europeo per la protezione dei dati[48] è di fondamentale importanza in questo settore.

Per garantire una cooperazione operativa strutturata e coordinata la Commissione ha già individuato la necessità di un'**unità congiunta per il ciberspazio**, che potrebbe includere un meccanismo di assistenza reciproca a livello dell'UE nei periodi di crisi. Sulla base dell'attuazione della raccomandazione relativa al programma[49], l'unità congiunta per il ciberspazio potrebbe instaurare un clima di fiducia tra i diversi operatori dell'ecosistema europeo della cibersicurezza e offrire un servizio essenziale agli Stati membri. La Commissione avvierà discussioni con i portatori di interessi pertinenti (a cominciare dagli Stati membri) e definirà entro la fine del 2020 una procedura, tappe e scadenze chiare.

Altrettanto importanti sono le norme comuni in materia di sicurezza delle informazioni e sicurezza informatica per l'insieme delle istituzioni, organi e agenzie dell'UE. L'obiettivo dovrebbe essere elaborare norme comuni obbligatorie e rigorose per lo scambio sicuro di informazioni e la sicurezza delle infrastrutture e dei sistemi digitali in tutte le istituzioni, gli organismi e le agenzie dell'UE. Questo nuovo quadro dovrebbe fungere da base per una cooperazione operativa forte ed efficiente sulla cibersicurezza in tutte le istituzioni, gli organismi e le agenzie dell'UE, incentrata sul ruolo della squadra di pronto intervento informatico (CERT-UE) per l'insieme delle istituzioni, degli organismi e delle agenzie dell'UE.

---

[45] Raccomandazione della Commissione sulla cibersicurezza delle reti 5G, C(2019) 2335 final, di cui è prevista, nel documento stesso, una revisione nell'ultimo trimestre del 2020.

[46] Cfr. la relazione del gruppo di cooperazione NIS sull'attuazione del pacchetto di strumenti del 24 luglio 2020.

[47] Regolamento 2019/881 relativo all'ENISA (Agenzia dell'Unione europea per la cibersicurezza) e alla certificazione della cibersicurezza delle tecnologie dell'informazione e della comunicazione (regolamento sulla cibersicurezza).

[48] Comunicazione sulla protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati, COM(2020) 264 final.

[49] Raccomandazione (UE) 2017/1584 della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.

Data la sua natura globale, la creazione e il mantenimento di solidi **partenariati internazionali** sono fondamentali per prevenire, scoraggiare e far fronte ai ciberattacchi. Il quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica")[50] stabilisce misure nell'ambito della politica estera e di sicurezza comune, ivi comprese misure restrittive (sanzioni), che possono essere utilizzate contro le attività che ledono gli interessi politici, di sicurezza e economici dell'UE. L'UE dovrebbe inoltre intensificare il proprio lavoro avvalendosi di fondi destinati allo sviluppo e alla cooperazione per creare capacità al fine di aiutare i paesi partner a rafforzare i loro ecosistemi digitali, adottare riforme legislative nazionali e rispettare le norme internazionali. In questo modo si rafforzerà la resilienza della comunità in generale e la sua capacità di contrastare e reagire adeguatamente alle minacce informatiche. Sarà necessario anche un lavoro specifico per promuovere le norme dell'UE e la legislazione pertinente al fine di rafforzare la cibersicurezza dei paesi partner del vicinato[51].

Protezione degli spazi pubblici

I recenti attentati terroristici si sono concentrati negli **spazi pubblici**, tra cui luoghi di culto e nodi di trasporto, sfruttando la loro natura aperta e accessibile. L'aumento degli atti di terrorismo scatenati dall'estremismo politico o ideologico ha reso questa minaccia ancora più grave. Ciò richiede il rafforzamento della protezione fisica di tali luoghi e sistemi di rilevamento adeguati, senza compromettere le libertà dei cittadini[52]. La Commissione rafforzerà la cooperazione tra settore pubblico e privato per la protezione degli spazi pubblici, con finanziamenti, scambi di esperienze e buone pratiche, orientamenti specifici[53] e raccomandazioni[54]. Nell'ambito di questo approccio sono previste anche azioni di sensibilizzazione, la fissazione di requisiti di prestazione, il collaudo di attrezzature di rilevamento e il rafforzamento dei controlli dei precedenti personali per far fronte alle minacce interne. Un aspetto importante su cui riflettere e che richiede particolare attenzione è il fatto che le minoranze e le persone vulnerabili possono essere colpite in modo sproporzionato, in particolare quando sono prese di mira per la loro religione o la loro identità di genere. Le autorità pubbliche regionali e locali svolgono un ruolo importante nel rafforzamento della sicurezza degli spazi pubblici. La Commissione contribuisce inoltre a promuovere nelle città l'innovazione in materia di sicurezza negli spazi pubblici[55]. L'avvio, nel novembre 2018, di un nuovo partenariato dell'agenda urbana[56] sulla "sicurezza negli spazi pubblici" riflette la chiara volontà degli Stati membri, della Commissione e delle città di affrontare in modo più adeguato le minacce alla sicurezza nello spazio urbano.

---

50 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

51 Cfr. le linee guida dell'UE per lo sviluppo delle capacità informatiche esterne, adottate nelle conclusioni del Consiglio del 26 giugno 2018.

52 I sistemi di identificazione biometrica remota meritano una particolare attenzione. Le osservazioni iniziali della Commissione figurano nel Libro bianco della Commissione del 19 febbraio 2020 sull'intelligenza artificiale, COM(2020) 65.

53 Come ad esempio gli orientamenti per la scelta di soluzioni appropriate per i sistemi di barriera ai fini della protezione dello spazio pubblico (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

54 Orientamenti in materia di buone pratiche sono contenuti nel documento SWD(2019) 140 che contiene una sezione sulla cooperazione pubblico-privato. I finanziamenti nell'ambito dell'ISF-Polizia sono incentrati in modo particolare sul rafforzamento della cooperazione pubblico-privato.

55 Tre città (Pireo in Grecia, Tampere in Finlandia e Torino in Italia) sperimenteranno nuove soluzioni nell'ambito delle "azioni innovative urbane", cofinanziate dal Fondo europeo di sviluppo regionale (FESR).

56 L'agenda urbana per l'UE è un nuovo metodo di lavoro a più livelli che promuove la collaborazione tra gli Stati membri, le città, la Commissione e altri portatori di interessi per incentivare la crescita, la vivibilità e l'innovazione nelle città europee e per individuare e affrontare con successo le sfide sociali.

Il mercato dei **droni** continua ad ampliarsi, con molti utilizzi validi e legittimi. Tuttavia i droni possono anche essere impropriamente utilizzati da criminali e terroristi, e in tal caso gli spazi pubblici sono particolarmente minacciati. Gli obiettivi possono includere individui, assembramenti di persone, infrastrutture critiche, autorità di contrasto, frontiere o spazi pubblici. Le conoscenze sull'uso dei droni nei conflitti potrebbero essere sfruttate in Europa sia direttamente (da parte dei combattenti terroristi stranieri di ritorno) che online. Le norme già elaborate dall'Agenzia europea per la sicurezza aerea costituiscono un primo passo importante anche per quanto riguarda la registrazione degli operatori di droni e l'identificazione remota obbligatoria dei droni. Adesso che i droni sono sempre più disponibili, economicamente accessibili e perfezionati, sono tuttavia necessari ulteriori interventi che potrebbero includere la condivisione di informazioni, orientamenti e buone pratiche ad uso di tutti, autorità di contrasto comprese, o la sperimentazione su più ampia scala di contromisure per i droni[57]. Inoltre, occorre analizzare e affrontare ulteriormente le implicazioni dell'uso dei droni negli spazi pubblici per la protezione della riservatezza dei dati.

Azioni principali
• Legislazione sulla protezione e la resilienza delle infrastrutture critiche • Revisione della direttiva sulla sicurezza delle reti e dell'informazione • Un'iniziativa sulla resilienza operativa del settore finanziario • Protezione e cibersicurezza delle infrastrutture energetiche critiche e codice di rete sulla cibersicurezza per i flussi transfrontalieri di energia elettrica • Una strategia europea per la sicurezza informatica • Prossime tappe verso la creazione di un'unità congiunta per il ciberspazio • Norme comuni in materia di sicurezza delle informazioni e cibersicurezza per le istituzioni, gli organi e le agenzie dell'UE • Rafforzamento della cooperazione per la protezione degli spazi pubblici, compresi i luoghi di culto • Condivisione delle migliori pratiche per contrastare l'uso improprio dei droni

2. Affrontare le minacce in evoluzione

Cibercriminalità

La tecnologia offre nuove opportunità per la società, e anche nuovi strumenti per il sistema giudiziario e le autorità di contrasto. Nello stesso tempo, tuttavia, offre nuove prospettive ai criminali. I software maligni, il furto di dati personali o commerciali mediante la pirateria e l'interruzione delle attività digitali con i relativi danni finanziari o di reputazione sono tutti in aumento. Il primo strumento di difesa è la creazione di un ambiente resiliente grazie ad una solida cibersicurezza. Le autorità di contrasto devono poter di lavorare nel settore delle indagini digitali disponendo di norme chiare per indagare e perseguire i reati e offrire alle vittime la protezione necessaria. Queste attività dovrebbero fondarsi sulla task force di azione congiunta contro la criminalità informatica di Europol e il protocollo di risposta alle emergenze delle autorità di contrasto istituiti per coordinare la risposta ai ciberattacchi su vasta scala. Occorrono inoltre meccanismi efficaci che consentano di istituire dei partenariati e una cooperazione tra il settore pubblico e quello privato.

[57] Di recente è stato istituito un programma pluriennale di test per aiutare gli Stati membri a mettere a punto una metodologia comune e una piattaforma di prova in questo ambito.

Parallelamente, la lotta alla cibercriminalità dovrebbe diventare una priorità strategica in materia di comunicazione in tutta l'UE, al fine di sensibilizzare i cittadini europei ai rischi e alle misure di prevenzione che possono adottare. Ciò dovrebbe iscriversi nell'ambito di un approccio proattivo. Un passo fondamentale è anche la piena attuazione dell'attuale quadro giuridico[58]: la Commissione è pronta a ricorrere ai procedimenti di infrazione, se necessario, e a sottoporre il quadro di riferimento a esami periodici per garantire che rimanga idoneo allo scopo. La Commissione esaminerà inoltre, in collaborazione con Europol e l'agenzia dell'UE per la cibersicurezza (ENISA), la fattibilità di un sistema di allarme rapido dell'UE relativo alla cibercriminalità che possa garantire il flusso delle informazioni e reazioni rapide nel caso di un aumento del fenomeno.

La cibercriminalità è una sfida a livello mondiale che richiede un'efficace cooperazione internazionale. L'UE sostiene la convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica; si tratta di un modello efficace e consolidato che consente a tutti i paesi di individuare i sistemi e i canali di comunicazione di cui hanno bisogno per collaborare efficacemente.

Quasi la metà dei cittadini dell'UE è preoccupata per l'uso improprio dei dati[59] e il **furto di identità** causa grandi apprensioni[60]. L'uso fraudolento dell'identità ai fini di profitto economico è un aspetto, ma può esserci anche un notevole impatto personale e psicologico, con post illegali pubblicati dal ladro di identità che possono rimanere online per anni. La Commissione esaminerà le misure pratiche che si potrebbero adottare per proteggere le vittime da tutte le forme di furto di identità, tenendo conto dell'iniziativa europea sull'identità digitale di prossima pubblicazione[61].

Affrontare la cibercriminalità significa guardare al futuro. La società utilizza i nuovi sviluppi tecnologici per rafforzare l'economia e la società, ma i criminali possono anche cercare di sfruttare questi strumenti a fini negativi. Ad esempio, i criminali possono utilizzare l'intelligenza artificiale per individuare e identificare password, per semplificare la creazione di software maligni o ancora per sfruttare immagini e file audio che possono essere usati per furti d'identità o frodi.

Moderni organismi di contrasto

Gli operatori della giustizia e delle attività di contrasto devono adeguarsi alle nuove tecnologie. Per stare al passo con l'evoluzione tecnologica e le minacce emergenti, le autorità di contrasto devono avvalersi di nuovi strumenti, acquisire nuove competenze e sviluppare tecniche investigative alternative. Ad integrazione delle azioni legislative volte a migliorare l'accesso transfrontaliero alle prove elettroniche nelle indagini penali, l'UE può aiutare le autorità di contrasto a sviluppare le capacità di cui hanno bisogno per individuare, proteggere e leggere i dati necessari alle indagini sui reati e per utilizzare tali dati come prove nei procedimenti giudiziari. La Commissione esaminerà misure volte a **rafforzare la capacità di contrasto nelle indagini digitali**, definendo le modalità per utilizzare al meglio

[58] Direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione.

[59] 46 % (Eurobarometro sulla posizione dei cittadini europei nei confronti della cibersicurezza, gennaio 2020).

[60] La grande maggioranza dei partecipanti (95 %) all'indagine Eurobarometro del 2018 sulla posizione dei cittadini europei nei confronti della sicurezza di Internet (Europeans' attitudes towards Internet security) considera il furto di identità come un reato grave e il 70% lo ritiene un reato molto grave. L'indagine Eurobarometro, pubblicata nel gennaio 2020, ha confermato le preoccupazioni relative alla cibercriminalità, alla frode online e al furto di identità: due terzi dei rispondenti sono preoccupati dalle frodi bancarie (67 %) o dal furto di identità (66 %).

[61] Comunicazione del 19 febbraio 2020 "Plasmare il futuro digitale dell'Europa", COM(2020) 67.

la ricerca e lo sviluppo al fine di creare nuovi strumenti di contrasto e precisando come fornire un adeguato insieme di competenze alle attività di contrasto e al sistema giudiziario attraverso azioni di formazione. Ciò comprenderà anche la messa a punto di valutazioni scientifiche e di metodi di prova rigorosi ad opera del Centro comune di ricerca della Commissione.

Approcci comuni possono anche garantire che **l'intelligenza artificiale, le capacità spaziali, i Big Data** e **il calcolo ad alte prestazioni** siano integrati nella politica di sicurezza in modo efficace, sia per quanto riguarda la lotta ai reati che per garantire i diritti fondamentali. L'intelligenza artificiale potrebbe agire come potente strumento per combattere la criminalità, aprendo enormi capacità investigative grazie all'analisi di grandi quantità di informazioni e all'individuazione di modelli e anomalie[62]. Può inoltre fornire strumenti concreti, ad esempio per contribuire a individuare i contenuti terroristici online, scoprire transazioni sospette nelle vendite di prodotti pericolosi o offrire assistenza ai cittadini in situazioni di emergenza. Realizzare questo potenziale significa creare ponti tra la ricerca, l'innovazione e gli utenti dell'intelligenza artificiale grazie a una governance e a infrastrutture tecniche adeguate, coinvolgendo attivamente il settore privato e il mondo accademico. Significa anche applicare i più elevati standard di conformità ai diritti fondamentali, garantendo nel contempo un'efficace protezione dei cittadini. In particolare, le decisioni che hanno un impatto sulle persone devono essere sottoposte a un controllo da parte di un essere umano e devono essere conformi al diritto dell'Unione applicabile in materia[63].

Le informazioni e le prove elettroniche sono necessarie per circa l'85 % delle indagini relative a reati gravi, e il 65 % delle richieste totali è rivolto a prestatori con sede in un'altra giurisdizione[64]. Il fatto che le tracce materiali tradizionali siano ora diventate tracce virtuali online amplia ulteriormente il divario tra le capacità degli organismi di contrasto e quelle dei criminali. È essenziale stabilire norme chiare per l'accesso transfrontaliero alle prove elettroniche nelle indagini penali. La rapida adozione da parte del Parlamento europeo e del Consiglio delle proposte relative alle prove elettroniche è pertanto fondamentale per fornire agli operatori uno strumento efficace. Anche l'accesso transfrontaliero alle prove elettroniche mediante negoziati internazionali multilaterali e bilaterali è fondamentale per definire norme compatibili a livello internazionale[65].

L'accesso alle prove digitali dipende anche dalla disponibilità di informazioni. Se i dati vengono cancellati troppo rapidamente, prove importanti possono scomparire impedendo di identificare e localizzare le persone sospettate e le reti criminali (oltre alle vittime). D'altro canto, i meccanismi di conservazione dei dati sollevano questioni relative alla tutela della vita privata. In funzione dell'esito delle cause pendenti dinanzi alla Corte di giustizia dell'Unione europea, la Commissione valuterà la via da seguire in materia di conservazione dei dati.

---

62 Ad esempio, nel caso dei reati finanziari.

63 Ciò implica il rispetto della legislazione vigente, compresi il regolamento generale sulla protezione dei dati (UE) 2016/679 e la direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie (UE) 2016/680, che disciplina il trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

64 Commissione europea, SWD (2018) 118 final.

65 In particolare, il secondo protocollo aggiuntivo alla convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica e un accordo tra l'UE e gli Stati Uniti sull'accesso transfrontaliero alle prove elettroniche.

L'accesso alle informazioni relative alla registrazione dei nomi di dominio Internet (dati WHOIS)[66] è importante per le indagini penali, la cibersicurezza e la protezione dei consumatori. Tuttavia, l'accesso a tali informazioni diventa sempre più difficile, in mancanza dell'adozione di una nuova politica per i dati WHOIS da parte dell'ICANN (*Internet Corporation for Assigned Names and Numbers*). La Commissione continuerà a collaborare con l'ICANN e la comunità multipartecipativa per garantire che i legittimi richiedenti l'accesso, compresi gli organismi di contrasto, possano ottenere un accesso efficiente ai dati WHOIS, in linea con i regolamenti in materia di protezione dei dati, sia dell'UE che internazionali. Ciò comprenderà la valutazione delle possibili soluzioni, compresa l'eventuale necessità di una legislazione che chiarisca le norme per l'accesso a tali informazioni.

Le autorità di contrasto e giudiziarie devono anche essere attrezzate per ottenere i dati e le prove necessari una volta che **l'architettura 5G per le telecomunicazioni mobili** sarà pienamente operativa nell'UE, in modo da rispettare la riservatezza delle comunicazioni. La Commissione sosterrà un approccio rafforzato e coordinato all'elaborazione di norme internazionali, definendo le migliori pratiche, i processi e l'interoperabilità tecnica in settori tecnologici fondamentali quali l'intelligenza artificiale, l'Internet delle cose o le tecnologie blockchain.

Attualmente una parte sostanziale delle indagini contro tutte le forme di criminalità e terrorismo implica **informazioni cifrate**. La cifratura è essenziale nel mondo digitale, in quanto rende sicuri i sistemi digitali e le transazioni e tutela una serie di diritti fondamentali, tra cui la libertà di espressione, la privacy e la protezione dei dati. Tuttavia, se utilizzata a fini criminali, può mascherare anche l'identità dei criminali e nascondere il contenuto delle loro comunicazioni. La Commissione esplorerà e sosterrà soluzioni tecniche, operative e giuridiche equilibrate rispetto alle sfide e promuoverà un approccio che mantenga l'efficacia della cifratura nel proteggere la privacy e la sicurezza delle comunicazioni, fornendo nel contempo una risposta efficace alla criminalità e al terrorismo.

Lotta ai contenuti illegali online

Allineare la sicurezza degli ambienti fisici e di quelli online significa continuare a mettere in atto azioni per **contrastare i contenuti illegali online**. Sempre più spesso, le minacce principali per i cittadini, quali il terrorismo, l'estremismo o gli abusi sessuali sui minori, fanno affidamento sull'ambiente digitale: ciò richiede un'azione concreta e un quadro per garantire il rispetto dei diritti fondamentali. Un primo passo essenziale in questa direzione è la rapida conclusione dei negoziati sulla proposta di legislazione[67] sui contenuti terroristici online, di cui va garantita l'attuazione. Il rafforzamento della cooperazione volontaria tra le autorità di contrasto e il settore privato nel **Forum dell'UE su Internet** è fondamentale anche per contrastare l'abuso di Internet da parte di terroristi, estremisti violenti e criminali. L'unità UE addetta alle segnalazioni su Internet di Europol continuerà a svolgere un ruolo cruciale nel monitorare l'attività dei gruppi terroristici online e le azioni intraprese dalle piattaforme[68] nonché nell'ulteriore sviluppo del **protocollo di crisi dell'UE**[69]. Inoltre, la Commissione continuerà a collaborare con i partner internazionali, anche partecipando al **Forum Internet mondiale per la lotta contro il terrorismo**, al fine di affrontare queste

[66] Conservati in banche dati gestite da 2 500 registrar e gestori di registro basati in tutto il mondo.

[67] Proposta sulla prevenzione della diffusione di contenuti terroristici online, COM (2018) 640, 12 settembre 2018.

[68] Europol, novembre 2019.

[69] A Europe that protects - EU Crisis Protocol: responding to terrorist content online(Un'Europa che protegge - Protocollo di crisi dell'UE: reagire ai contenuti terroristici online), (ottobre 2019).

sfide a livello mondiale. Proseguiranno i lavori volti a sostenere lo sviluppo di narrazioni alternative e contronarrazioni grazie al programma di responsabilizzazione della società civile[70].

Per prevenire e contrastare la diffusione di forme illegali di incitamento all'odio online, nel 2016 la Commissione ha introdotto il codice di condotta contro l'incitamento all'odio online, con l'impegno volontario da parte delle piattaforme online di rimuovere i contenuti dell'incitamento all'odio. L'ultima valutazione mostra che le imprese esaminano il 90 % dei contenuti segnalati entro 24 ore e rimuovono il 71 % del contenuto di incitamento all'odio considerato illegale. Tuttavia, le piattaforme devono migliorare ulteriormente la trasparenza e il feedback agli utenti e garantire una valutazione coerente dei contenuti segnalati[71].

Il Forum dell'UE su Internet agevolerà inoltre gli scambi sulle tecnologie, esistenti e in via di sviluppo, per affrontare le sfide legate agli abusi sessuali online sui minori. La lotta contro gli abusi sessuali online sui minori è al centro di una nuova strategia per potenziare la **lotta contro gli abusi sessuali su minori**[72], che intende sfruttare al massimo gli strumenti disponibili a livello dell'UE per contrastare tali reati. Le imprese devono essere in grado di continuare a lavorare per individuare e rimuovere i materiali pedopornografici online, e il danno causato da questo materiale richiede un quadro che stabilisca obblighi chiari e permanenti per affrontare il problema. Nel quadro della strategia sarà inoltre annunciato l'avvio della preparazione, da parte della Commissione, della legislazione specifica del settore per contrastare più efficacemente gli abusi sessuali online sui minori, nel pieno rispetto dei diritti fondamentali.

Più in generale, l'imminente legge sui servizi digitali consentirà inoltre di chiarire e aggiornare le norme in materia di responsabilità e sicurezza per i servizi digitali e di eliminare i disincentivi che frenano le azioni volte a contrastare i contenuti, i beni o i servizi illegali.

Inoltre, la Commissione continuerà a dialogare con i partner internazionali e con il **Forum Internet mondiale per la lotta contro il terrorismo**, anche attraverso il comitato consultivo indipendente, al fine di affrontare tali sfide a livello mondiale, preservando nel contempo i valori e i diritti fondamentali dell'UE. Dovrebbero essere affrontati anche nuovi temi come gli algoritmi o il gioco on line[73].

Minacce ibride

La portata e la diversificazione attuali delle minacce ibride non hanno precedenti. La crisi causata dalla COVID-19 ne offre numerosi esempi, con diversi soggetti statali e non statali che cercano di strumentalizzare la pandemia, in particolare attraverso la manipolazione dell'ambiente di informazione e ponendo sfide alle infrastrutture fondamentali. Ciò rischia di indebolire la coesione sociale e di minare la fiducia nelle istituzioni dell'UE e nei governi degli Stati membri.

L'approccio dell'UE alle minacce ibride è definito nel quadro congiunto del 2016[74] e nella comunicazione congiunta del 2018 sul rafforzamento della resilienza ibrida[75]. L'azione a

---

[70] In collegamento con le iniziative del programma di sensibilizzazione al problema della radicalizzazione, cfr. la sezione IV.3.

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] Una strategia per una lotta più efficace contro gli abusi sessuali sui minori, COM(2020) 607.

[73] I terroristi ricorrono sempre più spesso al sistema di messaggistica delle piattaforme di gioco per gli scambi e i giovani terroristi hanno nuovamente sferrato attacchi violenti nei videogiochi.

[74] Quadro congiunto per contrastare le minacce ibride: la risposta dell'Unione europea, JOIN (2016) 18.

[75] Rafforzamento della resilienza e Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride, JOIN (2018) 16.

livello dell'UE è sostenuta da un insieme consistente di strumenti che interessano anche il nesso tra sicurezza interna ed esterna e sono basati su un approccio esteso a tutta la società e sulla stretta cooperazione con i partner strategici, in particolare la NATO e il G7. Insieme alla presente strategia è pubblicata una relazione sull'attuazione dell'approccio dell'UE alle minacce ibride[76]. Sulla base della mappatura[77] presentata contestualmente alla presente strategia, i servizi della Commissione e il Servizio europeo per l'azione esterna istituiranno una **piattaforma online ristretta** che servirà da riferimento agli Stati membri per quanto riguarda gli strumenti e le misure per la lotta alle minacce ibride a livello dell'UE.

Sebbene, in ragione dei legami intrinseci con le politiche nazionali di sicurezza e difesa, la responsabilità di contrastare le minacce ibride incomba principalmente agli Stati membri, vi sono vulnerabilità comuni a tutti gli Stati membri e alcune minacce si estendono a livello transfrontaliero, come ad esempio il ricorso alle reti o alle infrastrutture transfrontaliere. La Commissione e l'Alto rappresentante presenteranno un approccio dell'UE alle minacce ibride che integri la dimensione esterna e quella interna in un flusso continuo e riunisca in un unico insieme le considerazioni nazionali e dell'UE. Tale approccio deve contemplare l'intera gamma di azioni, dalla diagnosi precoce e all'analisi, fino alla consapevolezza, la resilienza e la prevenzione passando attraverso la risposta alle crisi e la gestione delle conseguenze.

Oltre a rafforzare l'attuazione, vista la costante evoluzione delle minacce ibride, un'attenzione particolare sarà rivolta all'integrazione di **considerazioni sulle minacce ibride nel processo di elaborazione delle politiche**, al fine di stare al passo con il dinamismo degli sviluppi e garantire che non sia tralasciata nessuna iniziativa potenzialmente adeguata. Gli effetti delle nuove iniziative saranno anche valutati alla luce delle minacce ibride, comprese le iniziative in settori che finora non rientrano nelle competenze del quadro per contrastare le minacce ibride, quali l'istruzione, la tecnologia e la ricerca. Tale approccio trarrebbe vantaggio dal lavoro svolto sulla concettualizzazione delle minacce ibride, che fornisce una visione globale dei vari strumenti che possono essere utilizzati dagli avversari[78]. L'obiettivo perseguito è garantire che il processo decisionale sia sostenuto da relazioni periodiche basate su dati di intelligence globali sull'evoluzione delle minacce ibride. L'approccio si baserà in larga misura sui servizi di intelligence degli Stati membri e sull'ulteriore rafforzamento della cooperazione in materia di intelligence con i servizi competenti degli Stati membri tramite l'INTCEN dell'UE.

Per sviluppare la **conoscenza situazionale**, i servizi della Commissione e il Servizio europeo per l'azione esterna esamineranno le possibilità di razionalizzare i flussi di informazioni provenienti da diverse fonti, tra cui gli Stati membri, nonché le agenzie dell'UE come l'ENISA, Europol e Frontex. La cellula dell'UE per l'analisi delle minacce ibride rimarrà il punto di contatto dell'UE per le valutazioni delle minacce ibride. **Costruire la resilienza** è fondamentale per prevenire le minacce ibride e proteggersi da esse. È pertanto fondamentale seguire in maniera sistematica e misurare obiettivamente i progressi compiuti in questo campo. Un primo passo consisterà nell'individuare le i parametri di riferimento settoriali in materia di resilienza ibrida per gli Stati membri e le istituzioni e gli organi dell'UE. Infine, per intensificare i **preparativi della risposta a crisi causate dalle minacce**

[76] Relazione sull'attuazione del quadro congiunto per contrastare le minacce ibride del 2016 e comunicazione congiunta del 2018 "Rafforzamento della resilienza e potenziamento delle capacità di affrontare minacce ibride", SWD (2020) 153.

[77] Mappatura delle misure relative al rafforzamento della resilienza e al contrasto delle minacce ibride, SWD (2020) 152.

[78] Il panorama delle minacce ibride: modello concettuale (JRC117280) sviluppato congiuntamente dal Centro comune di ricerca e dal Centro di eccellenza per la lotta contro le minacce ibride.

ibride, il protocollo esistente dovrebbe essere riesaminato, come definito nel manuale tattico dell'UE per il 2016[79], in modo da tenere conto del più ampio riesame e del rafforzamento del sistema UE di risposta alle crisi attualmente all'esame[80]. L'obiettivo è massimizzare l'effetto dell'azione dell'UE riunendo in tempi rapidi le risposte settoriali e garantendo una cooperazione senza soluzione di continuità con i nostri partner, la NATO in primo luogo.

Azioni principali
• Garantire che la legislazione in materia di criminalità informatica sia attuata e adeguata allo scopo • Una strategia per una lotta più efficace contro gli abusi sessuali sui minori • Proposte per l'individuazione e la rimozione di materiale contenente abusi sessuali sui minori • Un approccio dell'UE per contrastare le minacce ibride • Riesame del protocollo operativo dell'UE per contrastare le minacce ibride (EU Playbook) • Valutazione delle modalità per rafforzare la capacità degli organismi di contrasto nelle indagini digitali

3. Proteggere gli europei dal terrorismo e dalla criminalità organizzata

Terrorismo e radicalizzazione

La minaccia terroristica nell'UE rimane elevata. Nonostante la diminuzione generale del loro numero, gli attentati possono ancora avere un effetto devastante. La radicalizzazione può inoltre indurre una più ampia polarizzazione e destabilizzare la coesione sociale. Gli Stati membri detengono la responsabilità primaria nella lotta al terrorismo e alla radicalizzazione. Tuttavia, la crescente dimensione transfrontaliera/intersettoriale della minaccia richiede ulteriori passi per quanto riguarda la cooperazione e il coordinamento a livello dell'UE. L'efficace attuazione della legislazione antiterrorismo dell'UE, comprese le misure restrittive[81], è una priorità. L'obiettivo di estendere il mandato della Procura europea ai reati di terrorismo transfrontalieri non è ancora realizzato.

La lotta al terrorismo inizia con l'affrontare le cause profonde del fenomeno. La polarizzazione della società, la discriminazione reale o percepita e altri fattori psicologici e sociologici possono rafforzare la vulnerabilità delle persone nei confronti del discorso radicale. In questo contesto, il contrasto della **radicalizzazione** va di pari passo con la promozione della coesione sociale a livello locale, nazionale ed europeo. Nell'ultimo decennio sono state sviluppate varie politiche e iniziative efficaci, in particolare attraverso la rete per la sensibilizzazione al problema della radicalizzazione e l'iniziativa "Le città dell'UE

[79] *EU operational protocol for countering hybrid threats* (EU Playbook), SWD(2016) 227 final

[80] A seguito della videoconferenza del 26 marzo 2020, i membri del Consiglio europeo hanno adottato una dichiarazione sulle azioni dell'UE in risposta all'epidemia di COVID19, invitando la Commissione a presentare proposte per un sistema di gestione delle crisi più ambizioso e di ampia portata all'interno dell'UE.

[81] Nell'intento di combattere il terrorismo, il Consiglio ha adottato misure restrittive riguardanti l'ISIL (Daesh) e Al-Qaeda e misure restrittive specifiche contro determinate persone ed entità. Per una panoramica di tutte le misure restrittive, cfr. la mappa delle sanzioni dell'UE (https://www.sanctionsmap.eu/#/main).

contro la radicalizzazione"[82]. È giunto il momento di prendere in considerazione azioni volte a integrare le politiche, le iniziative e i fondi dell'UE per contrastare la radicalizzazione. Tali azioni possono sostenere lo sviluppo di capacità e competenze, promuovere la cooperazione, rafforzare la base di conoscenze comprovate e contribuire a valutare i progressi compiuti, coinvolgendo tutti i portatori di interessi, compresi gli operatori di prima linea, i responsabili delle politiche e il mondo accademico[83]. Politiche non vincolanti quali l'istruzione, la cultura, i giovani e lo sport potrebbero contribuire a prevenire la radicalizzazione, offrendo opportunità per i giovani a rischio e favorendo la coesione all'interno dell'UE[84]. I settori prioritari comprendono i lavori per l'individuazione precoce e la gestione dei rischi, la creazione di resilienza e il disimpegno oltre alla riabilitazione e al reinserimento nella società.

I terroristi cercano di acquistare e di utilizzare come armi **materiali chimici, biologici, radiologici e nucleari** (CBRN)[85] e di sviluppare le conoscenze e le capacità per utilizzarli[86]. Il potenziale degli attacchi CBRN è posto in primo piano dalla propaganda terroristica. Data l'entità del danno potenziale, si tratta di una questione che merita grande attenzione. Sulla base dell'approccio utilizzato per regolamentare l'accesso ai precursori degli esplosivi, la Commissione cercherà di limitare l'accesso ad alcune sostanze chimiche pericolose che potrebbero essere utilizzate per compiere attentati. Sarà inoltre fondamentale sviluppare le capacità di risposta dell'UE per quanto riguarda la protezione civile (rescEU) sul campo nel settore CBRN. La cooperazione con i paesi terzi è importante anche per rafforzare una cultura comune in materia di sicurezza e protezione CBRN, facendo pieno uso dei centri di eccellenza dell'UE nel settore CBRN a livello mondiale. Tale cooperazione interesserà anche le differenze nazionali e le valutazioni del rischio, il sostegno a piani d'azione nazionali e regionali in materia di CBRN, lo scambio di buone prassi e le attività di sviluppo delle capacità CBRN.

L'UE ha sviluppato la legislazione più avanzata al mondo per limitare l'accesso ai **precursori di esplosivi**[87] e individuare operazioni sospette volte alla costruzione di ordigni esplosivi improvvisati. Ma la minaccia rappresentata dagli esplosivi artigianali, usati in molteplici attentati in tutta l'UE, rimane elevata[88]. Il primo passo deve essere l'attuazione delle norme, oltre a garantire che l'ambiente online non consenta di sfuggire ai controlli.

Anche l'efficace perseguimento di coloro che hanno commesso reati di terrorismo, inclusi i **combattenti terroristi stranieri** attualmente in Siria e in Iraq, costituisce un elemento importante della politica antiterrorismo. Sebbene tali questioni siano affrontate in primo luogo dagli Stati membri, il coordinamento e il sostegno dell'UE possono dare un contributo per affrontare le sfide comuni. Le misure in corso per attuare pienamente la legislazione sulla

[82] L'iniziativa pilota "Città dell'UE contro la radicalizzazione" ha il duplice obiettivo di promuovere lo scambio di competenze tra le città dell'UE e di raccogliere informazioni su come sostenere al meglio le comunità locali a livello dell'UE.

[83] Ad esempio, finanziamenti nel quadro del Fondo europeo per la sicurezza e del programma "Cittadinanza".

[84] Azioni dell'UE quali gli scambi virtuali Erasmus +, e-twinning.

[85] Negli ultimi due anni, ad esempio, si sono verificati diversi casi in Europa (Francia, Germania, Italia) e altrove (Tunisia, Indonesia) che implicavano agenti biologici (in genere tossine di origine vegetale).

[86] Il Consiglio ha adottato misure restrittive contro la proliferazione e l'uso delle armi chimiche.

[87] Le sostanze chimiche che potrebbero essere utilizzate impropriamente per fabbricare esplosivi artigianali. Esse sono disciplinate dal regolamento (UE) 2019/1148 relativo all'immissione sul mercato e all'uso di precursori di esplosivi.

[88] Gli attentati di Oslo (2011), Parigi (2015), Bruxelles (2016) e Manchester (2017) sono alcuni esempi di queste azioni devastanti. Un attentato compiuto a Lione (2019) con esplosivo artigianale ha provocato il ferimento di 13 persone.

sicurezza delle frontiere[89] e utilizzare al meglio tutte le pertinenti banche dati dell'UE per condividere informazioni su sospetti noti costituiranno un passo importante. Oltre ad individuare le persone ad alto rischio, occorre una politica di reinserimento e di riabilitazione. La cooperazione interprofessionale, anche con il personale penitenziario e di sorveglianza, rafforzerà la comprensione giudiziaria dei processi che portano alla radicalizzazione e all'estremismo violento e migliorerà l'approccio del settore giudiziario per quanto riguarda le condanne e le alternative alla detenzione.

La sfida costituita dai combattenti terroristi stranieri è emblematica del legame tra **sicurezza esterna** ed interna. La cooperazione in materia di lotta al terrorismo nonché prevenzione e contrasto della radicalizzazione e dell'estremismo violento è fondamentale per la sicurezza all'interno dell'UE[90]. Occorrono ulteriori misure per sviluppare partenariati e cooperazione in materia di lotta al terrorismo con i paesi del vicinato e oltre, attingendo alle competenze della rete per la lotta al terrorismo e agli esperti di sicurezza dell'UE. Il piano d'azione comune sulla lotta al terrorismo per i Balcani occidentali è un buon punto di riferimento per tale cooperazione mirata. In particolare, dovrebbero essere compiuti sforzi per sostenere la capacità dei paesi partner di individuare e localizzare i combattenti terroristi stranieri. L'UE continuerà inoltre a promuovere la cooperazione multilaterale, in collaborazione con i principali organismi globali in questo settore, quali le Nazioni Unite, la NATO, il Consiglio d'Europa, l'Interpol e l'OSCE. Si impegnerà inoltre con il Forum globale contro il terrorismo e la coalizione internazionale per combattere il Daesh, nonché con i relativi attori della società civile. Gli strumenti di politica esterna dell'Unione, compresi lo sviluppo e la cooperazione, svolgono anche un ruolo importante a livello di cooperazione con i paesi terzi per prevenire il terrorismo e la pirateria. La cooperazione internazionale è essenziale anche per prosciugare tutte le fonti di **finanziamento del terrorismo**, ad esempio attraverso il Gruppo di azione finanziaria internazionale.

Criminalità organizzata

La criminalità organizzata comporta enormi costi economici e personali. Si stima che la perdita economica dovuta alla criminalità organizzata e alla corruzione rappresenti una cifra compresa tra 218 e 282 miliardi di EUR l'anno[91]. Più di 5 000 gruppi della criminalità organizzata sono stati oggetto di indagini in Europa nel 2017, un aumento del 50 % rispetto al 2013[92]. La criminalità organizzata è sempre più attiva a livello transfrontaliero, anche quella proveniente dal vicinato immediato dell'UE, e richiede una cooperazione operativa e uno scambio di informazioni più intensi con i partner del vicinato.

Nuove sfide emergono e portano la criminalità online: la pandemia di COVID-19 ha fatto registrare un enorme aumento delle truffe online a danno di gruppi vulnerabili mentre prodotti sanitari e igienico-sanitari sono stati oggetto di furti e rapine[93]. L'UE deve intensificare la sua azione contro la criminalità organizzata, anche a livello internazionale, con maggiori strumenti per smantellare il modello di attività della criminalità organizzata.

---

89 Compreso il nuovo mandato dell'Agenzia europea della guardia di frontiera e costiera (Frontex).

90 Le conclusioni del Consiglio del 16 giugno 2020 hanno sottolineato la necessità di proteggere i cittadini dell'UE dal terrorismo e dall'estremismo violento, in tutte le loro forme e indipendentemente dalla loro origine, e di rafforzare ulteriormente l'impegno e l'azione esterna dell'UE in materia di antiterrorismo in determinate aree geografiche e tematiche prioritarie.

91 In termini di prodotto interno lordo (PIL); Relazione di Europol: *"Does crime still pay?" – Criminal asset recovery in the EU*, 2016 (I reati continuano a rendere? Il recupero dei proventi di reato nell'UE).

92 Europol, *Serious and Organised Threat Assessments* (SOCTA), 2013 e 2017 (Valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità).

93 Europol, 2020.

La lotta contro la criminalità organizzata richiede anche una stretta cooperazione con le amministrazioni locali e regionali oltre che con la società civile, tutti partner fondamentali nella prevenzione della criminalità e nel fornire assistenza e sostegno alle vittime, soprattutto nel caso delle amministrazioni nelle regioni frontaliere. Questi lavori saranno riuniti in un **programma per la lotta contro la criminalità organizzata**.

Più di un terzo dei gruppi della criminalità organizzata attivi nell'UE partecipano alla produzione, al traffico o alla distribuzione di stupefacenti. Nel 2019 la tossicodipendenza ha causato oltre 8 000 decessi per overdose nell'UE. La maggior parte del **traffico di droga** è di natura transfrontaliera e molti dei suoi proventi vengono immessi nell'economia legale[94]. Un nuovo programma dell'UE di lotta contro la droga[95] sosterrà gli sforzi dell'UE e degli Stati membri nei settori della riduzione della domanda e dell'offerta di droga, definendo azioni comuni per affrontare un problema comune e promuovendo il dialogo e la cooperazione in materia di droga tra l'UE e i partner esterni. A seguito di una valutazione dell'Osservatorio europeo delle droghe e delle tossicodipendenze, la Commissione valuterà se il mandato di questo organismo debba essere aggiornato per far fronte alle nuove sfide.

I gruppi della criminalità organizzata e i terroristi sono anche attivi nel traffico delle **armi da fuoco illegali**. Tra il 2009 e il 2018 in Europa sono state registrate 23 sparatorie di massa in cui hanno perso la vita più di 340 persone[96]. Spesso il traffico delle armi da fuoco penetra nell'UE attraverso i paesi dell'immediato vicinato[97]. Ciò indica la necessità di rafforzare il coordinamento e la cooperazione sia all'interno dell'UE che con i partner internazionali, in particolare Interpol, al fine di armonizzare la raccolta di informazioni e di segnalazioni sui sequestri di armi da fuoco. È altresì essenziale migliorare la tracciabilità delle armi, anche su Internet, e garantire lo scambio di informazioni tra le autorità preposte al rilascio delle licenze e le autorità di contrasto. La Commissione presenta un nuovo **piano d'azione dell'UE contro il traffico di armi da fuoco**[98] e valuterà se le norme in materia di autorizzazione di esportazione e le misure per l'importazione e il transito delle armi da fuoco costituiscano ancora strumenti efficienti[99].

Le organizzazioni criminali trattano alla stregua di merci i migranti e le persone bisognose di protezione internazionale. Il 90 % dei migranti irregolari è arrivato nell'EU grazie all'aiuto di una rete criminale[100]. Il traffico di migranti è spesso interconnesso anche con altre forme di criminalità organizzata, in particolare la tratta di esseri umani[101]. A parte l'enorme costo umano della tratta, Europol stima che, a livello globale, il profitto annuo generato per tutte le forme di sfruttamento connesse alla tratta di esseri umani ammonti a 29,4 miliardi di EUR. Siamo di fronte a un reato transnazionale che alimenta le richieste illegali all'interno e

---

94 EMCDDA e Europol, "*EU Drug Markets Report 2019*" (relazione 2019 sui mercati della droga nell'UE) (novembre 2019).

95 Programma dell'UE di lotta contro la droga e piano di azione 2021-2025, COM (2020) 606.

96 *Flemish Peace Institute, "Armed to kill"* (Istituto fiammingo per la pace, "Armato per uccidere") (ottobre 2019).

97 L'UE ha finanziato la lotta contro la proliferazione e il traffico di armi leggere e di piccolo calibro nella regione dal 2002; in particolare finanzia la rete di esperti di armi da fuoco nell'Europa sudorientale (SEEFEN). Dal 2019 i partner dei Balcani occidentali sono stati pienamente coinvolti nella piattaforma multidisciplinare europea di lotta alle minacce della criminalità (EMPACT), una priorità nella lotta alle armi da fuoco.

98 COM (2020) 608.

99 Regolamento (UE) n. 258/2012 che attua l'articolo 10 del protocollo delle Nazioni Unite contro la fabbricazione e il traffico illeciti di armi da fuoco.

100 Fonte: Europol.

101 Europol, EMSC, *4th Annual Report*.

all'esterno dell'UE e che ha un impatto su tutti gli Stati membri dell'UE. Gli scarsi risultati conseguiti per individuare, perseguire e condannare questi crimini richiedono un nuovo approccio che permetta di potenziare le azioni. Un nuovo **approccio globale alla tratta degli esseri umani** integrerà i diversi canali di azione. Inoltre, la Commissione presenterà un nuovo **piano d'azione dell'UE contro il traffico di migranti** per il periodo 2021-2025. Entrambe le iniziative saranno incentrate sulla lotta contro le reti criminali, la promozione della cooperazione e il sostegno ai lavori delle autorità di contrasto.

I gruppi della criminalità organizzata, come pure i terroristi, cercano anche opportunità in altri settori, in particolare in quelli che generano profitti elevati e a basso rischio di individuazione, come la **criminalità ambientale**. La caccia illegale e il commercio illegale di specie selvatiche, l'estrazione mineraria illegale, il disboscamento e lo smaltimento illegale dei rifiuti e le spedizioni illegali sono diventati la quarta attività criminale nel mondo per dimensione[102]. Si è anche osservato uno sfruttamento criminoso dei sistemi di scambio delle emissioni e dei sistemi di certificazione energetica, nonché l'uso improprio dei fondi stanziati per la resilienza ambientale e lo sviluppo sostenibile. Oltre a promuovere l'azione dell'UE, degli Stati membri e della comunità internazionale per intensificare gli sforzi contro la criminalità ambientale[103], la Commissione sta valutando se la direttiva sulla tutela penale dell'ambiente[104] sia ancora adeguata allo scopo. Anche il crescente **traffico di beni culturali** è diventato una delle attività criminali più lucrative, una fonte di finanziamento del terrorismo e della criminalità organizzata. Occorre esplorare misure per migliorare la tracciabilità online e offline dei beni culturali nel mercato interno, oltre alla cooperazione con i paesi terzi i cui beni culturali sono saccheggiati, ed è necessario fornire un sostegno attivo alle autorità di contrasto e alle comunità accademiche.

Pur essendo estremamente complessi, ogni anno i **reati economici e finanziari** colpiscono milioni di cittadini e migliaia di imprese nell'UE. La lotta alla frode è fondamentale e richiede un'azione a livello dell'UE. Europol, Eurojust, la Procura europea e l'Ufficio europeo per la lotta antifrode sostengono gli Stati membri e l'UE per proteggere i mercati economici e finanziari e tutelare il denaro dei contribuenti dell'UE. La Procura europea diventerà pienamente operativa verso la fine del 2020 e indagherà, perseguirà e rinvierà a giudizio i reati commessi contro il bilancio dell'UE, come la frode, la corruzione e il riciclaggio di denaro. Contrasterà inoltre la frode transfrontaliera in materia di IVA che costa ai contribuenti almeno 50 miliardi di EUR all'anno.

La Commissione sosterrà inoltre lo sviluppo delle competenze e di un quadro legislativo in materia di rischi emergenti, quali le criptoattività e i nuovi sistemi di pagamento. In particolare, la Commissione esplorerà misure atte a contrastare l'insorgenza di criptoattività come i bitcoin e alle conseguenze che queste nuove tecnologie avranno sulle modalità di emissione, scambio e condivisione delle risorse finanziarie e sui modi di accedervi.

Ci dovrebbe essere una tolleranza zero per il denaro illecito all'interno dell'Unione europea. Nell'arco di trent'anni, l'UE ha messo a punto un solido quadro normativo per prevenire e combattere il **riciclaggio di denaro** e il finanziamento del terrorismo, nel pieno rispetto della necessità di proteggere i dati personali. Vi è tuttavia un crescente consenso sul fatto che l'attuazione del quadro attuale debba essere notevolmente migliorata. Devono essere affrontate le profonde divergenze nel modo in cui viene applicata e delle gravi carenze

[102] UNEP-INTERPOL *Rapid Response Assessment: The Rise of Environmental Crime* (La crescita della criminalità ambientale), giugno 2016.
[103] Cfr.: Il Green Deal europeo, COM (2019) 640 final.
[104] Direttiva 2008/99/CE sulla tutela penale dell'ambiente.

riscontrate nell'applicazione delle norme. Come specificato nel piano d'azione del maggio 2020[105], sono in corso lavori per valutare le opzioni volte a rafforzare il quadro dell'UE in materia di lotta contro il riciclaggio di denaro e il finanziamento del terrorismo. Le aree da esplorare comprendono l'interconnessione dei registri nazionali centralizzati dei conti bancari, che potrebbero velocizzare notevolmente l'accesso alle informazioni finanziarie per le unità di informazione finanziaria e le autorità competenti.

Si stima che i **profitti dei gruppi della criminalità organizzata** nell'UE ammontino a 110 miliardi di EUR all'anno. L'attuale risposta comprende una legislazione armonizzata in materia di confisca e recupero dei beni[106], intesa a migliorare il congelamento e la confisca dei proventi di reato nell'UE e ad agevolare la fiducia reciproca e l'efficace cooperazione transfrontaliera tra Stati membri. Tuttavia, solo l'1 % circa di questi profitti viene confiscato[107], il che consente ai gruppi della criminalità organizzata di investire nell'espansione delle loro attività criminali e di infiltrarsi nell'economia legale; in particolare le piccole e medie imprese, che hanno difficoltà di accesso al credito, sono un obiettivo fondamentale per il riciclaggio di denaro. La Commissione analizzerà l'attuazione della legislazione[108] e l'eventuale necessità di ulteriori norme comuni, anche per quanto riguarda la confisca non basata sulla condanna. Gli uffici per il recupero dei beni[109], soggetti fondamentali nel processo di recupero dei beni, potrebbero anche essere dotati di strumenti migliori per individuare e rintracciare le attività in modo più rapido in tutta l'UE al fine di aumentare i tassi di confisca.

Vi è un forte legame tra la criminalità organizzata e la **corruzione**. Si stima che la corruzione costi da sola 120 miliardi di EUR l'anno all'economia dell'UE[110]. La prevenzione e la lotta contro la corruzione continueranno a essere soggette a un monitoraggio regolare nell'ambito del meccanismo per lo Stato di diritto e del semestre europeo. Il semestre europeo ha valutato le sfide riguardo alla lotta alla corruzione, quali gli appalti pubblici, la pubblica amministrazione, il contesto imprenditoriale o l'assistenza sanitaria. La nuova relazione annuale della Commissione sullo Stato di diritto comprenderà la lotta alla corruzione e consentirà un dialogo preventivo con le autorità nazionali e i portatori di interessi a livello nazionale e dell'UE. Anche le organizzazioni della società civile possono svolgere un ruolo chiave nel promuovere l'azione delle autorità pubbliche in materia di prevenzione e lotta contro la criminalità organizzata e la corruzione, e potrebbero utilmente essere riunite in un forum comune. Un'altra dimensione fondamentale, dato il carattere transfrontaliero, è rappresentata dalla cooperazione e dall'assistenza con le regioni limitrofe dell'UE in materia di criminalità organizzata e corruzione.

Azioni principali

[105] Piano d'azione per la prevenzione del riciclaggio e del finanziamento del terrorismo, COM (2020) 2800.

[106] Il diritto dell'UE impone che uffici per il recupero dei beni siano istituiti in tutti gli Stati membri.

[107] Relazione della Commissione - Recupero e confisca dei beni: garantire che "il crimine non paghi", COM (2020) 217 final.

[108] Direttiva 2014/42/UE relativa al congelamento e alla confisca dei beni strumentali e dei proventi da reato nell'Unione europea.

[109] Decisione 2007/845/GAI del Consiglio concernente la cooperazione tra gli uffici degli Stati membri per il recupero dei beni nel settore del reperimento e dell'identificazione dei proventi di reato o altri beni connessi.

[110] Nonostante gli sforzi compiuti da organi quali la Camera di commercio internazionale, *Transparency International*, il patto mondiale delle Nazioni Unite e il Forum economico mondiale, secondo cui la corruzione rappresenterebbe il 5 % del PIL mondiale, rimane difficile fornire una stima totale dei costi economici della corruzione.

- Programma di lotta al terrorismo dell'UE, comprese nuove azioni contro la radicalizzazione nell'UE
- Nuova cooperazione con i principali paesi terzi e le organizzazioni internazionali contro il terrorismo
- Programma di lotta alla criminalità organizzata, compresa la tratta di esseri umani
- Programma dell'UE sulla lotta alla droga e piano di azione 2021-2025
- Valutazione dell'Osservatorio europeo delle droghe e delle tossicodipendenze
- Piano d'azione dell'UE sul traffico di armi da fuoco 2020-2025
- Riesame della legislazione sul congelamento e la confisca e sugli uffici per il recupero dei beni
- Valutazione della direttiva sulla tutela penale dell'ambiente
- Piano d'azione dell'UE contro il traffico di migranti 2021-2025

4. Un forte ecosistema europeo della sicurezza

Un'Unione della sicurezza autentica ed efficace deve essere basata sullo sforzo comune di tutte le componenti della società. I governi, le autorità di contrasto, il settore privato, l'istruzione e i cittadini stessi devono essere impegnati, attrezzati e adeguatamente interconnessi per costruire la preparazione e la resilienza per tutti, in particolare per le persone più vulnerabili, le vittime e i loro parenti e i testimoni.

Tutte le politiche hanno bisogno della dimensione della sicurezza e l'UE può apportare un contributo a tutti i livelli. Nelle case, la violenza domestica è uno dei rischi più gravi per la sicurezza. Nell'UE il 22 % delle donne ha subito violenza da un partner[111]. L'adesione dell'UE alla convenzione di Istanbul sulla prevenzione e la lotta contro la violenza nei confronti delle donne e la violenza domestica rimane una priorità fondamentale. Qualora i negoziati rimangano bloccati, la Commissione adotterà altre misure per conseguire gli stessi obiettivi della convenzione, anche proponendo di aggiungere la violenza contro le donne nell'elenco dei reati dell'UE definiti nel trattato.

Cooperazione e scambio d'informazioni

Uno dei contributi più cruciali che l'UE può fornire alla protezione dei cittadini consiste nell'aiutare i responsabili della sicurezza a lavorare bene insieme. La cooperazione e lo scambio di informazioni sono gli strumenti più efficaci per combattere la criminalità e il terrorismo e far applicare la legge. Per essere efficienti, gli interventi devono essere mirati e tempestivi. Per essere affidabili, deve essere oggetto di salvaguardie e controlli comuni.

Sono stati messi a punto diversi strumenti e strategie settoriali dell'UE[112] per sviluppare ulteriormente la **cooperazione operativa nell'attività di contrasto** tra gli Stati membri. Uno dei principali strumenti dell'UE a sostegno della cooperazione tra gli Stati membri in materia di applicazione della legge è il sistema d'informazione Schengen, utilizzato per scambiare in tempo reale dati su persone e oggetti ricercati e scomparsi. Risultati sono stati messi a segno relativamente all'arresto di criminali, al sequestro di stupefacenti e al salvataggio di vittime potenziali[113]. Tuttavia, il livello di collaborazione potrebbe essere migliorato attraverso l'integrazione e l'aggiornamento degli strumenti disponibili. La

[111] Un'Unione dell'uguaglianza: la strategia per la parità di genere 2020-2025, COM(2020) 152.

[112] Come il piano d'azione della strategia per la sicurezza marittima dell'UE, che ha conseguito importanti risultati grazie alla cooperazione tra le pertinenti agenzie dell'UE nell'ambito delle funzioni di guardia costiera.

[113] La lotta dell'UE alla criminalità organizzata nel 2019 (Consiglio, 2020).

concezione della maggior parte del quadro giuridico dell'UE alla base della cooperazione operativa nell'attività di contrasto risale a 30 anni fa. La complessa rete di accordi bilaterali tra Stati membri, molti dei quali sono ormai obsoleti o sottoutilizzati, è a rischio di frammentazione. Nei paesi più piccoli o privi di sbocco sul mare, le autorità di contrasto che operano a livello transfrontaliero devono svolgere azioni operative in applicazione, in alcuni casi, di sette diversi corpora di norme: ne consegue che alcune operazioni, come gli inseguimenti di sospetti oltre le frontiere interne non sono semplicemente svolte. Anche la cooperazione operativa sulle nuove tecnologie, come i droni, non rientra nell'attuale quadro dell'UE.

L'efficacia operativa può essere sostenuta da una cooperazione specifica in materia di attività di contrasto, che può altresì contribuire a fornire contributi fondamentali ad altri obiettivi politici, come ad esempio contributi in materia di sicurezza relativi alla sicurezza per la nuova valutazione degli investimenti diretti esteri. La Commissione esaminerà in che modo un codice di cooperazione di polizia possa sostenere questo sforzo. Le autorità di contrasto degli Stati membri si avvalgono sempre più spesso di sostegno e competenze a livello dell'UE, mentre l'EU INTCEN ha svolto un ruolo chiave nel promuovere lo scambio di intelligence strategica tra i servizi di intelligence e di sicurezza degli Stati membri, fornendo alle istituzioni dell'UE conoscenza situazionale basata sull'intelligence[114]. **Europol** può inoltre svolgere un ruolo chiave nell'ampliare la cooperazione con i paesi terzi per contrastare la criminalità e il terrorismo, coerentemente con altre politiche e strumenti esterni dell'UE. Tuttavia, Europol si trova oggi ad affrontare una serie di gravi limitazioni - in particolare per quanto riguarda lo scambio diretto di dati personali con parti private - il che le impedisce di sostenere efficacemente gli Stati membri nella lotta al terrorismo e alla criminalità. Il mandato di Europol è attualmente esaminato a fini di un miglioramento che permetta all'Agenzia di svolgere pienamente i suoi compiti. In tale contesto, le autorità competenti a livello dell'UE (come OLAF, Europol, Eurojust e la Procura europea) dovrebbero inoltre cooperare più strettamente e migliorare lo scambio di informazioni.

Un altro elemento fondamentale per creare connessioni è l'ulteriore sviluppo di **Eurojust** per massimizzare la sinergia tra la cooperazione nell'attività di contrasto e la cooperazione giudiziaria. L'UE trarrebbe inoltre vantaggio da una maggiore coerenza strategica: **EMPACT**[115], il ciclo programmatico dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale, mette a disposizione delle autorità una metodologia basata sull'intelligence per affrontare congiuntamente le più importanti minacce criminali di cui è oggetto l'UE. Il ciclo ha portato a importanti risultati operativi[116] nell'ultimo decennio. Sulla base dell'esperienza raccolta dagli operatori, il meccanismo esistente dovrebbe essere razionalizzato e semplificato per affrontare meglio l'evoluzione delle minacce più urgenti nel nuovo ciclo programmatico 2022-2025.

Informazioni tempestive e pertinenti sono essenziali nelle attività quotidiane di contrasto alla criminalità. Nonostante nuove banche dati per la gestione della sicurezza e delle frontiere siano messe a punto a livello dell'UE, molte informazioni si trovano ancora nelle banche dati nazionali o sono scambiate al di fuori dei nuovi strumenti. Ne conseguono un notevole carico di lavoro aggiuntivo, ritardi e un aumento del rischio di perdere

[114] Il Centro UE di situazione e di intelligence (INTCEN) funge da unico punto di accesso per i servizi di intelligence e di sicurezza degli Stati membri per fornire all'UE una conoscenza situazionale basata sull'intelligence.

[115] EMPACT è l'acronimo di European Multidisciplinary Platform Against Criminal Threats (piattaforma multidisciplinare europea di lotta alle minacce della criminalità)

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

informazioni fondamentali. Processi migliori, più rapidi e semplificati, che coinvolgano tutte le comunità della sicurezza, porterebbero a risultati migliori. Strumenti adeguati sono essenziali per assicurare che lo scambio di informazioni risponda alle sue potenzialità in termini di efficace perseguimento della criminalità con le necessarie salvaguardie, in modo che la condivisione dei dati rispetti le leggi in materia di protezione dei dati e i diritti fondamentali. Alla luce degli sviluppi tecnologici, forensi e della protezione dei dati nonché delle mutate esigenze operative, l'UE potrebbe valutare la necessità di modernizzare alcuni strumenti, quali le **decisioni Prüm del 2008**, autorizzando lo scambio automatizzato di dati su DNA, impronte digitali e immatricolazione dei veicoli al fine di consentire, nelle indagini penali, lo scambio automatizzato di ulteriori categorie di dati già disponibili nelle banche dati giudiziarie o in altre banche dati degli Stati membri. Inoltre, la Commissione esaminerà la possibilità di scambiare i casellari giudiziari per contribuire a individuare eventuali precedenti penali in altri Stati membri e facilitare l'accesso a tali dati una volta identificati, con tutte le garanzie necessarie.

Le **informazioni sui viaggiatori** hanno contribuito a migliorare i controlli alle frontiere, ridurre la migrazione irregolare e individuare le persone che presentano rischi per la sicurezza. Le informazioni anticipate sui passeggeri sono costituite dai dati biografici di ogni passeggero raccolti dai vettori aerei durante il check-in e trasmessi in anticipo alle autorità di controllo delle frontiere del paese di destinazione. La revisione del quadro giuridico[117] potrebbe consentire un uso più efficace delle informazioni, garantendo al contempo il rispetto della legislazione in materia di protezione dei dati e agevolando il flusso di passeggeri. I dati del codice di prenotazione (Passenger Name Records — PNR) corrispondono ai dati forniti dai passeggeri al momento della prenotazione dei voli. L'attuazione della direttiva sul codice di prenotazione[118] è fondamentale al riguardo e la Commissione continuerà a sostenerne l'applicazione. Inoltre, come azione a medio termine, la Commissione avvierà una revisione dell'attuale approccio relativo al **trasferimento dei dati del codice di prenotazione (PNR) verso i paesi terzi**.

La **cooperazione giudiziaria** è necessaria per integrare gli sforzi della polizia volti a combattere la criminalità transfrontaliera ed ha subito profondi cambiamenti negli ultimi 20 anni. Organismi quali la **Procura europea** e **Eurojust** devono disporre dei mezzi per funzionare al meglio o devono essere rafforzati. La cooperazione tra gli operatori giudiziari potrebbe essere migliorata anche attraverso ulteriori iniziative sul riconoscimento reciproco delle decisioni giudiziarie, sulla formazione giudiziaria e sullo scambio di informazioni. L'obiettivo dovrebbe essere quello di aumentare la fiducia reciproca tra giudici e pubblici ministeri, elemento fondamentale per semplificare i procedimenti transfrontalieri. L'uso delle **tecnologie digitali** può migliorare anche l'efficienza dei nostri sistemi giudiziari. È in via di istituzione un nuovo sistema di scambio digitale per trasmettere con il sostegno di Eurojust ordini europei di indagine, richieste di assistenza giudiziaria reciproca e relative comunicazioni tra Stati membri. La Commissione collaborerà con questi ultimi per accelerare l'introduzione dei necessari sistemi informatici a livello nazionale.

La cooperazione internazionale è inoltre fondamentale ai fini di un'efficace applicazione della legge e della cooperazione giudiziaria. Gli accordi bilaterali con i principali partner svolgono un ruolo fondamentale nel garantire la sicurezza delle informazioni e delle prove provenienti da paesi terzi. **Interpol**, una delle più grandi organizzazioni di polizia criminale

[117] Direttiva 2004/82/CE del Consiglio concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate.

[118] Direttiva 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.

intergovernative, svolge un ruolo importante. La Commissione esaminerà possibili modalità per rafforzare la cooperazione con l'Interpol, compreso l'eventuale accesso alle banche dati dell'Interpol e il rafforzamento della cooperazione operativa e strategica. Le autorità di contrasto dell'UE si affidano anche ai principali paesi partner per individuare criminali e terroristi e svolgere le relative indagini. **Partenariati per la sicurezza tra l'UE e i paesi terzi** potrebbero venire potenziati al fine di intensificare la cooperazione per contrastare minacce condivise quali il terrorismo, la criminalità organizzata, la criminalità informatica, gli abusi sessuali sui minori e la tratta di esseri umani. Tale approccio si baserebbe su interessi comuni in materia di sicurezza e sui dialoghi consolidati in materia di cooperazione e sicurezza.

Oltre alle informazioni, lo scambio di conoscenze può essere particolarmente utile per aumentare la preparazione delle attività di contrasto nel caso di **minacce non tradizionali**. Oltre a incoraggiare lo scambio di buone pratiche, la Commissione esaminerà un eventuale **meccanismo di coordinamento a livello dell'UE per le forze di polizia** in caso di eventi di forza maggiore, quali le pandemie. L'attuale pandemia ha inoltre dimostrato che il controllo digitale del territorio da parte della polizia di prossimità, accompagnata da quadri giuridici per facilitare l'attività di polizia online, sarà fondamentale nella lotta alla criminalità e al terrorismo. Le forme di cooperazione tra polizia e comunità, offline e online, possono prevenire la criminalità e mitigare l'impatto della criminalità organizzata, della radicalizzazione e delle attività terroristiche. Il collegamento tra interventi di polizia a livello locale, regionale, nazionale e dell'UE è un fattore chiave per il successo dell'Unione della sicurezza nel suo complesso.

Il contributo di frontiere esterne solide

La gestione moderna ed efficiente delle frontiere esterne ha il duplice vantaggio di mantenere l'integrità di Schengen e di garantire la sicurezza ai nostri cittadini. Il coinvolgimento di tutti i soggetti interessati al fine di sfruttare al meglio la sicurezza alle frontiere può avere un impatto reale sulla prevenzione della criminalità transfrontaliera e del terrorismo. Le attività operative congiunte della guardia di frontiera e costiera europea[119], rafforzate di recente, contribuiscono alla prevenzione e all'individuazione della criminalità transfrontaliera alle **frontiere esterne** e al di fuori dell'UE. Le attività doganali volte a individuare i rischi per la sicurezza di tutte le merci prima che entrino nell'UE e a controllarle al loro arrivo sono fondamentali nella lotta contro la criminalità transfrontaliera e il terrorismo. Il prossimo piano d'azione sull'Unione doganale annuncerà azioni volte a rafforzare la gestione dei rischi e a migliorare la sicurezza interna, in particolare valutando la fattibilità di un collegamento tra i sistemi di informazione responsabili dell'analisi dei rischi in materia di sicurezza.

Il quadro per l'**interoperabilità tra i sistemi di informazione dell'UE** nel settore della giustizia e degli affari interni è stato adottato nel maggio 2019. La nuova architettura mira a migliorare l'efficienza e l'efficacia di sistemi d'informazione nuovi o aggiornati[120]. Ciò comporterà informazioni più rapide e più sistematiche per gli operatori delle autorità di contrasto, le guardie di frontiera e i responsabili della migrazione e contribuirà alla corretta identificazione e alla lotta contro la frode d'identità. Per realizzare questo obiettivo, occorre

[119] Composta dall'Agenzia europea della guardia di frontiera e costiera (Frontex), dalle guardie di frontiera degli Stati membri e dalle autorità di guardia costiera.

[120] Il sistema di ingressi/uscite (EES), il sistema europeo di informazione e autorizzazione ai viaggi (ETIAS), il sistema europeo di informazione sui casellari giudiziali (ECRIS-TCN) allargato, il sistema d'informazione Schengen, il sistema d'informazione visti e il futuro Eurodac aggiornato.

che l'attuazione dell'interoperabilità costituisca una priorità a livello sia politico che tecnico. Una stretta cooperazione tra le agenzie dell'UE e tutti gli Stati membri sarà fondamentale per raggiungere l'obiettivo della piena interoperabilità entro il 2023.

Il fenomeno della **falsificazione dei documenti di viaggio** è considerato uno dei reati commessi con maggiore frequenza. Facilita il movimento clandestino di criminali e terroristi e svolge un ruolo fondamentale nella tratta di esseri umani e nel commercio di stupefacenti[121]. La Commissione esaminerà come estendere i lavori in corso sulle norme di sicurezza dei documenti di soggiorno e di viaggio dell'UE, anche attraverso la digitalizzazione. A partire dall'agosto 2021, gli Stati membri inizieranno a rilasciare carte d'identità e titoli di soggiorno conformemente a norme di sicurezza armonizzate, compreso un chip contenente identificatori biometrici che può essere verificato da tutte le autorità di frontiera dell'UE. La Commissione monitorerà l'attuazione di queste nuove norme, compresa la graduale sostituzione dei documenti attualmente in circolazione.

Rafforzare la ricerca e l'innovazione in materia di sicurezza

I lavori volti a garantire la cibersicurezza e a combattere la criminalità organizzata, la criminalità informatica e il terrorismo dipendono in larga misura dallo sviluppo futuro di strumenti volti a: contribuire a creare nuove tecnologie più protette e sicure, affrontare le sfide poste dalle tecnologie e sostenere il lavoro delle autorità di contrasto. Ciò, a sua volta, dipende da partner privati e dalle industrie.

L'innovazione dovrebbe essere considerata uno strumento strategico per contrastare le attuali minacce e anticipare i rischi e le opportunità per il futuro. Le tecnologie innovative possono apportare nuovi strumenti a sostegno delle attività di contrasto e di altri attori della sicurezza. L'intelligenza artificiale e l'analisi dei Big Data potrebbero sfruttare il calcolo ad alte prestazioni per offrire un'analisi migliore, rapida e completa[122]. Un prerequisito fondamentale per lo sviluppo di tecnologie affidabili è costituito da insiemi di dati di elevata qualità a disposizione delle autorità competenti per la formazione, la prova e la convalida degli algoritmi[123]. Più in generale, si registra oggi un forte rischio di dipendenza tecnologica: l'UE, ad esempio, è un importatore netto di prodotti e servizi in materia di cibersicurezza, con tutte le conseguenze che ciò comporta per l'economia e le infrastrutture critiche. Al fine di padroneggiare la tecnologia e garantire la continuità dell'approvvigionamento anche in caso di eventi avversi e crisi, l'Europa ha bisogno di una presenza e di una capacità nelle parti critiche delle pertinenti catene di valore.

La ricerca, l'innovazione e lo sviluppo tecnologico dell'UE offrono l'opportunità di tener conto della dimensione della sicurezza nella fase di sviluppo e applicazione di queste tecnologie. La prossima generazione di proposte di finanziamento dell'UE può agire come importante stimolo in tal senso[124]. Le iniziative riguardanti i dati europei e le infrastrutture cloud hanno tenuto conto della sicurezza fin dall'inizio. Il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di

[121] Il rapporto tra la frode in materia di documenti e il traffico di esseri umani è illustrato nella seconda relazione sui progressi compiuti nella lotta contro la tratta degli esseri umani, COM (2018) 777 e nei documenti di accompagnamento: SWD (2018) 473 e la relazione di Europol 2016 sulla situazione della tratta di esseri umani nell'UE.

[122] Ciò dovrebbe basarsi sulla strategia della Commissione in materia di intelligenza artificiale.

[123] Una strategia europea per i dati (COM (2020) 66 final).

[124] Le proposte della Commissione per Orizzonte Europa, il Fondo Sicurezza interna, il Fondo per la gestione integrata delle frontiere, il programma EUInvest, il Fondo europeo di sviluppo regionale e il programma Europa digitale sosterranno tutti lo sviluppo e la diffusione di tecnologie e soluzioni innovative in materia di sicurezza lungo la catena del valore della sicurezza.

coordinamento[125] mirano a creare una struttura efficace ed efficiente per mettere in comune e condividere le capacità e i risultati della ricerca nel campo della cibersicurezza. Il programma spaziale dell'UE fornisce servizi a sostegno della sicurezza dell'UE, dei suoi Stati membri e dei suoi cittadini[126].

Con oltre 600 progetti avviati per un valore complessivo di quasi 3 miliardi di EUR dal 2007, la ricerca in materia di sicurezza finanziata dall'UE è uno strumento fondamentale per stimolare la tecnologia e le conoscenze a sostegno di soluzioni in materia di sicurezza. Nell'ambito del riesame del mandato di Europol, la Commissione esaminerà la creazione di un **polo europeo dell'innovazione per la sicurezza interna**[127], che mirerebbe a fornire soluzioni comuni alle sfide e alle opportunità comuni in materia di sicurezza, che gli Stati membri potrebbero non essere in grado di sfruttare da soli. La cooperazione è fondamentale per concentrare gli investimenti in modo da ottenere i risultati migliori e per sviluppare tecnologie innovative con un vantaggio in termini sia di sicurezza che economici.

Competenze e sensibilizzazione

La consapevolezza per quanto riguarda le questioni relative alla sicurezza e l'acquisizione delle competenze necessarie per affrontare potenziali minacce sono essenziali per costruire una società più resiliente nella quali le imprese, le amministrazioni e i singoli siano preparati meglio. Le sfide poste alle infrastrutture informatiche e ai sistemi elettronici hanno fatto emergere la necessità di migliorare la capacità delle persone sotto il profilo della preparazione e della risposta in materia di cibersicurezza. La pandemia ha inoltre messo in luce l'importanza della digitalizzazione in tutti i settori dell'economia e della società dell'UE.

Anche una **conoscenza di base delle minacce alla sicurezza** e di come combatterle può avere un impatto concreto sulla resilienza della società. La consapevolezza dei rischi della criminalità informatica insieme alla necessità di proteggersi sono elementi che possono integrare la protezione offerta dai fornitori di servizi per contrastare gli attacchi informatici. Le informazioni sui pericoli e sui rischi del traffico di droga possono rendere più difficile il successo dei criminali. L'UE può stimolare la diffusione delle migliori pratiche, ad esempio attraverso la rete di centri "Internet più sicuro"[128], e garantire che tali obiettivi siano presi in considerazione nei propri programmi.

Il futuro piano d'azione per l'istruzione digitale dovrebbe includere misure mirate per costruire competenze informatiche in materia di sicurezza per l'intera popolazione. L'agenda europea per le competenze[129], adottata di recente, sostiene lo sviluppo di competenze lungo tutto l'arco della vita e comprende azioni specifiche per aumentare il numero di laureati in scienza, tecnologia, ingegneria, arte e matematica necessari in settori all'avanguardia quali la cibersicurezza. Ulteriori azioni, finanziate dal programma Europa digitale, consentiranno ai

[125] Proposta della Commissione, del 12 settembre 2018, che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento (COM (2018) 630).

[126] Ad esempio, Copernicus fornisce servizi che consentono la sorveglianza delle frontiere esterne dell'UE e la sorveglianza marittima, contribuendo a combattere la pirateria e il contrabbando e a sostenere le infrastrutture critiche. Quando sarà pienamente operativo, Copernicus costituirà un fattore determinante per le missioni e le operazioni civili e militari.

[127] Il polo coopererebbe anche con EBCGA/Frontex, CEPOL, eu-LISA e il Centro comune di ricerca.

[128] Cfr. www.betterinternetforkids.eu: il portale centrale e i centri nazionali "Internet più sicuro" sono attualmente finanziati nell'ambito di CEF/Telecom, i finanziamenti futuri sono stati proposti nell'ambito del programma Europa digitale.

[129] Agenda per le competenze per le competenze per l'Europa per la competitività sostenibile, l'equità sociale e la resilienza (COM (2020) 274 final).

professionisti di tenere il passo con l'evoluzione delle minacce alla sicurezza e, al tempo stesso, di colmare le carenze in questo campo sul mercato del lavoro dell'UE. L'impatto generale perseguito con tutte queste azioni è di consentire alle persone di acquisire competenze per far fronte alle minacce alla sicurezza e alle imprese di trovare i professionisti di cui hanno bisogno in questo settore. I prossimi sistemi di programmi "Spazio europeo della ricerca" e "Spazio europeo dell'istruzione" promuoveranno inoltre le carriere nei settori della scienza, della tecnologia, dell'ingegneria, delle arti e della matematica.

Anche l'accesso delle **vittime** ai loro diritti è importante; esse devono ricevere l'assistenza necessaria e il sostegno di cui hanno bisogno nelle particolari circostanze in cui si trovano. Occorre un impegno particolare per quanto riguarda le minoranze e le vittime più vulnerabili, come i minori o le donne oggetto di tratta a fini di sfruttamento sessuale o esposti alla violenza domestica[130].

Un ruolo particolare spetta al miglioramento delle **competenze necessarie per le attività di contrasto**. Le minacce tecnologiche, attuali e future, richiedono maggiori investimenti volti a migliorare il livello delle competenze del personale degli organismi di contrasto sin dall'inizio della carriera e durante tutto il suo arco. CEPOL è un partner essenziale per assistere gli Stati membri in questo compito. La formazione delle autorità di contrasto in materia di razzismo e xenofobia e, più in generale, i diritti dei cittadini, devono costituire una componente essenziale di una cultura della sicurezza dell'UE. Anche i sistemi giudiziari nazionali e gli operatori della giustizia devono essere in grado di adattarsi e rispondere a sfide senza precedenti. La formazione è essenziale per consentire alle autorità sul campo di sfruttare tali strumenti nelle situazioni operative. Inoltre, dovrebbero essere compiuti tutti gli sforzi necessari per rafforzare l'integrazione della dimensione di genere e rafforzare la partecipazione delle donne nelle attività di contrasto.

Azioni principali
• Potenziamento del mandato di Europol • Valutazione delle possibilità di istituire un "codice di cooperazione di polizia" dell'UE e un coordinamento delle forze di polizia in tempi di crisi • Potenziamento di Eurojust per collegare tra loro le autorità giudiziarie e di polizia • Riesame della direttiva riguardante le informazioni anticipate sui passeggeri • Comunicazione sulla dimensione esterna del codice di prenotazione • Rafforzamento della cooperazione tra l'UE e Interpol • Un quadro per negoziare con i principali paesi terzi la condivisione delle informazioni • Migliori norme di sicurezza per i documenti di viaggio • Valutazione della creazione di un polo europeo dell'innovazione per la sicurezza interna

V. Conclusioni

In un mondo sempre più in preda a turbolenze di vario genere, l'Unione europea è ancora comunemente ritenuta uno dei luoghi più sicuri e meglio protetti. Tuttavia, questa situazione non può essere data per scontata.

[130] Cfr. la strategia per la parità di genere, COM (2020) 152), la strategia per i diritti delle vittime, COM (2020) 258. e la strategia europea per un'internet migliore per i ragazzi, COM (2012) 196.

La nuova strategia sull'Unione della sicurezza getta le basi per un ecosistema della sicurezza che si estende all'intera società europea. È fondata sulla consapevolezza che la sicurezza è una responsabilità condivisa. La sicurezza è una questione che interessa tutti: tutti gli organismi governativi, le imprese, le organizzazioni sociali, le istituzioni e i cittadini devono assumersi le proprie responsabilità al fine di rendere le nostre società più sicure.

Le questioni relative alla sicurezza devono ora essere considerate in una prospettiva molto più ampia rispetto al passato. È necessario superare le false distinzioni tra spazio fisico e spazio digitale. L'Unione della sicurezza dell'UE riunisce l'intera gamma delle esigenze in materia di sicurezza e si concentra su quelli che saranno i settori più critici per la sicurezza dell'UE negli anni a venire. Riconosce inoltre che le minacce alla sicurezza non si fermano ai confini geografici e prende atto dell'interconnessione crescente tra sicurezza interna ed esterna[131]. In tale contesto, sarà importante che l'UE cooperi con i partner internazionali per la protezione di tutti i cittadini dell'UE e mantenga uno stretto coordinamento con l'azione esterna dell'UE nell'attuazione della presente strategia.

La nostra sicurezza è legata ai nostri valori fondamentali. Tutte le azioni e le iniziative proposte in questa strategia rispetteranno pienamente i diritti fondamentali e i valori europei. Essi sono il fondamento dello stile di vita europeo e devono rimanere al centro di tutto il nostro lavoro.

Infine, la Commissione è pienamente consapevole del fatto che qualsiasi politica o intervento sono efficaci solo quanto lo è la loro attuazione. è pertanto necessario sottolineare costantemente l'importanza della corretta attuazione e applicazione della legislazione esistente e futura. Ciò sarà monitorato mediante relazioni periodiche dell'Unione sulla sicurezza, e la Commissione informerà e coinvolgerà appieno in tutte le azioni pertinenti il Parlamento europeo, il Consiglio e i portatori di interessi. Inoltre, la Commissione è pronta a partecipare e a organizzare dibattiti congiunti con le istituzioni sulla strategia dell'Unione della sicurezza al fine di fare il punto sui progressi compiuti, cercando nel contempo di affrontare insieme le sfide future.

La Commissione invita il Parlamento europeo e il Consiglio ad approvare la presente strategia dell'Unione della sicurezza quale base per la cooperazione e l'azione comune in materia di sicurezza nei prossimi cinque anni.

[131] Cfr. la strategia globale dell'UE.