



Bruxelles, 14.4.2021
COM(2021) 170 final

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

Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025

{SWD(2021) 74 final}

Introduzione

La criminalità organizzata, nascosta al pubblico a causa della natura opaca delle sue attività, rappresenta una minaccia considerevole per i cittadini, le imprese e le istituzioni statali europei, nonché per l'economia nel suo complesso. Come evidenziato nell'ultima **valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità dell'Unione europea** (*European Union Serious and Organised Crime Threat Assessment*, SOCTA dell'UE)¹ del 2021, in tutti gli Stati membri sono presenti gruppi di criminalità organizzata. Il panorama della criminalità organizzata è caratterizzato da un ambiente in rete in cui la cooperazione tra i criminali è fluida, sistematica e mossa da interessi incentrati sui profitti. I gruppi della criminalità organizzata utilizzano i loro ingenti profitti illeciti per infiltrarsi nell'economia lecita e nelle istituzioni pubbliche, anche mediante la corruzione, intaccando lo Stato di diritto e i diritti fondamentali e compromettendo il diritto alla sicurezza delle persone e la loro fiducia nelle autorità pubbliche. Nel 2019 gli introiti legati alla criminalità nei nove principali mercati criminali dell'Unione europea ammontavano a 139 miliardi di EUR², pari all'1 % del prodotto interno lordo dell'Unione. Come sottolineato nella strategia per l'Unione della sicurezza³, è necessario proseguire e rafforzare l'azione intrapresa a livello dell'UE per sostenere gli Stati membri nella lotta alla criminalità organizzata.

La complessità del modello di attività dei gruppi della criminalità organizzata è emersa in particolare nel 2020, nell'indagine congiunta condotta dalle autorità francesi e neerlandesi con il sostegno di Europol ed Eurojust e destinata a smantellare **EncroChat**, una rete telefonica cifrata ampiamente utilizzata dalle reti criminali. Il caso EncroChat ha portato finora a oltre 1 800 arresti e a più di 1 500 nuove indagini. Ha inoltre messo in luce in che misura i gruppi della criminalità organizzata operano a livello transnazionale e online in tutti i mercati criminali in un ambiente in rete, utilizzando modi operandi sempre più sofisticati e nuove tecnologie. Nel marzo 2021 un'altra operazione congiunta condotta in seguito all'intrusione abusiva in Sky ECC, una rete cifrata in cui si erano trasferiti molti ex utenti di EncroChat, ha contribuito alla prevenzione di oltre 70 incidenti violenti, al sequestro di oltre 28 tonnellate di sostanze stupefacenti e all'arresto di oltre 80 persone con l'accusa di coinvolgimento nella criminalità organizzata e nel traffico di droga in Belgio e nei Paesi Bassi. Sono state avviate più di 400 nuove indagini contro i gruppi della criminalità organizzata ad alto rischio.

¹ Europol, EU SOCTA 2021, 12 aprile 2021: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment>. La SOCTA dell'UE è un'analisi completa della minaccia rappresentata dalla criminalità organizzata, che identifica le aree di criminalità a priorità elevata ed è elaborata ogni quattro anni da Europol sulla base dei contributi forniti dagli Stati membri.

² Droghe illecite, tratta di esseri umani, traffico di migranti, frode (frode intracomunitaria dell'operatore inadempiente [MTIC], violazione dei diritti di proprietà intellettuale, frode alimentare), criminalità ambientale (rifiuti e specie selvatiche illecite), armi da fuoco illecite, tabacco illecito, criminalità informatica, reati organizzati contro il patrimonio: si veda lo studio *Mapping the risk of serious and organised crime infiltration in legitimate businesses*, marzo 2021, DR0221244ENN, <https://data.europa.eu/doi/10.2837/64101>.

³ Comunicazione della Commissione sulla strategia dell'UE per l'Unione della sicurezza (COM(2020) 605 final del 24.7.2020).

Nell'UE l'uso della violenza da parte di persone coinvolte nella criminalità organizzata è in aumento, così come la minaccia degli incidenti violenti causati dall'utilizzo frequente di armi da fuoco o esplosivi negli spazi pubblici⁴. L'agilità con cui i gruppi della criminalità organizzata si adattano e sfruttano i cambiamenti nell'ambiente in cui operano è stata confermata nel corso della pandemia di COVID-19. I gruppi criminali si sono serviti della pandemia per aumentare le attività online⁵ e per commettere frodi, inclusa la contraffazione dei dispositivi medici. La domanda elevata e prolungata di vaccini contro la COVID-19 crea un'opportunità allettante per i criminali, che cercano di produrre o fornire vaccini contraffatti o commettere operazioni fraudolente contro gli individui o le autorità pubbliche. I governi dell'UE hanno finora individuato tentativi di truffa e offerte fittizie ad opera di truffatori che hanno cercato di vendere oltre 1,1 miliardi di dosi di vaccino, per un importo totale di oltre 15,4 miliardi di EUR⁶. La crisi economica emersa a seguito della pandemia aumenta i rischi derivanti dalle attività della criminalità organizzata e associati alla sua possibilità di infiltrarsi ulteriormente nella società e nell'economia.

Le minacce transnazionali e lo sviluppo delle modalità operative dei gruppi della criminalità organizzata offline e online richiedono una risposta coordinata, più mirata e adeguata. Anche se le autorità nazionali che operano sul campo sono le principali responsabili della lotta alla criminalità organizzata, l'azione a livello dell'Unione e i partenariati globali sono fondamentali per garantire una cooperazione efficace e lo scambio di informazioni e conoscenze tra le autorità nazionali, con il sostegno di un quadro comune di diritto penale e da mezzi finanziari efficaci. Inoltre il problema della criminalità organizzata dimostra con la massima evidenza il legame tra sicurezza interna ed esterna. Per rispondere a questa sfida internazionale è necessario un impegno internazionale nella lotta alla criminalità organizzata, incluse ulteriori misure per sviluppare partenariati e cooperazione con i paesi nelle immediate vicinanze e oltre.

Sia il Parlamento europeo⁷ che il Consiglio⁸ hanno sottolineato che la criminalità organizzata provoca danni enormi e hanno evidenziato l'importanza di un'azione forte dell'UE per contrastarla in tutte le sue forme.

Basandosi sui risultati finora raggiunti, la presente strategia individua i filoni di lavoro prioritari per assicurare una migliore protezione dei cittadini e dell'economia contro i gruppi

⁴ Europol, relazione *EU Serious and Organised Threat Assessment* (SOCTA dell'UE 2021), 12 aprile 2021: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment>.

⁵ In un'operazione internazionale sostenuta da Europol e dall'Ufficio europeo per la lotta antifrode (OLAF), condotta tra marzo e dicembre 2020, le autorità di contrasto di 19 Stati membri e otto paesi terzi hanno sequestrato quasi 33 milioni di dispositivi medici contraffatti, tra cui maschere facciali, test e kit di diagnosi, 8 tonnellate di materie prime e 70 000 litri di disinfettanti.

⁶ Informazioni comunicate dalle autorità governative all'OLAF. Le autorità di contrasto, insieme a Europol e all'OLAF, stanno cooperando per contrastare questi tentativi di frode.

⁷ https://www.europarl.europa.eu/doceo/document/TA-9-2020-0378_IT.pdf Nell'ottobre 2016 il Parlamento europeo ha adottato inoltre una relazione che si concentra specificamente sulla lotta contro la corruzione: https://www.europarl.europa.eu/doceo/document/A-8-2016-0284_IT.pdf.

⁸ Conclusioni del Consiglio sulla sicurezza interna e sul partenariato europeo di polizia, 13083/1/20 REV 1, del 24 novembre 2020.

della criminalità organizzata e propone azioni concrete a medio e lungo termine, che saranno sviluppate nel pieno rispetto dei diritti fondamentali. Si tratta della prima strategia ad hoc in materia di criminalità organizzata dopo l'entrata in vigore del trattato di Lisbona⁹.

1. Promozione della cooperazione tra autorità di contrasto e autorità giudiziarie

La criminalità organizzata è oggi un'impresa internazionale. Il 65 % dei gruppi criminali attivi negli Stati membri dell'UE è composto da persone di diverse cittadinanze¹⁰. Le rotte di trasporto della droga, delle armi da fuoco o dei prodotti contraffatti attraversano tutti i continenti formando una catena di approvvigionamento globale. I gruppi mobili della criminalità organizzata coinvolti nei reati organizzati contro il patrimonio si spostano rapidamente tra più giurisdizioni per agire; operando in diverse giurisdizioni, evitano di essere scoperti e sfruttano le differenze tra le varie leggi nazionali applicabili.

1.1. Agevolare lo scambio di informazioni e permettere un accesso tempestivo alle informazioni

In uno spazio di libertà, sicurezza e giustizia senza controlli alle frontiere interne, per assicurare un elevato livello di sicurezza occorre una solida cooperazione giudiziaria e di polizia tra gli Stati membri. L'accesso tempestivo alle informazioni, nel pieno rispetto dei diritti fondamentali e in particolare della protezione dei dati, è essenziale per la lotta contro tutte le forme di criminalità organizzata. L'Unione europea ha fornito alle autorità di contrasto un'ampia gamma di strumenti per agevolare lo scambio di informazioni, che si è rivelato un fattore determinante per individuare le attività e le reti criminali.

Il **sistema d'informazione Schengen (SIS)** ha permesso ai funzionari in prima linea di individuare e localizzare rapidamente persone e oggetti coinvolti nella criminalità organizzata e di agire di conseguenza. Le informazioni contenute in questa banca dati comune possono aiutare i funzionari ad arrestare una persona, sequestrare un oggetto o scoprire gli spostamenti di persone coinvolte in un'indagine. Nel solo 2020 il sistema d'informazione Schengen è stato consultato 4 miliardi di volte, ottenendo più di 200 000 riscontri positivi. Il riesame del quadro del SIS del 2018¹¹ ha notevolmente rafforzato le funzionalità del sistema e ha

⁹ La criminalità organizzata è una priorità dell'UE sin dalla metà degli anni '90, come emerge dal programma di Tampere (che ha stabilito i primi obiettivi strategici pluriennali dell'UE nel settore della giustizia e degli affari interni) e dai successivi programmi pluriennali sulla giustizia e sugli affari interni, quali il programma dell'Aia del 2004, il programma di Stoccolma del 2009, l'agenda europea sulla sicurezza del 2015 e la recente strategia dell'UE per l'Unione della sicurezza del 2020. L'ultima strategia ad hoc in materia di criminalità organizzata risale al 2005: <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52005DC0232&from=EN>.

¹⁰ Europol, relazione *EU Serious and Organised Threat Assessment* (SOCTA dell'UE 2021), 12 aprile 2021: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment>.

¹¹ Regolamento (UE) 2018/1860 del Parlamento europeo e del Consiglio, del 28 novembre 2018, relativo all'uso del sistema d'informazione Schengen per il rimpatrio di cittadini di paesi terzi il cui soggiorno è irregolare (GU L 312 del 7.12.2018), regolamento (UE) 2018/1861 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore delle verifiche di frontiera, che modifica la convenzione di applicazione dell'accordo di Schengen e abroga il regolamento (CE) n. 1987/2006 (GU L 312 del 7.12.2018) e regolamento 2018/1862 del Parlamento europeo e del Consiglio, del 28 novembre 2018, sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen

introdotto una serie di nuovi strumenti, consentendo alle autorità nazionali di inserire segnalazioni su persone a rischio di sottrazione o di tratta di esseri umani, o di richiedere controlli di indagine su un indagato. La riforma estende inoltre a Europol l'accesso alle segnalazioni del SIS e allo scambio di informazioni supplementari e consente di utilizzare in modo più efficace i dati biometrici, introducendo la possibilità di usare immagini del volto a fini di identificazione e di includere profili DNA per agevolare l'identificazione delle persone scomparse. L'attuazione di queste novità sta procedendo a pieno ritmo per far sì che il nuovo sistema sia pienamente operativo entro la fine del 2021, gli atti di esecuzione e la documentazione tecnica siano completati, il lavoro sullo sviluppo tecnico del SIS sia ben avviato e siano stati intrapresi i primi passi per elaborare un manuale SIS e attività di formazione per gli utenti del SIS.

Il potenziale del SIS per contrastare la criminalità organizzata sarà ulteriormente rafforzato mediante il nuovo quadro per l'**interoperabilità** tra i sistemi di informazione dell'UE nel settore della giustizia e degli affari interni¹². È fondamentale compiere ogni sforzo per raggiungere la piena interoperabilità entro la fine del 2023. In questo modo si agevolerà l'accesso da parte delle autorità di contrasto alle informazioni pertinenti nei sistemi di informazione centralizzati dell'UE e si permetterà l'individuazione dei casi di identità multiple, essenziale nella lotta contro le frodi d'identità, spesso utilizzate dai criminali per commettere reati o sfuggire alla giustizia. Nell'ambito del quadro per l'interoperabilità si sta sviluppando la funzionalità del **rilevatore di identità multiple** che, controllando i dati mediante questi sistemi, aiuterà ad affrontare efficacemente l'uso fraudolento delle identità.

Gli investigatori che operano isolatamente in uno Stato membro spesso non sono in grado di scoprire il coinvolgimento di un gruppo della criminalità organizzata in un reato specifico. Il quadro di **Prüm** del 2008¹³ permette alle autorità di contrasto, nel corso delle loro indagini, di effettuare consultazioni sul DNA e sulle impronte digitali nelle banche dati di altri Stati membri in base ad un sistema "hit/no-hit" (riscontro positivo/riscontro negativo) mediante connessioni bilaterali, e di effettuare consultazioni sui dati di immatricolazione dei veicoli. Sebbene il quadro di Prüm si sia dimostrato utile per risolvere numerosi reati in Europa, la sua

(SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale, che modifica e abroga la decisione 2007/533/GAI del Consiglio e che abroga il regolamento (CE) n. 1986/2006 del Parlamento europeo e del Consiglio e la decisione 2010/261/UE della Commissione (GU L 312 del 7.12.2018).

¹² Il quadro per l'interoperabilità si applica al SIS, al sistema di informazione visti (VIS), a Eurodac, al sistema di ingressi/uscite (EES), al sistema europeo di informazione e autorizzazione ai viaggi (ETIAS) e al sistema europeo di informazione sui casellari giudiziali riguardo ai cittadini di paesi terzi (ECRIS-TCN). Regolamento (UE) 2019/817 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore delle frontiere e dei visti e che modifica i regolamenti (CE) n. 767/2008, (UE) n. 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 del Parlamento europeo e del Consiglio e le decisioni 2004/512/CE e 2008/633/GAI del Consiglio (GU L 135 del 22.5.2019), e regolamento (UE) 2019/818 del Parlamento europeo e del Consiglio, del 20 maggio 2019, che istituisce un quadro per l'interoperabilità tra i sistemi di informazione dell'UE nel settore della cooperazione di polizia e giudiziaria, asilo e migrazione, e che modifica i regolamenti (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (GU L 135 del 22.5.2019).

¹³ Decisione 2008/615/GAI del Consiglio sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera e decisione 2008/616/GAI del Consiglio relativa all'attuazione della decisione 2008/615/GAI (GU L 210 del 6.8.2008).

natura decentrata ha impedito che si stabilissero molte connessioni bilaterali tra le banche dati nazionali degli Stati membri a causa della complessità tecnica e delle importanti risorse finanziarie e umane che comporta. Inoltre le autorità possono impiegare settimane o addirittura mesi per condividere i dati personali in relazione a un riscontro. Per migliorare l'efficienza delle indagini penali e rafforzare lo scambio automatizzato di informazioni sui criminali, la Commissione proporrà di modernizzare il **quadro di Prüm per rispondere alle esigenze operative** delle autorità di contrasto, nel rispetto dei diritti fondamentali e dei requisiti di necessità e proporzionalità, e per allineare le disposizioni in materia di protezione dei dati alla direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie¹⁴. La Commissione sta esaminando le possibili opzioni per garantire la connessione delle banche dati pertinenti tra tutti gli Stati membri e per **accelerare lo scambio di informazioni** in caso di riscontro. La Commissione sta anche valutando la necessità di scambiare **ulteriori categorie di dati** pertinenti per le indagini penali, come immagini facciali, patenti di guida, precedenti penali e balistica, nel quadro di Prüm, e di aggiungere Europol come nuovo partner di tale quadro.

Data la dimensione transfrontaliera e internazionale della criminalità organizzata, le **informazioni di viaggio** sono essenziali per identificare i viaggiatori ad alto rischio che non sarebbero altrimenti noti alle autorità di contrasto e per stabilire collegamenti tra i membri dei gruppi criminali. Il trattamento dei **dati del codice di prenotazione (Passenger Name Record, PNR)** aiuta le autorità competenti a identificare le persone coinvolte nelle attività criminali commesse dai gruppi organizzati. Per garantire che il potenziale di questo strumento sia sfruttato appieno, la Commissione continuerà a monitorare la piena ed efficace attuazione della direttiva sui dati del codice di prenotazione¹⁵ e a sostenere la cooperazione e lo scambio di dati PNR tra gli Stati membri, in particolare attraverso lo scambio di migliori pratiche, la formazione e lo sviluppo delle capacità necessarie¹⁶. Le **informazioni anticipate sui passeggeri (Advanced Passenger Information, API)**, ossia i dati biografici dei passeggeri raccolti dai vettori aerei durante il check-in, sono altrettanto preziose¹⁷, anche per la loro complementarità con i dati del codice di prenotazione. Una revisione dell'attuale quadro

¹⁴ Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119 del 4.5.2016).

¹⁵ Direttiva 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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 (GU L 119 del 4.5.2016).

¹⁶ Come quelle indicate nel documento di lavoro dei servizi della Commissione che accompagna la relazione della Commissione sul riesame della direttiva PNR (SWD(2020) 128 final del 24.7.2020, pagg. 7-8).

¹⁷ Gli appelli reiterati a un maggiore utilizzo delle informazioni anticipate sui passeggeri da parte delle Nazioni Unite - cfr. UNSCR 2178(2014), UNSCR 2309(2016), UNSCR 2482(2019) - e l'impegno degli Stati partecipanti dell'Organizzazione per la sicurezza e la cooperazione in Europa per istituire sistemi di informazione anticipata sui passeggeri confermano l'importanza di questi dati. Inoltre, da febbraio 2018, l'istituzione di sistemi nazionali di informazione anticipata sui passeggeri costituisce un requisito dell'Organizzazione dell'aviazione civile internazionale, che la rende obbligatoria per tutti gli Stati contraenti della convenzione di Chicago.

giuridico¹⁸ consentirebbe una serie di miglioramenti, in particolare per quanto riguarda l'accuratezza e la completezza dei dati. Fatto ancora più importante, la Commissione analizzerà il potenziale utilizzo dei dati API per interrogare sistematicamente i dati Europol al fine di contrastare la criminalità organizzata, e la possibilità di estendere il loro utilizzo agli spostamenti intra-Schengen e ai vettori marittimi e ai pullman. Conformemente a tale obiettivo, la Commissione presenterà una proposta di revisione della direttiva riguardante le informazioni anticipate sui passeggeri nella prima metà del 2022, sulla base di una valutazione d'impatto in cui si esamineranno ulteriormente queste opzioni e il relativo impatto.

1.2. Quadri di cooperazione avanzata

Gran parte della cooperazione nell'attività di contrasto nell'UE si basa sulla convenzione di applicazione dell'accordo di Schengen del 1990. Tale fondamento è integrato da altri strumenti dell'UE, quali la decisione quadro 2006/960/GAI del Consiglio, relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge, e i capi 4 e 5 della decisione 2008/615/GAI del Consiglio, del 23 giugno 2008, sul potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera (Prüm).

Gli Stati membri hanno completato questo quadro con un insieme complesso di accordi bilaterali e multilaterali. Di conseguenza il livello di cooperazione tra gli Stati membri non è uniforme e crea ostacoli operativi che impediscono un'efficace cooperazione transfrontaliera.

La Commissione preparerà una proposta legislativa di **un codice di cooperazione di polizia dell'UE**. Tale proposta si baserà sui risultati di uno studio esterno in corso e su un processo di consultazione approfondito, tenendo conto della competenza degli Stati membri. L'obiettivo è di integrare e sviluppare i vari strumenti per la cooperazione nell'attività di contrasto, inclusi la normativa UE pertinente, gli orientamenti del Consiglio e le buone pratiche degli Stati membri derivanti da accordi bilaterali e multilaterali, in un corpus coerente e moderno che tratti anche gli strumenti investigativi.

Inoltre, al fine di affrontare i potenziali ostacoli alla cooperazione transfrontaliera, in particolare con riguardo alle strutture della criminalità organizzata, la Commissione ha avviato uno studio esterno per valutare se la **decisione quadro del Consiglio relativa alla criminalità organizzata**¹⁹ del 2008 sia ancora adeguata allo scopo.

Europol svolge un ruolo importante come **polo centrale dell'UE per le informazioni sulla criminalità**, sostenendo la cooperazione di polizia e lo scambio di informazioni ed elaborando ogni quattro anni la relazione di **valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità dell'Unione europea** (SOCTA

¹⁸ Direttiva 2004/82/CE del Consiglio concernente l'obbligo dei vettori di comunicare i dati relativi alle persone trasportate ("direttiva riguardante le informazioni anticipate sui passeggeri" o "direttiva API") (GU L 261 del 6.8.2004).

¹⁹ Decisione quadro 2008/841/GAI del Consiglio, del 24 ottobre 2008, relativa alla lotta contro la criminalità organizzata (GU L 300 dell'11.11.2008).

dell'UE)²⁰. Per rispondere alle pressanti esigenze operative, quali la cooperazione con le parti private o il trattamento di grandi insiemi di dati, la Commissione ha proposto nel dicembre 2020 di rafforzare il mandato di Europol²¹. Le nuove competenze e i nuovi strumenti che la proposta prevede consentiranno a Europol di intensificare il suo sostegno nella lotta alla criminalità organizzata. Sia il Parlamento europeo che il Consiglio stanno lavorando sui loro mandati in vista dei prossimi negoziati interistituzionali che dovrebbero iniziare nel corso dell'anno corrente. La Commissione faciliterà i negoziati e si propone di raggiungere un rapido accordo da parte dei legislatori entro la fine del 2021.

Uno dei principali strumenti per attuare la presente strategia e per intensificare gli sforzi contro le strutture della criminalità organizzata mediante operazioni coordinate è la **piattaforma multidisciplinare europea di lotta alle minacce della criminalità (*European Multidisciplinary Platform Against Criminal Threats, EMPACT*)**. Dal 2010 EMPACT consente agli Stati membri di identificare le minacce criminali prioritarie dell'UE per le quali è necessaria un'azione collettiva²² e di affrontare tali minacce mediante una cooperazione strutturata a livello di UE tra le autorità di contrasto, le autorità doganali, le autorità fiscali, i magistrati, le istituzioni e le agenzie europee e, se del caso, i paesi terzi, le organizzazioni internazionali e il settore privato²³.

Attraverso EMPACT gli Stati membri e i loro partner svolgono **ogni anno oltre 200 azioni operative comuni** volte a contrastare la criminalità organizzata, ad esempio sviluppando un quadro di intelligence criminale sulle priorità dell'UE in materia di lotta alla criminalità, sviluppando capacità di contrasto per perseguire reati specifici, rafforzando la cooperazione con i partner internazionali, svolgendo attività di prevenzione, indagini congiunte contro fenomeni criminali o gruppi criminali specifici e contrastando i metodi che questi gruppi criminali utilizzano per riciclare denaro, commettere reati online od ottenere documenti fraudolenti. Sebbene EMPACT realizzi già risultati operativi importanti, ad esempio in termini di droga sequestrata o di criminali arrestati, il suo potenziale non è attualmente

²⁰ La SOCTA dell'UE, elaborata ogni quattro anni da Europol sulla base di ampi contributi forniti dagli Stati membri e da altri portatori di interessi, identifica le principali minacce criminali nell'UE e propone le priorità dell'UE in materia di lotta alla criminalità per i prossimi quattro anni. La SOCTA dell'UE è il primo passo di ogni ciclo EMPACT e su di essa si basa il Consiglio per stabilire le priorità dell'UE in materia di criminalità su cui concentrarsi nei prossimi quattro anni.

²¹ Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2016/794 per quanto riguarda la cooperazione di Europol con le parti private, il trattamento dei dati personali da parte di Europol a sostegno di indagini penali e il ruolo di Europol in materia di ricerca e innovazione (COM(2020) 796 final) e proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2018/1862 sull'istituzione, l'esercizio e l'uso del sistema d'informazione Schengen (SIS) nel settore della cooperazione di polizia e della cooperazione giudiziaria in materia penale per quanto riguarda l'inserimento di segnalazioni da parte di Europol (COM(2020) 791 final del 9 dicembre 2020).

²² Per il periodo 2018-2021: criminalità informatica, traffico di droga, favoreggiamento dell'immigrazione illegale, reati organizzati contro il patrimonio, tratta di esseri umani (per tutte le forme di sfruttamento, compresi lo sfruttamento sessuale e del lavoro nonché tutte le forme di tratta di minori), frode in materia di accise e frode MTIC, traffico illecito di armi da fuoco, criminalità ambientale, fondi di origine illegale e riciclaggio di denaro, frode in materia di documenti.

²³ Il "ciclo programmatico dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale" era la dicitura utilizzata per definire il quadro di cooperazione per stabilire le priorità comuni, mentre "EMPACT" era la piattaforma operativa che permetteva la cooperazione tra gli operatori; entrambi i concetti sono ora designati con il termine "EMPACT".

utilizzato appieno. La sua complessità, la mancanza di consapevolezza tra i funzionari di prima linea e i finanziamenti insufficienti non sempre assicurano la titolarità e il coinvolgimento attivo degli Stati membri e dei partner esterni e ostacolano lo sviluppo di operazioni più complesse che nuocerebbero in modo più significativo ai gruppi della criminalità organizzata.

La Commissione lavorerà, insieme a tutti i portatori di interessi di EMPACT, all'introduzione di una serie di misure, delineate in dettaglio nel documento di lavoro dei servizi della Commissione che accompagna la presente strategia, al fine di utilizzare appieno il potenziale di EMPACT e trasformarlo in un vero e proprio strumento faro dell'UE per la **cooperazione operativa multidisciplinare e multiagenzia** nella lotta alla criminalità organizzata a livello di UE.

La Commissione valuterà anche se sia possibile inserire il meccanismo EMPACT nella normativa UE, consolidandone il ruolo di strumento fondamentale dell'UE per la cooperazione sul piano operativo tra gli Stati membri e le agenzie e gli organismi dell'UE competenti per la lotta alla criminalità organizzata e alle forme gravi di criminalità internazionale. EMPACT diventerebbe il vettore permanente della cooperazione strutturale tra le strategie e le azioni europee e nazionali in materia di criminalità, con una metodologia e un approccio armonizzati, fornendo una base giuridica per partenariati congiunti ad hoc basati su esigenze operative. La Commissione cercherà anche di rafforzare in modo significativo il finanziamento di EMPACT per consentire lo sviluppo di operazioni più complesse. Esaminerà inoltre, insieme a tutti i portatori di interessi, la possibilità di razionalizzare l'attuale EMPACT sulla base di quattro pilastri modernizzati e aggiornati²⁴, integrati da principi guida per la lotta alla criminalità organizzata, e si adopererà per rafforzare il ruolo delle reti e dei gruppi di esperti europei nel sostenere le azioni EMPACT. Infine la Commissione, insieme al servizio europeo per l'azione esterna, promuoverà una maggiore associazione dei paesi terzi alle attività di EMPACT e lo sviluppo della metodologia EMPACT al di fuori dell'UE, adeguandola alle esigenze operative.

Per assicurare i criminali alla giustizia, le autorità di contrasto e giudiziarie devono lavorare a stretto contatto: una risposta efficace alla criminalità organizzata richiede misure aggiuntive per rafforzare ulteriormente la cooperazione giudiziaria. Le raccomandazioni del Parlamento²⁵ e le conclusioni del Consiglio²⁶ invitano a migliorare il funzionamento pratico del **mandato d'arresto europeo**²⁷. La Commissione sta quindi assicurando la corretta attuazione, in seguito

²⁴ Sequenza aggiornata dei quattro pilastri: 1) osservare, rilevare e orientare; 2) decidere e pianificare insieme; 3) contrastare, prevenire e smantellare; 4) trattenere, imparare e ripetere.

²⁵ https://www.europarl.europa.eu/doceo/document/TA-9-2021-0006_IT.html

²⁶ <https://data.consilium.europa.eu/doc/document/ST-13214-2020-INIT/it/pdf>

²⁷ Cfr. Manuale sull'emissione e l'esecuzione del mandato d'arresto europeo (GU C 335 del 6.10.2017): [https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017XC1006\(02\)&from=DA](https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52017XC1006(02)&from=DA).

alla sua relazione sull'attuazione del mandato d'arresto europeo²⁸, e fornirà orientamenti in un manuale aggiornato.

Inoltre, al fine di evitare indagini parallele sui criminali che operano in più giurisdizioni, potrebbero essere necessarie norme comuni che consentano agli Stati membri il trasferimento dei procedimenti penali in un altro Stato membro, ad esempio nello Stato membro di cittadinanza dell'indagato, tenendo conto della decisione quadro sulla prevenzione dei conflitti relativi all'esercizio della giurisdizione²⁹. Attualmente la Commissione sta esaminando ulteriormente tale questione per valutare la necessità di un'azione da parte dell'UE in questo settore. La Commissione sta inoltre analizzando i problemi che sorgono in relazione alla raccolta, al trasferimento e all'utilizzo delle prove nei procedimenti transfrontalieri e i possibili modi di procedere³⁰.

Poiché la comunicazione e la condivisione delle informazioni all'interno delle squadre investigative comuni è essenziale, la Commissione intende lavorare allo sviluppo di una piattaforma di collaborazione tra le squadre investigative comuni e al potenziamento della cooperazione di Eurojust con i paesi terzi. Inoltre, come annunciato nella comunicazione sulla digitalizzazione della giustizia nell'UE³¹, la Commissione presenterà entro la fine del 2021 una proposta per consentire la comunicazione elettronica e lo scambio sicuri di informazioni e documenti tra gli organi giurisdizionali, le autorità nazionali e, se del caso, le agenzie del settore "Giustizia e affari interni". La Commissione intende inoltre sostenere la modernizzazione del sistema di gestione dei casi di Eurojust per aiutare l'Agenzia a fornire riscontri alle autorità nazionali e sviluppare collegamenti giudiziari tra le indagini in corso. In tale modo si dovrebbe garantire che Eurojust lavori in modo efficiente con i suoi partner, in particolare Europol e la Procura europea (EPPO), aiutando a coordinare le indagini a livello nazionale e a evitare indagini parallele nell'intento di garantire azioni penali efficaci.

1.3. Cooperazione internazionale

La cooperazione tra le autorità di contrasto al di fuori dell'Unione è necessaria per smantellare le reti criminali e le rotte di trasporto globali. È essenziale intensificare la cooperazione internazionale anche attraverso le attività delle agenzie del settore "Giustizia e affari interni" competenti, in particolare in relazione ai paesi del vicinato e dell'allargamento.

È urgente sviluppare ulteriormente l'intelligence sulla criminalità organizzata e sulle forme gravi di criminalità presso Europol e rafforzare lo scambio di informazioni e le indagini con i paesi terzi e le regioni che costituiscono i principali centri della criminalità organizzata ad alto rischio che interessa gli Stati membri dell'UE, anche attraverso i funzionari di collegamento

²⁸ Relazione della Commissione al Parlamento europeo e al Consiglio sull'attuazione della decisione quadro del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri, 2 luglio 2020 (COM(2020) 270 final del 2.7.2020).

²⁹ Decisione quadro 2009/948/GAI del Consiglio, del 30 novembre 2009, sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali (GU L 328 del 15.12.2009).

³⁰ Nel marzo 2020 è stato intrapreso uno studio intitolato *Cross-border use of evidence*.

³¹ Comunicazione della Commissione *Digitalizzazione della giustizia nell'Unione europea – Un pacchetto di opportunità* (COM(2020) 710 final del 2.12.2020).

bilaterali degli Stati membri distaccati in tali aree critiche. La Commissione ha ricevuto direttive per negoziare accordi internazionali con i paesi terzi per quanto riguarda lo scambio di dati personali con Europol³² e per consentire la cooperazione giudiziaria con Eurojust³³ e si impegnerà a compiere progressi in questi difficili negoziati.

Inoltre i progetti e i programmi di cooperazione internazionale dell'UE sono importanti per la creazione di reti transcontinentali dei servizi di contrasto e di giustizia penale. La Commissione continuerà a rafforzare il sostegno a tali reti e alle operazioni congiunte.

L'approccio dell'UE alla sicurezza esterna nel quadro della politica estera e di sicurezza comune e della politica di sicurezza e di difesa comune rimane un elemento essenziale dell'attività dell'UE volta a contrastare la criminalità organizzata al fine di rafforzare la stabilità e proteggere gli interessi di sicurezza europei. L'alto rappresentante/vicepresidente, sostenuto dal servizio europeo per l'azione esterna, continuerà a svolgere un ruolo chiave nel rafforzamento della cooperazione strategica e operativa con i paesi terzi e le organizzazioni internazionali, avvalendosi appieno dei suoi strumenti esterni, quali i dialoghi ad alto livello, la rete di esperti in materia di antiterrorismo/sicurezza nelle delegazioni dell'UE e, se del caso, missioni e operazioni di politica di sicurezza e di difesa comune. Inoltre la Commissione e il servizio europeo per l'azione esterna continueranno a dare priorità ai progetti di sviluppo delle capacità nei paesi terzi e in particolare nei paesi del vicinato e dell'allargamento, sia per sostenere la cooperazione operativa con gli Stati membri e le agenzie dell'UE, sia per dotare i partner degli strumenti che consentano loro di sradicare le complesse strutture criminali che potrebbero avere effetti nell'UE.

Interpol è un altro attore fondamentale per quanto riguarda la cooperazione internazionale contro la criminalità organizzata. Le 18 banche dati di Interpol contengono oltre 100 milioni di informazioni relative ai casellari giudiziari, comprese quelle su criminali ricercati, sospetti terroristi, impronte digitali, veicoli rubati, documenti di viaggio persi e rubati, armi e armi da fuoco. Tali banche dati consentono alle autorità giudiziarie e di contrasto di individuare i collegamenti e quindi agevolare le indagini contro la criminalità organizzata transnazionale. La Commissione intende adottare, parallelamente a questa strategia, **una raccomandazione al Consiglio per avviare negoziati con Interpol** in merito a un accordo di cooperazione UE-Interpol al fine di migliorare la cooperazione e rispondere alle esigenze operative.

Il principale strumento internazionale che consente la cooperazione e l'assistenza giudiziaria reciproca nelle indagini sulla criminalità organizzata è la **convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale** (*United Nations Convention against Transnational Organized Crime*, UNTOC) cui hanno aderito l'UE e gli Stati membri. Nel 2021 la Commissione aggiornerà la dichiarazione di competenza per allinearla alle modifiche del trattato di Lisbona³⁴ e per garantire che la **Procura europea** (EPPO) possa

³² Algeria, Egitto, Giordania, Israele, Libano, Marocco, Nuova Zelanda, Tunisia e Turchia.

³³ Algeria, Argentina, Armenia, Bosnia-Erzegovina, Brasile, Colombia, Egitto, Giordania, Israele, Libano, Marocco, Tunisia e Turchia.

³⁴ L'entrata in vigore del trattato di Lisbona il 1° dicembre 2009 e la fine del periodo di transizione per gli strumenti dell'ex terzo pilastro il 1° dicembre 2014 hanno modificato i limiti delle competenze dell'UE pertinenti

avvalersi delle norme dell'UNTOC sull'assistenza giudiziaria reciproca per cooperare con le autorità dei paesi terzi. Inoltre la Commissione esaminerà la possibilità di informare l'EPPO in qualità di autorità responsabile nel contesto degli accordi di cooperazione esistenti a livello di Unione con i paesi terzi e, se necessario, prenderà in considerazione l'avvio di negoziati con paesi terzi prioritari selezionati. Come espresso nella dichiarazione di Kyoto adottata in occasione del quattordicesimo Congresso delle Nazioni Unite sulla prevenzione del crimine e la giustizia penale, l'Unione e gli Stati membri sono pienamente impegnati a rafforzare il quadro internazionale che promuove lo Stato di diritto, la prevenzione della criminalità e la giustizia penale, anche attraverso un impegno attivo nei processi in corso volti a riesaminare l'attuazione dell'UNTOC e la convenzione delle Nazioni Unite contro la corruzione (*United Nations Convention against Corruption, UNCAC*).

Azioni principali

La Commissione intende:

- proporre di rafforzare **il quadro di Prüm** (4° trimestre 2021);
- proporre la creazione di un **codice di cooperazione di polizia** dell'UE (4° trimestre 2021);
- proporre la revisione della direttiva riguardante le **informazioni anticipate sui passeggeri** (1° trimestre 2022);
- stabilire una **piattaforma di collaborazione** per le squadre investigative comuni (4° trimestre 2021);
- collaborare con tutti i portatori di interessi per **integrare, espandere e modernizzare** la piattaforma multidisciplinare europea di lotta alle minacce della criminalità (**EMPACT**) e farla diventare **lo strumento faro dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale** mediante una serie di azioni e una proposta legislativa (2023);
- **rafforzare** in modo significativo **il finanziamento** di EMPACT attraverso il Fondo sicurezza interna per il periodo 2021-2027;
- avviare negoziati per accordi di **cooperazione** tra **Eurojust** e paesi terzi;
- intensificare i negoziati sulla cooperazione tra **Europol** e i paesi terzi;
- rafforzare, insieme al servizio europeo per l'azione esterna, la **cooperazione internazionale** con i paesi terzi e le organizzazioni internazionali.

Il Parlamento europeo e il Consiglio sono invitati a:

- portare avanti i negoziati legislativi sulla **revisione del regolamento Europol**, comprese le modifiche del regolamento sul sistema d'informazione Schengen, con l'obiettivo di raggiungere un **rapido accordo**.

ai fini dell'attuazione di tale convenzione. L'UE ha acquisito nuove competenze di cui al titolo V del TFUE (articoli 82 e 83) e ha esercitato la propria competenza legiferando nei settori politici pertinenti. Inoltre il processo di riesame dell'UNTOC dovrebbe essere basato su una dichiarazione di competenza aggiornata.

Il Consiglio è invitato a:

- adottare la raccomandazione per avviare i negoziati con **Interpol** su un accordo di cooperazione UE-Interpol.

2. Indagini efficaci: smantellare le strutture della criminalità organizzata e contrastare i reati altamente prioritari

2.1. Intensificazione degli sforzi per contrastare le strutture della criminalità organizzata

Le indagini delle autorità di contrasto non dovrebbero focalizzarsi esclusivamente sul sequestro di oggetti illegali o sull'arresto di criminali di basso livello, bensì perseguire attori e reti che costituiscono la colonna portante degli ecosistemi criminali.

Poiché la maggior parte delle organizzazioni criminali è strutturata intorno a un gruppo centrale o in modo gerarchico³⁵, il panorama della criminalità organizzata è caratterizzato da un ambiente in rete in cui diversi gruppi e individui cooperano sistematicamente attraverso "joint venture" all'interno di reti criminali elastiche e fluide. Le organizzazioni criminali che coordinano le catene di rifornimento nei mercati criminali internazionali cooperano con gruppi più piccoli specializzati in determinate attività e con individui in ruoli chiave che forniscono servizi ai criminali come la frode in materia di documenti, la consulenza legale, le comunicazioni cifrate o il trasporto. La capacità dei gruppi criminali di creare legami tra di loro compromette gli sforzi delle autorità di contrasto, poiché ogni segmento della catena criminale può essere facilmente sostituito in caso di intervento delle autorità di contrasto.

In questo panorama è fondamentale intensificare lo **smantellamento delle strutture della criminalità organizzata**, concentrandosi sui gruppi che rappresentano un rischio maggiore per la sicurezza dell'Europa e sugli individui ai vertici delle organizzazioni criminali. A tal fine alcuni Stati membri hanno istituito strutture a livello nazionale o organismi specializzati all'interno dei servizi di contrasto e del sistema giudiziario per la lotta alle organizzazioni di stampo mafioso. Tali esperienze si sono dimostrate efficaci nello stimolare un approccio strategico che promuova gli sforzi tesi allo smantellamento delle infrastrutture criminali. Inoltre la creazione di unità di polizia o di organi giudiziari ad hoc favorirebbe una maggiore cooperazione transfrontaliera. La Commissione promuoverà lo scambio di migliori pratiche per favorire la riproducibilità di tali modelli negli Stati membri adeguati alle specificità nazionali.

A livello europeo la cooperazione operativa contro i gruppi della criminalità organizzata di stampo mafioso attuata attraverso la **rete @ON**³⁶ agevola l'intervento sul campo di investigatori specializzati in tutti gli Stati membri per prestare assistenza nelle indagini sui

³⁵ Secondo la relazione SOCTA dell'UE 2021, il 43 % dei gruppi della criminalità organizzata è strutturato intorno a un gruppo centrale, il 40 % in modo gerarchico e il 17 % è costituito da reti elastiche.

³⁶ Sono 16 gli Stati membri che attualmente partecipano alla rete @ON, creata nel 2014.

gruppi della criminalità organizzata transfrontaliera. Un'altra tappa importante è costituita dal lavoro svolto da Europol, insieme agli Stati membri, per identificare **obiettivi selezionati di alto valore**³⁷, ossia presunti membri di organizzazioni criminali che rappresentano un rischio particolarmente elevato per due o più Stati membri, e svolgere attività di intelligence e investigative nei loro confronti.

Per rafforzare la lotta alle organizzazioni criminali, è indispensabile un'ulteriore cooperazione strutturale. Lo sviluppo di **criteri comuni** a tutti gli Stati membri **per identificare obiettivi di alto valore** e agevolare la cooperazione operativa in tempo reale e lo scambio di informazioni permetterebbe di svolgere maggiori indagini congiunte e sistematiche sulle persone con un ruolo chiave in una rete criminale. L'attuale rete @ON dovrebbe essere rafforzata accogliendo tutti gli Stati membri e sviluppando migliori pratiche, nonché instaurando un legame più saldo con EMPACT nella sua attività di lotta alle reti criminali.

Il rafforzamento delle indagini sulla criminalità organizzata richiede inoltre un **quadro di intelligence** più solido **sui gruppi della criminalità organizzata** che sono al centro del complesso intreccio di reti della criminalità organizzata. Europol e gli Stati membri dovrebbero continuare il loro lavoro per sviluppare quadri strategici e tattici basati sull'intelligence per contrastare i gruppi che rappresentano una minaccia più grave per la sicurezza dell'Europa, anche sviluppando relazioni ad hoc che completino la valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità (SOCTA) dell'UE. Lo scambio di informazioni strategiche con altri attori, anche attraverso missioni e operazioni di politica di sicurezza e di difesa comune, può essere utile in questo senso. Inoltre è necessaria una migliore visione globale della dimensione delle attività criminali e delle azioni intraprese dagli Stati membri. Data la natura opaca della criminalità organizzata, è difficile misurare e quantificare tali attività; inoltre i dati e le statistiche a disposizione dell'Unione europea sono frammentati e raccolti principalmente tramite obblighi di dichiarazione disseminati in vari atti legislativi. Sulla base dei risultati di uno studio approfondito già realizzato³⁸, la Commissione valuterà la necessità di una raccolta più sistematica di statistiche in questo settore.

2.2. Risposta su misura a forme specifiche di criminalità

Secondo la relazione SOCTA dell'UE 2021, i gruppi della criminalità organizzata attivi in Europa sono coinvolti in molteplici attività criminali e la maggior parte è implicata nel traffico di droga, nei reati organizzati contro il patrimonio, seguiti dalla frode (tra cui la frode doganale, la frode in materia di accise e in materia di IVA), dal traffico di migranti e dalla tratta di esseri umani. Mentre alcuni gruppi sono specializzati in un particolare mercato criminale, altri si dedicano sempre più a una **pluralità di attività criminali**, usando i profitti

³⁷ Dal 2018 questa iniziativa ha portato all'arresto di 75 obiettivi di alto valore e di 2 529 consociati e al sequestro di beni per un valore di 310 milioni di EUR.

³⁸ Studio *Overview of the availability, comparability and consistency of administrative statistical data on recorded crime and on the stages of the criminal justice process in the EU*, marzo 2021, DR0121067ENN, <https://data.europa.eu/doi/10.2837/065004>.

di un'attività per finanziare l'espansione in altri settori della criminalità. Forme specifiche di criminalità richiedono una risposta ad hoc dal punto di vista legislativo e strategico.

L'UE ha stabilito norme per quanto riguarda i reati gravi, come il traffico di migranti³⁹, per individuare e vietare nuove sostanze psicoattive⁴⁰, per controllare il possesso e il commercio di armi da fuoco e per impedire la riattivazione delle armi neutralizzate⁴¹. Il traffico di droga rimane una delle principali fonti di reddito per i gruppi della criminalità organizzata; nella **strategia dell'UE in materia di droga per il periodo 2021-2025**⁴², adottata dal Consiglio nel dicembre 2020, l'UE ha stabilito sue le priorità in questo settore per i prossimi cinque anni. In seno al Consiglio proseguono le discussioni sul **piano d'azione in materia di droga** collegato alla strategia, mentre la Commissione sta preparando le prime iniziative volte ad attuare la strategia e il piano d'azione⁴³.

Le armi da fuoco sono un fattore determinante della violenza crescente dei gruppi criminali, poiché consentono di intimidire gli avversari e di esercitare il controllo sui loro membri e mercati. Al fine di limitare la disponibilità delle armi da fuoco nelle mani dei criminali, la Commissione ha avviato l'attuazione del nuovo piano d'azione dell'UE **contro il traffico di armi da fuoco** per il periodo 2020-2025. La Commissione pubblicherà la relazione di applicazione della direttiva sulle armi da fuoco, individuando le prime soluzioni per migliorare il quadro giuridico.

Il traffico di migranti rimane un'attività di massimo rilievo per i gruppi della criminalità organizzata, che mette in pericolo i migranti e compromette gli obiettivi della gestione della migrazione dell'UE. Nel 2021 la Commissione adotterà un **nuovo piano d'azione contro il traffico di migranti** per contrastare le reti criminali coinvolte in tale reato, sostenere la cooperazione tra autorità di contrasto e tra agenzie e stimolare la cooperazione con i paesi terzi e, se del caso, con le missioni e le operazioni di politica di sicurezza e di difesa comune.

La tratta di esseri umani, una forma di criminalità particolarmente ripugnante, è spesso svolta da gruppi della criminalità organizzata che sempre più spesso reclutano le loro vittime online, falsificano documenti di identità e permessi di lavoro e sfruttano le vittime a fini sessuali, di lavoro forzato, di criminalità o accattonaggio forzati. Sebbene le priorità e le azioni della presente strategia riguardino la tratta di esseri umani, la Commissione propone anche, parallelamente alla presente strategia, una strategia ad hoc dell'UE per la lotta contro la tratta di esseri umani nel periodo 2021-2025 volta ad affrontare le specificità di tale reato.

³⁹ Decisione quadro 2002/946/GAI del Consiglio, del 28 novembre 2002, relativa al rafforzamento del quadro penale per la repressione del favoreggiamento dell'ingresso, del transito e del soggiorno illegali (GU L 328 del 5.12.2002).

⁴⁰ Regolamento (UE) 2017/2101 del Parlamento europeo e del Consiglio, del 15 novembre 2017, che modifica il regolamento (CE) n. 1920/2006 per quanto riguarda lo scambio di informazioni, il sistema di allerta precoce e la procedura di valutazione del rischio in relazione alle nuove sostanze psicoattive (GU L 305 del 21.11.2017).

⁴¹ https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/trafficking-in-firearms_en.

⁴² Conclusioni del Consiglio *Strategia dell'UE in materia di droga per il periodo 2021-2025*, 14178/20, 18 dicembre 2020.

⁴³ <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12854-Alternatives-to-coercive-sanctions-for-drug-using-offenders>.

La **criminalità informatica** sta diventando più aggressiva e conflittuale. Il rapido progresso della digitalizzazione della società, che ha registrato un'impennata con la pandemia di COVID-19, crea nuove vulnerabilità che possono essere sfruttate dai criminali coinvolti nei reati dipendenti dall'informatica. Gli attacchi informatici, come la creazione e la diffusione di software maligni, la pirateria per rubare dati personali o industriali sensibili o gli attacchi di negazione del servizio, sono aumentati nell'ultimo anno sia in termini di numero che in grado di complessità⁴⁴.

Il **Centro europeo per la lotta alla criminalità informatica di Europol (EC3)**, istituito nel 2013, ha svolto un ruolo chiave nel monitorare lo sfruttamento della pandemia di COVID-19 da parte della criminalità organizzata e nell'elaborare relazioni e materiali di sensibilizzazione per informare gli Stati membri e il pubblico, oltre che nel sostenere le indagini sulle truffe online perpetrate da gruppi della criminalità organizzata. Inoltre l'EC3 ha pubblicato le sue relazioni periodiche di **valutazione della minaccia della criminalità organizzata su Internet (IOCTA)**, che forniscono un'importante fonte di informazioni per definire le priorità operative e strategiche⁴⁵.

In linea con la strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori⁴⁶ del 2020 e la strategia globale dell'UE sui diritti dei minori (2021-2025), nel 2021 la Commissione proporrà una normativa per migliorare la protezione dei minori contro gli **abusi sessuali su minori**, anche imponendo ai prestatori di servizi online pertinenti di individuare il materiale pedopornografico noto e di segnalarlo alle autorità pubbliche. La legislazione garantirà inoltre la coerenza con altre iniziative legislative, in particolare con la proposta relativa alla legge sui servizi digitali⁴⁷. La Commissione continua anche a sostenere il Parlamento europeo e il Consiglio per raggiungere un accordo quanto prima sulla proposta di regolamento riguardante gli sforzi volontari di alcuni prestatori di servizi nella lotta contro gli abusi sessuali su minori online⁴⁸. In parallelo Europol ha incoraggiato l'espansione della sua campagna di successo "Trace an Object", che raccoglie tramite crowdsourcing informazioni sui singoli oggetti nelle immagini che mostrano abusi sessuali su minori, il che può aiutare a delimitare la posizione geografica di un abuso e quindi in ultimo contribuire all'identificazione e al soccorso delle vittime.

⁴⁴ Cfr. la valutazione della minaccia della criminalità organizzata su Internet (*Internet Organised Crime Threat Assessment*, IOCTA) del 2020 all'indirizzo <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment> e altre relazioni di Europol all'indirizzo <https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know>.

⁴⁵ <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment>.

⁴⁶ Comunicazione della Commissione *Strategia dell'UE per una lotta più efficace contro gli abusi sessuali su minori* (COM(2020) 607 final del 24.7.2020).

⁴⁷ Proposta di regolamento del Parlamento europeo e del Consiglio relativo a un mercato unico dei servizi digitali (legge sui servizi digitali) e che modifica la direttiva 2000/31/CE (COM(2020) 825 final del 15.12.2020).

⁴⁸ Proposta di regolamento del Parlamento europeo e del Consiglio relativo a una deroga temporanea a talune disposizioni della direttiva 2002/58/CE del Parlamento europeo e del Consiglio per quanto riguarda l'uso di tecnologie da parte dei fornitori di servizi di comunicazione interpersonale indipendenti dal numero per il trattamento di dati personali e di altro tipo ai fini della lotta contro gli abusi sessuali sui minori online (COM(2020) 568 final del 10.9.2020).

La transizione verso economie senza contanti, ulteriormente accelerata dalla pandemia, ha creato maggiori opportunità di frodi e falsificazioni di **mezzi di pagamento diversi dai contanti** come le carte di credito e gli strumenti di pagamento online⁴⁹, il che rappresenta una seria minaccia alla sicurezza dell'UE. Tali reati costituiscono un'importante fonte di reddito per la criminalità organizzata e favoriscono attività criminali come il traffico di droga e la tratta di esseri umani. Nel 2019 l'UE ha adottato norme più severe⁵⁰, che gli Stati membri devono attuare entro il 31 maggio 2021. La Commissione monitorerà attentamente i progressi per garantire la piena efficacia delle nuove norme.

La **frode**, incluse la frode doganale, la frode in materia di accise e la frode in materia di IVA, è un altro settore della criminalità che sta diventando sempre più allettante per la criminalità organizzata. Oltre agli attuali sforzi dispiegati da Europol ed Eurojust in questo settore, l'**EPPO** indagherà e perseguirà i reati relativi alla partecipazione a un'organizzazione criminale, se l'attività criminosa di tale organizzazione criminale è incentrata sulla commissione di reati che colpiscono il bilancio dell'Unione, comprese le gravi frodi transfrontaliere in materia di IVA.

La **contraffazione** dei prodotti è un reato ad alto impatto. I prodotti contraffatti rappresentano il 6,8 % delle importazioni dell'UE⁵¹ e sono una significativa fonte di reddito per i gruppi della criminalità organizzata. I prodotti medici, sanitari e igienici costituiscono una parte considerevole e in crescita della contraffazione, un fenomeno che è aumentato in modo allarmante con la pandemia di COVID-19. La criminalità organizzata si è adoperata per la produzione e la fornitura di dispositivi di protezione, kit di analisi e farmaci contraffatti e vi è il rischio che i gruppi della criminalità organizzata cerchino di sfruttare le opportunità che emergono dall'elevata richiesta di vaccini nell'UE. Le autorità di contrasto, insieme a Europol e all'Ufficio europeo per la lotta antifrode, stanno realizzando con successo operazioni importanti che hanno portato ad arresti e sequestri significativi di prodotti contraffatti, compresi dispositivi medici, giocattoli, prodotti alimentari e bevande⁵². Tuttavia occorre fare di più per rafforzare la cooperazione operativa volta a contrastare la contraffazione. I gruppi della criminalità organizzata sono sempre più implicati in reati quali la contraffazione di pesticidi e l'uso fraudolento del logo biologico dell'UE. Basandosi sul suo quadro per i controlli ufficiali e di applicazione, la Commissione continuerà a intensificare i propri sforzi per contrastare le frodi alimentari e si adopererà per dare potere alle autorità nazionali, creare una politica di tolleranza zero e aumentare la prevenzione, i controlli, la dissuasione e le sanzioni efficaci.

⁴⁹ <https://www.europol.europa.eu/newsroom/news/beyond-pandemic-what-will-criminal-landscape-look-after-covid-19>.

⁵⁰ Direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti (GU L 123 del 10.5.2019).

⁵¹ OCSE/EUIPO (2019), *Trends in Trade in Counterfeit and Pirated Goods, Illicit Trade*, edizioni OCSE, Parigi/Ufficio dell'Unione europea per la proprietà intellettuale: <https://doi.org/10.1787/g2g9f533-en>.

⁵² Cfr. ad esempio le operazioni **Pangea XIII** (prodotti medicali), **LUDUS** (giocattoli) e **Opson IX** (prodotti alimentari e bevande). Durante l'operazione coordinata Shield di Europol, conclusa nel settembre 2020, sono stati sequestrati quasi 33 milioni di dispositivi medici contraffatti legati alla COVID-19, tra cui 8 tonnellate di materie prime, maschere facciali, test e kit di diagnosi.

A tal fine nel novembre 2020 la Commissione ha adottato il piano d'azione sulla proprietà intellettuale⁵³ e nel 2022 istituirà un **pacchetto di strumenti dell'UE per contrastare la contraffazione**, che stabilirà i principi dell'azione congiunta, della cooperazione e della condivisione dei dati tra titolari dei diritti, intermediari e autorità di contrasto. Dato che la contraffazione dei dispositivi medici avviene per lo più in paesi terzi, è importante rafforzare la governance globale, in particolare attraverso l'adesione alla convenzione del Consiglio d'Europa sulla **contraffazione dei dispositivi medici** ("convenzione Medicrime") e la sua ratifica da parte degli Stati membri dell'UE ed eventualmente dell'Unione stessa. Tale convenzione è stata firmata da quattordici Stati membri, solo sei dei quali l'hanno ratificata⁵⁴.

La **criminalità ambientale** merita particolare attenzione a causa dei suoi effetti nocivi per la biodiversità e l'ambiente, nonché per la salute e la coesione sociale all'interno dell'UE e nei paesi terzi. Tutti i tipi di specie selvatiche (piante, animali e prodotti derivati) nonché gli animali da compagnia continuano a essere commerciati illegalmente, spesso su larga scala e talvolta con effetti potenzialmente devastanti. La gestione e le spedizioni illegali di rifiuti danneggiano le industrie legittime responsabili del trattamento e del riciclaggio dei rifiuti. L'UE ha adottato una normativa per regolare il commercio legale delle specie selvatiche⁵⁵ e dei rifiuti⁵⁶ e ha richiesto agli Stati membri di qualificare come reato un'ampia gamma di reati ambientali⁵⁷ e stabilire delle sanzioni al riguardo. Tali strumenti legislativi sono stati integrati con il piano d'azione 2016 contro il traffico illegale di specie selvatiche e il piano d'azione 2018 sulla conformità e la governance ambientali. L'Ufficio europeo per la lotta antifrode ha sviluppato significativamente le sue attività operative nella lotta al commercio illecito di beni che mettono in pericolo l'ambiente.

Nonostante questi sforzi, le autorità di controllo, di contrasto e giudiziarie spesso non dispongono della capacità e delle risorse per accertare, indagare e perseguire efficacemente i reati ambientali. È il caso in particolare degli Stati membri dove non vi sono organismi di contrasto o pubblici ministeri specializzati e non è stato definito un approccio strategico per contrastare la criminalità ambientale. Occorre rafforzare la capacità delle autorità di contrasto a livello nazionale e dell'UE. Le sanzioni imposte non sono sufficientemente dissuasive e il coordinamento e lo scambio di informazioni all'interno e tra gli Stati membri, in particolare

⁵³ Comunicazione della Commissione *Sfruttare al meglio il potenziale innovativo dell'UE – Piano d'azione in materia di proprietà intellettuale per sostenere la ripresa e la resilienza dell'UE* (COM(2020) 760 final del 25.11.2020).

⁵⁴ Convenzione STCE n. 211. La convenzione è stata ratificata da Belgio, Spagna, Francia, Croazia, Ungheria e Portogallo. È stata firmata ma non ancora ratificata da Danimarca, Germania, Italia, Cipro, Lussemburgo, Austria, Slovenia e Finlandia. Oltre alla convenzione Medicrime, la direttiva 2011/62/UE del Parlamento europeo e del Consiglio, dell'8 giugno 2011, che modifica la direttiva 2001/83/CE, recante un codice comunitario relativo ai medicinali per uso umano, al fine di impedire l'ingresso di medicinali falsificati nella catena di fornitura legale (GU L 174 dell'1.7.2011) stabilisce norme e meccanismi per rafforzare gli obblighi di verifica a carico del fabbricante del medicinale a tal fine.

⁵⁵ https://ec.europa.eu/environment/cites/legislation_en.htm.

⁵⁶ Cfr. articolo 50 del regolamento n. 1013/2006 del Parlamento europeo e del Consiglio, del 14 giugno 2006, relativo alle spedizioni di rifiuti (GU L 190 del 12.7.2006).

⁵⁷ Direttiva 2008/99/CE del Parlamento europeo e del Consiglio sulla tutela penale dell'ambiente (direttiva sulla tutela penale dell'ambiente) (GU L 328 del 6.12.2008).

tra le autorità amministrative e gli organismi di contrasto, è insufficiente⁵⁸. La Commissione sta procedendo al riesame del **regolamento dell'UE relativo alle spedizioni di rifiuti** e del **piano d'azione contro il traffico di specie selvatiche**. La **direttiva sulla tutela penale dell'ambiente** sarà oggetto di revisione al fine di chiarire l'ambito di applicazione dei reati ambientali, offrire maggiore precisione per quanto riguarda le sanzioni, agevolare l'utilizzo di strumenti investigativi efficaci e promuovere la cooperazione e la condivisione delle informazioni a livello transfrontaliero. In più sarà rafforzata la cooperazione tramite le reti europee per il controllo ambientale. Infine, poiché la dimensione internazionale del traffico di specie selvatiche è fondamentale, la Commissione promuoverà l'adozione di un protocollo aggiuntivo nel quadro dell'UNTOC.

Il traffico di **beni culturali** ha un impatto devastante sul patrimonio culturale dei paesi, fornisce mezzi di finanziamento alle organizzazioni criminali e viene utilizzato per il riciclaggio di denaro. Per contrastare efficacemente tale reato è necessario migliorare il monitoraggio e lo scambio di informazioni, rafforzare la cooperazione delle autorità di contrasto e doganali, potenziare la cooperazione tra giustizia e affari interni e politica di sicurezza e di difesa comune in questo settore e avvalersi delle competenze di diversi attori pubblici e privati. La possibilità di disporre in tempi rapidi di archeologi e storici dell'arte può contribuire notevolmente alle indagini sul traffico di beni culturali. Per contrastare questa forma unica di criminalità, la Commissione continuerà a sostenere lo sviluppo di capacità tra gli esperti di beni culturali, compresa una rete costituita da tali esperti, di cui gli Stati membri potrebbero servirsi nel quadro di EMPACT. La loro cooperazione strutturata con le autorità di contrasto sarà sostenuta in modo da agevolare le indagini e il finanziamento di progetti relativi al traffico di beni culturali. Inoltre la Commissione esaminerà altre azioni necessarie per contrastare questo fenomeno, anche attraverso il miglioramento della tracciabilità online e offline dei beni culturali nel mercato interno e la cooperazione con i paesi terzi i cui beni culturali sono saccheggiati. A tal fine la Commissione proporrà nel 2022 un piano d'azione sulla lotta al commercio illecito di beni culturali.

Azioni principali

La Commissione intende:

- proporre modifiche della **direttiva sulla tutela penale dell'ambiente** (4° trimestre 2021);
- rafforzare le disposizioni in materia di applicazione della normativa contro le spedizioni illegali di rifiuti nell'ambito della sua proposta di modifica del regolamento relativo alle spedizioni di rifiuti (2° trimestre 2021);
- istituire un **pacchetto di strumenti dell'UE per contrastare la contraffazione**, che stabilisca i principi dell'azione congiunta, della cooperazione e della condivisione dei dati tra **autorità di contrasto**, titolari dei diritti e intermediari (2022);

⁵⁸ *Evaluation of the Directive 2008/99/EC of the European Parliament and of the Council of 19 November 2008 on the protection of the environment through criminal law (Environmental Crime Directive)* (SWD(2020) 259 final del 28.10.2020).

- proporre un piano d'azione sul traffico di beni culturali (2022);
- esaminare la possibilità che l'Unione aderisca alla convenzione Medicrime del Consiglio d'Europa.

Gli Stati membri sono esortati a:

- **unirsi alla rete @ON** relativa ai gruppi della criminalità organizzata di stampo mafioso e **rafforzarla**, nonché considerare la possibilità di integrare in modo più strutturato un **approccio mirato contro le reti criminali nell'ambito di EMPACT**;
- istituire o sviluppare ulteriormente strutture di coordinamento a livello nazionale od **organismi specializzati** all'interno delle autorità di contrasto e delle autorità giudiziarie, che si occupino della lotta alle strutture della criminalità organizzata;
- aderire alla **convenzione Medicrime** e ratificarla.

Gli Stati membri ed Europol sono esortati a:

- sviluppare criteri comuni di identificazione per selezionare e indagare sugli **obiettivi di alto valore** e dare priorità alle indagini contro gli individui e le reti criminali che rappresentano il rischio più elevato per la sicurezza nell'UE;
- sviluppare un **quadro di intelligence** strategica e tattica sui gruppi della criminalità organizzata ad alto rischio;
- rafforzare la **cooperazione** strategica e operativa nella lotta alla **contraffazione dei dispositivi medici**, anche con l'Ufficio europeo per la lotta antifrode e l'Ufficio dell'Unione europea per la proprietà intellettuale e a livello globale.

3. Eliminare gli utili generati dalla criminalità organizzata e prevenirne l'infiltrazione nell'economia legale e nella società

3.1. Rafforzamento delle misure di recupero dei beni e di lotta al riciclaggio di denaro, promozione delle indagini finanziarie

La criminalità organizzata nell'UE dipende fondamentalmente dalla capacità di riciclare ingenti quantità di profitti illegali. Se tre quarti delle organizzazioni criminali utilizza ancora metodi elementari per nascondere i guadagni illeciti, come investire in immobili o in altri beni di alto valore, altre organizzazioni si affidano a metodi sempre più sofisticati con l'aiuto di riciclatori che appartengono ai colletti bianchi⁵⁹. La pista finanziaria che i criminali si lasciano dietro è un indicatore chiave della loro attività, poiché fornisce indizi utili per gli investigatori e prove preziose per incriminare gli autori del reato. Pertanto la lotta ai fondi di origine illegale è fondamentale per individuare le attività criminali, scoraggiare la criminalità e prevenirne l'infiltrazione nell'economia legale e nella società.

⁵⁹ Europol, relazione *EU Serious and Organised Threat Assessment* (SOCTA dell'UE 2021), 12 aprile 2021: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment>.

Nonostante lo sviluppo di quadri giuridici per la lotta al riciclaggio di denaro e il recupero dei beni, solo una piccola parte delle attività di riciclaggio è scoperta ed è confiscato solo l'1 % dei proventi di reato⁶⁰. Tale situazione si è aggravata a causa dell'utilizzo crescente di circuiti finanziari con una supervisione più limitata rispetto al settore bancario, come le **valute virtuali**.

Occorre rafforzare la lotta ai fondi di origine illegale. Come evidenziato nel piano d'azione contro il riciclaggio del 2020⁶¹, il quadro dell'UE per la lotta al riciclaggio deve essere notevolmente migliorato per eliminare le profonde divergenze nel modo in cui viene applicato e le gravi carenze riscontrate nell'applicazione delle norme. Il potenziale delle indagini finanziarie non è sfruttato appieno, in parte a causa dell'insufficiente capacità da parte delle autorità di contrasto di svolgere tali indagini complesse e onerose.

Inoltre la capacità di privare i criminali dei loro beni acquisiti illegalmente è ulteriormente ostacolata dal fatto che il quadro giuridico in materia di confisca ha un ambito di applicazione circoscritto in termini di beni e attività criminali contemplate. Inoltre gli uffici per il recupero dei beni incontrano attualmente difficoltà a rintracciarli, poiché non dispongono ad esempio di poteri di congelamento temporaneo al fine di prevenire la dispersione dei beni o l'accesso diretto e immediato a taluni registri pubblici come i registri catastali centrali e i registri centrali delle imprese⁶². Per di più, non sempre i beni recuperati sono gestiti sempre in modo efficiente e utilizzati in misura sufficiente per risarcire le vittime o per arrecare beneficio alla società.

Come annunciato nel piano d'azione contro il riciclaggio del 2020, è prioritario garantire l'effettiva attuazione del quadro dell'UE in vigore per la lotta al riciclaggio di denaro. Oltre a impegnarsi per garantire un'attuazione adeguata, la Commissione sta preparando proposte legislative volte a rafforzare e sviluppare il **quadro dell'UE per la lotta al riciclaggio di denaro**, proponendo nel secondo trimestre del 2021 l'elaborazione di un codice unico europeo direttamente applicabile, il rafforzamento della supervisione a livello dell'UE e l'istituzione di un meccanismo di coordinamento e sostegno dell'UE per le unità di informazione finanziaria.

È parimenti necessario favorire una cultura che promuova **indagini finanziarie tempestive** in tutti gli Stati membri e potenziare la capacità degli investigatori di affrontare la dimensione finanziaria della criminalità organizzata. Le conclusioni del Consiglio sul rafforzamento delle indagini finanziarie del 2020⁶³ invitano gli Stati membri a provvedere affinché le indagini finanziarie siano parte di tutti i tipi di indagini penali riguardanti la criminalità organizzata.

⁶⁰ Europol, *Does crime still pay? Criminal Asset Recovery in the EU – Survey of statistical information 2010-2014*, Europol, 2016, consultabile al seguente indirizzo: <https://www.europol.europa.eu/publications-documents/does-crimestill-pay>.

⁶¹ Comunicazione della Commissione relativa a un piano d'azione per una politica integrata dell'Unione in materia di prevenzione del riciclaggio di denaro e del finanziamento del terrorismo (C(2020) 2800 final del 7.5.2020).

⁶² Cfr. conclusioni del Consiglio sul rafforzamento delle indagini finanziarie per combattere la criminalità organizzata e le forme gravi di criminalità, 8927/20, 17 giugno 2020.

⁶³ Conclusioni del Consiglio sul rafforzamento delle indagini finanziarie per combattere la criminalità organizzata e le forme gravi di criminalità, 8927/20, 17 giugno 2020.

Inoltre, attraverso l'istituzione del Centro europeo per la lotta alla criminalità finanziaria ed economica, Europol ha rafforzato le sue capacità di sostenere gli Stati membri nello svolgimento di indagini finanziarie.

È altresì essenziale intensificare gli sforzi in materia di **congelamento e confisca** attraverso un quadro giuridico ulteriormente rafforzato a livello dell'UE e capacità operative più solide degli **uffici per il recupero dei beni**. Occorre esaminare le misure di confisca non basate sulla condanna, che possono contribuire ad aumentare la quantità di beni confiscati quando, ad esempio, non è possibile stabilire un nesso tra i beni acquisiti e una condanna penale⁶⁴. Per prevedere un regime di confisca più solido e dotare gli uffici nazionali per il recupero dei beni di un mandato più efficace, nel 2022 la Commissione proporrà una revisione della **direttiva relativa alla confisca** del 2014 e della decisione del Consiglio del 2007 concernente gli **uffici per il recupero dei beni**⁶⁵, al fine di estendere l'ambito di applicazione dei reati contemplati, introdurre norme più efficaci sulla confisca non basata sulla condanna, garantire una gestione efficace e il riutilizzo sociale dei beni confiscati e il risarcimento delle vittime di reato e rafforzare la capacità degli uffici per il recupero dei beni di rintracciare e identificare i beni illeciti⁶⁶.

Inoltre la Commissione prenderà in considerazione le possibili opzioni per quanto riguarda **l'avvio sistematico di indagini finanziarie** e di indagini finanziarie dopo una condanna. Il rapido accesso alle informazioni finanziarie è essenziale per effettuare indagini finanziarie efficaci e per rintracciare e confiscare con successo i beni. È quindi della massima importanza che gli Stati membri recepiscono tempestivamente la **direttiva sull'agevolazione dell'uso di informazioni finanziarie**, che fornisce alle autorità di contrasto l'accesso ai registri centralizzati dei conti bancari e rafforza la cooperazione tra le autorità di contrasto e le unità di informazione finanziaria. La Commissione rivedrà anche la direttiva, unitamente al quadro per la lotta al riciclaggio di denaro, per fornire alle autorità di contrasto l'accesso alla futura piattaforma di interconnessione dei registri dei conti bancari in tutta l'Unione.

Contestualmente sarà necessario migliorare la cooperazione internazionale per quanto riguarda la risposta repressiva al riciclaggio di denaro. Gli Stati membri dovrebbero avvalersi di tutte le possibilità offerte dalla **rete operativa contro il riciclaggio di denaro (AMON)**, una rete internazionale informale di unità per la lotta al riciclaggio delle autorità di contrasto, e dalla **rete interagenzie Camden per il recupero dei beni (CARIN)**, una rete informale di operatori delle autorità di contrasto e delle autorità giudiziari specializzati nel campo del reperimento, del congelamento, del sequestro e della confisca dei beni. La Commissione proporrà anche la ratifica, a nome dell'UE, della **convenzione di Varsavia** del Consiglio d'Europa sul riciclaggio, il congelamento e la confisca dei beni.

⁶⁴ Cfr. anche *Analysis of non-conviction-based confiscation measures in the European Union* (SWD(2019) 1050 final del 12.4.2019).

⁶⁵ <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12725-Freezing-and-confiscation-of-the-proceeds-of-crime>.

⁶⁶ Relazione della Commissione al Parlamento europeo e al Consiglio, *Recupero e confisca dei beni: garantire che "il crimine non paghi"* (COM(2020) 217 final del 2.6.2020).

3.2. Rafforzamento delle misure di lotta alla corruzione

La corruzione è un elemento centrale del *modus operandi* dei gruppi della criminalità organizzata, che ricorrono a corruzione, intimidazione e coercizione nei confronti dei funzionari pubblici e del personale di organismi chiave, come i porti, per rimanere inosservati, ottenere informazioni o agire più facilmente. In base alle attuali norme di lotta alla corruzione dell'UE gli Stati membri sono tenuti a qualificare come reato la corruzione sia attiva che passiva dei funzionari pubblici, a stabilire sanzioni adeguate e a garantire che gli imprenditori che corrompono i funzionari siano perseguiti penalmente. Tuttavia tali strumenti non contemplano taluni reati connessi alla corruzione, come il traffico d'influenza, l'abuso di potere, l'arricchimento illecito, l'appropriazione indebita o altre forme di distrazione di beni da parte di un funzionario pubblico. Più recentemente l'Unione ha introdotto una nuova normativa che protegge gli informatori e prevede la creazione di canali sicuri attraverso i quali denunciare le pratiche di corruzione. La relazione annuale sullo Stato di diritto esamina la situazione degli Stati membri anche in relazione alle politiche di lotta alla corruzione.

Per intensificare gli sforzi a livello dell'UE, la Commissione **valuterà le norme vigenti di lotta alla corruzione dell'UE**⁶⁷, che sono state adottate vent'anni fa, per verificare se siano aggiornate rispetto all'evoluzione delle pratiche criminali e se contemplino tutti i reati connessi alla corruzione.

Le varie forme di corruzione legate alla criminalità organizzata in un contesto transnazionale giustificano inoltre la necessità di una migliore condivisione di competenze, migliori pratiche, dati e informazioni tra gli Stati membri e con la società civile. Per sostenere efficacemente le indagini penali attraverso lo scambio di dati è fondamentale disporre di una visione globale e comprendere i rischi e le minacce causati dalla corruzione prima che si materializzino sotto forma di reati connessi alla corruzione.

La pandemia di COVID-19 aggiunge un'altra serie grave di rischi di corruzione: la mobilitazione di risorse su larga scala per rispondere alla crisi sanitaria ed economica ha creato indirettamente nuove possibilità di corruzione. È necessario rafforzare la capacità delle autorità nazionali di occuparsi di casi di corruzione estremamente complessi connessi alla criminalità organizzata, in particolare istituendo strutture specializzate nella lotta alla corruzione. È importante che gli Stati membri ricorrano maggiormente ai finanziamenti disponibili e agli strumenti tecnici di sostegno forniti dalla Commissione al fine di rafforzare il loro approccio strutturale e strategico, gli strumenti normativi e operativi e la capacità nel settore della lotta alla corruzione. Inoltre, dato il ruolo cruciale dei media nell'individuare i casi di corruzione, è di fondamentale importanza garantire la sicurezza dei giornalisti investigativi in tutta l'Unione, anche contro l'abuso delle azioni legali. Come annunciato nel piano d'azione per la democrazia europea, nel 2021 la Commissione pubblicherà una

⁶⁷ Decisione quadro 2003/568/GAI del Consiglio, del 22 luglio 2003, relativa alla lotta contro la corruzione nel settore privato e convenzione del 1997 relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità europee o degli Stati membri dell'Unione europea (GU L 192 del 31.7.2003).

raccomandazione sulla sicurezza dei giornalisti e presenterà un'iniziativa per contrastare l'abuso delle azioni legali nei confronti dei giornalisti e dei difensori dei diritti.

L'UE è parte della **convenzione delle Nazioni Unite contro la corruzione** dal 2008 e la sua applicazione della convenzione sarà sottoposta a esame secondo le disposizioni previste. L'UE e gli Stati membri si stanno adoperando nel quadro del Gruppo di Stati del Consiglio d'Europa contro la corruzione (GRECO) e del G20 per compiere ulteriori progressi nella prevenzione e lotta alla corruzione. La sessione speciale dell'Assemblea generale delle Nazioni Unite, prevista per giugno 2021, rappresenterà una grande opportunità per progredire nella lotta alla corruzione a livello globale.

Gli Stati membri sono inoltre tenuti a qualificare come reato e perseguire gli atti di corruzione commessi dai cittadini e dalle imprese dell'UE nei paesi partner, in linea con gli obblighi derivanti dalla **convenzione dell'OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali**. Azioni penali e condanne coerenti degli atti di corruzione commessi all'estero svolgeranno un ruolo importante nella lotta alla corruzione a livello globale.

3.3. Lotta all'infiltrazione nell'economia e nella società

I gruppi criminali investono parte dei loro cospicui proventi in attività legali che rientrano nei più svariati settori come l'immobiliare, l'edilizio, l'alberghiero e il settore dei trasporti⁶⁸. Mediante il controllo delle imprese di questi settori le organizzazioni criminali sono in grado di riciclare i beni acquisiti illegalmente e massimizzare i loro profitti. L'infiltrazione della criminalità organizzata danneggia l'economia lecita e provoca distorsioni delle regole di mercato. A causa della situazione economica generata dalla pandemia di COVID-19, è cresciuto il rischio che la criminalità organizzata assuma il controllo di imprese già fragili e si infilti in interi settori di attività. Sono già stati dimostrati tentativi di reato volti a frodare i vari meccanismi finanziari introdotti per sostenere la ripresa economica⁶⁹. Per affrontare tale minaccia e individuare punti fondamentali di intervento e sensibilizzazione, occorre che gli Stati membri ed Europol istituiscano un quadro di intelligence che riveli la portata e il livello degli investimenti criminali, i metodi di infiltrazione e i settori a rischio.

Si potrebbero trarre insegnamenti dallo scambio di migliori pratiche promosso tramite la rete europea sull'**approccio amministrativo**⁷⁰, un metodo con il quale le autorità locali, in collaborazione con le autorità di contrasto e la società civile, utilizzano strumenti amministrativi, come le procedure per ottenere autorizzazioni, appalti e sovvenzioni, per

⁶⁸ Studio *Mapping the risk of serious and organised crime infiltration in legitimate businesses*, marzo 2021, DR0221244ENN, <https://data.europa.eu/doi/10.2837/64101>.

⁶⁹ Europol, relazione *EU Serious and Organised Threat Assessment* (SOCTA dell'UE 2021), 12 aprile 2021: <https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment>.

⁷⁰ L'approccio amministrativo alla criminalità organizzata e alle forme gravi di criminalità integra le attività tradizionali di contrasto e offre strumenti aggiuntivi per prevenire e contrastare l'uso improprio dell'infrastruttura giuridica attraverso la cooperazione multiagenzia, condividendo informazioni e adottando azioni per erigere barriere contro le infiltrazioni.

prevenire l'infiltrazione della criminalità organizzata nelle attività legali e nelle infrastrutture amministrative. Le autorità locali dovrebbero avere la facoltà, nel pieno rispetto dei diritti fondamentali, di erigere barriere che proteggano il tessuto economico dalla criminalità organizzata.

Anche la **dimensione locale** è fondamentale per ridurre lo spazio che consente ai gruppi criminali di ingrandirsi. Gli individui che crescono in un ambiente di criminalità organizzata e in aree economicamente e socialmente svantaggiate sono più esposti a essere reclutati nei gruppi criminali. Partendo da reati o ruoli minori nell'organizzazione, questi individui ne possono diventare in futuro membri e leader. Le azioni mirate nei quartieri e nelle comunità si sono dimostrate efficaci nell'offrire alternative che consentano ai giovani di sfuggire a una vita di violenza e criminalità. Inoltre le attività di prevenzione della criminalità, come la polizia di prossimità o le campagne di sensibilizzazione nelle aree particolarmente colpite dalle attività criminali, sono essenziali per rafforzare la resilienza della società nei confronti delle attività dei gruppi della criminalità organizzata. La Commissione potenzierà lo scambio di conoscenze e di migliori pratiche in materia attraverso la **rete europea di prevenzione della criminalità**.

Azioni principali

La Commissione intende:

- proporre la revisione della **direttiva relativa alla confisca** e della decisione del Consiglio concernente gli **uffici per il recupero dei beni** (2022);
- valutare le vigenti **norme di lotta alla corruzione dell'UE** (2022);
- promuovere la **cooperazione** e lo scambio di informazioni sul **legame tra corruzione e criminalità organizzata**, anche attraverso Europol.

Gli Stati membri sono esortati a:

- **svolgere sistematicamente indagini finanziarie** nell'ambito delle indagini sulla criminalità organizzata e, non appena il contesto finanziario indichi la presenza di proventi di reato, avviare sistematicamente indagini per il recupero dei beni;
- recepire in tempi rapidi la **direttiva sull'agevolazione dell'uso di informazioni finanziarie** entro il termine previsto dell'agosto 2021;
- **scambiare informazioni strategiche** con i **settori a rischio** di infiltrazione da parte della criminalità organizzata (partenariati tra il settore pubblico e quello privato);
- migliorare la **specializzazione** dei servizi di contrasto e rafforzare gli organismi responsabili delle indagini, delle azioni penali e dei procedimenti giudiziari relativi ai casi di **corruzione** ad alto livello.

Gli Stati membri ed Europol sono esortati a:

- migliorare il **quadro di intelligence** che indica la minaccia di **infiltrazione** nell'economia legale, valutando i rischi e i metodi utilizzati dai gruppi della criminalità organizzata.

4. Adeguamento dei servizi di contrasto e del sistema giudiziario all'era digitale

4.1. Accesso a indizi e prove digitali

La ricerca di indizi e prove, compreso l'accesso legittimo ai dati di comunicazione, costituisce la componente più importante delle indagini delle autorità di contrasto e delle azioni penali e consente di consegnare i criminali alla giustizia. Poiché oggi più che mai le nostre vite e attività si svolgono online, le impronte lasciate dalla criminalità sono anche digitali. La criminalità organizzata è pianificata, attuata e nascosta online, mediante la commercializzazione di sostanze e prodotti illegali e l'elaborazione di modi ingegnosi per riciclare i profitti senza gli ostacoli derivanti dalle frontiere fisiche. L'entità del problema è amplificata dalle tecnologie in rapido sviluppo. Il passaggio di alcuni indizi e prove da uno spazio fisico a uno spazio online comporta una serie di sfide, tra cui la velocità con cui i dati possono essere spostati tra le giurisdizioni o la capacità di occultamento dietro la cifratura. Inoltre alcuni **strumenti e misure di acquisizione delle prove concepiti per le prove fisiche non sono ancora completamente adeguati al mondo digitale**⁷¹, il che può ostacolare o rallentare le indagini e le azioni penali, poiché i dati non sono disponibili o accessibili in modo tempestivo.

Le indagini sulla criminalità organizzata richiedono in genere l'accesso ai dati relativi alle comunicazioni elettroniche per stabilire un nesso tra il reato, l'autore e le sue vittime, nonché per rintracciare le reti criminali. Considerando la portata e la struttura delle reti della criminalità organizzata, le autorità di contrasto incontrano difficoltà nel rintracciare tali comunicazioni se non hanno accesso retrospettivo ai metadati delle comunicazioni. La mancanza di tali dati rende particolarmente difficile identificare gli attori principali che tirano le fila dietro le quinte. Pertanto l'identificazione e l'arresto colpiscono spesso soltanto persone che appartengono ai ranghi più bassi di queste reti, ossia coloro che si trovavano sul luogo del reato, piuttosto che gli attori principali⁷². Inoltre i gruppi della criminalità organizzata utilizzano la tecnologia moderna per organizzare la successiva consegna di droga, condividere obiettivi promettenti per il successivo furto con scasso, concordare il punto d'incontro per una rapina a mano armata o, nel caso di gruppi della criminalità organizzata nel settore informatico, attuare attacchi di software maligni ai servizi bancari online.

Per consentire l'accesso alle prove digitali e agli indizi investigativi, gli Stati membri hanno istituito **quadri in materia di conservazione dei dati**. Tenuto conto del principio di riservatezza delle comunicazioni elettroniche, i fornitori di servizi di comunicazione potrebbero aver cancellato i metadati nel momento in cui le autorità di contrasto ne richiedono l'accesso. In tali casi si rischia di perdere prove importanti, a meno che i fornitori non siano tenuti per legge a conservare i metadati delle comunicazioni per un periodo ragionevolmente più lungo in conformità di un quadro giuridico in materia di conservazione dei dati. Ciò

⁷¹ https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en#internaleurulesproposaloneevidence.

⁷² https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/180611_MINDESTSPEICHERFRISTEN.html.

rischia di ostacolare lo svolgimento di indagini sui reati o l'identificazione delle vittime. I metadati delle comunicazioni sono ad esempio di particolare importanza nell'indagine e nel perseguimento dei reati informatici, costituiscono spesso il principale strumento per accertare il reato e fungono da elementi di prova fondamentali. Possono inoltre costituire un mezzo importante per corroborare (o confutare) altri tipi di prove relative ai fatti in questione. Inoltre la complessità delle attività della criminalità organizzata, come il traffico illegale di droga, la tratta di essere umani o il riciclaggio di denaro, e il tempo necessario per l'indagine, nel corso della quale possono emergere nuovi sospetti, rende importante conservare i dati.

Al contempo le misure di conservazione dei dati sollevano questioni importanti in relazione alla loro ingerenza nei diritti fondamentali, compreso il diritto al rispetto della vita privata e alla protezione dei dati personali. Nelle sue recenti sentenze sulla conservazione dei dati⁷³, la Corte di giustizia dell'Unione europea ha confermato la sua precedente giurisprudenza secondo cui i dati delle comunicazioni elettroniche sono riservati e, in linea di principio, i dati relativi al traffico e all'ubicazione non possono essere conservati in maniera generalizzata e indifferenziata. La portata delle misure di conservazione dei dati può essere giustificata, in relazione alla loro ingerenza nei diritti fondamentali, solo quando le misure sono necessarie e proporzionate rispetto alla finalità perseguita. La Corte ha stabilito eccezioni circoscritte a tale norma che riguardano la sicurezza nazionale, la difesa e la sicurezza pubblica o la prevenzione, l'indagine, l'accertamento e il perseguimento dei reati⁷⁴. La Commissione analizzerà e delinea possibili approcci e soluzioni, in linea con le sentenze della Corte, che rispondano alle esigenze delle autorità di contrasto e giudiziarie in un modo che sia operativamente utile, tecnicamente possibile e giuridicamente valido, anche nel pieno rispetto dei diritti fondamentali. Entro la fine di giugno 2021 essa consulterà gli Stati membri per definire il modo in cui procedere.

Una risposta efficace delle autorità di contrasto richiede inoltre la tempestività di accesso alle prove digitali quando sono detenute da fornitori in una giurisdizione diversa. Nel 2018 la Commissione ha proposto **il pacchetto sulle prove elettroniche** per agevolare l'accesso transfrontaliero alle prove elettroniche sulla base di ordini europei di produzione e di conservazione. Il Parlamento europeo e il Consiglio stanno ora partecipando a discussioni interistituzionali, sostenute dalla Commissione, al fine di giungere a un accordo che porti alla rapida adozione di tali proposte. Inoltre nell'ambito degli sforzi per accelerare la digitalizzazione dei servizi di contrasto e del sistema giudiziario⁷⁵, tutti gli Stati membri dovrebbero partecipare al sistema digitale di scambio di prove elettroniche (*e-Evidence Digital Exchange System*, eEDES). In parallelo sono necessari rapidi progressi nei negoziati

⁷³ Sentenza del 6 ottobre 2020, *Privacy International*, C-623/17, sentenza del 6 ottobre 2020, *La Quadrature du Net* e a., C-511/18, C-512/18 e C-520/18 e sentenza del 2 marzo 2021, *H.K./Prokuratuur*, C-746/18.

⁷⁴ La Corte ha consentito in particolare la conservazione generalizzata e indifferenziata dell'identità civile degli utenti a fini di lotta contro tutti i reati e la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione a fini di lotta contro i reati gravi. Le argomentazioni della Corte di giustizia si basano sulla Carta dei diritti fondamentali e sull'analisi della necessità e della proporzionalità dell'ingerenza in tali diritti.

⁷⁵ Comunicazione della Commissione *Digitalizzazione della giustizia nell'Unione europea – Un pacchetto di opportunità* (COM(2020) 710 final del 2.12.2020).

internazionali multilaterali e bilaterali per agevolare la cooperazione con i partner internazionali e stabilire norme compatibili a livello internazionale per l'accesso transfrontaliero alle prove elettroniche⁷⁶.

In considerazione degli attacchi sempre più su larga scala, è essenziale per il buon esito delle indagini, che aumentano l'effetto dissuasivo, acquisire prove elettroniche nel più breve tempo possibile e prima di ricorrere a provvedimenti correttivi. A tal fine le autorità di contrasto e la comunità della sicurezza informatica dovrebbero cooperare a stretto contatto per garantire una risposta collettiva ed esaustiva. Inoltre le indagini richiedono un accesso rapido e affidabile ai dati WHOIS per aiutare, tra l'altro, a identificare i gruppi della criminalità organizzata che fanno regolarmente abuso del sistema dei nomi di dominio (*Domain Name System*, DNS) e di altri protocolli Internet nei loro attacchi informatici o per altri reati come le truffe o la diffusione di prodotti e servizi illegali.

La **cifratura** è essenziale nel mondo digitale, in quanto rende sicuri i sistemi digitali e le transazioni e tutela anche una serie di diritti fondamentali, tra cui la libertà di espressione, il diritto alla vita privata e la protezione dei dati⁷⁷. Tuttavia, se utilizzata a fini criminali, può mascherare l'identità dei criminali e nascondere il contenuto delle loro comunicazioni. La Commissione ha proposto, nella sua undicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza⁷⁸, una serie di sei misure pratiche per aiutare le autorità di contrasto e giudiziarie nelle indagini penali in cui si riscontra l'uso della cifratura dei dati memorizzati sui dispositivi (come telefoni o dischi rigidi), senza vietare, limitare o indebolire la cifratura. Nell'ambito di queste misure il nuovo strumento di decrittografia di Europol, avviato dalla Commissione nel dicembre 2020, contribuirà ad affrontare tali problemi. Il Gruppo europeo di formazione e istruzione in materia di criminalità informatica (*European Cybercrime Training and Education Group*, ECTEG), finanziato attraverso il Fondo sicurezza interna-Polizia, ha sviluppato moduli di formazione ed erogato i corsi pilota. Tali corsi rientreranno nell'offerta di formazione abituale dell'Accademia europea di polizia (CEPOL).

Al di là dei dispositivi tradizionali, è in crescita il mercato di nicchia dei dispositivi di comunicazione cifrati, che sono acquistati e utilizzati anche dai gruppi della criminalità organizzata. Come emerge dalle recenti operazioni "EncroChat" e "Sky ECC", è necessario che le autorità di contrasto dell'UE sviluppino continuamente la loro capacità di usare le informazioni cifrate nell'ambito delle indagini penali, in linea con il diritto applicabile.

⁷⁶ 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.

⁷⁷ Comunicazione della Commissione sulla strategia dell'UE per l'Unione della sicurezza (COM(2020) 605 final del 24.7.2020); comunicazione della Commissione *Prima relazione sui progressi compiuti nella strategia dell'UE per l'Unione della sicurezza* (COM(2020) 797 final del 9.12.2020).

⁷⁸ *Undicesima relazione sui progressi compiuti verso un'autentica ed efficace Unione della sicurezza* (COM(2017) 608 final del 18.10.2017).

Nel dicembre 2020 il Consiglio ha adottato una risoluzione⁷⁹ che invita a instaurare un dibattito attivo con l'industria del settore tecnologico e a elaborare un quadro normativo appropriato che consenta alle autorità nazionali di svolgere efficacemente i loro compiti operativi, tutelando nel contempo la vita privata, i diritti fondamentali e la sicurezza delle comunicazioni. Inoltre il Consiglio ha chiesto un migliore coordinamento degli sforzi degli Stati membri, delle istituzioni e degli organi dell'Unione europea. Come già annunciato nel programma di lotta al terrorismo⁸⁰, la Commissione si sta impegnando per individuare soluzioni tecniche, operative e giuridiche per garantire l'accesso legittimo alle informazioni cifrate, mantenendo l'efficacia della cifratura nella protezione della vita privata e della sicurezza delle comunicazioni.

Nel 2020 la Commissione, insieme all'industria, agli esperti di crittografia, ai membri delle organizzazioni della società civile e alle autorità competenti, ha svolto una consultazione degli esperti per identificare le soluzioni tecniche che possano aiutare le imprese a individuare specificamente gli abusi sessuali su minori nelle comunicazioni elettroniche cifrate da punto a punto. La Commissione sosterrà la ricerca per identificare le soluzioni tecniche più praticabili che possono essere estese e attuate in modo fattibile e legittimo dalle imprese.

Più in generale, la Commissione guiderà il processo volto ad analizzare, insieme ai portatori di interessi, le capacità e gli approcci esistenti per consentire l'accesso legittimo e mirato alle informazioni cifrate nell'ambito delle indagini e delle azioni penali. Queste iniziative non dovrebbero causare un indebolimento generale della cifratura o comportare una sorveglianza indiscriminata. L'analisi non sarà incentrata soltanto sul superamento degli ostacoli attuali, ma anticiperà anche la probabile evoluzione delle tecnologie di cifratura e di decrittografia e la necessaria cooperazione con il mondo accademico e il settore privato a tale scopo. Inoltre la Commissione sta intensificando i suoi sforzi nel campo della standardizzazione per preservare la possibilità di effettuare intercettazioni legali nel contesto del 5G e in oltre. Al termine di questo processo, nel 2022 la Commissione suggerirà **un percorso da seguire** per affrontare la questione dell'accesso legittimo e mirato alle informazioni cifrate nell'ambito delle indagini e delle azioni penali, che si baserà su una mappatura approfondita indicante le modalità di utilizzo della cifratura da parte degli Stati membri, unitamente a un processo di consultazione dei portatori di interessi per esaminare e valutare le opzioni concrete (giuridiche, etiche e tecniche).

4.2. Strumenti e tecnologie efficaci

Le autorità di contrasto spesso non dispongono dei mezzi per acquistare gli strumenti giusti che sono necessari per svolgere le indagini digitali. Oltre l'80 % dei reati ha oggi una componente digitale; anche quando i reati sono commessi offline, è necessario che quasi ogni funzionario delle autorità di contrasto e ogni procuratore conosca i concetti di base per sapere

⁷⁹ Risoluzione del Consiglio sulla crittografia – *La sicurezza attraverso la crittografia e nonostante la crittografia*, 13084/1/20 REV 1, 24.11.2020.

⁸⁰ Comunicazione della Commissione *Un programma di lotta al terrorismo dell'UE: prevedere, prevenire, proteggere e reagire* (COM(2020) 795 final del 9.12.2020).

come indagare sui reati online⁸¹. Per individuare e perseguire la criminalità organizzata, gli investigatori devono rilevare attività online sospette, rintracciare operazioni criminali in valute virtuali, comprendere ciò che trovano (i dati possono essere cifrati o devono essere contestualizzati tenendo conto di altri dati), conservare i dati e usarli come prova elettronica dinanzi al giudice.

È urgente aumentare la capacità e le competenze delle autorità di contrasto e dei pubblici ministeri non specializzati⁸². Inoltre si registra una carenza di competenze nelle indagini digitali in settori specifici come la scienza forense nell'ambito dell'Internet degli oggetti⁸³. Le autorità di contrasto e giudiziarie devono stare al passo con le tecnologie in rapido sviluppo utilizzate dai criminali e con le loro attività transfrontaliere. Ciò richiede un coordinamento nello sviluppo di strumenti e formazioni tra gli Stati membri e tra i diversi settori in ambiti come la scienza forense digitale, l'intelligence da fonte aperta, le criptovalute e le indagini sul darkweb, ad esempio per ottenere l'accesso ai forum che vendono beni e servizi illegali e, ove possibile, eliminarli. Inoltre le autorità nazionali non sono sempre in grado di utilizzare soluzioni tecniche open-source, perché non sono abbastanza consapevoli di quali soluzioni siano state sviluppate e siano disponibili, perché sussistono differenze nei requisiti e nei livelli di competenza e per mancanza di sostegno all'ulteriore sviluppo e mantenimento di tali soluzioni. Al contempo la mancanza di coordinamento tra le varie autorità e gli Stati membri comporta il rischio di duplicazione delle iniziative. I meccanismi UE esistenti (EMPACT, agenzie dell'UE come Europol, CEPOL ed Eurojust, reti di operatori, programmi di finanziamento come il Fondo sicurezza interna) possono svolgere un ruolo chiave nel promuovere un approccio più efficace alle indagini online attraverso azioni coordinate e ben mirate per sviluppare capacità e competenze.

Occorre identificare in modo affidabile le esigenze degli investigatori online. Europol, in conformità del suo mandato, e il polo UE dell'innovazione per la sicurezza⁸⁴ dovrebbero coordinare un'**analisi esaustiva delle lacune e delle esigenze tecnologiche nel settore delle indagini digitali**, così come un'analisi prospettica, che permetta di orientare i programmi di ricerca, innovazione e sviluppo e gli strumenti politici che contribuiscono allo sviluppo delle capacità. È importante che i soggetti e le reti pertinenti sostengano⁸⁵ questo lavoro. Su tale base Europol e il polo UE dell'innovazione per la sicurezza dovrebbero stabilire delle priorità

⁸¹ Documento di lavoro dei servizi della Commissione – *Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings* (SWD(2018) 118 final del 17.4.2018).

⁸² Cfr. la comunicazione della Commissione *Garantire la giustizia nell'UE – Una strategia europea di formazione giudiziaria per il periodo 2021-2024* (COM(2020) 713 final del 2.12.2020) che evidenzia la necessità di consentire ai professionisti di affrontare nuove sfide.

⁸³ Analisi forense dei dispositivi connessi e dei dati relativi ai sistemi dell'Internet degli oggetti.

⁸⁴ Il polo UE dell'innovazione per la sicurezza interna è una rete di collaborazione per sostenere i laboratori di innovazione delle agenzie dell'UE, degli Stati membri, del Centro comune di ricerca della Commissione europea e di altri soggetti pertinenti nella fornitura di prodotti innovativi e all'avanguardia.

⁸⁵ ENFSI, ENLETS, i-LEAD, ILEAnet.

per la ricerca e lo sviluppo che dovranno essere convalidate dagli Stati membri⁸⁶. Per fornire una prospettiva chiara dei meccanismi pratici in vigore e delle risorse disponibili per sostenere la capacità delle autorità di contrasto nel settore delle indagini digitali e per chiarire i ruoli e le responsabilità dei soggetti coinvolti, la Commissione consulterà gli Stati membri e gli altri portatori di interessi entro la fine del 2021 e agirà di conseguenza.

La **ricerca e l'innovazione** sono necessarie sia per le tecnologie di indagine sia per contrastare i reati agevolati dalla tecnologia. Il programma di ricerca e innovazione dell'UE, Orizzonte 2020, ha finanziato lo sviluppo di soluzioni tecnologiche innovative per migliorare la capacità delle autorità nazionali di contrastare la criminalità organizzata. Tale attività sarà ulteriormente rafforzata con il nuovo programma Orizzonte Europa, che finanzia progetti di ricerca per migliorare il quadro di intelligence sulla criminalità organizzata, sviluppare strumenti e programmi di formazione e rafforzare la cooperazione tra le agenzie.

La Commissione agevolerà l'accesso a **insiemi di dati di elevata qualità necessari per lo sviluppo di strumenti d'indagine**, compresi i sistemi di intelligenza artificiale, che rispondono alle esigenze delle autorità di contrasto nelle indagini penali, ad esempio per l'analisi di grandi quantità di dati o per le indagini sulla darknet. A tal fine la Commissione sosterrà nell'ambito del programma Europa digitale la creazione di uno spazio europeo dei dati in materia di sicurezza⁸⁷ che sarà fondamentale per sviluppare, formare e valutare gli strumenti per le autorità di contrasto e contribuire alla strategia europea per i dati nel pieno rispetto dei diritti fondamentali. Inoltre la Commissione aiuterà gli Stati membri ad avviare progetti pilota sulle soluzioni di intelligenza artificiale⁸⁸ che contribuiscano a promuovere l'adozione dell'innovazione da parte delle autorità di contrasto. Le autorità di contrasto, l'industria e il mondo accademico dovrebbero cooperare in una rete sostenuta dai finanziamenti dell'UE **per sviluppare strumenti e soluzioni a livello dell'UE che rispondano alle esigenze delle autorità di contrasto dell'UE**⁸⁹, sostenendo così il lavoro svolto Europol per fornire servizi e soluzioni tecniche alle autorità di contrasto dell'UE. Tale rete dovrebbe assicurare la sostenibilità dei progetti di Orizzonte Europa e del Fondo sicurezza interna e sostenere Europol in tali attività.

⁸⁶ La *Clearing Board* di Europol e la task force dell'UE sulla cybercriminalità (*EU Cybercrime Task Force*, EUCTF), ossia il gruppo che riunisce i responsabili delle unità di lotta alla criminalità informatica delle autorità di contrasto dell'UE, costituirebbero le strutture tra cui scegliere per la consultazione degli Stati membri.

⁸⁷ Il programma di lavoro 2021-2022 del programma Europa digitale prevede un'azione volta a istituire il quadro di un'architettura federata di dati per l'innovazione della sicurezza, finanziando la creazione delle componenti nazionali di uno spazio europeo dei dati in materia di sicurezza per l'innovazione. In tal modo si favorirebbero l'innovazione e lo sviluppo creando un ecosistema a livello dell'UE per condividere, sviluppare, sperimentare, addestrare e convalidare gli algoritmi per gli strumenti di IA ai fini di contrasto e di sicurezza basati su vari tipi di insiemi di dati, compresi quelli resi anonimi e pseudo-operativi, in linea con la strategia europea per i dati (comunicazione della Commissione *Una strategia europea per i dati*, COM(2020) 66 final del 19.2.2020). Nel primo trimestre del 2022 sarà presentato un invito a formulare proposte che prevede il coinvolgimento di almeno sei servizi di contrasto e di due imprese per un valore di 5-10 milioni di EUR sotto forma di una sovvenzione con un cofinanziamento del 50 %.

⁸⁸ In linea con l'iniziativa sull'intelligenza artificiale presentata dalla Commissione nel *Libro bianco sull'intelligenza artificiale* (COM(2020) 65 final del 19.2.2020).

⁸⁹ A tal fine la Commissione europea sta ad esempio finanziando la *European Anti-Cybercrime Technology Development Association* (<https://www.eactda.eu/>) nell'ambito del programma di lavoro annuale del 2020 del Fondo sicurezza interna (Polizia).

La rete dovrebbe fornire a titolo gratuito i suoi risultati alle autorità di contrasto attraverso Europol e migliorare continuamente le soluzioni esistenti. A tal fine Europol dovrebbe diventare lo "sportello unico" per l'accesso a strumenti e servizi, come l'analisi di software maligni, da parte delle autorità di contrasto nazionali.

4.3. Migliorare l'accesso alle competenze, alle conoscenze e alle competenze operative

Mentre la ricerca e l'analisi delle prove digitali sono al centro di gran parte delle indagini, il livello delle competenze necessarie nel campo della procedura penale, delle tattiche e delle tecniche di indagine digitale o di scienza forense digitale non è ancora disponibile in alcuni Stati membri e nella maggior parte di essi deve essere ampliato e approfondito. Inoltre l'accesso a competenze operative di punta in settori specifici come la scienza forense nell'ambito dell'Internet degli oggetti continua ad essere un problema per vari Stati membri.

Lo sviluppo della formazione dovrebbe basarsi su una definizione delle competenze richieste per svolgere indagini digitali e dei relativi profili professionali (ad esempio analista di dati, investigatore online o esperto di scienza forense digitale). A tal fine Europol e CEPOL dovrebbero collaborare con gli Stati membri⁹⁰ per definire e aggiornare periodicamente un **"quadro sulle competenze di formazione"**. Su tale base la Commissione dovrebbe sostenere lo sviluppo di materiale formativo attraverso il Gruppo europeo di formazione e istruzione in materia di criminalità informatica (ECTEG) e sostenere l'offerta formativa a livello nazionale attraverso gli strumenti disponibili⁹¹.

CEPOL e la rete europea di formazione giudiziaria (REFG) dovrebbero valutare regolarmente le esigenze di formazione e su questa base stabilire le priorità in materia di offerta formativa, anche al fine di sviluppare ulteriormente la competenza digitale generale delle autorità di contrasto e giudiziarie. Sulla base del quadro sulle competenze di formazione, CEPOL dovrebbe inoltre operare a stretto contatto con gli operatori⁹² e gli Stati membri per creare **sistemi di certificazione/accreditamento per gli esperti in indagini digitali**. Tali schemi 1) aumenterebbero il numero di esperti in grado di erogare formazione in settori specifici; 2) agevolerebbero la cooperazione transfrontaliera, poiché la certificazione/l'accreditamento fornirebbe garanzie riguardo all'acquisizione e all'utilizzo delle prove, garantendone l'ammissibilità dinanzi al giudice anche in altre giurisdizioni; 3) agevolerebbero l'identificazione di investigatori specializzati.

Le indagini digitali possono richiedere competenze che scarseggiano nell'UE, come quelle sulle criptovalute, sul ransomware⁹³ o nelle indagini sul darkweb. Gli Stati membri dovrebbero identificare esperti che abbiano sviluppato competenze all'avanguardia in questi

⁹⁰ Nel quadro della task force dell'Unione europea sulla criminalità informatica (EUCTF), istituita nel 2010, che comprende i responsabili delle unità nazionali di lotta alla criminalità informatica dei vari Stati membri e i rappresentanti di Europol, della Commissione Europea e di Eurojust: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf>

⁹¹ Ad esempio attraverso il Fondo sicurezza interna e lo strumento di sostegno tecnico.

⁹² Il Gruppo europeo di formazione e istruzione in materia di criminalità informatica (ECTEG) ha già svolto un lavoro considerevole sul tema nel quadro del progetto di certificazione per la lotta alla criminalità informatica globale (<https://www.ecteg.eu/running/gcc/>).

⁹³ Europol ha collaborato con l'industria per creare il progetto *No More Ransom* (<https://www.nomoreransom.org/>) che fornisce consigli di prevenzione e strumenti di decrittografia.

settori affinché si sostengano a vicenda nelle operazioni in cui tali competenze sono necessarie. La Commissione aiuterà Europol a istituire meccanismi volti a garantire che le autorità e gli esperti degli Stati membri siano adeguatamente incentivati a far parte di un gruppo di esperti.

Azioni principali

La Commissione intende:

- analizzare e delineare possibili approcci e soluzioni sulla **conservazione dei dati** per le autorità di contrasto e giudiziarie e consultare gli Stati membri in merito entro la fine di giugno 2021;
- proporre un percorso da seguire per affrontare la questione dell'accesso legittimo e mirato da parte delle autorità di contrasto alle **informazioni cifrate** nell'ambito delle indagini penali; tale approccio dovrebbe essere basato su una mappatura approfondita indicante le modalità di utilizzo della cifratura da parte degli Stati membri, e su un processo di consultazione dei portatori di interessi per esaminare e valutare le opzioni concrete e legittime;
- incoraggiare e agevolare la piena e rapida **partecipazione degli Stati membri al sistema digitale di scambio di prove elettroniche (e-EDES)**;
- sviluppare, attraverso il suo Centro comune di ricerca, uno strumento di monitoraggio per raccogliere informazioni sulle attività illegali che si sviluppano nella **darknet**;
- sostenere lo **sviluppo di moduli e materiali di formazione** e sostenere l'erogazione della formazione da parte di CEPOL, della REFG e degli istituti di formazione nazionali.

Europol è esortata a:

- coordinare un'**analisi esaustiva** delle lacune e delle esigenze tecnologiche nel settore delle indagini digitali;
- creare un **archivio di strumenti**, consentendo alle autorità di contrasto di identificare soluzioni all'avanguardia e di accedervi;
- istituire e mantenere una banca dati di **esperti in materia di indagini e di scienza forense** in settori specializzati come l'Internet degli oggetti o le criptovalute.

CEPOL è esortata a:

- creare **sistemi di certificazione/accreditamento** per gli esperti in indagini digitali;
- fornire e aggiornare periodicamente un **quadro sulle competenze di formazione** insieme a Europol.

Il Parlamento europeo e il Consiglio sono esortati a:

- adottare con urgenza le proposte concernenti le **prove elettroniche** per garantire alle autorità un accesso rapido e affidabile alle prove elettroniche.

Conclusioni

La presente strategia stabilisce le priorità, le azioni e gli obiettivi da raggiungere nei prossimi cinque anni per dotare l'UE di una base più forte per la lotta alla criminalità organizzata. Tuttavia il fenomeno criminale è in continua evoluzione ed è essenziale identificare le nuove tendenze e reagire rapidamente ai nuovi sviluppi. L'Unione e i suoi Stati membri devono mantenere una posizione di vantaggio rispetto alle organizzazioni criminali.

È quindi il momento di intensificare l'azione collettiva dell'Unione contro la criminalità organizzata, rafforzando gli strumenti esistenti per sostenere la cooperazione transfrontaliera, compresa la cooperazione attraverso le agenzie nel settore "Giustizia e affari interni", affrontando i reati ad alta priorità e smantellando le strutture sottostanti, intervenendo con vigore contro i fondi di origine illegale e i metodi corrotti che la criminalità utilizza per infiltrarsi nell'economia e contrastando l'uso delle nuove tecnologie da parte dei criminali. La qualità di una normativa dipende dalla sua attuazione: è quindi importante che gli Stati membri attuino in modo completo e corretto gli strumenti esistenti dell'UE. La Commissione continuerà a svolgere il suo ruolo sostenendo gli Stati membri e fornendo loro continui orientamenti, e sarà pronta a intervenire in modo rapido in caso di violazione del diritto dell'UE.

Le autorità sul campo devono essere in grado di sfruttare appieno il potenziale degli strumenti esistenti per smantellare le attività criminali e il modello di attività delle organizzazioni criminali. Per consentire di raggiungere tale obiettivo, le misure nell'ambito della presente strategia devono essere accompagnate da una nuova cultura, in cui le autorità di contrasto e giudiziarie verifichino sistematicamente i possibili collegamenti transfrontalieri e internazionali durante le indagini sui casi di criminalità organizzata. Lo scambio di funzionari delle autorità di contrasto, procuratori e giudici, anche con paesi terzi, così come ulteriori opportunità di formazione, possono contribuire a realizzare tale cambiamento.

La Commissione si impegna a dare il proprio contributo nell'ambito di questa lotta rinnovata alla criminalità organizzata e invita il Parlamento europeo e il Consiglio ad adoperarsi a favore dello sforzo comune, che è essenziale per garantire la sicurezza nell'UE, proteggere l'economia europea e salvaguardare lo Stato di diritto e i diritti fondamentali.