Consiglio
dell'Unione europea

Bruxelles, 22 novembre 2019
(OR. en)

14297/19

LIMITE

COSI 239
ENFOPOL 508
ENFOCUSTOM 196
FRONT 333
DAPIX 346
CYBER 322
JAI 1217

NOTA

Origine:	presidenza
Destinatario:	Comitato dei rappresentanti permanenti/Consiglio
Oggetto:	Futuro indirizzo della sicurezza interna dell'UE - Risultati delle discussioni - Relazione della presidenza

La rapida evoluzione del contesto di sicurezza richiede un approccio integrato per affrontare nuove minacce e sfide. Un approccio globale alla sicurezza interna costituisce un modo sostenibile per affrontare minacce più complesse e variegate rispetto al passato, consentendo un'impostazione che includa tutta la società quanto alle risposte fornite.

Nel quadro dell'attuazione dell'agenda strategica 2019-2024 nel settore della giustizia e degli affari interni, la presidenza ha condotto una serie di discussioni tematiche per approfondire la riflessione sul futuro indirizzo della sicurezza interna dell'UE. La presidenza ha delineato tre principi fondamentali per guidare tali riflessioni: offrire ai propri cittadini uno spazio di libertà, sicurezza e giustizia, combattere l'esclusione sociale e la discriminazione e promuovere i valori dell'Unione.

Le discussioni sono state avviate nel luglio 2019 nella riunione informale del comitato permanente per la cooperazione operativa in materia di sicurezza interna (COSI), in preparazione del Consiglio informale "Giustizia e affari interni" (Consiglio GAI), durante la quale è stata sollevata una serie di importanti temi orizzontali[1]. Le discussioni tematiche hanno avuto luogo anche nell'ambito dei gruppi pertinenti, quali il Gruppo "Applicazione della legge", il Gruppo "Terrorismo" e il Gruppo "Scambio di informazioni e protezione dei dati", e sono state ulteriormente approfondite in sede di COSI in vista del dibattito ministeriale. Vari argomenti sono stati affrontati nel dettaglio, ad esempio il rafforzamento del quadro di cooperazione operativa per le attività di contrasto, l'impatto delle nuove tecnologie e delle minacce ibride sulla sicurezza interna, il ruolo delle agenzie GAI dell'UE, la gestione e l'automazione delle informazioni e la formazione delle autorità di contrasto. I dettagli di tali discussioni sono presentati nei documenti elaborati per le varie riunioni e figuranti nell'allegato della presente relazione.

Nella presente relazione sono esaminati aspetti specifici che riflettono il punto di vista della presidenza sulle questioni principali emerse dalle discussioni summenzionate da riportare al ciclo legislativo 2019-2024.

1. Approccio proattivo alle nuove tecnologie

Gli sviluppi tecnologici hanno un forte impatto sulla vita dei cittadini dell'UE e, di conseguenza, sulle attività di contrasto. L'insieme di tali sviluppi, quali l'intelligenza artificiale, gli aeromobili senza equipaggio, le nuove reti di comunicazione e gli ambienti online, per citarne solo alcuni, possono sì sostenere il lavoro delle autorità, ma possono anche essere utilizzati per scopi illeciti. Ad esempio, sia le autorità di contrasto che i servizi di primo intervento possono fare uso di droni, ad esempio nella lotta al terrorismo le prime e a seguito di un attentato terroristico i secondi. Il ritmo crescente dell'innovazione mette a dura prova la capacità dei servizi di contrasto di adattarsi al mondo tecnologico in rapida evoluzione. Nel contesto della digitalizzazione sarebbe necessario valutare in che misura i quadri giuridici in cui operano le autorità di contrasto e le pertinenti agenzie dell'UE corrispondono alle attuali esigenze[2]. La salvaguardia e la promozione dei diritti fondamentali dovrebbero essere alla base di tali sviluppi, nel rispetto dei rigorosi requisiti in materia di attività di contrasto derivanti dal quadro giuridico sulla protezione dei dati, in cui l'Unione occupa una posizione di leadership nella definizione delle norme.

---

1 Documento della presidenza sul futuro indirizzo della sicurezza interna nell'UE (WK 13264/19)

2 Documenti 12496/19 e 12224/19 - Nuove tecnologie e sicurezza interna.

L'obiettivo è quello di assegnare alle autorità di contrasto dell'UE un ruolo proattivo per poter trarre vantaggio dalle nuove tecnologie, anticipando e controllando al contempo i rischi ad esse associati. È necessario un approccio globale e integrato a livello dell'UE in questo settore. Il raggiungimento di tale obiettivo è favorito dalla creazione di un laboratorio congiunto per l'innovazione all'interno di Europol per gestire gli sviluppi e le tendenze, nonché l'innovazione e la ricerca in ambito tecnologico e valutare la loro potenziale rilevanza per le attività di contrasto e il dialogo con l'industria e il mondo accademico. Il pieno sfruttamento delle nuove tecnologie richiede una ricerca e una formazione costanti. Il fatto di centralizzare alcune attività e di mettere in comune i risultati delle attività delle reti esistenti nell'ambito del laboratorio per l'innovazione apporterebbe vantaggi in termini di razionalizzazione ed efficienza sotto il profilo dei costi, in particolare nei settori in cui gli Stati membri non dispongono di risorse sufficienti per agire da soli o in cui la cooperazione e lo scambio delle migliori pratiche generano un valore aggiunto.

Poiché la ricerca e lo sviluppo in ambito tecnologico hanno spesso luogo nelle università e nel settore privato, le autorità di contrasto sono coinvolte in una fase relativamente tardiva. Al fine di tener conto delle preoccupazioni delle autorità di contrasto per il futuro, la presidenza ritiene opportuno adoperarsi per coinvolgere proattivamente le autorità di contrasto nei processi di sviluppo tecnologico sin dall'inizio, in particolare rafforzando ulteriormente la partecipazione e il coordinamento degli operatori preposti all'azione di contrasto nei programmi di ricerca e sviluppo in materia di sicurezza finanziati dall'UE.

La presidenza incoraggia le autorità di contrasto a partecipare in modo proattivo allo sviluppo di nuove tecnologie. Il laboratorio per l'innovazione dovrebbe fungere da piattaforma per sostenere tale obiettivo. È importante che le esigenze delle autorità di contrasto siano riconosciute e prese in considerazione nella fase iniziale del processo di sviluppo di nuove tecnologie che influenzeranno il lavoro di tali autorità o che sono necessarie ai fini di una loro risposta più efficace. Inoltre, gli interessi di sicurezza interna e di contrasto dovrebbero essere presi maggiormente in considerazione nella legislazione in materia di nuove tecnologie, al fine di ridurre le limitazioni proprie del quadro giuridico, in particolare affrontando sistematicamente tali interessi nelle valutazioni delle minacce.

2. Gestione efficace delle informazioni

La cooperazione a livello di UE in materia di attività di contrasto sarà sempre più basata su soluzioni tecnologiche e sistemi di informazione più avanzati ed efficienti e sulla loro interoperabilità[3]. In un'epoca di grandi volumi di dati digitali, le autorità di contrasto hanno accesso a maggiori quantità di dati e informazioni rispetto al passato. Ciò deve riflettersi nelle soluzioni tecniche e nelle capacità offerte. Nel contempo non si dispone di statistiche fondamentali su vari settori della criminalità. Pertanto, è particolarmente importante garantire che i sistemi di informazione siano alimentati con dati completi e di elevata qualità e utilizzati in modo efficace. Dobbiamo garantire che le autorità nazionali competenti abbiano accesso a tali sistemi e dispongano di una formazione sufficiente per consentirne il pieno utilizzo.

L'analisi criminale rimane al centro dell'attività di contrasto e fornisce valore aggiunto ai dati grezzi, trasformandoli in informazioni sfruttabili che possono essere utilizzate a livello nazionale, nonché in operazioni transfrontaliere in tutta l'UE. Si riscontra tuttavia la mancanza e l'esigenza di una chiara visione delle norme a livello dell'UE per quanto riguarda i lavori di analisi criminale. In ogni caso, questa costituisce parte integrante di tutti i processi d'informazione nell'ambito delle attività di contrasto. Ciò richiede risorse umane e finanziarie sufficienti per trattare e analizzare le informazioni. Per arrivare a buon fine, il miglioramento e la standardizzazione dell'analisi richiedono pertanto una migliore comprensione delle esigenze in materia di attività di contrasto nel loro complesso e, in particolare, dei vari processi d'informazione connessi, compresi quelli relativi alle indagini penali e alla raccolta di intelligence criminale.

I regolamenti in materia di interoperabilità[4] sono entrati in vigore l'11 giugno 2019; garantire una loro efficace attuazione è di fondamentale importanza. La rivoluzione tecnologica dei sistemi informatici dell'UE richiederà una grande quantità di risorse e il rispetto delle scadenze, sia a livello dell'UE che negli Stati membri. Nel costruire l'architettura di interoperabilità, è importante che le soluzioni tecniche tengano sempre conto delle esigenze degli utenti finali. Inoltre, è fondamentale prevedere una formazione adeguata e continua per gli utenti finali al fine di poter utilizzare tali nuovi sistemi di informazione e completarne l'interoperabilità. È evidente che l'interoperabilità non comporta soltanto lo sviluppo di sistemi informatici, ma anche un cambio di mentalità. Pertanto, un'attuazione efficace richiede anche un'evoluzione delle nostre culture operative e amministrative.

---

3 Documento 13510/19 - Gestione delle informazioni dell'UE - Automazione, accesso, scambio e analisi delle informazioni.

4 Regolamenti (UE) 2019/817 e (UE) 2019/818.

Su una scala più ampia, il rafforzamento dello scambio di informazioni non consiste solo in uno sviluppo tecnico. Per ottenere i benefici desiderati occorre garantire che le competenze, le risorse e le interfacce degli utenti finali a livello nazionale siano adatte allo scopo. Le informazioni non sono un valore assoluto: devono essere utilizzabili e condurre all'azione. In mancanza di un'attuazione corretta, questi sviluppi e i relativi benefici possono essere compromessi.

Oltre a condurre efficacemente le indagini, le autorità di contrasto dovrebbero concentrarsi anche sulla prevenzione e sullo smantellamento della criminalità. Contribuiscono a questo obiettivo informazioni efficaci e di elevata qualità, al momento e nel posto giusto. Per quanto riguarda le attività di contrasto basate sull'intelligence, Europol e Frontex sono in una posizione privilegiata per sostenere questo lavoro con le loro capacità di analisi, anche grazie al loro più ampio accesso al sistema d'informazione Schengen (SIS), sempre che gli Stati membri forniscano loro sistematicamente dati grezzi di elevata qualità.

La presidenza chiede un quadro completo UE di gestione delle informazioni, al fine di garantire che tutte le informazioni necessarie esistenti siano accessibili, trattate e scambiate in modo rapido ed efficiente per dare adito ad azioni basate sull'intelligence.

3. Cooperazione transfrontaliera multidisciplinare

Il rafforzamento della cooperazione operativa intersettoriale attraverso la riduzione delle duplicazioni e l'aumento dell'efficacia del coordinamento è fondamentale perché l'azione sia efficace. A causa della natura trasversale e in continua evoluzione delle varie minacce alla sicurezza, quali le armi CBRN e le attività ibride, le azioni intraprese per rispondere a tali attività e prevenirle richiedono un approccio orizzontale, sempre tenendo conto della competenza degli Stati membri in materia di sicurezza nazionale. È necessario un approccio integrato e coerente per garantire una cooperazione operativa multidisciplinare che vada oltre la cooperazione transfrontaliera in materia di contrasto, coinvolgendo in tal modo anche altre autorità, quali gli attori della protezione civile.

Le differenze tra i processi decisionali, le legislazioni e i modelli operativi nazionali rappresentano sfide imponenti per la cooperazione operativa transfrontaliera. Inoltre, la cooperazione transfrontaliera è ostacolata dalle incoerenze nelle pratiche nazionali di raccolta e trattamento dei dati, derivanti dalle differenze tra i singoli Stati membri in termini di sistemi amministrativi, soluzioni tecniche e modalità di funzionamento. Un'altra sfida consiste nell'individuare e rimuovere gli ostacoli alla cooperazione operativa tra le autorità di contrasto, come ad esempio affrontare la questione delle frequenze radio incompatibili nelle zone di frontiera, le barriere linguistiche e la necessità di integrare le basi giuridiche esistenti con accordi bilaterali più dettagliati. In situazioni urgenti, le entità nazionali possono non essere a conoscenza del ventaglio disponibile di alternative operative, disseminate tra diversi strumenti dell'UE, e di canali per lo scambio di informazioni.

La cooperazione operativa multidisciplinare tra le autorità di contrasto dovrebbe essere intensificata elaborando e utilizzando nuovi metodi di collaborazione e scambio di informazioni e affidandosi nel contempo a nuove applicazioni e nuovi strumenti tecnologici. Tali applicazioni possono includere, ad esempio, sistemi autonomi senza equipaggio, tecnologie per il riconoscimento automatico delle targhe o interfacce che permettono di effettuare un'unica ricerca tra tutte le banche dati disponibili. Esistono chiaramente lo slancio e l'opportunità per proseguire e sostenere ulteriormente questo sviluppo.

L'apprendimento e la formazione lungo tutto l'arco della vita assumono ancora più importanza al fine di sfruttare tutte le possibilità esistenti e prepararsi alle sfide future. La formazione fornita dalle agenzie dell'UE deve essere utilizzata in modo efficiente. Allo stesso tempo, occorre garantire che le attività delle agenzie dell'UE si completino a vicenda e che le sovrapposizioni siano eliminate.

Dobbiamo tenere conto delle differenze regionali e delle specificità nazionali, mirando nel contempo a una cultura comune in materia di contrasto tra le autorità di contrasto dell'UE. Migliorare le competenze linguistiche, acquisire conoscenze reciproche sulle rispettive culture e scambiare migliori pratiche contribuiscono a comprendere meglio le differenze regionali e culturali e a sostenere l'obiettivo comune.

Gli accordi bilaterali e multilaterali restano importanti per la cooperazione a livello locale e regionale, e occorre flessibilità per garantire il rispetto delle diversità regionali e dei differenti interessi operativi. In tutti gli sviluppi futuri occorre tenere conto della definizione della ripartizione delle competenze, della giurisdizione e della sovranità.

Le agenzie GAI dell'UE continuano a svolgere un ruolo significativo nel sostenere gli sforzi degli Stati membri nell'ambito dei rispettivi mandati. È ampiamente riconosciuto che una vera cooperazione transfrontaliera tra le autorità degli Stati membri, fortemente sostenuta dalle pertinenti agenzie dell'UE, rappresenta il modo più praticabile per realizzare un'Unione della sicurezza e per affrontare in modo sostenibile le minacce sia esistenti che nuove in un contesto in continua evoluzione[5].

Gli sviluppi futuri nel settore della sicurezza interna richiederebbero pertanto un ruolo costantemente attivo delle agenzie, con un previsto aumento del volume dei compiti esistenti e nuove responsabilità, derivanti da esigenze sia politiche che operative. Date le risorse limitate, è necessario discutere il contesto in cui le agenzie possono creare più efficacemente valore aggiunto, ad esempio i settori in cui gli Stati membri potrebbero aver bisogno di accedere a risorse o ad attrezzature tecniche tramite la messa in comune delle risorse, in cui le capacità di analisi dei dati potrebbero essere potenziate e in cui si potrebbe fornire un maggiore sostegno operativo. È opportuno stabilire criteri trasparenti per decidere in quali settori gli Stati membri hanno più bisogno di sostegno, tenendo conto dei progressi tecnologici e delle specifiche esigenze materiali o di altre risorse. Nello sviluppare il ruolo delle agenzie, l'obiettivo dovrebbe essere una soluzione equilibrata che tenga conto delle esigenze degli Stati membri. È essenziale adottare un approccio coordinato e olistico per rafforzare le competenze e i punti di forza essenziali di ciascuna agenzia come pure per creare valore aggiunto in modo efficace sotto il profilo dei costi e senza sovrapposizioni di compiti e funzioni.

Occorre approfondire la cooperazione e la condivisione di informazioni basate sulle agenzie, in quanto le minacce attuali ed emergenti alla sicurezza interna sono sempre più complesse e di natura transfrontaliera. È altresì necessaria un'interazione più efficace con i soggetti privati nel quadro della condivisione delle informazioni. In particolare, è necessario valutare la base giuridica di Europol per la richiesta e la ricezione di dati personali direttamente da soggetti privati[6].

---

5 Il ruolo delle agenzie dell'UE è stato specificamente trattato nella riunione informale del COSI e al Consiglio informale di luglio (docc. WK 13271/19 e WK 13266/19) e ha costituito un tema trasversale in tutte le discussioni.

6 La cooperazione di Europol con soggetti privati è stata discussa in sede di Gruppo "Applicazione della legge": docc. 10494/19, 11832/19, 12858/1/19.

Al fine di rafforzare l'approccio multidisciplinare di Europol in materia di contrasto nel lungo termine, è opportuno continuare a sviluppare la cooperazione tra le autorità doganali e Europol aumentando il numero di ufficiali di collegamento delle dogane presso Europol, promuovendo l'uso di SIENA da parte delle dogane in tutti gli Stati membri dell'UE e rafforzando lo scambio regolare e strutturato di informazioni tra le parti, comprese le informazioni in materia di gestione del rischio e di intelligence. Un obiettivo a breve termine dovrebbe essere il rafforzamento del contributo e dell'integrazione delle dogane nell'attuazione degli OAP dell'EMPACT. Tali azioni proseguirebbero l'evoluzione positiva della cooperazione tra le dogane e Europol degli ultimi anni.

Occorre affrontare le sfide della cooperazione tra l'Unione europea e Interpol. È importante che le banche di dati che fungono da principali fonti di informazione per la cooperazione in materia di contrasto con i paesi terzi continuino ad essere efficacemente utilizzate dalle autorità degli Stati membri dell'UE in futuro. Nel contempo, è chiaro che la legislazione applicabile in materia di protezione dei dati deve essere pienamente rispettata.

La presidenza sottolinea che è necessario riesaminare il quadro giuridico per la cooperazione transfrontaliera in materia di contrasto e il mandato di Europol al fine di adeguarlo alle attuali contingenze e alle sfide future. È opportuno continuare a sostenere lo sviluppo di una cultura comune in materia di contrasto tra le autorità di contrasto dell'UE.

4. Approccio globale alla sicurezza

È prevedibile che in un prossimo futuro si verifichino una serie di tendenze e sviluppi che incideranno sul panorama delle minacce nell'UE. La criminalità continua ad essere trainata dalla domanda e dalla disponibilità di opportunità per le imprese criminali. Inoltre, i cambiamenti sul piano della sicurezza nelle regioni limitrofe e varie forme di radicalizzazione violenta in Europa continuano a rappresentare una minaccia per la nostra sicurezza interna. Un approccio globale alla sicurezza con un migliore coordinamento e migliori risorse e capacità tecnologiche richiede una conoscenza situazionale e una preparazione migliori per una varietà di sfide.

Le autorità di contrasto, quelle della protezione civile e altre autorità competenti dovrebbero continuare a sviluppare la loro preparazione per contrastare le minacce ibride. La cooperazione in materia di prevenzione e lotta contro le minacce ibride tra le pertinenti autorità nazionali, in funzione dei rispettivi mandati, nonché le istituzioni, gli organi e le agenzie dell'UE nell'ambito del nesso tra sicurezza interna ed esterna, deve essere costantemente migliorata e integrata. Al tempo stesso, è importante aumentare le sinergie ed evitare la duplicazione degli sforzi, anche attraverso metodi di lavoro orizzontali, un maggiore scambio di informazioni, e formazione ed esercitazioni intersettoriali.

Si sottolinea la necessità di proseguire le discussioni sulla dimensione interna delle minacce ibride, in particolare sui ruoli delle agenzie GAI nel rafforzare le capacità dell'UE e degli Stati membri di individuare le azioni ibride e le loro fonti.

Inoltre, per affrontare in modo efficace la disinformazione occorre un approccio globale. In quest'ottica, dovrebbe essere considerata la partecipazione delle autorità di contrasto, anche in meccanismi dell'UE già esistenti, come il sistema di allarme rapido. Le autorità di contrasto rafforzano la resilienza dell'UE e degli Stati membri ed è quindi necessario tener conto della lotta alla disinformazione[7]. La presidenza sottolinea la necessità di un migliore utilizzo degli strumenti esistenti e del rafforzamento del coordinamento globale a livello dell'UE. In tale contesto è necessario trattare anche il sostegno fornito dalle agenzie GAI agli Stati membri.

L'uso della tecnologia e di Internet nell'organizzazione di attività criminali continuerà a crescere. Ad esempio, si prevede un aumento dell'uso di piattaforme online, sia sul web visibile che sul web oscuro, per gli scambi commerciali di una vasta gamma di beni illeciti. Inoltre, la sfera online può essere utilizzata impropriamente in maniera efficace per radicalizzare, reclutare e istigare alla violenza. Occorre prevenire in modo efficace la diffusione di contenuti terroristici e pedopornografici online e rimuovere rapidamente i contenuti in questione.

[7] Minacce ibride e sicurezza interna: comunicazione strategica sulle attività di contrasto e lotta alla disinformazione (doc. 11831/19).

Viene inoltre messo in evidenza il ruolo della prevenzione della radicalizzazione violenta quale parte integrante di un approccio globale alla lotta contro il terrorismo. La collaborazione e il sostegno agli operatori in prima linea continuano a essere fondamentali per prevenire e lottare contro l'estremismo violento. È necessario affrontare l'estremismo violento di matrice politica o ideologica in tutte le sue forme. D'ora in avanti, si dovrebbe continuare a focalizzare l'attenzione sulla lotta e la prevenzione dell'estremismo violento e del terrorismo utilizzando un approccio di ampio respiro, tenendo conto anche delle tendenze emergenti nell'estremismo violento.

È necessario affrontare la minaccia posta dall'estremismo violento e dal terrorismo di destra tramite la creazione di un quadro situazionale migliore, la continua condivisione di buone pratiche, la cooperazione con i principali paesi terzi e la lotta alla diffusione di contenuti illeciti di estremismo di destra, sia online che offline. È opportuno affrontare la sfida rappresentata dal rimpatrio dei combattenti terroristi stranieri, anche attraverso un uso più efficiente del SIS.

La presidenza sottolinea la necessità di un approccio globale alla sicurezza che includa tutta la società al fine di affrontare le varie minacce alla sicurezza interna. Si sottolinea l'importanza di lavorare in tutti i pertinenti settori d'intervento in maniera più strategica, coordinata e coerente.

ALLEGATO

Subject	Meeting	Reference Number
Future Direction of internal security in the EU	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13264/19
Hybrid threats and internal security	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13265/19
Twenty Years of Europol - what next?	Informal COSI meeting on 8-9 July 2019, The Hague	WK 13266/19
The future of EU Internal Security	Informal Council meeting on 18-19 July 2019, Helsinki	WK 13271/19
The future direction of EU internal security: new technologies and internal security	JHA Council on 2 October 2019	12496/19
Hybrid threats and Internal Security	JHA Council on 2 October 2019	12495/19
Right-wing violent extremism and terrorism	JHA Council on 2 October 2019	12494/19
EU Information Management - Automation, access to, sharing of, and analysis of information	COSI meeting on 19 November 2019	13510/19
The future of EU law enforcement: Training for law enforcement	COSI meeting on 19 November 2019	13973/19