Consiglio dell'Unione europea

Bruxelles, 9 dicembre 2021
(OR. en)

14205/21
ADD 2

Fascicolo interistituzionale: 2021/0411(COD)

IXIM 260
ENFOPOL 460
JAI 1279
CODEC 1519
COMIX 576
IA 202

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	9 dicembre 2021
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, segretario generale del Consiglio dell'Unione europea
n. doc. Comm.:	SWD(2021) 377 final
Oggetto:	DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO che accompagna il documento Proposta di direttiva del Parlamento europeo e del Consiglio relativa allo scambio di informazioni tra le autorità di contrasto degli Stati membri, che abroga la decisione quadro 2006/960/GAI del Consiglio

Si trasmette in allegato, per le delegazioni, il documento SWD(2021) 377 final.

All.: SWD(2021) 377 final

COMMISSIONE
EUROPEA

Bruxelles, 8.12.2021
SWD(2021) 377 final

DOCUMENTO DI LAVORO DEI SERVIZI DELLA COMMISSIONE

SINTESI DELLA RELAZIONE SULLA VALUTAZIONE D'IMPATTO

che accompagna il documento

Proposta di direttiva del Parlamento europeo e del Consiglio

relativa allo scambio di informazioni tra le autorità di contrasto degli Stati membri, che abroga la decisione quadro 2006/960/GAI del Consiglio

{COM(2021) 782 final} - {SEC(2021) 420 final} - {SWD(2021) 374 final}

Scheda di sintesi

Valutazione d'impatto relativa a una proposta per modernizzare l'attuale cooperazione nell'attività di contrasto all'interno dell'Unione mediante la creazione di un codice di cooperazione di polizia dell'UE sullo scambio e la comunicazione di informazioni

A. Necessità di intervenire

Per quale motivo? Qual è il problema da affrontare?

La sicurezza e la criminalità transfrontaliera (compresi i reati fiscali) sono per definizione una questione internazionale. Come menzionato nella strategia dell'UE per l'Unione della sicurezza del 2020, **il panorama della sicurezza in Europa, in costante evoluzione**, è oggetto di minacce alla sicurezza mutevoli e sempre più complesse. Tali minacce si propagano oltre frontiera e assumono la forma di gruppi criminali organizzati e terroristici dediti a un'ampia gamma di attività criminose. Anche un reato commesso apparentemente a livello locale può connesso con altri reati che hanno avuto luogo altrove in Europa e sono ascrivibili agli stessi autori. Inoltre **la mobilità crescente all'interno dell'UE** crea ulteriori problemi per la prevenzione di tutte le forme di minacce criminali e gli interventi per contrastarle.

Il panorama criminale in rapida evoluzione e la mobilità crescente delle persone rendono fondamentale la cooperazione transfrontaliera tra le autorità di contrasto nell'UE per contrastare i reati e consentire ai cittadini dell'UE di godere in tutta sicurezza dei loro diritti di libera circolazione in futuro.

Tuttavia continuano a sussistere ostacoli allo scambio di dati tra le autorità di contrasto, consentendo a numerosi criminali e terroristi che agiscono in più di uno Stato membro di trarre vantaggio dalla presenza di zone d'ombra e scappatoie. La natura transfrontaliera della lotta alla criminalità e degli interventi per migliorare la sicurezza impone agli Stati membri di fare affidamento gli uni sugli altri per colmare le lacune in termini di informazione.

Le autorità di contrasto nell'UE cooperano e scambiano informazioni, in particolare sulla base della decisione quadro (2006/960/GAI) relativa alla semplificazione dello scambio di informazioni e intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge (decisione quadro svedese); esistono tuttavia lacune significative.

Le autorità di contrasto **non riescono a scambiare informazioni in modo efficace ed efficiente** con le loro controparti in altri Stati membri a causa di **tre problemi di natura giuridica, strutturale e tecnica**:

1) **le norme a livello nazionale ostacolano un flusso di informazioni efficace ed efficiente.** Di fatto la decisione quadro svedese del 2006 non viene pienamente attuata, impedendo alle autorità di contrasto di altri Stati membri di ricevere le informazioni in modo efficace ed efficiente;
2) **le strutture a livello nazionale non sono sempre istituite in modo sufficientemente efficiente ed efficace né sono dotate di strumenti idonei.** In effetti gli Stati membri non dispongono sempre delle strutture necessarie per ricevere le richieste di informazioni da altri Stati membri, inoltrarle alle autorità competenti a livello nazionale e fornire le informazioni richieste;
3) **la libera scelta dei canali di comunicazione tra gli Stati membri causa una duplicazione ricorrente delle richieste.** Le autorità di contrasto degli Stati membri utilizzano infatti una serie di canali diversi per inviare le richieste di informazioni ad altri Stati membri e rispondere ad esse, il che ostacola uno scambio di informazioni efficace ed efficiente.

Questi tre problemi, tra loro interconnessi, impongono l'adozione di scelte politiche coraggiose, che richiedono una valutazione dettagliata dei fattori alla base dei problemi, dei relativi obiettivi, delle opzioni strategiche disponibili e del loro impatto.

Qual è l'obiettivo dell'iniziativa?

La presente iniziativa dovrebbe essenzialmente coadiuvare gli Stati membri a concretizzare i loro impegni in materia di cooperazione nell'attività di contrasto. Essa risponde a urgenti esigenze operative e all'invito formulato dal Consiglio a considerare *"l'eventualità di consolidare il quadro giuridico dell'UE per rafforzare ulteriormente la cooperazione transfrontaliera nell'attività di contrasto nonché appoggiare lo sviluppo di uno scambio di informazioni agevole e rapido e l'ulteriore sviluppo di strutture e piattaforme pertinenti"*.

L'iniziativa si propone di conseguire gli **obiettivi** seguenti:

1) obiettivo I: agevolare un **accesso equivalente per le autorità di contrasto** alle informazioni in possesso di un altro Stato membro (analogo all'accesso alle informazioni garantito all'interno di uno Stato membro) nel rispetto dei diritti fondamentali, inclusi gli obblighi di protezione dei dati;

2) obiettivo II: garantire che tutti gli Stati membri dispongano di un **punto di contatto unico** (SPOC) che funzioni efficacemente, anche quando è richiesta un'**autorizzazione giudiziaria** per fornire i dati su richiesta di un altro Stato membro, e assicurare la sua cooperazione effettiva con i **centri di cooperazione di polizia e doganale** (PCCC);

3) obiettivo III: stabilire un **canale di comunicazione predefinito obbligatorio** per lo scambio di informazioni sull'attività di contrasto tra gli Stati membri (laddove pertinente).

Qual è il valore aggiunto dell'intervento a livello dell'UE?

Si prevede che l'azione dell'UE porti benefici all'intera Unione con un effetto a catena sui paesi associati Schengen, rafforzando globalmente la sicurezza e la fiducia tra gli Stati membri e contribuendo a realizzare il principio fondamentale di Schengen (uno spazio privo di controlli alle frontiere interne).

Regole, norme e obblighi minimi comuni a livello dell'UE miglioreranno notevolmente il flusso di informazioni in linea con **norme di livello elevato in materia di sicurezza e protezione dei dati**.

Inoltre l'adozione di norme comuni consente un certo livello di automazione nei flussi di lavoro relativi allo scambio di informazioni, sgravando così le autorità di contrasto da determinate attività manuali dispendiose in termini di tempo e carico di lavoro.

B. Soluzioni

Quali opzioni strategiche legislative e di altro tipo sono state prese in considerazione? Ne è stata prescelta una? Per quale motivo?

Sono state prese in considerazione diverse opzioni strategiche di carattere legislativo. In seguito a una preselezione sono state rapidamente scartate alcune opzioni. Le altre **opzioni sono state valutate in modo dettagliato**:

1) opzioni strategiche che perseguono **l'obiettivo I**: *("agevolare un accesso equivalente alle informazioni")*

- opzione strategica 1.1: proposta legislativa che aggiorna la decisione quadro svedese del 2006 per garantire il suo allineamento con la direttiva del 2016 sulla protezione dei dati nelle attività di polizia e giudiziarie + misure soft di accompagnamento (formazione, orientamenti della Commissione);
- opzione strategica 1.2: opzione 1.1 + semplificazione nell'utilizzo della decisione quadro svedese + maggiore chiarezza sulle serie di dati nazionali disponibili per un eventuale scambio;
- opzione strategica 1.3: opzione 1.2 + disposizioni che assicurano il rispetto dei termini entro i quali i dati devono essere messi a disposizione di un altro Stato membro (anche quando è richiesta un'autorizzazione giudiziaria);

2) opzioni strategiche che perseguono **l'obiettivo II**: *("garantire che tutti gli Stati membri dispongano di un punto di contatto unico (SPOC) che funzioni efficacemente, anche quando è richiesta un'autorizzazione giudiziaria per fornire i dati su richiesta di un altro Stato membro, e assicurare la sua cooperazione effettiva con i centri di cooperazione di polizia e doganale (PCCC)")*

- opzione strategica 2.1: proseguire con gli orientamenti non vincolanti del Consiglio relativi ai punti di contatto unici nazionali + misure soft di accompagnamento (formazione, sostegno finanziario, orientamenti);
- opzione strategica 2.2: *ravvicinamento delle norme minime* sulla composizione dei punti di contatto unici (compresa la presenza obbligatoria di un'autorità giudiziaria), le rispettive funzioni, il personale e i sistemi informatici nonché sulla loro cooperazione con le strutture regionali come i centri di cooperazione di polizia e doganale + misure soft di accompagnamento (formazione, sostegno finanziario, orientamenti);
- opzione strategica 2.3: *ravvicinamento* delle norme sulla composizione dei punti di contatto unici (compresa la presenza obbligatoria di un'autorità giudiziaria), le rispettive funzioni, il personale e i sistemi informatici nonché sulla loro cooperazione con le strutture regionali come i centri di cooperazione di polizia e doganale + misure soft di accompagnamento (formazione, sostegno

finanziario, orientamenti);

3) opzioni strategiche che perseguono **l'obiettivo III**: *("stabilire un canale di comunicazione predefinito obbligatorio per lo scambio di informazioni sull'attività di contrasto tra gli Stati membri (se del caso)")*

- opzione strategica 3.1: proseguire con gli orientamenti e le raccomandazioni non vincolanti del Consiglio che prevedono di mettere in copia Europol quando si ricorre a SIENA[1] nei casi che rientrano nel suo mandato + misure soft di accompagnamento (formazione, sostegno finanziario);
- opzione strategica 3.2: obbligo di utilizzare lo stesso canale di comunicazione per le stesse finalità (rendendo l'applicazione SIENA di Europol il canale predefinito, se del caso) + obbligo di mettere in copia Europol quando si ricorre a SIENA nei casi che rientrano nel suo mandato + misure soft di accompagnamento (come nell'opzione 3.1);
- opzione strategica 3.3: obbligo di ricorrere a SIENA come sistema predefinito per tutti gli scambi bilaterali di informazioni (a meno che ciò non sia disciplinato diversamente dal diritto dell'UE) + obbligo di mettere in copia Europol nei casi che rientrano nel suo mandato sia dopo la fine di un periodo di transizione sia nell'ambito del sostegno del Fondo Sicurezza interna per l'attuazione di SIENA + misure di accompagnamento (come nell'opzione strategica 3.1).

In seguito a una valutazione dettagliata dell'impatto delle principali opzioni strategiche, il **pacchetto delle opzioni strategiche prescelte** consiste nelle **opzioni strategiche 1.3, 2.2 e 3.3**.

Chi sono i sostenitori delle varie opzioni?

I portatori di interessi sono in genere favorevoli allo sviluppo di uno scambio di informazioni agevole e tempestivo e all'ulteriore sviluppo di strutture e piattaforme pertinenti.

Gli Stati membri dovrebbero sostenere la maggior parte delle misure previste dall'opzione prescelta. Al contempo gli Stati membri sono consapevoli dell'importanza della loro sovranità nazionale nel settore delle attività di contrasto da un punto di vista operativo e procedurale. I pareri positivi espressi a livello di esperti potrebbero non essere ulteriormente condivisi a livello politico.

Il probabile punto di discussione principale riguarda l'opzione 3.3 (rendere l'applicazione SIENA di Europol il canale obbligatorio di comunicazione tra gli Stati membri, quando ciò non sia disciplinato diversamente dal diritto dell'UE). Tale opzione è stata tuttavia difesa dagli Stati membri in sede di Consiglio: *"l'applicazione di SIENA come canale di comunicazione predefinito contribuirebbe a snellire lo scambio di informazioni tra le autorità di contrasto e ad aumentare il livello di sicurezza nel contesto della cooperazione di polizia nell'Unione. Al contempo ciò consentirebbe di concentrare gli sforzi sullo sviluppo di un'unica soluzione anziché di numerose soluzioni, favorendo in tal modo l'obiettivo di raggiungere una maggiore sicurezza interna dell'UE".*

Ci si aspetta che il Parlamento europeo verifichi l'esistenza di garanzie solide in materia di protezione dei dati. Le discussioni con tutti i portatori di interessi hanno infatti messo in luce l'importanza di adottare misure di salvaguardia appropriate per assicurare il rispetto dei diritti fondamentali, in particolare il diritto alla protezione dei dati personali.

C. Impatto dell'opzione prescelta

Quali sono i vantaggi delle opzioni prescelte (o in mancanza di queste ultime, delle opzioni principali)?

L'opzione prescelta, che segnerebbe una svolta, permetterebbe di rispondere efficacemente ai problemi individuati, rafforzando al contempo il sostegno di Europol agli Stati membri, con l'obiettivo finale di **prevenire e individuare i reati e di indagare su di essi** nel pieno **rispetto dei diritti fondamentali**.

I **beneficiari finali dell'opzione prescelta sono i cittadini**. Essi trarranno beneficio direttamente e indirettamente da una lotta più efficace alla criminalità e da tassi di criminalità più bassi. In termini di efficienza i **principali beneficiari sono le autorità di contrasto nazionali**.

Quali sono i costi delle opzioni prescelte (o in mancanza di queste ultime, delle opzioni principali)?

L'opzione prescelta richiede investimenti sia a livello dell'UE che degli Stati membri, relativi essenzialmente alla

[1] "Applicazione di rete per lo scambio sicuro di informazioni" di Europol.

formazione e agli aggiornamenti informatici. che varieranno significativamente da uno Stato membro all'altro, a seconda dell'efficienza e dell'efficacia del loro punto di contatto unico e dei centri di cooperazione di polizia e doganale nazionali (se presenti).

L'opzione prescelta consente di affrontare efficacemente i problemi, offrendo soluzioni che altrimenti sarebbero più costose, scarsamente compatibili o meno efficienti.

Tuttavia è difficile quantificare i costi di alcune delle opzioni strategiche. Secondo i dati di Europol, i costi relativi all'integrazione dell'applicazione SIENA di Europol in 20 sistemi di gestione dei casi (CMS) degli Stati membri e lo sviluppo di CMS in 10 Stati membri ammontano a 2,5 milioni di EUR (investimento una tantum). I benefici in termini di efficienza compenserebbero tuttavia questi costi (meno risorse necessarie per la gestione dei casi, ossia più risorse impiegate per la loro risoluzione).

L'opzione prescelta non contiene obblighi normativi per i cittadini/consumatori, pertanto non genera costi aggiuntivi a loro carico.

Quale sarà l'incidenza su aziende, PMI e microimprese?

L'opzione prescelta potrebbe avere un lieve impatto positivo sulle piccole e medie imprese, dato l'aumento della domanda di prodotti e servizi informatici.

L'impatto sui bilanci e sulle amministrazioni nazionali sarà significativo?

Come menzionato in precedenza, l'opzione prescelta richiede investimenti a livello degli Stati membri, relativi essenzialmente alla formazione e agli aggiornamenti informatici. Tuttavia è difficile quantificare i costi di alcune delle opzioni strategiche. Detti costi potrebbero variare significativamente da uno Stato membro all'altro, a seconda dell'efficienza e dell'efficacia del loro punto di contatto unico e dei centri di cooperazione di polizia e doganale nazionali (se presenti).

Secondo i dati di Europol, i costi di sviluppo di un sistema di gestione dei casi a livello nazionale potrebbero essere dell'ordine di 150 000 EUR (una tantum) per Stato membro. I benefici in termini di efficienza compenserebbero tuttavia questi costi (meno risorse necessarie per la gestione dei casi, ossia più risorse impiegate per la loro risoluzione).

Gli aggiornamenti informatici necessari sia per gli SPOC che per i PCCC potrebbero ammontare a un totale complessivo massimo di **11,5 milioni** di EUR (2,5 milioni di EUR per gli SPOC + 9 milioni di EUR per i PCCC).

Tali costi (investimento una tantum), considerati accettabili, sono **proporzionati** al problema individuato e non vanno oltre quanto necessario per conseguire l'obiettivo specifico. Il Fondo Sicurezza interna dell'UE garantirà un sostegno (essenzialmente attraverso i programmi nazionali).

Sono previsti altri impatti significativi?

L'opzione prescelta conferisce ai poli di informazione nazionali e regionali degli Stati membri maggiori poteri al fine di accedere ai dati esistenti e condividerli in modo più efficace ed efficiente.

Essa garantisce inoltre il pieno allineamento di una nuova direttiva sullo scambio di informazioni e comunicazioni con la direttiva del 2016 sulla protezione dei dati nelle attività di polizia e giudiziarie. Tale allineamento garantisce una esplicita conformità ai diritti fondamentali, cosa che attualmente non avviene con la decisione quadro svedese del 2006.

L'opzione prescelta risponde a un **obiettivo di interesse generale** ed è **strettamente limitata a quanto necessario e proporzionato** per il conseguimento di tale obiettivo.

D. Tappe successive

Quando saranno riesaminate le misure proposte?

[Due] anni dopo il termine di recepimento e in seguito ogni [quattro] anni, la Commissione dovrà presentare al Parlamento europeo e al Consiglio due relazioni: **la prima relazione** per valutare in che misura gli Stati membri abbiano adottato le misure necessarie per conformarsi alla nuova direttiva; **la seconda relazione** per valutare i risultati conseguiti rispetto agli obiettivi e stabilire se i principi di base siano ancora validi e quali siano le eventuali implicazioni per le opzioni future.