



Bruxelas, 22 de novembro de 2019
(OR. en)

14297/19

LIMITE

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

NOTA

de:	Presidência
para:	Comité de Representantes Permanentes/Conselho
Assunto:	Orientação futura da segurança interna da UE – Resultados dos debates – Relatório da Presidência

A rápida mutação do ambiente de segurança exige uma abordagem integrada para fazer face a novas ameaças e desafios. Uma abordagem global da segurança interna é uma forma viável de enfrentar ameaças que são mais complexas e variadas do que no passado, permitindo uma abordagem das respostas apresentadas que englobe toda a sociedade.

Na execução da Agenda Estratégica 2019-2024 no domínio da justiça e dos assuntos internos, a Presidência realizou uma série de debates temáticos para aprofundar a reflexão sobre o caminho a seguir no que respeita à orientação futura da segurança interna da UE. A Presidência definiu três princípios fundamentais para orientar estas reflexões: oferecer um espaço de liberdade, segurança e justiça aos seus cidadãos; combater a exclusão social e a discriminação; e promover os valores da União.

Os debates foram lançados em julho de 2019, na reunião informal do Comité Permanente para a Cooperação Operacional em matéria de Segurança Interna (COSI), em preparação da reunião informal do Conselho Justiça e Assuntos Internos (Conselho JAI), com base numa série de tópicos horizontais fundamentais¹. Realizaram-se também debates temáticos nos grupos de trabalho pertinentes, como o Grupo da Aplicação da Lei, o Grupo do Terrorismo e o Grupo do Intercâmbio de Informações (DAPIX IE), que foram desenvolvidos mais aprofundadamente no COSI para o debate ministerial. Foram abordados em pormenor vários tópicos, como o reforço do quadro de cooperação operacional para a aplicação da lei, o impacto das novas tecnologias e das ameaças híbridas para a segurança interna, o papel das agências JAI da UE, a gestão e a automatização da informação e a formação das autoridades responsáveis pela aplicação da lei. Os elementos pormenorizados destes debates são apresentados nos documentos elaborados para as várias reuniões e enumerados no anexo do presente relatório.

O presente relatório abrange determinados aspetos, refletindo o ponto de vista da Presidência sobre as principais questões que emergiram desses debates para transitarem para o ciclo legislativo 2019-2024.

1. Abordagem proativa das novas tecnologias

A evolução tecnológica tem um grande impacto na vida dos cidadãos da UE e, subsequentemente, no trabalho das autoridades responsáveis pela aplicação da lei. Todos estes desenvolvimentos, como a inteligência artificial, os veículos aéreos não tripulados, as novas redes de comunicação e os ambientes em linha, para citar apenas alguns, podem apoiar o trabalho das autoridades, mas podem também ser utilizados para fins ilegais. Por exemplo, tanto as autoridades policiais como os intervenientes de primeira linha podem recorrer a drones, nomeadamente no âmbito da luta contra o terrorismo e também na sequência de um ataque terrorista. O ritmo crescente da inovação constitui um desafio à capacidade de os serviços responsáveis pela aplicação da lei se adaptarem ao rápido desenvolvimento do mundo tecnológico. No contexto da digitalização, será necessário avaliar em que medida os quadros jurídicos em que operam as autoridades responsáveis pela aplicação da lei e as agências competentes da UE correspondem às necessidades atuais². A preservação e a promoção dos direitos fundamentais devem alicerçar tais desenvolvimentos, sem deixar de respeitar os requisitos estritos em matéria de atividades de aplicação da lei decorrentes do quadro de proteção de dados, em que a União ocupa uma posição de liderança na definição de normas.

¹ Documento da Presidência sobre a orientação futura da segurança interna na UE (WK 13264/19)

² Documentos 12496/19 e 12224/19, novas tecnologias e segurança interna

O objetivo é dotar as autoridades responsáveis pela aplicação da lei na UE de um papel proativo, a fim de poderem beneficiar das novas tecnologias, antecipando e controlando simultaneamente os riscos que lhes estão associados. Neste domínio, é necessária uma abordagem integrada e abrangente a nível da UE. A criação de um laboratório comum de inovação no âmbito da Europol para tirar partido da evolução e das tendências tecnológicas, da inovação e da investigação, e para avaliar a sua potencial relevância para a aplicação da lei e o diálogo com a indústria e o meio académico vai ao encontro deste objetivo. A plena exploração das novas tecnologias exige investigação e formação constantes. A centralização de certas atividades e a partilha dos resultados do trabalho das redes existentes no laboratório de inovação traria benefícios em termos de racionalização e eficiência de custos, especialmente em domínios em que os Estados-Membros não dispõem de recursos suficientes para agir isoladamente ou em que há valor acrescentado na ação conjunta e no intercâmbio de boas práticas.

Uma vez que a investigação e o desenvolvimento tecnológicos ocorrem frequentemente nas universidades e no setor privado, as autoridades responsáveis pela aplicação da lei só se envolvem numa fase relativamente tardia. A fim de ter em conta as preocupações das autoridades responsáveis pela aplicação da lei relativamente ao futuro, a Presidência considera que devem ser envidados esforços no sentido de envolver proativamente as autoridades responsáveis pela aplicação da lei logo na fase incipiente dos processos de desenvolvimento tecnológico, nomeadamente através do reforço da participação e da coordenação dos profissionais responsáveis pela aplicação da lei nos programas de investigação e desenvolvimento para a segurança financiados pela UE.

A Presidência incentiva as autoridades responsáveis pela aplicação da lei a participarem de forma proativa no desenvolvimento de novas tecnologias. O laboratório de inovação deverá funcionar como uma plataforma para apoiar este objetivo. É importante que as necessidades das autoridades responsáveis pela aplicação da lei sejam conhecidas e tidas em conta numa fase precoce do desenvolvimento de novas tecnologias que influenciem o seu trabalho ou que sejam necessárias para uma resposta mais eficaz em termos de aplicação da lei. Além disso, os aspetos de segurança interna e de aplicação da lei devem ser tidos em conta de forma mais adequada na legislação relativa às novas tecnologias, a fim de atenuar as limitações do quadro jurídico, nomeadamente através da sua abordagem sistemática nas avaliações das ameaças.

2. Gestão eficaz da informação

A cooperação em matéria de aplicação da lei a nível da UE basear-se-á cada vez mais em melhores e mais eficientes soluções tecnológicas e sistemas de informação, bem como na sua interoperabilidade³. Numa era de grandes volumes de dados digitais, as autoridades responsáveis pela aplicação da lei têm acesso a mais dados e informações do que nunca. Tal deve refletir-se nas soluções técnicas e na capacidade disponíveis. Ao mesmo tempo, faltam estatísticas fundamentais sobre vários domínios da criminalidade. Por conseguinte, é particularmente importante assegurar que os sistemas de informação sejam alimentados com dados completos e de elevada qualidade e utilizados de forma eficaz. Temos de garantir que as autoridades nacionais competentes têm acesso a estes sistemas e recebem formação suficiente para permitir a sua plena utilização.

A análise criminal continua a estar no cerne da aplicação da lei. A análise fornece valor acrescentado aos dados em bruto, transformando-os em informações práticas que podem ser utilizadas a nível nacional, bem como em operações transfronteiras em toda a UE. No entanto, falta e é necessária uma visão clara das normas a nível da UE em matéria do trabalho de análise criminal. Em todo o caso, a análise é parte integrante de todos os processos de informação no âmbito da aplicação da lei. Para tal, é necessário dispor de recursos humanos e financeiros suficientes para tratar e analisar as informações. A fim de conseguir reforçar e normalizar a análise importa, por conseguinte, compreender melhor as necessidades em matéria de aplicação da lei em geral e os vários processos de informação envolvidos em particular, incluindo os processos de investigação criminal e de recolha de informações criminais.

Os regulamentos sobre interoperabilidade⁴ entraram em vigor em 11 de junho de 2019. É extremamente importante garantir a aplicação eficaz dos regulamentos. Esta revolução tecnológica dos sistemas informáticos da UE exigirá um grande volume de recursos e o cumprimento do calendário, tanto a nível da UE como dos Estados-Membros. Na construção da arquitetura de interoperabilidade, é importante que as soluções técnicas tenham sempre em conta as necessidades dos utilizadores finais. Além disso, é fundamental proporcionar formação adequada e contínua aos utilizadores finais, a fim de que possam utilizar estes novos sistemas de informação e concluir a sua interoperabilidade. É evidente que a interoperabilidade é muito mais do que desenvolver sistemas informáticos; implica também uma mudança de mentalidade. Por conseguinte, a aplicação bem-sucedida exige também uma mudança nas nossas culturas operacionais e administrativas.

³ Documento 13510/19, Gestão da informação na UE – automatização, acesso, intercâmbio e análise de informações.

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

Numa escala mais vasta, o reforço do intercâmbio de informações não se limita a um desenvolvimento técnico. Para alcançar os benefícios pretendidos, é necessário garantir que as competências, os recursos e as interfaces dos utilizadores finais a nível nacional são adequados ao fim a que se destinam. A informação não é um valor absoluto; tem de ser utilizável e conduzir a uma ação. Sem uma aplicação adequada, estes desenvolvimentos e os seus benefícios podem ficar comprometidos.

Paralelamente à eficácia das investigações, o trabalho das autoridades responsáveis pela aplicação da lei deve igualmente centrar-se na prevenção e no desmantelamento da criminalidade.

Informações de elevada qualidade no local adequado e no momento certo contribuem para este objetivo. No que diz respeito à aplicação da lei baseada na obtenção de informações, a Europol e a Frontex estão em posição privilegiada para apoiar este trabalho com as suas capacidades analíticas, nomeadamente através de um acesso mais alargado ao Sistema de Informação Schengen (SIS), desde que os Estados-Membros lhes forneçam sistematicamente dados em bruto de elevada qualidade.

A Presidência apela a um quadro global da UE em matéria de gestão da informação, a fim de assegurar que todas as informações existentes necessárias sejam acessíveis, processadas e trocadas de forma rápida e eficiente, de modo a que possam dar origem a ações baseadas na obtenção de informações.

3. Cooperação multidisciplinar transfronteiras

O reforço da cooperação operacional intersetorial através da redução das duplicações e do aumento da coordenação eficaz é essencial para o êxito da ação. Devido à natureza transversal e em constante evolução das várias ameaças à segurança, como as armas QBRN e as atividades híbridas, as medidas tomadas para reagir e prevenir estas atividades requerem uma abordagem horizontal, tendo simultaneamente em conta a competência dos Estados-Membros em matéria de segurança nacional. É necessária uma abordagem integrada e coerente para garantir uma cooperação operacional multidisciplinar, que vá além da cooperação transfronteiras em matéria de aplicação da lei e envolva também outras autoridades, como os intervenientes da proteção civil.

As diferenças entre os processos de tomada de decisões, a legislação e os modelos operacionais nacionais representam grandes desafios para a cooperação operacional transfronteiras. Além disso, as inconsistências entre as práticas nacionais de recolha e tratamento de dados, resultantes das diferenças entre os Estados-Membros em termos de sistemas administrativos, soluções técnicas e disposições funcionais, entravam a cooperação transfronteiras. Outro desafio consiste em identificar e eliminar os obstáculos à cooperação operacional entre as autoridades responsáveis pela aplicação da lei, como as radiofrequências incompatíveis em zonas fronteiriças, as barreiras linguísticas e a necessidade de complementar as bases jurídicas existentes com acordos bilaterais mais pormenorizados. Em situações urgentes, as entidades nacionais podem não estar conscientes da gama de alternativas operacionais existentes – que estão fragmentadas em vários instrumentos da UE – e dos canais de intercâmbio de informações disponíveis.

A cooperação operacional multidisciplinar entre as autoridades responsáveis pela aplicação da lei deverá ser intensificada através do desenvolvimento e da utilização de novos métodos de trabalho em conjunto e do intercâmbio de informações, com base em novas aplicações e instrumentos tecnológicos. Estas aplicações podem incluir, por exemplo, sistemas autónomos não tripulados, tecnologias de reconhecimento automático de matrículas ou interfaces de pesquisa única para as bases de dados disponíveis. Existe, atualmente, um contexto e uma oportunidade favoráveis para prosseguir e apoiar esta evolução.

A aprendizagem e a formação ao longo da vida são ainda mais importantes para explorar todas as possibilidades existentes e estar preparado para os desafios futuros. A formação ministrada pelas agências da UE deve ser utilizada de forma eficiente. Ao mesmo tempo, há que assegurar que as atividades das agências da UE se complementam entre si e que as sobreposições são eliminadas.

Devemos ter em conta as diferenças regionais e as especificidades nacionais, procurando simultaneamente uma cultura comum de aplicação da lei entre as autoridades competentes da UE. A melhoria das competências linguísticas, a aprendizagem mútua sobre as diferentes culturas e o intercâmbio de boas práticas ajudam a compreender melhor as diferenças regionais e culturais e a alcançar o objetivo comum.

Os acordos bilaterais e multilaterais continuam a ser importantes para a cooperação local e regional, e é necessária flexibilidade para garantir o respeito pela diversidade regional e pelos diferentes interesses operacionais. A definição da divisão de responsabilidades, da competência jurisdicional e da soberania deve ser tida em conta em quaisquer desenvolvimentos futuros.

As agências JAI da UE continuam a desempenhar um papel importante no apoio aos esforços dos Estados-Membros no âmbito dos respetivos mandatos. É amplamente aceite que uma verdadeira cooperação transfronteiras entre as autoridades dos Estados-Membros, fortemente apoiada pelas agências competentes da UE, é a forma mais viável de avançar no sentido de uma União da Segurança e de combater, de forma sustentável, as ameaças existentes e as novas ameaças num ambiente em constante evolução⁵.

A evolução futura no domínio da segurança interna exigirá, assim, a manutenção de um papel ativo das agências, envolvendo o aumento previsto do volume de tarefas existentes e de novas responsabilidades decorrentes das necessidades políticas e operacionais. Tendo em conta as limitações de recursos, é necessário debater o contexto em que as agências podem mais eficazmente criar valor acrescentado como, por exemplo, domínios em que os Estados-Membros possam ter de obter acesso a recursos ou a equipamento técnico através da partilha de recursos, em que as capacidades de análise de dados possam ser reforçadas, ou em que possa ser prestado um apoio operacional mais forte. Deverão ser estabelecidos critérios transparentes para decidir quais os domínios em que os Estados-Membros necessitam de maior apoio, tendo em conta os progressos tecnológicos e as necessidades específicas de materiais ou de outros recursos. Ao desenvolver o papel das agências, deverá procurar-se uma solução equilibrada que tenha em conta as necessidades dos Estados-Membros. É essencial aplicar uma abordagem coordenada e holística, a fim de reforçar as competências principais e os pontos fortes de cada agência, bem como criar valor acrescentado de uma forma eficaz em termos de custos e sem criar sobreposições de tarefas e funções.

É necessário aprofundar a partilha de informações e a cooperação das agências, uma vez que as ameaças existentes e emergentes no domínio da segurança interna estão a tornar-se cada vez mais complexas e de natureza transfronteiras. É também necessária uma interação mais eficaz com os intervenientes privados no quadro da partilha de informações. Em especial, é necessário avaliar a base jurídica da Europol para solicitar e receber dados pessoais diretamente de organismos privados⁶.

⁵ O papel das agências da UE foi especificamente abordado nas reuniões informais do COSI e do Conselho em julho, WK 13271/19 e WK 13266/19, e tem sido um tema transversal em todos os debates.

⁶ Os debates sobre a cooperação da Europol com organismos privados tiveram lugar no Grupo da Aplicação da Lei: docs. 10494/19, 11832/19, 12858/1/19.

A fim de reforçar a abordagem multidisciplinar da Europol em matéria de aplicação da lei a longo prazo, a cooperação entre as autoridades aduaneiras e a Europol deverá continuar a ser desenvolvida através do aumento do número de agentes de ligação aduaneiros na Europol, da promoção da utilização da rede SIENA pelas autoridades aduaneiras em todos os Estados-Membros da UE e do reforço do intercâmbio regular e estruturado de informações entre as partes, incluindo a gestão dos riscos e os dados dos serviços de informações. Um objetivo a curto prazo deverá ser o reforço da contribuição e da integração das autoridades aduaneiras no que diz respeito à execução dos planos de ação operacionais da EMPACT. Tais ações darão continuidade ao desenvolvimento positivo dos últimos anos da cooperação entre as autoridades aduaneiras e a Europol.

É necessário abordar os desafios da cooperação entre a União Europeia e a Interpol. É importante que as bases de dados que servem de principais fontes de informação para a cooperação policial com países terceiros continuem a ser utilizadas de forma eficaz no futuro pelas autoridades dos Estados-Membros da UE. Ao mesmo tempo, a legislação aplicável em matéria de proteção de dados tem, naturalmente, de ser plenamente respeitada.

A Presidência sublinha a necessidade de rever o quadro jurídico para a cooperação transfronteiras no domínio da aplicação da lei e o mandato da Europol, a fim de os adaptar às realidades atuais e aos desafios futuros. O desenvolvimento de uma cultura comum de aplicação da lei entre as autoridades responsáveis pela aplicação da lei da UE deverá continuar a ser apoiado.

4. Abordagem global da segurança

Prevê-se uma série de tendências e desenvolvimentos num futuro próximo, que afetarão o cenário das ameaças na UE. A criminalidade continua a ser impulsionada pela procura, bem como pela disponibilidade de oportunidades para iniciativas criminosas. Além disso, as alterações a nível da segurança nas regiões vizinhas e as várias formas de radicalização violenta na Europa continuam a representar uma ameaça para a nossa segurança interna. Uma abordagem global da segurança, com melhor coordenação, recursos e capacidades tecnológicas, exige um melhor conhecimento das situações e uma preparação para diferentes desafios.

As autoridades responsáveis pela aplicação da lei, a proteção civil e outras autoridades competentes deverão continuar a desenvolver o seu grau de preparação para combater as ameaças híbridas. A cooperação na prevenção e na luta contra as ameaças híbridas entre as autoridades nacionais competentes, com base nos respetivos mandatos, bem como entre as instituições, órgãos e agências da UE em matéria de correlação entre a segurança interna e externa, deverá ser continuamente melhorada e integrada. Ao mesmo tempo, é importante aumentar as sinergias e evitar a duplicação de esforços, nomeadamente através de métodos de trabalho horizontais, do aumento do intercâmbio de informações e da formação e de exercícios transversais a vários setores.

Salienta-se a necessidade de prosseguir os debates sobre a dimensão interna das ameaças híbridas, em particular sobre os papéis das agências JAI no reforço das capacidades da UE e dos Estados-Membros para identificar ações híbridas e respetivas fontes.

Além disso, a luta eficaz contra a desinformação requer uma abordagem global. Neste sentido, deverá ser considerada a participação das autoridades responsáveis pela aplicação da lei, incluindo nos mecanismos existentes da UE, como o Sistema de Alerta Rápido. As autoridades responsáveis pela aplicação da lei reforçam a resiliência da UE e dos seus Estados-Membros, e a luta contra a desinformação deve ser tido em conta⁷. A Presidência salienta a necessidade de uma melhor utilização dos instrumentos existentes e do reforço da coordenação holística a nível da UE. O apoio das agências JAI aos Estados-Membros deve também ser abordado neste contexto.

A utilização da tecnologia e da Internet na organização de atividades criminosas continuará a aumentar. Por exemplo, prevê-se um aumento da utilização de plataformas em linha tanto na "Internet visível" como na "Internet obscura" para o comércio de um vasto leque de bens ilícitos. Por outro lado, o espaço em linha pode ser utilizado eficazmente para a radicalização, o recrutamento e o incitamento à violência. A divulgação em linha de conteúdos terroristas e de abuso de crianças deverá ser prevenida eficazmente, e os conteúdos em causa deverão ser rapidamente suprimidos.

⁷ Ameaças híbridas e segurança interna: Comunicação estratégica para a aplicação da lei e luta contra a desinformação (Doc. 11831/19).

Além disso, destaca-se o papel da prevenção da radicalização violenta enquanto parte integrante de uma abordagem global da luta contra o terrorismo. A colaboração e o apoio aos profissionais no terreno continuam a ser essenciais para prevenir e combater o extremismo violento. É necessário combater o extremismo violento em todas as suas formas, quer tenha motivações políticas ou ideológicas. Doravante, a tónica no combate e na prevenção do extremismo violento e do terrorismo deverá continuar a alicerçar-se numa abordagem assente numa base alargada, tendo igualmente em conta as tendências emergentes no âmbito do extremismo violento.

A ameaça que o extremismo violento e o terrorismo de direita representam tem de ser combatida através da definição de um melhor quadro geral da situação, da partilha contínua de boas práticas, da cooperação com os países terceiros mais importantes e do combate à disseminação de conteúdos ilegais de extremismo de direita, em linha e fora de linha. O problema do regresso dos combatentes terroristas estrangeiros deverá ser abordado, nomeadamente através de uma utilização mais eficiente do SIS.

A Presidência sublinha a necessidade de uma abordagem global da segurança, que integre toda a sociedade, a fim de fazer face às várias ameaças à segurança interna. Sublinha-se a importância de trabalhar de forma mais estratégica, coordenada e coerente em todos os setores políticos relevantes.

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