Conselho
da União Europeia

Bruxelas, 3 de abril de 2025
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	2 de abril de 2025
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2025) 148 final
Assunto:	COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES sobre a ProtectEU: uma Estratégia Europeia de Segurança Interna

Envia-se em anexo, à atenção das delegações, o documento COM(2025) 148 final.

Anexo: COM(2025) 148 final

COMISSÃO
EUROPEIA

Estrasburgo, 1.4.2025
COM(2025) 148 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

sobre a ProtectEU: uma Estratégia Europeia de Segurança Interna

1. ProtectEU: uma Estratégia Europeia de Segurança Interna

A segurança é o alicerce de todas as nossas liberdades. A democracia, o Estado de direito, os direitos fundamentais, o bem-estar dos europeus, a competitividade e a prosperidade dependem da nossa capacidade de garantir um nível básico de segurança. Na nova era de ameaças à segurança em que vivemos, a capacidade dos Estados-Membros de garantir a segurança dos seus cidadãos depende, mais do que nunca, de uma **abordagem europeia unificada que proteja a nossa segurança interna**. Numa conjuntura geopolítica em evolução, a Europa deve continuar a honrar a sua promessa duradoura de paz.

Já foram dados os primeiros passos para a construção de um aparelho de segurança europeu. Na última década, dotámos a União de melhores mecanismos coletivos de ação nos domínios da cooperação policial e judiciária, da segurança das fronteiras, da luta contra a criminalidade grave e organizada, da luta contra o terrorismo e o extremismo violento e da proteção das infraestruturas físicas e digitais críticas da UE. A correta aplicação da legislação anteriormente adotada e das políticas desenvolvidas continua a ser fundamental.

A natureza das ameaças atuais e a ligação intrínseca entre a segurança interna e externa da UE obrigam-nos a ir mais longe.

O cenário de ameaças é preocupante. Tornou-se mais difícil distinguir entre **ameaças híbridas** e guerra aberta. A Rússia tem vindo a travar uma campanha híbrida em linha e fora de linha contra a UE e os seus parceiros, com o intuito de perturbar e comprometer a coesão social e os processos democráticos e de testar a solidariedade da UE para com a Ucrânia. Estados estrangeiros hostis e agentes patrocinados por Estados procuram infiltrar e perturbar as nossas cadeias de abastecimento e infraestruturas críticas, roubar dados sensíveis e posicionar-se de forma a causar o máximo de perturbações no futuro. Utilizam o crime como um serviço e criminosos como intermediários. Além disso, as nossas dependências de países terceiros em termos de cadeias de abastecimento tornam-nos mais vulneráveis a campanhas híbridas por parte de Estados hostis.

Na Europa, proliferam poderosas **redes de criminalidade organizada**, que se desenvolvem em linha e invadem a nossa economia, afetando a nossa sociedade, como salientado na Avaliação da Ameaça da Criminalidade Grave e Organizada da União Europeia (SOCTA), recentemente apresentada pela Europol[1]. Quando a criminalidade organizada se instala numa comunidade ou num setor económico, erradicá-la torna-se uma batalha difícil: um terço das redes criminosas mais perigosas estão ativas há mais de dez anos. As criptomoedas e os sistemas financeiros paralelos facilitam o branqueamento de capitais e a ocultação dos produtos do crime.

A **ameaça terrorista continua a ser uma realidade na Europa**. As crises regionais fora da UE criam um efeito dominó, dando nova motivação aos terroristas de todo o espetro ideológico para recrutarem, mobilizarem ou reforçarem as suas capacidades. Estes dirigem os seus esforços de radicalização e recrutamento especificamente aos setores mais vulneráveis das nossas sociedades e, concretamente, a determinados jovens. Inspiram ataques de «lobos solitários» e um aumento do extremismo antissistema, com o objetivo de perturbar a ordem jurídica democrática.

Os **avanços tecnológicos** notáveis estão a dar origem a ferramentas essenciais para reforçar o nosso aparelho de segurança. No entanto, os ciberataques e a manipulação da informação por parte de agentes estrangeiros são cada vez mais frequentes, explorando novas tecnologias como a inteligência artificial. As crianças, os jovens e os idosos são particularmente vulneráveis em

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

linha e a propagação do ódio no mundo virtual ameaça a liberdade de expressão e a coesão social.

As nossas vidas tornaram-se menos seguras, e os europeus sentem-no cada vez mais. Quando questionados sobre o futuro, 64 % tendem a afirmar-se preocupados com a segurança da UE, o que reflete uma deterioração da sua **perceção da segurança e proteção na UE**[2]. As empresas estão também cada vez mais preocupadas: as informações incorretas e a desinformação, as atividades ilícitas e criminosas e a ciberespionagem figuram entre os dez principais riscos identificados no relatório do Fórum Económico Mundial de 2025 sobre os riscos à escala mundial[3].

Os europeus devem **poder viver sem medo**, seja na rua, em casa, em locais públicos, no metro ou na Internet. A proteção das pessoas, sobretudo das mais vulneráveis a ataques, como as crianças, as mulheres e as minorias, incluindo as comunidades judaica e muçulmana, é central no trabalho da UE em matéria de segurança. Este trabalho é essencial para construir sociedades resilientes e coesas.

A Comissão está a definir uma **Estratégia Europeia de Segurança Interna** para combater mais eficazmente as ameaças nos próximos anos. Com um conjunto de instrumentos jurídicos mais eficazes, uma cooperação aprofundada e uma maior partilha de informações, reforçaremos a nossa resiliência e a nossa capacidade coletiva para antecipar, prevenir, detetar e responder eficazmente às ameaças à segurança. Uma abordagem unificada da segurança interna pode ajudar os Estados-Membros a tirar partido do poder da tecnologia para fortalecer, e não enfraquecer, a segurança e, ao mesmo tempo, promover um espaço digital seguro para todos. Além disso, apoia uma resposta comum dos Estados-Membros às mudanças políticas e económicas globais que afetam a segurança interna da União.

Esta estratégia assenta em **três princípios** e integra no seu cerne o respeito pelo Estado de direito e pelos direitos fundamentais.

Em primeiro lugar, declara a ambição de uma mudança de cultura em matéria de segurança. Precisamos de uma **abordagem que abranja toda a sociedade** que envolva todos os cidadãos e partes interessadas, incluindo a sociedade civil, os investigadores, o meio académico e as entidades privadas. As ações no âmbito da estratégia adotam, por conseguinte, sempre que possível, uma abordagem integrada e multilateral.

Em segundo lugar, **as considerações em matéria de segurança devem ser integradas e assimiladas em toda a legislação, políticas e programas da UE**, incluindo a ação externa. A legislação, as políticas e os programas terão de ser elaborados, revistos e aplicados numa perspetiva de segurança, garantindo que são tidas em conta as considerações de segurança necessárias, a fim de promover uma abordagem coerente e abrangente da segurança.

Por último, uma Europa segura, protegida e resiliente exige **um investimento sério por parte da UE, dos seus Estados-Membros e do setor privado**. As prioridades e ações desta estratégia exigem recursos humanos e financeiros suficientes para garantir a sua execução. Como previsto na comunicação intitulada Roteiro para o próximo quadro financeiro plurianual[4], a Europa terá de aumentar a despesa pública em segurança e promover a investigação e o investimento no domínio da segurança, reforçando a sua autonomia estratégica.

[2] Eurobarómetro Flash FL550: Dificuldades e prioridades da UE.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, p. 17.
[4] COM(2025) 46 final.

A presente estratégia complementa a **Estratégia para uma União da Preparação**[5], que define uma abordagem integrada que abranja todos os riscos tendo em vista a preparação para conflitos, catástrofes naturais e de origem humana e crises, e o **Livro Branco Conjunto sobre a Prontidão da Defesa Europeia 2030**[6], que apoia o desenvolvimento e a aquisição de capacidades de defesa a nível da UE para dissuadir adversários estrangeiros. A Comissão proporá igualmente um **Escudo Europeu da Democracia** para reforçar a resiliência democrática na UE. Em conjunto, estas iniciativas definem uma visão para uma UE segura, protegida e resiliente.

Uma nova governação europeia da segurança interna

A Comissão trabalhará em estreita colaboração com os Estados-Membros e com as agências da UE para melhorar a abordagem da UE em matéria de segurança interna, tanto a nível estratégico como operacional.

Este processo passará por:

- **identificar sistematicamente as potenciais implicações em matéria de segurança e preparação de iniciativas novas e revistas da Comissão, desde o início e ao longo do processo de negociação;**
- **reuniões regulares do Grupo de Projeto da Comissão para a Segurança Interna Europeia, apoiadas por uma colaboração intersetorial estratégica a nível da Comissão;**
- **apresentações das análises de ameaças relacionadas com a segurança interna para apoiar o trabalho do colégio de comissários reunido em «formato de segurança»;**
- **debates com os Estados-Membros no Conselho sobre a evolução dos desafios em matéria de segurança interna com base na análise das ameaças e no intercâmbio sobre as principais prioridades políticas;**
- **apresentação regular de relatórios ao Parlamento Europeu e ao Conselho para acompanhar e apoiar a execução sistemática das principais iniciativas em matéria de segurança.**

2. Integração do conhecimento da situação e da análise das ameaças

Dotaremos a UE de novas formas de partilhar e combinar informações e de apresentar uma análise regular das ameaças à segurança interna da UE, contribuindo para uma avaliação abrangente dos riscos e das ameaças.

A segurança começa com uma **antecipação eficaz**. A UE deve basear-se num conhecimento da situação e numa análise das ameaças abrangentes, suficientemente autónomos e atualizados. A informação acionável, que os Estados-Membros são incentivados a reforçar através da Capacidade Única de Análise de Informações (SIAC), enquanto ponto de entrada único das informações dos Estados-Membros, é vital para avaliar e combater as ameaças, sendo tida em conta, em última análise, na adoção de medidas políticas e legislativas[7]. Temos de tirar partido das **análises baseadas em informações** e das **avaliações das ameaças** a nível da UE de forma mais eficaz e colaborativa.

[5] JOIN(2025) 130 final.
[6] JOIN(2025) 120 final.
[7] *Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness (Mais seguros juntos: reforçar a preparação e a prontidão civil e militar da Europa)*, p. 23.

Com base nas várias avaliações dos riscos e das ameaças realizadas a nível da UE e em setores específicos[8], a Comissão elaborará **análises regulares das ameaças à segurança interna da UE**, a fim de identificar os principais desafios em matéria de segurança, com vista a fundamentar as prioridades políticas. Estas medidas ajudarão a desenvolver uma política de segurança interna ágil e reativa que dê uma resposta eficaz às ameaças em evolução, proteja melhor as pessoas e as empresas contra ataques e permita intervenções estratégicas específicas em tempo útil. Estas análises das ameaças para a segurança interna da UE contribuirão igualmente para a **avaliação global dos riscos e ameaças a nível da UE (transetorial e multirriscos)** desenvolvida pela Comissão e pela alta representante, tal como previsto na Estratégia para uma União da Preparação.

A confiança e o tratamento seguro são essenciais para a partilha de informações, o que exige infraestruturas fiáveis e seguras. As instituições, órgãos e organismos da UE têm de garantir que têm capacidade para utilizar **canais de comunicação seguros** para o intercâmbio de informações sensíveis e classificadas entre si e com os Estados-Membros. Os investimentos em **sistemas seguros interoperáveis** e tecnologias fiáveis reforçarão a autonomia da UE e a sua capacidade para gerir crises e assegurar a resiliência operacional. Neste contexto, a Comissão insta os colegisladores a concluírem as negociações sobre a **proposta de regulamento relativo à segurança da informação nas instituições, órgãos e organismos da União**, nomeadamente para assegurar um quadro comum para o tratamento de informações sensíveis não classificadas e de informações classificadas[9].

A fim de assegurar a sua própria segurança operacional e conhecimento da situação, a Comissão reverá o seu quadro de governação da segurança institucional e criará um **Centro Integrado de Operações de Segurança (CIOS)** para proteger as pessoas, os ativos físicos e as operações em todos os locais da Comissão. A Comissão reforçará igualmente as suas capacidades operacionais e analíticas para identificar e atenuar as ameaças híbridas.

Em consonância com a Estratégia para uma União da Preparação, as considerações em matéria de preparação e segurança serão integradas e assimiladas na legislação, nas políticas e nos programas da UE. Ao elaborar ou rever legislação, políticas ou programas numa perspetiva de preparação e segurança, a Comissão identificará sistematicamente os potenciais impactos da opção política preferida em matéria de preparação e segurança. Esta ação será apoiada por uma formação regular dos decisores políticos da Comissão.

Para apoiar os Estados-Membros, a Comissão debaterá com o Conselho a evolução dos desafios em matéria de segurança interna e as principais prioridades políticas e informá-lo-á regularmente sobre a execução da estratégia. Além disso, a Comissão manterá o Parlamento Europeu e as partes interessadas informados e envolvidos em todas as ações relevantes.

Principais ações

A Comissão irá:

- **desenvolver e apresentar análises regulares das ameaças para os diferentes desafios de segurança interna da UE.**

[8] As avaliações setoriais das ameaças que contribuirão para fundamentar esta análise das ameaças incluem a Avaliação da Ameaça da Criminalidade Grave e Organizada da União Europeia (SOCTA), o Relatório sobre a Situação e Tendências do Terrorismo na Europa (TE-SAT), o relatório conjunto de avaliação da cibersegurança (JCAR) e futuras avaliações das ameaças, riscos e métodos de branqueamento de capitais e de financiamento do terrorismo a levar a cabo pela Comissão e pela Autoridade para o Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo.

[9] COM(2022) 119 final.

Os Estados-Membros são convidados a:

- **reforçar a partilha de informações com a SIAC e assegurar uma melhor partilha de informações com as agências e organismos da UE.**

O Parlamento Europeu e o Conselho são incentivados a:

- **concluir as negociações sobre a proposta de regulamento relativo à segurança da informação nas instituições, órgãos e organismos da União.**

3. Reforço das capacidades de segurança da UE

Desenvolveremos novos instrumentos para a aplicação da lei, como uma Europol renovada, e melhores meios para coordenar e garantir o intercâmbio seguro e o acesso lícito aos dados.

Para combater eficazmente as ameaças em constante evolução, a UE deve reforçar as suas capacidades de segurança e promover a inovação. Enquanto principais intervenientes na luta contra as ameaças à segurança interna, as autoridades policiais e judiciais precisam dos instrumentos e das capacidades operacionais certos para agirem de forma rápida e eficaz. É importante que estas autoridades possam comunicar e coordenar-se além-fronteiras e entre serviços, a fim de prevenir, detetar, investigar e instaurar ações penais de forma eficiente.

Agências e organismos da UE para a segurança interna

As agências e organismos da UE nos domínios da justiça, dos assuntos internos e da cibersegurança desempenham um papel fundamental na arquitetura de segurança da UE – um papel que continua a crescer à medida que as suas responsabilidades se alargam.

Atualmente, 25 anos após a sua criação, a **Europol** é mais central do que nunca para o quadro de segurança da UE. Apoia investigações transnacionais complexas, facilita o intercâmbio de informações, desenvolve instrumentos inovadores para o policiamento e disponibiliza conhecimentos especializados avançados para a aplicação da lei. No entanto, existem vários fatores que impedem a Europol de explorar todo o seu potencial operacional no apoio às atividades de investigação e operacionais de combate à criminalidade transfronteiras: estes vão desde a insuficiência de recursos até ao facto de o seu atual mandato não abranger novas ameaças à segurança, como a sabotagem, as ameaças híbridas ou a manipulação da informação. É por esta razão que a Comissão proporá **uma revisão ambiciosa do mandato da Europol**, com o objetivo de a transformar numa agência policial verdadeiramente operacional, capaz de apoiar melhor os Estados-Membros. O objetivo é reforçar as competências tecnológicas e as capacidades da Europol para apoiar as autoridades policiais nacionais, intensificar a coordenação com outras agências e organismos e com os Estados-Membros, fortalecer as parcerias estratégicas com os países parceiros e com o setor privado, e assegurar uma supervisão reforçada da Europol.

Além disso, a Comissão trabalhará no sentido de continuar a **melhorar a eficácia e a complementaridade das agências e organismos da UE em prol da segurança interna e de reforçar a cooperação integrada** entre os mesmos.

O mandato da **Eurojust** será avaliado e reforçado para uma cooperação judiciária mais eficaz, melhorando a complementaridade e a cooperação com a Europol. Este processo inclui o reforço da eficiência da Eurojust e da sua capacidade para prestar apoio e análise proativos às autoridades judiciárias dos Estados-Membros. Além disso, tendo em conta a competência exclusiva da **Procuradoria Europeia** para investigar e exercer ação penal relativamente a crimes que lesem os interesses financeiros da União, a Comissão analisará a melhor forma de

melhorar a capacidade da Procuradoria Europeia para proteger os fundos da União. Essa melhoria passará pelo reforço da cooperação entre a Procuradoria Europeia e a Europol.

O **intercâmbio de informações eficiente e seguro entre as agências** é crucial para a cooperação. A Europol e a Frontex precisam de um intercâmbio mútuo de informações rápido, inclusive para fins operacionais, dando seguimento à Declaração Conjunta de janeiro de 2024[10]. A **eu-LISA** tem um papel central na garantia da segurança do armazenamento e da disponibilidade de dados para uma melhor coordenação e um intercâmbio de informações mais eficiente entre as agências. A **Agência dos Direitos Fundamentais da UE** disponibiliza conhecimentos especializados em matéria de proteção dos direitos fundamentais no desenvolvimento e na execução de políticas de segurança.

A **Autoridade para o Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo (ACBC)** foi habilitada a cruzar informações, com base em respostas positivas/negativas, com as informações disponibilizadas pela Europol, pela Procuradoria Europeia, pela Eurojust e pelo Organismo Europeu de Luta Antifraude (OLAF), com o objetivo de realizar análises conjuntas de casos transfronteiriços.

A **ENISA** desempenha um papel central na aplicação da legislação europeia em matéria de cibersegurança. Na próxima **revisão do Regulamento Cibersegurança**, a Comissão avaliará o seu mandato e proporá que seja modernizado para reforçar o seu valor acrescentado da UE.

A cooperação entre as autoridades aduaneiras e outros serviços de polícia será reforçada com a proposta de criação da **Autoridade Aduaneira da UE** e da **Plataforma de Dados Aduaneiros da UE** no âmbito do pacote da reforma aduaneira da UE. As informações provenientes da futura plataforma e os dados correspondentes da Europol, da Eurojust, da Procuradoria Europeia, do OLAF, da ACBC e da Frontex, no âmbito das respetivas competências, reforçarão a análise conjunta e contribuirão para uma maior coerência das atividades operacionais, sobretudo nas fronteiras externas. A Comissão incentiva os colegisladores a concluírem rapidamente as negociações sobre a reforma aduaneira da UE e continuará a prestar-lhes assistência para o efeito.

O reforço da complementaridade entre a Procuradoria Europeia, o OLAF, a Europol, a Eurojust, a ACBC e a eventual Autoridade Aduaneira da UE basear-se-á igualmente nos resultados da revisão em curso da **arquitetura antifraude da UE**. A segurança interna pode beneficiar desta abordagem holística, centrada numa melhor utilização dos meios criminais e administrativos, na interoperabilidade dos sistemas informáticos e numa cooperação reforçada.

Comunicações críticas

Atualmente, os **sistemas de comunicações críticas**[11] são operados, na maioria dos casos, isoladamente a nível nacional. Isto significa que, muitas vezes, os elementos de primeira intervenção deixam de conseguir comunicar com os seus homólogos quando atravessam a fronteira para outros Estados-Membros. Nalguns Estados-Membros, existem também limitações nas comunicações entre diferentes tipos de elementos de primeira intervenção (por exemplo, entre a polícia e as ambulâncias). As normas da maioria destes sistemas não satisfazem os requisitos atuais em termos de funcionalidade e resiliência, o que limita significativamente a capacidade de reação dos elementos de primeira intervenção, sobretudo em contextos transfronteiriços.

Para reforçar a capacidade de reação da UE em situações de crise, a Comissão proporá legislação com vista à criação de um **Sistema Europeu de Comunicações Críticas (EUCCS)**

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

[11] Ou seja, as redes utilizadas pela polícia, guardas de fronteira, autoridades aduaneiras, proteção civil, bombeiros, equipas de emergência médica e outros intervenientes essenciais para a segurança pública.

que interligue a nova geração de sistemas de comunicações críticas dos Estados-Membros. O objetivo é que o EUCCS assente em três pilares estratégicos: mobilidade operacional, forte resiliência e autonomia estratégica. A iniciativa do EUCCS estabelecerá requisitos harmonizados e contribuirá para a modernização dos sistemas de comunicações críticas dos Estados-Membros, permitindo-lhes funcionar sem descontinuidades. Alargará igualmente a cobertura do sistema através do futuro sistema multiorbital IRIS[212]. A UE financiará projetos para desenvolver as capacidades técnicas necessárias à execução do EUCCS recorrendo principalmente a fornecedores de tecnologia europeus, a fim de promover a autonomia estratégica da UE neste setor sensível.

Acesso lícito aos dados

As autoridades policiais e judiciárias têm de poder investigar e atuar contra a criminalidade. Atualmente, quase todas as formas de criminalidade grave e organizada deixam uma pegada digital[13]. Cerca de 85 % das investigações criminais dependem agora da capacidade dos serviços de polícia de acederem a informações digitais[14].

O **Grupo de Alto Nível sobre o acesso aos dados para uma aplicação eficaz da lei** salientou, no seu relatório final[15], que, ao longo da última década, as autoridades policiais e judiciárias têm perdido terreno para os criminosos, que utilizam ferramentas e produtos disponibilizados por fornecedores de outras jurisdições que tomaram medidas para impedir a cooperação com pedidos legítimos dessas autoridades em processos penais individuais. Assim, é essencial uma cooperação sistemática entre os serviços de polícia e as entidades privadas, incluindo os prestadores de serviços, nos futuros esforços para neutralizar as redes e criminosos mais perigosos, tanto dentro como fora da União.

À medida que a digitalização se torna mais omnipresente e constitui uma fonte crescente de novos instrumentos para os criminosos, torna-se indispensável um quadro de acesso aos dados que responda à necessidade de aplicar a lei e proteger os nossos valores. Ao mesmo tempo, é essencial garantir que os sistemas digitais continuam protegidos contra o acesso não autorizado, para preservar a cibersegurança e garantir a proteção contra as ameaças à segurança emergentes. Estes quadros de acesso devem também respeitar os direitos fundamentais, assegurando, nomeadamente, a devida proteção da privacidade e dos dados pessoais.

Nos últimos anos, a UE tomou medidas para combater **a criminalidade na Internet e facilitar o acesso à prova digital para todos os crimes**, com a adoção de regras em matéria de prova eletrónica que serão plenamente aplicáveis a partir de agosto de 2026[16]. Estas serão complementadas por instrumentos internacionais para o intercâmbio de informações e de provas. A Comissão proporá em breve a assinatura e a celebração da nova **Convenção das Nações Unidas contra o Cibercrime**.

Para dar seguimento às recomendações do Grupo de Alto Nível[17], a Comissão apresentará, no primeiro semestre de 2025, um **roteiro com as medidas legislativas e práticas** que propõe

[12] Infraestrutura da UE para a Resiliência, a Interconectividade e a Segurança por Satélite.
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[14] https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52019PC0070.
[15] *Concluding report of the High-Level Group on access to data for effective law enforcement* (Relatório final do Grupo de Alto Nível sobre o acesso aos dados para uma aplicação eficaz da lei) de 15.11.2024, 4802e306-c364-4154-835b-e986a9a49281_en.
[16] Regulamento (UE) 2023/1543 do Parlamento Europeu e do Conselho, de 12 de julho de 2023, relativo às ordens europeias de produção e às ordens europeias de conservação para efeitos de prova eletrónica em processos penais e para efeitos de execução de penas privativas de liberdade na sequência de processos penais (JO L 191 de 28.7.2023).
[17] Conclusões do Conselho sobre o acesso aos dados para uma aplicação eficaz da lei (12 de dezembro de 2024) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/pt/pdf.

adotar **para assegurar o acesso lícito e efetivo aos dados**. No seguimento deste roteiro, a Comissão dará prioridade a uma avaliação do impacto das **regras de conservação de dados** a nível da UE e à redação de um **roteiro tecnológico sobre cifragem**, a fim de identificar e avaliar soluções tecnológicas que permitam às autoridades policiais aceder a dados cifrados de forma lícita, salvaguardando a cibersegurança e os direitos fundamentais.

Cooperação operacional

A Comissão trabalhará com os Estados-Membros, as agências e organismos da UE e com países parceiros para reforçar a cooperação operacional, o que é essencial para uma abordagem mais eficaz da luta contra a criminalidade organizada transnacional e o terrorismo.

Enquanto principal quadro da UE para a ação conjunta contra a criminalidade grave e organizada, a **Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas (EMPACT)** obteve resultados operacionais substanciais. O próximo ciclo da EMPACT, no período de 2026-2029, constitui uma oportunidade para continuar a reforçar este quadro. Para neutralizar as redes e criminosos mais perigosos, a União deve racionalizar e centrar os seus esforços nas prioridades mais prementes, reforçando os compromissos dos Estados-Membros e assegurando uma utilização eficaz dos recursos.

Para o efeito, a Comissão trabalhará com as Presidências do Conselho e os Estados-Membros para **maximizar o potencial da EMPACT e abordar as principais prioridades para o próximo ciclo da EMPACT, no período de 2026-2029.** Nestes domínios prioritários, são necessárias informações sobre as redes criminosas mais perigosas, investigações conjuntas e unidades operacionais, bem como uma resposta judicial robusta, incluindo uma abordagem de seguimento da pista do dinheiro. Além disso, a União tem de combater o recrutamento e a infiltração de criminosos, reforçando a cooperação e a formação multiagências e a nível internacional em matéria de aplicação da lei.

A Comissão apoiará igualmente outras formas de **cooperação operacional transfronteiriça em matéria de aplicação da lei entre os Estados-Membros e os países associados a Schengen**. O espaço Schengen, sem controlos nas fronteiras internas, exige uma estreita cooperação e o intercâmbio de informações entre as autoridades policiais dos Estados-Membros, a fim de assegurar um elevado nível de segurança interna. Atualmente, as autoridades policiais continuam a enfrentar desafios durante a vigilância ou a realização de intervenções urgentes a nível transfronteiriço[18], e a luta contra as ameaças híbridas exige também uma cooperação transfronteiras reforçada. Deve ser criado um **grupo de alto nível sobre o futuro da cooperação operacional em matéria de aplicação da lei**, com a missão de desenvolver uma visão estratégica comum.

A eficácia da cooperação transfronteiriça requer também um intercâmbio eficiente de dados entre as autoridades policiais. Depois de implantada, a **arquitetura de interoperabilidade** proporcionará às autoridades policiais e à Europol acesso efetivo a informações cruciais. Ao mesmo tempo, a UE e os seus Estados-Membros devem dar prioridade ao intercâmbio bilateral e multilateral de informações, através da aplicação jurídica e técnica do **Regulamento Prüm II**[19], em cooperação com a eu-LISA e com a Europol. Desta forma, será possível um

[18] Como referido na avaliação, pela Comissão, da colocação em prática, por parte dos Estados-Membros, da Recomendação (UE) 2022/915 do Conselho, de 9 de junho de 2022, sobre a cooperação operacional em matéria de aplicação da lei (5909/25).

[19] Regulamento (UE) 2024/982 do Parlamento Europeu e do Conselho, de 13 de março de 2024, relativo à consulta e ao intercâmbio automatizados de dados para efeitos de cooperação policial e que altera as Decisões 2008/615/JAI e 2008/616/JAI do Conselho e os Regulamentos (UE) 2018/1726, (UE) 2019/817 e (UE) 2019/818 do Parlamento Europeu e do Conselho (Regulamento «Prüm II») (JO L, 2024/982, 5.4.2024).

intercâmbio automatizado seguro de impressões digitais, perfis de ADN, dados de registo de veículos, imagens faciais e registos criminais através dos encaminhadores da UE. A nível nacional, os Estados-Membros têm de aplicar a **Diretiva Intercâmbio de Informações**[20], reforçando os canais de intercâmbio de informações para um fluxo transfronteiriço de informações sem descontinuidades, assegurando simultaneamente a sua integração com os sistemas a nível da União, como a SIENA[21].

Uma cooperação transfronteiriça eficaz assenta igualmente na promoção de uma **cultura comum de aplicação da lei na UE**. A formação conjunta, os centros de excelência e os programas de mobilidade são essenciais para alcançar este objetivo. A Comissão estudará a melhor forma de a UE apoiar a formação das autoridades dos Estados-Membros, utilizando a **CEPOL** como agência da UE para a formação policial.

Reforçar a segurança nas fronteiras

O reforço da resiliência e da segurança nas fronteiras externas é crucial para combater as ameaças híbridas, como a instrumentalização da migração, para prevenir a entrada na UE de entidades e mercadorias que representem ameaças, e para combater eficazmente a criminalidade transnacional e o terrorismo. **Existem planos para o reforço do Sistema de Informação de Schengen (SIS)** em 2026, a fim de permitir que os Estados-Membros introduzam indicações sobre nacionais de países terceiros envolvidos no terrorismo, incluindo combatentes terroristas estrangeiros, e noutros crimes graves, com base em dados partilhados por países terceiros com a Europol.

A melhoria da **interoperabilidade** dos sistemas de informação de grande escala da UE facultará aos Estados-Membros informações essenciais sobre as pessoas provenientes de países terceiros que atravessam ou tencionam atravessar as fronteiras externas, ajudando as autoridades a avaliar as condições de autorização da sua entrada no território dos Estados-Membros[22]. A Comissão continuará a trabalhar em estreita colaboração com os Estados-Membros e com a eu-LISA para a rápida implantação destes sistemas, nomeadamente o **Sistema de Entrada/Saída (SES), o Sistema Europeu de Informação e Autorização de Viagem (ETIAS) e o Sistema de Informação sobre Vistos (VIS) revisto**, a fim de assegurar o seu bom funcionamento e benefícios em termos de segurança.

Para reforçar a segurança das fronteiras e a cooperação da UE face à evolução das ameaças, **a Comissão proporá o reforço da Frontex**. A Guarda Europeia de Fronteiras e Costeira deverá triplicar gradualmente, atingindo um efetivo de 30 000 pessoas. A Agência deve dispor de tecnologias avançadas de vigilância e conhecimento da situação, incluindo informações necessárias para a gestão integrada das fronteiras e acesso a serviços públicos eficientes de observação da Terra da UE para o controlo das fronteiras, a implantar até 2027. Desta forma, deverá reforçar-se a capacidade de detetar, prevenir e combater a criminalidade transnacional nas fronteiras externas, aumentando o seu apoio aos Estados-Membros na execução dos

[20] Diretiva (UE) 2023/977 do Parlamento Europeu e do Conselho, de 10 de maio de 2023, relativa ao intercâmbio de informações entre as autoridades de aplicação da lei dos Estados-Membros e que revoga a Decisão-Quadro 2006/960/JAI do Conselho (JO L 134 de 22.5.2023, p. 1).

[21] Aplicação de Intercâmbio Seguro de Informações.

[22] Concretamente, o Sistema de Entrada/Saída (SES) permitirá aos Estados-Membros identificar os nacionais de países terceiros nas fronteiras externas do espaço Schengen e registar as suas entradas e saídas, possibilitando a identificação sistemática das pessoas que ultrapassem o período de estada autorizada. Antes da chegada de um nacional de país terceiro às fronteiras externas, o Sistema Europeu de Informação e Autorização de Viagem (ETIAS) e o Sistema de Informação sobre Vistos (VIS) permitirão aos Estados-Membros avaliar previamente se a presença de um nacional de um país terceiro no território da UE representaria um risco para a segurança.

regressos, em especial no que diz respeito aos nacionais de países terceiros que representem um risco para a segurança.

A **fraude documental e de identidade** facilita a introdução clandestina de migrantes, o tráfico de seres humanos, os movimentos criminosos clandestinos e o tráfico de mercadorias ilícitas. Quando estiver operacional, o **detetor de identidades múltiplas (MID)**[23] melhorará a capacidade das autoridades nacionais para identificar pessoas que utilizem identidades múltiplas e combater a fraude de identidade. A Comissão explorará formas de reforçar a segurança dos documentos de viagem e de residência emitidos aos cidadãos da UE e aos nacionais de países terceiros. Além disso, avaliará a forma como as carteiras europeias de identidade digital, que serão introduzidas no âmbito do Regime Europeu para a Identidade Digital até ao final de 2026, podem contribuir para reforçar a segurança dos documentos de viagem e melhorar a verificação da identidade. Tal complementará as propostas relativas às credenciais de viagem digitais e à aplicação digital da UE para viagens (EU Digital Travel)[24].

As **informações de viagem** são cruciais para permitir às autoridades identificar e investigar os movimentos de criminosos, terroristas e outros indivíduos que representem ameaças à segurança. Embora exista um quadro da UE para as informações sobre voos comerciais[25], o tratamento dos dados provenientes de outros modos de transporte para fins de aplicação da lei é fragmentado. Essa fragmentação permite aos criminosos e terroristas explorar diferentes modos de transporte para atividades ilegais sem serem detetados. A Comissão trabalhará com os Estados-Membros e o setor dos transportes para **reforçar o quadro de informação sobre viagens**, através de um regime da União que exija que os operadores de voos privados recolham e transfiram dados dos passageiros, avaliando as regras de tratamento dos registos de identificação dos passageiros e estudando formas de simplificar o tratamento das informações sobre viagens marítimas. Para o transporte rodoviário, a Comissão avaliará a hipótese de alargar a utilização dos sistemas de **reconhecimento automático de matrículas** e aumentará as possibilidades de sinergias com o SIS.

Prospetiva, inovação e abordagem centrada nas capacidades

A Comissão desenvolverá uma **abordagem prospetiva abrangente em matéria de segurança interna a nível da UE**, com base nas boas práticas identificadas a nível nacional. Esta abordagem contribuirá para a elaboração de políticas e orientará os investimentos na investigação e inovação financiada pela UE no domínio da segurança.

A investigação e a inovação desempenham um papel crucial na segurança interna, criando soluções para combater as ameaças emergentes, incluindo a utilização abusiva das tecnologias[26]. A UE deve continuar a investir, através da investigação e inovação financiadas pela UE no domínio da segurança[27], no desenvolvimento de ferramentas e soluções inovadoras para fazer face às ameaças à segurança, respeitando simultaneamente as regras da UE e os direitos fundamentais. A Comissão deve apoiar a transição da investigação para a implantação,

[23] O MID é um dos componentes de interoperabilidade introduzidos pelo Regulamento (UE) 2019/818 e pelo Regulamento 2019/817.
[24] https://ec.europa.eu/commission/presscorner/detail/pt/ip_24_5047.
[25] Quadro em matéria de registo de identificação dos passageiros (PNR) e de informações antecipadas sobre os passageiros (API) estabelecido pela Diretiva (UE) 2016/681 («Diretiva PNR») e pelos Regulamentos (UE) 2025/12 e (UE) 2025/13 («Regulamentos API»).
[26] Ver o relatório do Centro Comum de Investigação da Comissão, «Emerging risks and opportunities for EU internal security stemming from new technologies», https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.
[27] *Study on strengthening EU-funded security research and innovation – 20 years of EU-Funded Civil Security Research and Innovation – 2025*, https://data.europa.eu/doi/10.2837/0004501.

a fim de assegurar a adoção efetiva dessas capacidades modernas, dando prioridade a **novas tecnologias** como a inteligência artificial (IA). Esta abordagem deve incluir formação para melhorar a utilização dos sistemas de IA e de outras capacidades técnicas pelos serviços de polícia e pelas autoridades judiciárias. Além disso, quando adequado, importa explorar o potencial de dupla utilização das tecnologias em ambos os sentidos (do civil para a defesa e da defesa para o civil)[28].

O **Polo da UE de Inovação para a Segurança Interna**[29], uma rede de laboratórios de inovação que disponibiliza as mais recentes inovações e soluções eficazes para apoiar o trabalho no domínio da segurança interna na UE e nos Estados-Membros, ajudará a integrar a investigação na prática e nas políticas. Para melhorar a eficácia da Europol, é necessário reforçar o Repositório de Instrumentos da Europol, permitindo-lhe identificar, desenvolver, adquirir em conjunto e aplicar operacionalmente tecnologias avançadas. Além disso, a Comissão criará um **Campus de Investigação e Inovação em Segurança** no seu Centro Comum de Investigação, reunindo investigadores para encurtar o ciclo desde os resultados da investigação até à inovação, para um desenvolvimento e execução bem-sucedidos, reduzindo simultaneamente os custos de desenvolvimento, ensaio e validação.

O nosso **Espaço Europeu da Investigação** é, pela sua própria natureza, colaborativo e, por conseguinte, permeável à ingerência estrangeira e à desinformação. Na sequência da adoção da Recomendação do Conselho relativa ao reforço da segurança da investigação[30], a Comissão e os Estados-Membros estão a tomar medidas para capacitar os intervenientes relevantes, nomeadamente através da criação de um centro de conhecimentos sobre segurança da investigação.

Principais ações

A Comissão adotará:

- **uma proposta legislativa para transformar a Europol numa agência policial verdadeiramente operacional em 2026;**
- **uma proposta legislativa para reforçar a Eurojust em 2026;**
- **uma proposta legislativa para reforçar o papel e as funções da Frontex em 2026;**
- **uma proposta legislativa para a criação de um Sistema Europeu de Comunicações Críticas em 2026.**

A Comissão irá:

- **apresentar um roteiro que defina o caminho a seguir em matéria de acesso lícito e efetivo aos dados para efeitos de aplicação da lei em 2025;**
- **realizar uma avaliação de impacto em 2025 com vista a atualizar as regras em matéria de conservação de dados a nível da UE, se for caso disso;**
- **apresentar um roteiro tecnológico sobre cifragem para identificar e avaliar soluções tecnológicas que permitam o acesso lícito aos dados por parte dos serviços de polícia em 2026;**
- **trabalhar no sentido da criação de um grupo de alto nível para reforçar a cooperação operacional em matéria de aplicação da lei;**
- **criar um Campus de Investigação e Inovação em Segurança no seu Centro Comum de Investigação em 2026.**

[28] Conforme referido no relatório Niinistö.
[29] Polo da UE de Inovação para a Segurança Interna | Europol.
[30] JO C/2024/3510, 30.5.2024.

A Comissão, em cooperação com os Estados-Membros e as agências competentes da UE, irá:

- **reforçar a arquitetura da EMPACT;**
- **trabalhar no sentido da rápida implantação da arquitetura de interoperabilidade e da aplicação do Regulamento Prüm II;**
- **reforçar o quadro de informação sobre viagens.**

Os Estados-Membros são convidados a:

- **transpor e aplicar integralmente a Diretiva Intercâmbio de Informações.**

4. Resiliência contra ameaças híbridas e outros atos hostis

Reforçaremos a resiliência contra as ameaças híbridas aumentando a proteção das infraestruturas críticas, reforçando a cibersegurança, protegendo as plataformas de transporte e os portos e combatendo as ameaças em linha.

A frequência e a sofisticação dos atos hostis que comprometem a segurança da UE aumentaram, com os intervenientes mal-intencionados a expandirem significativamente o seu arsenal. As campanhas híbridas dirigidas à UE, aos seus Estados-Membros e aos seus parceiros intensificaram-se, com atos de sabotagem dirigidos às infraestruturas críticas, fogo posto, ciberataques, ingerência eleitoral, manipulação da informação e ingerência por parte de agentes estrangeiros (FIMI), incluindo a desinformação, e instrumentalização da migração. Devido ao seu papel político e operacional e à natureza das informações que tratam, as instituições, órgãos e organismos da União («entidades da União») não são poupadas.

A UE deve **reforçar a sua resiliência**, utilizar eficazmente os instrumentos atuais e desenvolver novas formas de fazer face a estas ameaças em evolução provenientes de intervenientes estatais e não estatais, tanto agora como no futuro.

Infraestruturas críticas

As ameaças a **infraestruturas críticas**, incluindo ameaças híbridas como a sabotagem e a ciberatividade maliciosa, constituem uma grave preocupação, nomeadamente para as infraestruturas que ligam os Estados-Membros – quer se trate de interligações energéticas, cabos de comunicação ou transportes transfronteiras. Desde a guerra de agressão da Rússia contra a Ucrânia, os atos de sabotagem dirigidos a infraestruturas críticas aumentaram, sobretudo em 2024, afetando numerosos Estados-Membros. A cooperação entre os serviços de polícia, os serviços de segurança e cibersegurança, a proteção militar e civil e os operadores privados é essencial para antecipar, detetar, prevenir e responder eficazmente a estes atos.

É imperativo reduzir as vulnerabilidades e reforçar a resiliência das entidades críticas para assegurar a prestação ininterrupta de serviços essenciais vitais para a economia e a sociedade. A transposição atempada e a correta aplicação por todos os Estados-Membros da **Diretiva Resiliência das Entidades Críticas (CER)**[31] e da **Diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (SRI 2)**[32] são, por conseguinte, cruciais a este respeito.

[31] Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho.

[32] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2).

A fim de assegurar progressos rápidos, a Comissão apoiará os Estados-Membros na identificação das entidades críticas[33] e no intercâmbio de boas práticas sobre estratégias nacionais e avaliações de risco dos serviços essenciais, em cooperação com o **Grupo para a Resiliência das Entidades Críticas e com o grupo de cooperação SRI**. Caso ocorram perturbações nas infraestruturas críticas com um impacto transfronteiriço significativo, o **Plano de Ação da UE para as Infraestruturas Críticas** coordenará as respostas a nível da UE. A Comissão incentiva o Conselho a adotar rapidamente o **Plano de Ação da UE para a Cibersegurança**, que reforçará a coordenação no contexto da gestão de crises, promovendo uma colaboração mais estreita entre as autoridades em matéria de resiliência física e digital. Após o êxito dos testes de esforço no setor da energia em 2023, a Comissão promoverá **testes de esforço voluntários** noutros setores-chave para a segurança interna. Além disso, a Comissão apresentará uma **panorâmica a nível da União dos riscos transfronteiriços e intersetoriais** para a prestação de serviços essenciais, a fim de apoiar as avaliações de risco dos Estados-Membros e contribuir para uma avaliação exaustiva dos riscos a nível da UE. Em consonância com a Estratégia para uma União da Preparação, a Comissão colaborará com os Estados-Membros para identificar outros setores e serviços não abrangidos pela legislação em vigor em relação aos quais poderá ser necessário agir.

O **grupo de trabalho UE-OTAN sobre a resiliência de infraestruturas críticas** promoveu uma excelente cooperação na partilha de boas práticas e no reforço da resiliência nos setores da energia, dos transportes, das infraestruturas digitais e do espaço. Este trabalho prosseguirá no âmbito do **diálogo estruturado UE-OTAN sobre a resiliência**. O **conjunto de instrumentos da UE contra as ameaças híbridas** oferece um apoio sólido aos Estados-Membros e aos parceiros na preparação e na luta contra as ameaças híbridas. As **equipas de resposta rápida às ameaças híbridas**[34] prestam assistência a curto prazo personalizada, mediante pedido, aos Estados-Membros e a várias missões e parceiros da UE. Além disso, a Comissão prosseguirá a cooperação da UE em matéria de luta contra a sabotagem através de atividades de peritos[35], incluindo um **programa de trabalho conjunto específico** para os peritos, a fim de racionalizar o intercâmbio de informações e identificar contramedidas.

Os incidentes que afetam os **cabos submarinos** na Europa sublinham a necessidade de medidas mais fortes e de respostas mais claras. Como referido no **Plano de Ação da UE para a Segurança dos Cabos**[36], a Comissão, juntamente com a alta representante, colaborará com os Estados-Membros, as agências da UE e parceiros como a OTAN para prevenir, detetar, responder e dissuadir as ameaças aos cabos submarinos. A fim de desenvolver um quadro de situação integrado das ameaças, a Comissão trabalhará com os Estados-Membros para desenvolver e implantar, a título voluntário, um mecanismo integrado de vigilância dos cabos submarinos, por bacia marítima, começando por um polo regional nórdico/báltico.

Cibersegurança

A natureza persistente da **ciberatividade mal-intencionada**, que muitas vezes faz parte de uma gama mais vasta de ameaças multidimensionais e híbridas, exige atenção e ação permanentes a nível europeu. Nos últimos anos, a União adotou legislação em matéria de cibersegurança que

[33] Os setores abrangidos pela diretiva são a energia, os transportes, o setor bancário, as infraestruturas do mercado financeiro, a saúde, a água potável, o saneamento, as infraestruturas digitais, a administração pública, o espaço e a produção, transformação e distribuição de alimentos.
[34] Bússola Estratégica para a Segurança e a Defesa 2022, p. 22.
[35] Os consultores da UE em matéria de segurança, a Rede Europeia de Inativação de Engenhos Explosivos, a rede Atlas, a Rede de Risco Elevado para a Segurança, o Grupo Consultivo para a segurança QBRN e o Grupo para a Resiliência das Entidades Críticas.
[36] JOIN(2025) 9 final.

reforça a ciber-resiliência das entidades SRI 2 que operam em setores críticos da UE, bem como das entidades da União[37], melhoram a segurança dos produtos digitais (Regulamento de Ciber-Resiliência) e estabelecem um quadro de apoio à preparação e à resposta a incidentes (Regulamento de Cibersolidariedade). Em janeiro de 2025, a Comissão adotou o **Plano de Ação Europeu para a Cibersegurança dos Hospitais e dos Prestadores de Cuidados de Saúde**[38], a fim de melhorar a deteção de ameaças, a preparação e a resposta a situações de crise. A sua plena aplicação é fundamental. Ao mesmo tempo, para fazer face a novas ameaças e acontecimentos, temos de intensificar as nossas ações, sobretudo nos domínios do intercâmbio de informações, da segurança da cadeia de abastecimento, do *software* de sequestro e dos ciberataques, bem como da soberania tecnológica.

Além disso, a sua aplicação exige que se colmate o atual défice de competências em matéria de cibersegurança, que corresponde a 299 000 pessoas. A Comissão trabalhará com os Estados-Membros no âmbito da União das Competências[39] para expandir a força de trabalho no domínio da cibersegurança, nomeadamente utilizando a nova Academia de Competências de Cibersegurança. O Plano Estratégico para o Ensino das CTEM[40] contribui para melhorar a reserva de talentos e a resposta da Europa às necessidades do mercado de trabalho no domínio da cibersegurança.

Paralelamente ao reforço da sua resiliência, a UE continuará a tirar pleno partido do quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas (o **conjunto de instrumentos de ciberdiplomacia**) para prevenir, dissuadir e responder a ciberameaças provenientes de intervenientes estatais e não estatais.

Segurança das cadeias de abastecimento de TIC

O **conjunto de instrumentos da UE para a cibersegurança das redes 5G** constitui o quadro de proteção das redes 5G, mas atualmente não é suficientemente aplicado pelos Estados-Membros. Continuam a existir riscos de segurança inaceitáveis, concretamente no que diz respeito à substituição de prestadores de alto risco. Uma abordagem harmonizada da segurança da cadeia de abastecimento das TIC pode ajudar a resolver a atual fragmentação do mercado interno causada pelas diferentes abordagens a nível nacional, evitar dependências críticas e reduzir os riscos das nossas cadeias de abastecimento de TIC face a prestadores de alto risco, protegendo desta forma as nossas infraestruturas críticas.

Em consonância com esta abordagem, na próxima **revisão do Regulamento Cibersegurança**, a Comissão analisará de um modo mais geral a segurança e a resiliência das cadeias de abastecimento e infraestruturas de TIC. Além disso, a Comissão proporá melhorar o **enquadramento europeu para a certificação da cibersegurança** a fim de assegurar que os futuros sistemas de certificação possam ser adotados em tempo útil e responder às necessidades políticas.

Com base nas avaliações setoriais existentes ou em curso[41], a Comissão desenvolverá, em conjunto com os Estados-Membros, um **planeamento estratégico para avaliações coordenadas dos riscos de cibersegurança**.

---

[37] Regulamento (UE, Euratom) 2023/2841 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, que estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança nas instituições, órgãos e organismos da União (JO L, 2023/2841, 18.12.2023).

[38] https://digital-strategy.ec.europa.eu/pt/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.

[39] COM(2025) 90 final.

[40] COM(2025) 89 final.

[41] Como as relativas às redes 5G, às telecomunicações, à eletricidade, às energias renováveis e aos veículos conectados.

Os serviços na nuvem e de telecomunicações tornaram-se um elemento fundamental das cadeias de abastecimento de infraestruturas críticas, empresas e organismos do setor público. A Comissão tomará medidas para incentivar as entidades críticas a escolherem **serviços na nuvem e de telecomunicações que ofereçam um nível de cibersegurança adequado**, tendo em conta não só os riscos técnicos, mas também os riscos e dependências estratégicos.

Software de sequestro e ciberataques

Um grande desafio persistente na UE e a nível mundial é o ***software* de sequestro** (*ramsomware*) que, segundo estimativas apresentadas num relatório, implicará um custo anual global superior a 250 mil milhões de EUR até 2031[42]. Tanto a **Diretiva SRI 2** como o **Regulamento de Ciber-Resiliência** melhorarão significativamente a postura de segurança das entidades, tornando eventuais ataques mais onerosos para as redes de *software* de sequestro. Além disso, a Comissão trabalhará em estreita colaboração com os Estados-Membros para assegurar que mais ataques com *software* de sequestro, em especial ameaças persistentes avançadas, e pagamentos de resgate sejam denunciados às autoridades, facilitando as investigações.

Para prevenir e travar os ciberataques, a UE tem de reforçar o intercâmbio de informações entre os serviços de polícia, as autoridades e entidades de cibersegurança e os organismos privados, sob a égide da Europol e da Agência da União Europeia para a Cibersegurança (ENISA).

A Europol e a Eurojust devem continuar na senda dos sucessos obtidos no desmantelamento de operações de *software* de sequestro, apoiando a cooperação policial. Para o efeito, as autoridades policiais devem utilizar plenamente os mecanismos de cooperação, incluindo o **Modelo da Europol de Resposta Internacional ao *Software* de Sequestro** e a **Iniciativa Internacional de Combate ao Software de Sequestro (CRI)**[43], e a ENISA e a Europol devem cooperar para expandir o repositório de ferramentas de decifragem de estirpes de *software* de sequestro[44].

Soberania tecnológica

A cibersegurança e a soberania tecnológica estão estreitamente interligadas, sendo prioritário resolver a questão das dependências tecnológicas. A União deve **orientar o desenvolvimento e a implantação de novas tecnologias**, enquanto a Comissão trabalha no sentido de **reforçar as capacidades em tecnologias estratégicas**, como a IA, a computação quântica, a conectividade avançada, a nuvem, a computação periférica e a Internet das coisas[45], através de iniciativas futuras, incluindo, nomeadamente, o Plano de Ação Continente da IA e a Estratégia das Tecnologias Quânticas[46]. A Comissão continuará a apoiar a implantação oportuna dos mais recentes **protocolos Internet** internacionalmente acordados, que são essenciais para manter uma Internet potencialmente expansível e eficiente, com um nível reforçado de cibersegurança. São igualmente necessárias outras ações para dar resposta aos **desafios relacionados com o espetro radioelétrico**, nomeadamente no que diz respeito à falsificação ou ao empastelamento do GNSS e aos riscos e dependências da cadeia de abastecimento, como a utilização de

[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[43] https://counter-ransomware.org/.
[44] Disponível através do projeto No More Ransom, https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en?prefLang=pt.
[46] Por exemplo, a Empresa Comum HPC https://eurohpc-ju.europa.eu/index_en, a página inicial da iniciativa emblemática para as tecnologias quânticas | Quantum Flagship, a Rede 3C (COM(2024) 81 final) e o Plano de Ação da UE para a Segurança dos Cabos (JOIN(2025) 9 final).

tecnologias de deteção quântica e a exploração do desenvolvimento de capacidades de controlo das radiofrequências.

A implantação de soluções de **criptografia pós-quântica** será crucial para salvaguardar as comunicações sensíveis e os dados em repouso e para proteger as identidades digitais na nova era quântica. A Comissão está a trabalhar com os Estados-Membros, com base na Recomendação de 2024 sobre um roteiro para a execução coordenada da transição para a criptografia pós-quântica[47], de forma a promover essa transição. A este respeito, os Estados-Membros devem identificar os casos de alto risco em entidades críticas e assegurar a cifragem segura do ponto de vista quântico para estes casos de alto risco o mais rapidamente possível e, o mais tardar, até ao final de 2030. A Comissão está também a trabalhar com os Estados-Membros e a Agência Espacial Europeia (AEE) para desenvolver e implantar a **Infraestrutura Europeia de Comunicação Quântica (EuroQCI)**[48], com base na distribuição de chaves quânticas, no âmbito do **IRIS²**, o Programa Conectividade Segura da UE. Ambas as iniciativas permitirão às entidades, em última análise, transmitir dados e armazenar informações de forma segura.

As **tecnologias quânticas** desempenharão também um papel fundamental nas aplicações de segurança: no âmbito da **Estratégia das Tecnologias Quânticas**, será desenvolvido um **roteiro para a deteção quântica em aplicações de segurança**. Na mesma ordem de ideias, a Comissão está a trabalhar no sentido de proteger contra ataques quânticos os seus sistemas institucionais críticos para a segurança, incluindo os seus sistemas informáticos classificados.

Um quadro de cibersegurança favorável às empresas

A futura revisão do Regulamento Cibersegurança constitui uma oportunidade para **simplificar a legislação da UE em matéria de cibersegurança**, em consonância com a Bússola para a Competitividade. A Comissão trabalhará em estreita colaboração com os Estados-Membros para assegurar uma aplicação rápida, coerente e favorável às empresas do quadro horizontal para a cibersegurança estabelecido na Diretiva SRI 2, no Regulamento de Ciber-Resiliência e no Regulamento de Cibersolidariedade, promovendo a simplicidade e a coerência e evitando a fragmentação ou a duplicação das regras de cibersegurança na legislação nacional e da UE.

Para permitir o acesso seguro a serviços em linha e reforçar a segurança digital em toda a UE, o **Regime Europeu para a Identidade Digital** oferecerá a todos os cidadãos e residentes da UE carteiras europeias de identidade digital fiáveis até ao final de 2026. A futura **carteira empresarial europeia** promoverá interações transfronteiras seguras entre empresas e administrações públicas. Ambos são pré-requisitos para um funcionamento seguro e mais eficiente do mercado único baseado em dados, com ferramentas como a plataforma digital única, a faturação eletrónica, a contratação pública eletrónica e o passaporte digital do produto.

Segurança na Internet

Algumas das ameaças híbridas mais graves que põem em risco a segurança das pessoas na Europa e comprometem a esfera democrática da UE acontecem na Internet. Estas ameaças incluem atividades ilegais e conteúdos ilegais em linha, manipulação da informação com amplificação artificial, informação enganosa e FIMI.

A aplicação rigorosa do **Regulamento dos Serviços Digitais (RSD)** é fundamental para garantir um ambiente em linha seguro e acessível, com intervenientes responsáveis que sejam, além disso, resilientes às ameaças híbridas. O RSD obriga os fornecedores de plataformas em

[47] Recomendação da Comissão sobre um roteiro para a execução coordenada da transição para a criptografia pós-quântica |Construir o futuro digital da Europa.

[48] https://digital-strategy.ec.europa.eu/pt/policies/european-quantum-communication-infrastructure-euroqci.

linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão a realizar avaliações dos riscos e a aplicar medidas de atenuação dos riscos sistémicos decorrentes da conceção, do funcionamento ou da utilização dos seus serviços. Esses riscos podem incluir efeitos negativos no discurso cívico e nos processos eleitorais, bem como na segurança pública, como as ingerências profundas de intervenientes estatais estrangeiros mal-intencionados, por exemplo, nos processos eleitorais. É importante dar formação às autoridades competentes dos Estados-Membros sobre a utilização de instrumentos jurídicos para remover prontamente conteúdos ilegais da Internet, sobretudo no que diz respeito à ciberviolência baseada no género. O RSD prevê um mecanismo de resposta a situações de crise, que pode ser ativado sempre que circunstâncias extraordinárias causem uma ameaça grave para a segurança pública ou a saúde pública na União ou em partes significativas da União. Para complementar este mecanismo, a Comissão e as autoridades nacionais competentes designadas como coordenadoras dos serviços digitais também desenvolveram um **quadro voluntário de resposta a incidentes no âmbito do RSD**. Os coordenadores dos serviços digitais tomaram igualmente medidas para ajudar a proteger a integridade das eleições, por exemplo através da organização de mesas-redondas e testes de esforço eleitorais[49]. O RSD, juntamente com o Regulamento Propaganda Política[50], prevê uma das várias vertentes relacionadas com a salvaguarda da democracia e da integridade dos processos democráticos, que são vulneráveis a ataques de intervenientes hostis, nomeadamente através de ferramentas digitais e das redes sociais.

A aplicação do conjunto de instrumentos **FIMI** é outra componente importante que presta um apoio fundamental a nível da UE. O apoio à literacia digital e mediática e ao pensamento crítico é também fundamental para estes esforços[51].

Luta contra a instrumentalização da migração

A Rússia, com a ajuda e o apoio decisivo da Bielorrússia, instrumentalizou deliberadamente a migração e facilitou ilegalmente os fluxos de migração para as fronteiras externas da UE, com o objetivo de desestabilizar as nossas sociedades e minar a unidade da União Europeia. Tal compromete não só a segurança nacional e a soberania dos Estados-Membros, como também a segurança e a integridade do espaço Schengen e a segurança da União no seu conjunto. Nas suas conclusões de outubro de 2024, o Conselho Europeu salientou que não se pode permitir que a Rússia e a Bielorrússia, ou qualquer outro país, abusem dos nossos valores, nomeadamente do direito de asilo, nem que ponham em causa a nossa democracia.

Como referido na Comunicação da Comissão de 2024 sobre a instrumentalização da migração, para além de um forte apoio político, a União envidou esforços financeiros, operacionais e diplomáticos, nomeadamente em cooperação com os países de origem e de trânsito, para dar uma resposta eficaz a estas ameaças[52]. Esta resposta implica a utilização do novo quadro estabelecido pelo Conselho para sancionar os indivíduos e as organizações envolvidos em ações e políticas como a instrumentalização da migração pela Rússia, mediante a imposição do congelamento de bens e da proibição de viajar[53]. A UE continuará a recorrer a este quadro sempre que necessário e a apoiar os Estados-Membros na luta contra esta ameaça.

[49] Conjunto de ferramentas para as eleições do RSD destinado aos coordenadores dos serviços digitais, de 2025 https://digital-strategy.ec.europa.eu/pt/library/dsa-elections-toolkit-digital-services-coordinators.
[50] Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho, de 13 de março de 2024, sobre a transparência e o direcionamento da propaganda política (JO L, 2024/900, 20.3.2024.
[51] Plano de Ação para a Educação Digital (2021-2027) – Espaço Europeu da Educação.
[52] COM(2024) 570 final.
[53] Regulamento (UE) 2024/2642 do Conselho, de 8 de outubro de 2024, que impõe medidas restritivas tendo em conta as atividades desestabilizadoras da Rússia, ST/8744/2024/INIT (JO L, 2024/2642, 9.10.2024).

Segurança dos transportes

Os portos marítimos, os aeroportos e as infraestruturas terrestres são pontos cruciais de entrada e saída. Desempenham um papel vital na economia e na sociedade da UE e são essenciais para a mobilidade militar. No entanto, estas plataformas e meios de transporte são também alvos privilegiados de ameaças externas e de atividades criminosas. Incidentes recentes, incluindo violações da segurança do transporte aéreo de carga e ataques a infraestruturas ferroviárias, evidenciam os riscos graves neste domínio. Os **operadores de transportes** podem ser tanto alvos como instrumentos para agentes mal-intencionados. Os instrumentos jurídicos da UE em vigor reforçaram a segurança da aviação[54], mas o elevado nível de ameaça para a aviação civil requer um meio que permita prever incidentes e consultar rapidamente os Estados-Membros relevantes. A Comissão colaborará com os Estados-Membros para alterar a legislação de execução em vigor no domínio da segurança da aviação, a fim de partilhar informações classificadas sobre **ocorrências relacionadas com a segurança da aviação**. Além disso, a Comissão ponderará a adoção de **medidas regulamentares** para fazer face a novas ameaças, como os **incidentes relacionados com o transporte aéreo de carga**, e reforçar as normas de segurança da aviação. Para tal, será igualmente necessário um reforço da **legislação em matéria de segurança da aviação**, a fim de permitir medidas de resposta imediata, mantendo simultaneamente o ponto de controlo de segurança único nos aeroportos da UE.

Ao desenvolver a futura **Estratégia dos Portos da UE**, com base na **Aliança Europeia dos Portos**, a Comissão explorará formas de reforçar a legislação em matéria de proteção do transporte marítimo, a fim de combater eficazmente as ameaças emergentes, garantir a segurança dos portos e reforçar a segurança da cadeia de abastecimento da UE. Para o efeito, a Comissão assegurará a sua aplicação consistente e trabalhará na harmonização das práticas nacionais e no reforço das verificações de antecedentes nos portos. Para além dos protocolos de segurança estabelecidos para a carga aérea, a Comissão trabalhará com os Estados-Membros e o setor privado na expansão desses protocolos para garantir a segurança das cadeias de transporte marítimo.

A Autoridade Aduaneira da UE proposta analisará e avaliará os riscos com base em **informações aduaneiras** relacionadas com as mercadorias que entram, saem e transitam pela UE, a fim de apoiar os Estados-Membros na prevenção da exploração das cadeias de abastecimento internacionais por agentes mal-intencionados. Em consonância com a Estratégia de Segurança Marítima da União Europeia[55], o futuro **Pacto Europeu dos Oceanos** desempenhará um papel fundamental no reforço da segurança marítima nas bacias marítimas da UE e não só, nomeadamente incentivando a expansão das operações e dos exercícios marítimos polivalentes.

Resiliência das cadeias de abastecimento

A Europa tem de reduzir o seu recurso a tecnologias de países terceiros, que pode conduzir a riscos de dependência e de segurança. A Comissão pretende atenuar as dependências de fornecedores estrangeiros únicos, reduzir os riscos para as nossas cadeias de abastecimento decorrentes de fornecedores de alto risco e garantir as infraestruturas críticas e a capacidade industrial no solo da UE, tal como especificado na **Bússola para a Competitividade[56]** e no **Pacto da Indústria Limpa[57]**. A Comissão promoverá uma **política industrial em prol da**

[54] Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002 (JO L 97 de 9.4.2008, p. 72).
[55] JOIN(2023) 8 final.
[56] COM(2025) 30 final.
[57] COM(2025) 85 final.

segurança interna, colaborando com as indústrias da UE em setores-chave (por exemplo, plataformas de transportes, infraestruturas críticas), a fim de produzir soluções de segurança como equipamentos de deteção, tecnologias biométricas e drones, incorporando características de segurança desde a conceção. Ao **rever as regras de contratação pública da UE**, a Comissão avaliará se as considerações de segurança constantes da Diretiva de 2009 relativa aos contratos públicos nos domínios da defesa e da segurança[58] são suficientes para dar resposta às necessidades em matéria de aplicação da lei e de resiliência das entidades críticas.

A Comissão apoiará os Estados-Membros na **análise do investimento direto estrangeiro (IDE)** e na aquisição de equipamento para plataformas logísticas, assegurando que as tecnologias e as infraestruturas críticas continuam seguras.

Quando estiver em vigor, o **Regulamento de Emergência e Resiliência do Mercado Interno (ERMI)** ajudará a UE a gerir crises suscetíveis de perturbar as cadeias de abastecimento críticas e a livre circulação de bens, serviços e pessoas. Permitirá uma coordenação rápida e a identificação de bens e serviços relevantes em situação de crise e proporcionará um conjunto de instrumentos para garantir a sua disponibilidade. Além disso, em estreita cooperação com os Estados-Membros, a Comissão proporá a criação de um **mecanismo multiagências de alerta de segurança no domínio dos transportes e da cadeia de abastecimento** para garantir a partilha segura e atempada das informações necessárias para antecipar e combater as ameaças.

Além disso, com a aplicação do Regulamento Matérias-Primas Críticas e do Regulamento Indústria Neutra em Carbono, a maior utilização dos critérios de sustentabilidade, resiliência e preferência europeia na contratação pública da UE promoverá o desenvolvimento de mercados-piloto. O reforço dos laços comerciais, por exemplo através de parcerias no domínio das matérias-primas e de parcerias de comércio e investimento limpos, ajudará a diversificar as cadeias de abastecimento.

Resiliência e preparação para ameaças químicas, biológicas, radiológicas e nucleares

A guerra de agressão da Rússia contra a Ucrânia aumentou o risco de **ameaças químicas, biológicas, radiológicas e nucleares (QBRN)**. Para contrariar a potencial aquisição e utilização de materiais QBRN como arma, a Comissão apoiará os Estados-Membros e os países parceiros através de ações de formação e exercícios específicos. A Comissão reforçará igualmente as capacidades de preparação e de resposta QBRN, com a definição de prioridades em matéria de ameaças, o financiamento da inovação para contramedidas, as capacidades rescEU e a constituição de reservas de contramedidas médicas, no âmbito de um novo **plano de ação de preparação e resposta QBRN**. Além disso, a **Estratégia da UE para as Contramedidas Médicas** apoiará o desenvolvimento de contramedidas médicas, desde a investigação até ao fabrico e distribuição, a fim de proteger a UE de pandemias e ameaças QBRN.

Com base na experiência adquirida com a pandemia de COVID-19, a UE reforçou o quadro de segurança sanitária[59]. A Comissão está a designar laboratórios de referência da UE no domínio da saúde pública para reforçar as capacidades de vigilância e deteção rápida da UE e a nível nacional. Em 2025, será publicado um plano da União em matéria de preparação, prevenção e resposta em matéria de segurança sanitária.

[58] Diretiva 2009/81/CE do Parlamento Europeu e do Conselho, de 13 de julho de 2009, relativa à coordenação dos processos de adjudicação de determinados contratos de empreitada, contratos de fornecimento e contratos de serviços por autoridades ou entidades adjudicantes nos domínios da defesa e da segurança, e que altera as Diretivas 2004/17/CE e 2004/18/CE (JO L 216 de 20.8.2009, p. 76).

[59] Nomeadamente através do Regulamento (UE) 2022/2371 relativo às ameaças transfronteiriças graves para a saúde.

Principais ações

A Comissão irá:

- **reexaminar e rever o Regulamento Cibersegurança em 2025;**
- **tomar medidas para assegurar a utilização segura dos serviços na nuvem;**
- **propor uma Estratégia dos Portos da UE em 2025;**
- **rever as regras de contratação pública da UE no domínio da defesa e da segurança em 2026;**
- **apresentar um novo plano de ação em matéria de preparação e resposta QBRN em 2026.**

A Comissão, em cooperação com os Estados-Membros, irá:

- **desenvolver e implantar a Infraestrutura Europeia de Comunicação Quântica (EuroQCI);**
- **assegurar a aplicação efetiva do Regulamento dos Serviços Digitais;**
- **trabalhar no sentido de combater a instrumentalização da migração;**
- **estabelecer um sistema de ocorrências no domínio da segurança da aviação;**
- **trabalhar no sentido de criar um mecanismo multiagências de alertas de segurança no domínio dos transportes e da cadeia de abastecimento.**

O Conselho é convidado a:

- **adotar a recomendação do Conselho sobre o Plano de Ação da UE para a Cibersegurança.**

Os Estados-Membros são convidados a:

- **transpor e aplicar integralmente as Diretivas CER e SRI 2.**

5. Apertar o cerco à criminalidade grave e organizada

Ajudaremos a erradicar a criminalidade organizada, propondo regras mais rigorosas para combater as redes de criminalidade organizada, nomeadamente a nível dos inquéritos, bem como para tornar os jovens na UE menos vulneráveis ao recrutamento para a criminalidade e intensificar as medidas contra o acesso aos instrumentos e bens de origem criminosa.

A criminalidade organizada explora um panorama em evolução e está a proliferar exponencialmente. Tira partido de tecnologias avançadas, está ativa em múltiplas jurisdições e tem fortes ligações para além das fronteiras da UE. Tendo em conta estas ameaças complexas e transnacionais, a coordenação e o apoio a nível da UE são vitais.

Prevenção da criminalidade

O recrutamento de jovens para a criminalidade organizada é uma preocupação crescente na UE. A luta contra a criminalidade organizada exige um combate das suas **causas profundas** mediante a oferta de educação e alternativas a uma vida de crime, através de uma abordagem que envolva toda a sociedade. A Comissão apoiará a integração de considerações de segurança nas políticas de educação, sociais, de emprego e regionais da UE. A UE **promoverá políticas**

de prevenção da criminalidade baseadas em dados concretos[60] e adaptadas aos contextos locais.

Para proteger os destinatários de serviços em linha, em especial os menores, nomeadamente contra autores de crimes de abuso sexual de crianças, traficantes de seres humanos e do recrutamento em linha para fins de criminalidade ou extremismo violento, as medidas ao abrigo do **Regulamento dos Serviços Digitais** exigem que os fornecedores de plataformas em linha acessíveis a menores controlem os riscos e tomem medidas contra os conteúdos ilegais, incluindo o discurso de ódio. A Comissão tenciona emitir **orientações sobre a proteção dos menores**, a fim de ajudar os fornecedores de plataformas em linha a garantir um elevado nível de privacidade, segurança e proteção dos menores em linha. As orientações incluirão um conjunto de recomendações para todos os serviços digitais que operam na União, a fim de reforçar a proteção dos menores em linha. Em 2025, a Comissão tenciona igualmente promover uma solução da UE de **verificação da idade com proteção da privacidade**, que colmatará a lacuna antes de a carteira europeia de identidade digital ser disponibilizada no final de 2026. A Comissão apresentará igualmente um Plano de Ação contra a Ciberintimidação.

Além disso, a Comissão continuará a apoiar o diálogo multilateral voluntário com as plataformas em linha e outros intervenientes relevantes, nomeadamente através do Fórum Internet da UE e de códigos de conduta específicos ao abrigo do Regulamento dos Serviços Digitais, como o Código de Conduta para a luta contra os discursos ilegais de incitação ao ódio em linha, de 2025. O objetivo é aumentar a sensibilização, responder conjuntamente às ameaças atuais e emergentes e produzir e partilhar boas práticas em matéria de medidas de atenuação.

A nível local, o impacto da criminalidade organizada reforça a necessidade de soluções regionais para reduzir a vulnerabilidade às atividades ilegais e a sua atratividade. A Agenda da UE para as Cidades abordará os desafios de segurança nas cidades, com base na iniciativa «Cidades da UE contra a Radicalização». A Comissão apoiará os Estados-Membros no reforço da segurança urbana e regional através do Fundo Europeu de Desenvolvimento Regional.

Uma melhor educação e mais competências são as bases para sociedades resilientes e coesas. Através da **União das Competências** e do **Plano de Ação para a Integração e a Inclusão**, a União trabalhará no sentido de ajudar as pessoas a tornarem-se mais resilientes à informação incorreta e à desinformação, à radicalização e ao recrutamento para a criminalidade.

Entre os objetivos fundamentais da UE está o de proteger as crianças de todas as formas de violência, incluindo a criminalidade e a violência física ou mental, tanto em linha como fora. Para dar resposta às necessidades específicas dos grupos particularmente vulneráveis, como as crianças, que estão cada vez mais expostos ao recrutamento e à radicalização, ao aliciamento e ao abuso sexual de crianças, à ciberintimidação, à desinformação e a outras ameaças, a UE elaborará um **plano de ação para a proteção das crianças contra a criminalidade**, que deverá abranger as dimensões física e virtual. Este plano estabelecerá uma abordagem coerente e coordenada assente nos quadros e instrumentos disponíveis, incluindo o futuro Centro da UE contra o Abuso Sexual de Crianças, bem como outros organismos e agências da UE, e proporá vias a seguir nos casos em que subsistem lacunas.

Desmantelamento das redes criminosas e dos seus facilitadores

É necessário intensificar a luta contra as redes criminosas de alto risco, os seus líderes e os facilitadores. Embora os êxitos recentes sejam notáveis[61], as regras desatualizadas e as definições incoerentes de redes criminosas dificultam uma resposta eficaz da justiça penal e a cooperação transfronteiriça. A Comissão irá rever a legislação desatualizada neste domínio,

[60] https://www.eucpn.org/.
[61] Incluindo casos recentes da EMPACT.

propondo um **quadro jurídico revisto em matéria de criminalidade organizada**, de forma a reforçar a resposta.

A execução administrativa pode complementar a aplicação da lei para obter resultados mais rápidos – como demonstrado pela Procuradoria Europeia e pelo Organismo Europeu de Luta Antifraude (OLAF) na luta contra a **fraude transfronteiras e os crimes lesivos dos interesses financeiros da UE**. Os autores de fraudes nas subvenções centram-se em setores como as energias renováveis, os programas de investigação e o setor agrícola[62]. A Comissão explorará formas de coordenar a utilização de instrumentos penais e administrativos, reforçando a cooperação com a Europol, a Eurojust e a Procuradoria Europeia. A Comissão continuará igualmente a apoiar a aplicação mais ampla da **abordagem administrativa** para capacitar as autoridades locais e outras autoridades administrativas para combater a infiltração criminosa[63].

A UE está a trabalhar no sentido de reforçar o seu quadro jurídico em matéria de luta contra a **corrupção**[64]. O Parlamento Europeu e o Conselho devem concluir rapidamente as negociações sobre o quadro atualizado de luta contra a corrupção proposto pela Comissão. A Comissão apresentará uma Estratégia Anticorrupção da UE para promover a integridade e reforçar a coordenação entre todas as autoridades e partes interessadas neste domínio.

As armas de fogo são um facilitador essencial da crescente violência perpetrada por grupos de criminalidade organizada. A Comissão proporá normas comuns de direito penal em matéria de tráfico ilícito de armas de fogo. Um novo **Plano de Ação da UE sobre o Tráfico de Armas de Fogo** centrar-se-á na proteção do mercado lícito, na redução das atividades criminosas, com base em melhores informações e no reforço da cooperação internacional, com especial destaque para a Ucrânia e os Balcãs Ocidentais.

Os artigos de pirotecnia comercializados ilegalmente, utilizados em crimes, exigem medidas para melhorar a sua prevenção e rastreabilidade. A Comissão está atualmente a avaliar a Diretiva Artigos de Pirotecnia e ponderará igualmente a aplicação de **sanções penais ao tráfico de artigos de pirotecnia**.

Seguir a pista do dinheiro

Seguir a pista do dinheiro é crucial para combater a criminalidade organizada e o terrorismo, mas continua a ser muito difícil. A ligação entre a criminalidade organizada e os fluxos financeiros exige esforços intensos e concertados para impedir o acesso das redes criminosas a fontes de financiamento e proteger melhor as pessoas, as empresas e os orçamentos públicos.

A UE intensificou os seus esforços com as novas regras em matéria de luta contra o branqueamento de capitais, incluindo a criação da **Autoridade para o Combate ao Branqueamento de Capitais e ao Financiamento do Terrorismo (ACBC)**[65]. A colaboração entre a ACBC, o OLAF, a Procuradoria Europeia, a Eurojust e a Europol é essencial para que seja possível realizar investigações financeiras eficazes. A Comissão apoiará a criação de **parcerias**, tanto as que facilitam a cooperação interagências como as que envolvem o setor privado.

[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.
[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.
[64] Proposta de Diretiva do Parlamento Europeu e do Conselho relativa à luta contra a corrupção, que substitui a Decisão-Quadro 2003/568/JAI do Conselho e a Convenção relativa à luta contra a corrupção em que estejam implicados funcionários das Comunidades Europeias ou dos Estados-Membros da União Europeia e que altera a Diretiva (UE) 2017/1371 do Parlamento Europeu e do Conselho, COM(2023) 234 final, de 3.5.2023.
[65] https://www.amla.europa.eu/index_en?prefLang=pt.

Para desmantelar os motivos financeiros que sustentam a criminalidade organizada, é essencial apreender bens e confiscar os ganhos de origem criminosa. As regras mais rigorosas recentemente adotadas em matéria de **recuperação e perda de bens**[66] devem ser transpostas sem demora pelos Estados-Membros e plenamente aplicadas. O combate aos sistemas financeiros paralelos que contornem o quadro da UE em matéria de luta contra o branqueamento de capitais, incluindo sistemas baseados em criptoativos, exige igualmente ações inovadoras, a partilha de boas práticas entre os Estados-Membros e um maior apoio da Europol e da Eurojust. A Comissão explorará a viabilidade de um novo sistema à escala da UE para rastrear os lucros da criminalidade organizada e o financiamento do terrorismo, e para incentivar fluxos de informação céleres e amplos entre as **Unidades de Informação Financeira** para aplicação da lei. A Comissão explorará formas de colmatar as lacunas, apoiará os Estados-Membros no reforço das suas capacidades e continuará a trabalhar no reforço da cooperação com países terceiros utilizados pelos criminosos para operações bancárias clandestinas.

Luta contra os crimes graves

Para além do desmantelamento das redes criminosas, a luta contra os crimes graves exige esforços específicos. Para reforçar a nossa capacidade de combater a **fraude em linha** – que está a causar prejuízos financeiros muito significativos[67] – a Comissão apoiará medidas de prevenção e de aplicação da lei mais eficazes e trabalhará com os Estados-Membros e as partes interessadas para apoiar e proteger as vítimas, nomeadamente prestando assistência na recuperação dos seus fundos. Estes esforços serão formalizados num **plano de ação contra a fraude em linha**.

Com base na Estratégia da UE de 2020-2025 para a luta contra o **abuso sexual de crianças**[68], a Comissão apoiará os colegisladores na finalização das duas propostas legislativas[69] para prevenir e combater o abuso sexual de crianças na Internet e para reforçar a eficácia da aplicação da lei contra o abuso e a exploração sexual de crianças. Com as regras provisórias em vigor até abril de 2026, é essencial estabelecer um quadro jurídico permanente, e a Comissão incentiva os colegisladores a encetarem negociações sobre o projeto de regulamento que estabelece regras para prevenir e combater o abuso sexual de crianças. Os colegisladores são igualmente convidados a avançar no sentido das negociações sobre a Diretiva relativa à luta contra o abuso sexual e a exploração sexual de crianças e o material com imagens de abusos sexuais de crianças, que estabelecerá regras mínimas relativas à definição dos crimes e sanções no domínio da exploração sexual de crianças.

Metade das redes criminosas mais perigosas da UE estão envolvidas no **tráfico de droga** violento. Embora a UE tenha recentemente reforçado a sua luta contra este crime[70], nomeadamente através do alargamento do mandato da **Agência da União Europeia sobre Drogas**, são necessárias mais ações. A Comissão trabalhará em estreita cooperação com os Estados-Membros para propor uma nova **Estratégia da UE em matéria de Drogas**. Procederá igualmente à revisão do **quadro jurídico em matéria de precursores de drogas** e proporá um **Plano de Ação Europeu contra o Tráfico de Droga**, a fim de perturbar as rotas e os modelos de negócio. A parceria público-privada da Aliança Europeia dos Portos, que visa reforçar a proteção dos portos, será alargada de modo a incluir os portos de menores dimensões e interiores e a garantir a aplicação das regras de segurança marítima. Reconhecendo os graves

[66] Diretiva (UE) 2024/1260 do Parlamento Europeu e do Conselho, de 24 de abril de 2024, relativa à recuperação e perda de bens (JO L, 2024/1260, 2.5.2024).
[67] *Global Anti-Scam Report 2024*.
[68] COM(2020) 607 final
[69] COM(2022) 209 final e COM(2024) 60 final.
[70] COM(2023) 641 final.

impactos locais do tráfico de droga, a Comissão continuará a apoiar uma política equilibrada de luta contra a droga, baseada em dados concretos e multidisciplinar, e preparada para lidar com afluxos súbitos de drogas, nomeadamente de opioides sintéticos.

Para combater a exploração de pessoas, a UE adotou novas regras[71] e introduzirá uma **Estratégia renovada da UE em matéria de Luta contra o Tráfico de Seres Humanos** (2026-2030), que abrangerá todas as fases, desde a prevenção até à ação penal, com ênfase no apoio às vítimas, tanto a nível da UE como a nível internacional.

Na luta contra a **introdução clandestina de migrantes**, a Comissão liderará os esforços conjuntos com os principais parceiros através da nova Aliança Mundial contra o Tráfico de Migrantes, em cooperação com a Europol, a Eurojust e a Frontex, nomeadamente na sua dimensão em linha. As propostas da Comissão em matéria de luta contra a introdução clandestina de migrantes[72] devem ser adotadas e aplicadas sem demora. Além disso, na sequência da adoção do **conjunto de instrumentos para os operadores de transportes**[73], a Comissão aumentou os contactos com as autoridades e os operadores estrangeiros e continuará a colaborar com o setor da aviação e as organizações da aviação civil[74] para aumentar a sensibilização para a introdução clandestina de migrantes por via aérea[75].

A **criminalidade ambiental** ameaça o ambiente, a saúde pública e as economias a longo prazo. A Comissão apoiará os Estados-Membros na aplicação da Diretiva Criminalidade Ambiental[76] e reforçará as redes e ações operacionais neste domínio[77]. É essencial uma aplicação rigorosa. Além disso, a Convenção do Conselho da Europa sobre a proteção do ambiente através do direito penal[78], recentemente adotada, contribuirá para assegurar esforços fortes e comparáveis para combater a criminalidade ambiental, tanto na Europa como mais além.

A resposta da justiça penal

A criminalidade e o terrorismo podem afetar qualquer pessoa, pelo que é essencial apoiar e salvaguardar os direitos das **vítimas**, reduzir os danos e aumentar a segurança global e a confiança nas autoridades. Com base na Diretiva Direitos das Vítimas, a Comissão introduzirá uma nova **Estratégia da UE sobre os Direitos das Vítimas**.

Os **sistemas de justiça penal da UE** precisam de instrumentos eficazes para fazer face às ameaças emergentes. Para o efeito, a Comissão lançou um **Fórum de Alto Nível sobre o Futuro da Justiça Penal na UE**. Este fórum reúne os Estados-Membros, o Parlamento Europeu, as agências e organismos da UE e outras partes interessadas. Tem por objetivo debater

[71] Diretiva (UE) 2024/1712 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que altera a Diretiva 2011/36/UE relativa à prevenção e luta contra o tráfico de seres humanos e à proteção das vítimas (JO L, 2024/1712, 24.6.2024).
[72] COM(2023) 755 final e COM(2023) 754 final.
[73] Conjunto de instrumentos sobre a utilização de meios de transporte comerciais para facilitar a migração irregular para a UE.
[74] Incluindo a Organização da Aviação Civil Internacional (OACI).
[75] A Comissão apoiará igualmente a conclusão do Regulamento relativo a medidas contra os operadores de transportes que facilitam o tráfico de pessoas ou a introdução clandestina de migrantes no que diz respeito à entrada ilegal no território da União Europeia, ou que neles participem, COM(2021) 753 final.
[76] Diretiva (UE) 2024/1203 do Parlamento Europeu e do Conselho, de 11 de abril de 2024, relativa à proteção do ambiente através do direito penal e que substitui as Diretivas 2008/99/CE e 2009/123/CE (JO L, 2024/1203, 30.4.2024).
[77] Rede Europeia para a Implementação e Execução da Legislação Ambiental (IMPEL), Rede Europeia de Procuradores para o Meio Ambiente (ENPE), EnviCrimeNet e o Fórum da União Europeia de Juízes para o Meio Ambiente (EUFJE).
[78] Comité de peritos para a proteção do ambiente através do direito penal (PC-ENV) – Comité Europeu para os Problemas Criminais.

formas de assegurar que os nossos sistemas de justiça penal continuem a ser eficazes, justos e resilientes num contexto de desafios em constante evolução, reforçando simultaneamente a cooperação judiciária e reforçando a confiança mútua, nomeadamente através da digitalização[79].

Principais ações

A Comissão irá:

- **apresentar uma proposta legislativa para modernizar as regras em matéria de criminalidade organizada em 2026;**
- **apresentar uma proposta legislativa para rever o quadro jurídico em matéria de precursores de drogas em 2025;**
- **apresentar uma proposta legislativa relativa a normas comuns de direito penal em matéria de tráfico ilícito de armas de fogo em 2025;**
- **avaliar a necessidade de rever a Diretiva Artigos de Pirotecnia e a Diretiva Explosivos para Utilização Civil;**
- **avaliar a necessidade de reforçar a decisão europeia de investigação e o mandado de detenção europeu;**
- **apresentar uma nova Estratégia da UE em matéria de Luta contra o Tráfico de Seres Humanos em 2026;**
- **apresentar uma nova Estratégia da UE sobre os Direitos das Vítimas em 2026;**
- **apresentar um plano de ação da UE para a proteção das crianças contra a criminalidade até 2027;**
- **apresentar um Plano de Ação Europeu contra o Tráfico de Droga em 2025;**
- **apresentar um Plano de Ação da UE sobre o Tráfico de Armas de Fogo em 2026;**
- **alargar sucessivamente a Aliança Europeia dos Portos a partir de 2025;**
- **adotar orientações baseadas no RSD sobre a proteção dos menores em 2026;**
- **apresentar um Plano de Ação da UE contra a Ciberintimidação em 2026.**

Os Estados-Membros são convidados a:

- **transpor e aplicar integralmente as novas regras em matéria de recuperação e perda de bens até ao final de 2026;**
- **aplicar a abordagem administrativa na luta contra a infiltração criminosa;**
- **criar parcerias público-privadas contra o branqueamento de capitais;**
- **transpor e aplicar integralmente a Diretiva relativa à prevenção e ao combate à violência contra as mulheres e à violência doméstica.**

O Parlamento Europeu e o Conselho são incentivados a:

- **avançar no sentido das negociações sobre o regulamento que estabelece regras para prevenir e combater o abuso sexual de crianças e a Diretiva relativa à luta contra o abuso sexual e a exploração sexual de crianças e o material com imagens de abusos sexuais de crianças;**
- **concluir as negociações sobre a Diretiva relativa à luta contra a corrupção.**

[79] Nomeadamente de uma comunicação sobre justiça eletrónica através do intercâmbio de dados em linha (e-CODEX) e do Sistema Europeu de Informação sobre os Registos Criminais de nacionais de países terceiros (ECRIS-TCN).

6. Luta contra o terrorismo e o extremismo violento

Introduziremos uma agenda global de luta contra o terrorismo para prevenir a radicalização, garantir a segurança dos espaços públicos e em linha, cortar os canais de financiamento e responder aos ataques, quando estes ocorrem.

A ameaça terrorista continua a ser elevada na UE, e está estreitamente ligada aos efeitos colaterais dos acontecimentos geopolíticos, das novas tecnologias e dos novos meios de financiamento do terrorismo. Temos de assegurar que a UE está bem equipada para antecipar ameaças, prevenir a radicalização (tanto em linha como fora), proteger os cidadãos e os espaços públicos contra ataques e responder eficazmente aos ataques quando estes ocorrem. Em 2025, será apresentada uma **nova agenda da UE para a prevenção e a luta contra o terrorismo e o extremismo violento**, a fim de definir a ação futura da UE. Em consonância com a nova agenda, a UE e os Balcãs Ocidentais assinarão o novo **plano de ação conjunto** para a prevenção e a luta contra o terrorismo e o extremismo violento em 2025.

Prevenção da radicalização e proteção das pessoas em linha

À semelhança da luta contra a criminalidade organizada, a luta contra o terrorismo e o extremismo violento começa pelo **combate às suas causas profundas**. O **Polo de Conhecimentos da UE sobre a Prevenção da Radicalização** intensificará o seu apoio aos profissionais e aos decisores políticos através de um novo **conjunto abrangente de instrumentos de prevenção**, a fim de permitir uma identificação precoce e intervenções centradas nas pessoas vulneráveis, em especial os menores. A radicalização ocorre frequentemente nas prisões e, para ajudar os Estados-Membros a resolver esta questão, a Comissão emitirá novas recomendações.

Os terroristas e extremistas violentos utilizam plataformas na Internet para difundir conteúdos terroristas e nocivos, angariar fundos e recrutar elementos. Os utilizadores vulneráveis, em especial os menores, estão a ser radicalizados em linha a um ritmo alarmante. O **Regulamento Conteúdos Terroristas em Linha** tem sido fundamental para combater a sua propagação, permitindo a rápida remoção do material mais hediondo e perigoso[80]. A Comissão está atualmente a avaliar o seu funcionamento e avaliará a melhor forma de reforçar este quadro.

O **Protocolo de Crise da UE** para uma resposta conjunta e rápida das autoridades policiais e da indústria tecnológica a ataques terroristas será alterado, a fim de assegurar que pode ser expandido e que tem flexibilidade suficiente para responder à crescente dimensão em linha dos ataques terroristas. O Fórum Internet da UE continuará a ser a principal via de cooperação voluntária com a indústria tecnológica para combater os conteúdos terroristas e nocivos em linha. Além disso, a Comissão está a participar em iniciativas internacionais, como a Christchurch Call Foundation e o Fórum Mundial da Internet contra o Terrorismo.

Luta contra o financiamento do terrorismo

Os terroristas financiam as suas atividades através de campanhas de financiamento colaborativo, criptoativos, neobancos ou plataformas de pagamento em linha. As autoridades policiais têm de detetar e investigar estes fluxos financeiros. Tal requer meios, ferramentas e conhecimentos especializados. A **Rede de Investigadores Financeiros para o Combate ao Terrorismo** desempenha um papel fundamental neste contexto. A Comissão explorará a criação de um **novo sistema à escala da UE para rastrear o financiamento do terrorismo**, abrangendo as transações intra-UE e SEPA, as transferências de criptoativos, os pagamentos

[80] Até 31 de dezembro de 2024, foram emitidas 1 426 decisões de remoção de conteúdos terroristas ou de bloqueio do acesso aos mesmos, a grande maioria dos quais referentes a conteúdos de terrorismo jiadista, mas também a conteúdos terroristas de direita.

em linha e por transferência bancária, complementando o Acordo UE-EUA sobre o Programa de Deteção do Financiamento do Terrorismo.

O orçamento da UE deve ser **protegido contra a utilização abusiva para promover pontos de vista radicais/extremistas** nos Estados-Membros. O **Regulamento Financeiro** revisto prevê atualmente a condenação por «incitamento à discriminação, ao ódio ou à violência» como motivo de exclusão do financiamento da UE. A Comissão continuará a explorar a melhor forma de utilizar plenamente o conjunto de instrumentos, nomeadamente na seleção de potenciais beneficiários. A proteção do orçamento da UE depende igualmente de uma forte cooperação e partilha de informações com as autoridades nacionais, as agências e organismos da UE.

Proteção contra ataques

Para além do investimento na prevenção da radicalização, uma componente importante da proteção dos cidadãos consiste na restrição dos meios utilizados pelos terroristas e criminosos para perpetrar ataques. São necessárias medidas tanto no que diz respeito aos instrumentos utilizados pelos terroristas como para proteger os alvos em risco de ataque.

Para além das ações relativas às armas de fogo, a Comissão irá também **rever as regras** relativas aos **precursores de explosivos**, a fim de incluir produtos químicos de alto risco. Os **espaços públicos** continuam a ser os alvos mais comuns para os ataques terroristas, em especial os perpetrados por «lobos solitários». Para proteger os cidadãos, o **programa de consultores da UE em matéria de segurança** será reforçado para realizar avaliações da vulnerabilidade dos espaços públicos, das infraestruturas críticas e dos eventos de alto risco, a pedido dos Estados-Membros e financiadas pelo orçamento da UE ao abrigo do Fundo para a Segurança Interna. A UE procurará aumentar o financiamento disponível para a proteção dos espaços públicos. A Comissão presta apoio às autoridades dos Estados-Membros e aos operadores privados através de orientações e instrumentos específicos, como a Plataforma de Conhecimento sobre a proteção dos espaços públicos[81], tendo sido já disponibilizados 70 milhões de EUR para apoiar a proteção dos espaços públicos desde 2020.

A Comissão estudará igualmente a introdução de requisitos para que as organizações ponderem ou apliquem medidas de segurança nos locais acessíveis ao público, em diálogo com as autoridades locais e os parceiros privados.

Tendo em conta as vulnerabilidades manifestas, a **Estratégia da UE para combater o antissemitismo e apoiar a vida judaica (2021-2030)** continuará a orientar as ações da Comissão para proteger a comunidade judaica. A Comissão assegurará igualmente a existência de instrumentos adequados para apoiar os Estados-Membros na luta contra o **ódio antimuçulmano**.

A utilização de **drones** para espionagem e ataques representa um desafio crescente em matéria de segurança. A Comissão desenvolverá uma **metodologia de ensaio harmonizada para os sistemas de combate aos drones**, criará um **centro de excelência de combate aos drones** e avaliará a necessidade de harmonizar a legislação e os procedimentos dos Estados-Membros[82].

Combatentes terroristas estrangeiros

Para identificar os combatentes terroristas estrangeiros que regressam ou entram nas fronteiras externas da UE, são necessários dados sobre as pessoas que representam uma ameaça terrorista. Para o efeito, a Comissão, juntamente com a Europol, reforçará a sua **cooperação com os principais países terceiros para obter dados biográficos e biométricos sobre pessoas que**

[81] Plataforma de Conhecimento sobre a proteção dos espaços públicos.
[82] Na sequência do conjunto de ações-chave previsto na Comunicação Combate aos Drones de 2023, COM(2023) 659 final.

possam constituir uma ameaça terrorista, incluindo combatentes terroristas estrangeiros, para que sejam inseridos no Sistema de Informação de Schengen, em plena conformidade com os quadros jurídicos nacionais e da UE aplicáveis. Por conseguinte, é fundamental que os Estados-Membros utilizem todos os instrumentos existentes. Tal inclui a inserção de todas as informações relevantes no **SIS**, o reforço dos controlos biométricos e a realização dos controlos sistemáticos obrigatórios de todas as pessoas nas fronteiras externas da UE[83]. Além disso, os **indicadores de risco comuns** desenvolvidos pela Frontex continuarão a apoiar as autoridades de controlo das fronteiras dos Estados-Membros na identificação e avaliação do risco de viagens suspeitas de potenciais combatentes terroristas estrangeiros.

Além disso, para garantir que os Estados-Membros mantêm o acesso às **provas obtidas no campo de batalha** pela equipa de investigação das Nações Unidas para promover a responsabilização por crimes cometidos pelo Daexe/EIIL (UNITAD) tendo em vista a repressão de combatentes terroristas estrangeiros, a Comissão, juntamente com a Eurojust, avaliará a possibilidade de armazenar essas provas na base de dados central de provas de crimes internacionais da Eurojust. Além disso, o novo **Registo Judiciário Europeu em matéria de Contraterrorismo** continuará a apoiar os sistemas judiciários dos Estados-Membros na rápida identificação de ligações transfronteiras em casos de terrorismo.

Principais ações

A Comissão irá:

- **adotar uma nova agenda da UE para a prevenção e a luta contra o terrorismo e o extremismo violento em 2025;**
- **assinar um novo plano de ação conjunto com os Balcãs Ocidentais para a prevenção e a luta contra o terrorismo e o extremismo violento em 2025;**
- **desenvolver um novo conjunto abrangente de instrumentos de prevenção com a Plataforma de Conhecimento da UE;**
- **avaliar a aplicação do Regulamento Conteúdos Terroristas em Linha em 2026;**
- **alterar o Protocolo de Crise da UE em 2025;**
- **apresentar uma proposta legislativa de revisão do Regulamento sobre a comercialização e utilização de precursores de explosivos em 2026;**
- **explorar a viabilidade de um novo sistema à escala da UE para acompanhar o financiamento do terrorismo.**

Os Estados-Membros são convidados a:

- **reforçar os controlos biométricos e realizar os controlos sistemáticos obrigatórios nas fronteiras externas da UE;**
- **utilizar plenamente o Registo Judiciário Europeu em matéria de Contraterrorismo.**

7. A UE como um interveniente forte na segurança a nível global

Para reforçar a segurança da UE, reforçaremos a cooperação operacional através de parcerias com regiões fundamentais, como os nossos parceiros do alargamento e da vizinhança, a América Latina e a região mediterrânica. Os interesses da UE em matéria de segurança serão tidos em conta na cooperação internacional, nomeadamente através da mobilização de ferramentas e instrumentos da UE.

[83] Em plena conformidade com o Código das Fronteiras Schengen e o Regulamento Triagem.

Os últimos anos revelaram as ligações intrínsecas entre a segurança externa e interna da UE. A guerra de agressão da Rússia contra a Ucrânia, o conflito em Gaza, a situação na Síria e os conflitos emergentes em todo o mundo tiveram graves repercussões na segurança interna da UE. Para contrariar o impacto da instabilidade mundial na sua segurança interna, a **UE tem de defender ativamente os seus interesses em matéria de segurança**, combatendo as ameaças externas, desmantelando as rotas de tráfico e salvaguardando os corredores de interesse estratégico, nomeadamente as rotas comerciais. Simultaneamente, a UE continuará a ser um forte aliado para os países parceiros, trabalhando em conjunto para reforçar a segurança global e desenvolver a resiliência mútua contra as ameaças.

Nos últimos anos, a UE tomou medidas significativas para reforçar a sua cooperação em matéria de segurança, tendo celebrado acordos operacionais de cooperação policial e judiciária e outros tipos de acordos com países parceiros. Prossegue ativamente novos acordos internacionais, em conformidade com as diretrizes de negociação do Conselho, e iniciativas de reforço das capacidades, promovidas pelas agências e organismos da UE. O Instrumento de Vizinhança, de Cooperação para o Desenvolvimento e de Cooperação Internacional – Europa Global (IVCDCI – Europa Global) é também crucial para reforçar a segurança com os países parceiros.

A **ordem internacional assente em regras** é uma pedra angular do reforço da segurança global. Os diálogos sobre segurança, incluindo os temáticos, são vitais para estimular estes esforços. A execução da **Bússola Estratégica para a Segurança e a Defesa**, juntamente com quadros de cooperação bilateral e multilateral, como os acordos de estabilização e associação e os acordos de associação, bem como a colaboração com organizações como as Nações Unidas e a OTAN, são cruciais para o desenvolvimento de soluções de segurança eficazes. A UE continuará a desempenhar o seu papel nas instâncias multilaterais[84] e reforçará a sua cooperação com as organizações e os quadros internacionais e regionais pertinentes, incluindo a OTAN, as Nações Unidas, o Conselho da Europa, a Interpol, o G7, a OSCE e a sociedade civil.

Cooperação regional

A título prioritário, a continuação do apoio inabalável da UE à **Ucrânia** e o reforço da segurança e da resiliência dos **países do alargamento da UE** constituem um imperativo político e geoestratégico. O apoio à segurança da UE deve ser acompanhado da **integração acelerada dos países candidatos** na **arquitetura de segurança da UE**, paralelamente à consolidação da sua cooperação regional. A Comissão utilizará a política de alargamento da UE para apoiar as capacidades dos países candidatos e potenciais candidatos para responder a ameaças, reforçar a cooperação operacional e o intercâmbio de informações e assegurar o alinhamento com os princípios, a legislação e os instrumentos da UE. O Instrumento de Assistência de Pré-Adesão (IPA III), bem como os mecanismos para a Ucrânia, a Moldávia e os Balcãs Ocidentais são cruciais para reforçar a segurança tanto nos países candidatos como nos potenciais candidatos.

A UE continuará também a integrar os **parceiros da vizinhança** na arquitetura de segurança da UE. Através do **Novo Pacto para o Mediterrâneo** e da futura **Abordagem Estratégica para o Mar Negro**, a União procurará continuar a desenvolver a cooperação regional e parcerias estratégicas abrangentes e bilaterais com uma dimensão de segurança, se for caso disso através de diálogos regulares de alto nível em matéria de segurança. A cooperação operacional com o Norte de África, o **Médio Oriente e o Golfo** será reforçada, em especial em

[84] Fórum Mundial contra o Terrorismo, coligação internacional contra o Estado Islâmico, Fórum Mundial da Internet contra o Terrorismo, Christchurch Call Foundation e Coligação Mundial para combater as Ameaças ligadas às Drogas Sintéticas.

matéria de luta contra o terrorismo, luta contra o branqueamento de capitais, tráfico de armas de fogo e produção e tráfico de droga, nomeadamente de Captagon**.**

Para fazer face ao aumento das atividades terroristas e criminosas e às suas potenciais repercussões na **África Subsariana, nomeadamente no Sael, no Corno de África e na África Ocidental**, a UE reforçará o apoio à União Africana, às Comunidades Económicas Regionais (CER) e aos países da região. Em consonância com a Estratégia de Segurança Marítima da UE[85], a UE reforçará a cooperação no **Golfo da Guiné, no Mar Vermelho e no Oceano Índico** para combater o tráfico e a pirataria, apoiando a cooperação intra-África e regional, nomeadamente com o apoio das presenças marítimas coordenadas (PMC) da UE e do Centro de Análise e Operações Marítimas – Narcóticos (MAOC-N).

Com a **América Latina e as Caraíbas**, a UE reforçará a cooperação operacional para desmantelar e reprimir as redes criminosas de alto risco e desmantelar as atividades ilícitas e as rotas de tráfico, reforçando os quadros de cooperação, como o UE-CLASI (Comité Latino-Americano de Segurança Interna) e o Mecanismo de Coordenação e Cooperação em matéria de Droga UE-CELAC. A resiliência e as parcerias dos polos logísticos e as abordagens «sigam a pista do dinheiro» estarão entre as prioridades da UE. A UE continuará a apoiar o desenvolvimento da Comunidade de Polícias da América (Ameripol) para se tornar o equivalente regional da Europol e reforçar a cooperação judiciária entre os Estados-Membros e a região. Trabalhará igualmente com a **Ásia Central e Meridional** sobre os desafios comuns em matéria de segurança relacionados com o terrorismo, o tráfico de mercadorias ilícitas, incluindo drogas, o tráfico de seres humanos e a introdução clandestina de migrantes.

Além disso, a UE apoiará os quadros de cooperação regional em países terceiros, a fim de os ajudar a pôr termo ao tráfico ilícito na origem, em conformidade com o princípio da responsabilidade partilhada por toda a cadeia de abastecimento criminosa. Além disso, a UE fará o seu contributo para reforçar a segurança dos centros logísticos no estrangeiro, coordenando **inspeções conjuntas em portos de países terceiros**.

Cooperação operacional

A **Estratégia Global Gateway** apoiará projetos de infraestruturas sustentáveis e de alta qualidade nos setores digital, do clima e da energia, dos transportes, da saúde, da educação e da investigação. A Comissão incluirá agora considerações de segurança, se for caso disso, nos futuros investimentos da Estratégia Global Gateway. Tal incluirá iniciativas essenciais para a autonomia estratégica da UE e dos seus países parceiros, nomeadamente projetos de infraestruturas que incorporem avaliações de segurança e medidas de atenuação dos riscos.

A Comissão prosseguirá a celebração de novos **acordos entre a UE e países terceiros sobre a cooperação com a Europol e a Eurojust**, nomeadamente com os países da América Latina.

Além disso, a participação proativa de países terceiros na **EMPACT** é um dos meios mais eficazes para reforçar a cooperação operacional. A UE continuará a incentivar a participação de países terceiros no seu quadro, nomeadamente dos Balcãs Ocidentais, da Vizinhança Oriental, da África Subsariana, do Norte de África, do Médio Oriente, da América Latina e das Caraíbas. Outro instrumento que contribuirá para intensificar a cooperação com países terceiros no combate à criminalidade é a unidade operacional entre os Estados-Membros e coordenada pela Europol, onde os países terceiros podem participar. A Comissão pretende também concluir as negociações do acordo internacional **UE-Interpol**[86], assegurando uma abordagem mais unificada das ameaças à segurança mundial e do combate à criminalidade transnacional.

[85] JOIN(2023) 8 final.
[86] Decisão 2021/1312 do Conselho e Decisão (UE) 2021/1313 do Conselho, ambas de 19 de julho de 2021.

A **União deve estar presente no terreno no âmbito de uma abordagem da Equipa Europa**. O pessoal especializado da União e dos Estados-Membros desempenha um papel fundamental para assegurar que a ação externa da União seja bem informada, coordenada e reativa. Para elevar esta abordagem para um novo nível, a Comissão, apoiada pela alta representante para os Negócios Estrangeiros e a Política de Segurança, reforçará as **redes de ligação** e promoverá o destacamento de **agentes de ligação regionais da Europol e da Eurojust**, em consonância com as necessidades operacionais dos Estados-Membros.

A UE procurará uma cooperação operacional policial e judiciária mais estreita e promoverá a partilha de informações em tempo real e operações conjuntas através de **equipas de investigação conjuntas** em países terceiros, com o apoio da Europol e da Eurojust. A Comissão apoiará igualmente os Estados-Membros na criação de **centros de fusão conjuntos** que reúnam peritos e serviços locais de polícia em países terceiros estratégicos.

Instrumentos da Política Externa e de Segurança Comum (PESC)

As **missões da Política Comum de Segurança e Defesa (PCSD)** serão também utilizadas em todo o seu potencial para melhor identificar e combater as ameaças externas à segurança interna da UE, em conformidade com os respetivos mandatos definidos pelo Conselho. Para reforçar as capacidades dos países terceiros, a alta representante para os Negócios Estrangeiros e a Política de Segurança e a Comissão apoiarão as ações da PCSD com instrumentos de financiamento específicos e explorarão todas as vias de financiamento adequadas.

As **medidas restritivas da UE** são um instrumento bem estabelecido da PESC, também utilizado na luta contra o terrorismo. Com base nas sugestões da alta representante para os Negócios Estrangeiros e a Política de Segurança, dos Estados-Membros ou da Comissão, o Conselho poderá avaliar a forma como as atuais medidas restritivas autónomas da UE (lista UE de terroristas) poderão tornar-se mais eficazes, operacionais e ágeis. Além disso, poderão ponderar a possibilidade de explorar medidas restritivas adicionais contra as redes criminosas, em consonância com os objetivos da PESC.

Política de vistos e intercâmbio de informações

A política de vistos da UE é um instrumento fundamental para a cooperação com os países terceiros e a segurança das nossas fronteiras, controlando a entrada na UE e estabelecendo as condições para a mesma. A Comissão integrará plenamente as **considerações de segurança na política de vistos da UE** através de uma futura Estratégia da UE sobre a Política de Vistos. A Comissão trabalhará com os colegisladores para adotar a proposta de revisão e racionalização do mecanismo de suspensão, em especial para casos específicos de utilização abusiva do regime de isenção de vistos[87]. Os países terceiros serão incentivados a partilhar informações sobre pessoas que possam constituir ameaças à segurança, que serão introduzidas nos sistemas de informação e nas bases de dados da UE.

A fim de alcançar a coordenação das políticas e os esforços a montante, desbloqueando uma cooperação mais eficiente, célere e harmoniosa, a Comissão trabalhará no sentido de estabelecer **mecanismos de fluxo de dados** e formas de **reforçar o intercâmbio de informações** com países terceiros de confiança para efeitos de aplicação da lei e de gestão das fronteiras, em conformidade com os direitos fundamentais e as regras em matéria de proteção de dados.

Principais ações
A Comissão irá:

[87] COM(2023) 642.

- **celebrar acordos internacionais entre a UE e países terceiros prioritários em matéria de cooperação com a Europol e a Eurojust;**
- **incentivar a participação dos países parceiros na EMPACT para combater a criminalidade organizada e o terrorismo;**
- **apoiar as agências e organismos da UE na criação e no reforço de acordos de trabalho com os países parceiros;**
- **refletir mais aprofundadamente as considerações de segurança na política de vistos da UE através da futura Estratégia da UE sobre a Política de Vistos;**
- **reforçar o intercâmbio de informações com países terceiros de confiança para efeitos de aplicação da lei e de gestão das fronteiras.**

A Comissão, em cooperação com a alta representante para os Negócios Estrangeiros, irá:

- **tirar pleno partido das missões civis da Política Comum de Segurança e Defesa (PCSD);**
- **coordenar inspeções conjuntas em portos de países terceiros até 2027.**

A Comissão, em cooperação com a alta representante para os Negócios Estrangeiros e os Estados-Membros, irá:

- **reforçar as redes de ligação e a cooperação no âmbito de uma abordagem da Equipa Europa;**
- **criar equipas operacionais conjuntas e centros de fusão em países terceiros a partir de 2025.**

O Parlamento Europeu e o Conselho são incentivados a:

- **concluir as negociações sobre a revisão do mecanismo de suspensão de vistos.**

8. Conclusão

Num mundo de incerteza, é necessário reforçar a capacidade da União para antecipar, prevenir e responder a ameaças à segurança.

Não basta apenas responder às crises quando estas ocorrem. É necessário aumentar a nossa consciencialização com uma panorâmica completa das ameaças à medida que estas evoluem, e garantir que os nossos instrumentos e capacidades estão à altura.

O conjunto abrangente de medidas descritas na presente estratégia contribuirá para criar uma União mais forte no mundo: uma União capaz de antecipar, planear e garantir a sua própria segurança, capaz de responder eficazmente às ameaças à sua segurança interna, responsabilizar os seus autores e proteger as suas sociedades e democracias abertas, livres e prósperas.

Tal exige uma mudança de mentalidade em matéria de segurança interna. Trabalharemos no sentido de ajudar a promover uma nova cultura de segurança da UE, em que as considerações de segurança sejam tidas em conta em toda a nossa legislação, políticas e programas – desde o início até à sua execução, bem como nos casos em que a colaboração entre os domínios de intervenção nos permita explorar novos caminhos.

Esta não é uma tarefa para uma única instituição, governo ou interveniente. É uma missão comum da Europa.