COMISSÃO
EUROPEIA

Bruxelas, 9.12.2020
COM(2020) 797 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

Primeiro relatório intercalar sobre a Estratégia da UE para a União da Segurança

I INTRODUÇÃO

A segurança é uma das principais preocupações dos cidadãos, e a recente vaga de atentados terroristas em solo europeu evidenciou ainda mais a necessidade de uma ação por parte da UE. Em 24 de julho de 2020, a Comissão adotou a **Estratégia da UE para a União da Segurança 2020-2025**[1], no sentido de orientar as ações para os domínios prioritários em que a UE pode trazer valor acrescentado aos esforços nacionais. Assenta nos progressos alcançados anteriormente no âmbito da Agenda Europeia para a Segurança 2015-2020[2] e propicia um novo foco, para garantir que a política de segurança da UE reflete o cenário de ameaça em mutação; na construção de uma resiliência sustentável a longo prazo; no envolvimento das instituições e agências da UE, dos governos, do setor privado e dos indivíduos, numa abordagem mobilizadora de toda a sociedade e que congregue os muitos domínios de ação com um impacto direto na segurança. O pleno respeito dos direitos fundamentais é central neste trabalho, dado que a segurança da União só pode ser assegurada se os cidadãos estiverem seguros de que os seus direitos fundamentais são plenamente respeitados.

A ameaça das redes terroristas transnacionais é um demonstra claramente a absoluta necessidade de uma ação coordenada por parte da UE para uma ação eficaz de proteção dos europeus, defendendo os nossos valores comuns e o nosso modo de vida europeu. O caso do terrorismo é emblemático da forma como têm vindo a surgir ameaças à segurança transfronteiras e transectoriais cada vez mais complexas, que tornam ainda mais essencial uma cooperação mais estreita em matéria de segurança a todos os níveis, da criminalidade organizada ao comércio de drogas – mas também no mundo digital, onde os ciberataques e a cibercriminalidade continuam a aumentar. Todos estes desafios são também aplicáveis para lá das nossas fronteiras, com uma clara interligação entre a segurança interna e externa. A crise da COVID-19 pôs igualmente em evidência a situação da segurança europeia, tendo posto à prova a resiliência das infraestruturas críticas da Europa, a preparação para situações de crise, as cadeias de valor estratégicas e os sistemas de gestão de crises, bem como a resiliência das nossas sociedades face à interferência manipuladora e à desinformação.

A Estratégia para a União da Segurança é composta por quatro prioridades de ação estratégicas a nível da UE: um ambiente de segurança a longo prazo, fazer face à evolução das ameaças, proteger os europeus do terrorismo e da criminalidade organizada e criar um sólido ecossistema europeu de segurança. A questão da aplicação é central para a estratégia, pelo que constitui o tema central do presente relatório: a aplicação requer o empenho total das autoridades nacionais na linha da frente da segurança na UE. O presente é o primeiro relatório de execução no âmbito da estratégia, cumprindo o compromisso assumido pela Comissão de apresentar relatórios regulares sobre os progressos[3]. Abrange o período com início em 31 de outubro de 2019, quando foi publicado o último relatório intercalar da União da Segurança ao abrigo do mandato da anterior Comissão[4].

II UM AMBIENTE DE SEGURANÇA A LONGO PRAZO

1. *Proteção e resiliência das infraestruturas críticas*

[1] COM (2020) 605.
[2] COM(2016) 230.
[3] Durante a audição do vice-presidente Margaritis Schinas perante o Parlamento Europeu, em 3.10.2019.
[4] COM(2019) 552.

A vida diária dos cidadãos depende de uma infraestrutura física e digital cada vez mais interligada e interdependente. Esta infraestrutura é essencial para o funcionamento da economia e da sociedade. Sem um aprovisionamento energético fiável, transportes previsíveis, sistemas de saúde abrangentes ou uma rede financeira baseada no digital, o nosso modo de vida atual não seria possível. A pandemia de COVID-19 tornou ainda mais evidente a importância de **garantir a resiliência dos setores e dos operadores críticos**. A UE reconheceu o interesse comum em proteger as infraestruturas críticas contra as ameaças, quer sejam catástrofes, naturais ou de origem humana, ou ataques terroristas. O quadro atual das ameaças com que as infraestruturas críticas se defrontam é amplo. Inclui: terrorismo, ações híbridas, ciberataques, incidentes internos; ameaças associadas a tecnologias novas e emergentes (como os drones, a 5G e a inteligência artificial); desafios relacionados com as alterações climáticas; perturbações nas cadeias de abastecimento e interferência em eleições. As nossas regras atuais precisam de ser modernizadas e alargadas[5]. É necessário transferir o foco da proteção para a resiliência, trazendo mais coerência e consistência à cobertura setorial, e centrar a atenção nas entidades críticas que prestam serviços essenciais.

Este será o objetivo das propostas a apresentar brevemente no sentido de promover a resiliência das **infraestruturas físicas e digitais**. O objetivo geral é aumentar a preparação a nível nacional e da UE, criando capacidades sólidas para prevenir, detetar, dar resposta e atenuar as ameaças, e estar preparado para agir em situações de crise. A legislação em vigor tem conseguido aumentar e melhorar a gestão dos riscos nos setores críticos, num esforço que precisa de ser intensificado. Um dos principais objetivos da Diretiva Infraestruturas Críticas revista será promover um elevado nível comum de resiliência num leque suficiente de setores essenciais. Do mesmo modo, a atualização da Diretiva Segurança das Redes e da Informação (SRI) visará uma maior consistência na identificação, pelos Estados-Membros, dos «operadores de serviços essenciais»[6]. De um modo mais geral, e apesar dos progressos consideráveis, as capacidades de cibersegurança nos Estados-Membros ainda são desiguais, pelo que a revisão procurará aumentar a cibersegurança em termos globais[7]. Os resultados serão abordagens mais alargadas e mais coerentes em matéria de resiliência das infraestruturas físicas e digitais.

À medida que os trabalhos avançam no sentido de alcançar este quadro mais coerente, foram lançadas **iniciativas setoriais** que complementam estes trabalhos e visam vulnerabilidades específicas. Com base na recomendação da Comissão de 2019[8], estão a ser envidados atualmente esforços no sentido de progredir no que respeita aos desafios específicos da cibersegurança para o setor da energia, tendo em conta características do setor como a necessidade de atuar em tempo real, o risco de efeitos em cascata e a combinação dos sistemas herdados com as novas tecnologias. Estão em curso trabalhos relativos a um código de rede próprio para a cibersegurança dos fluxos transfronteiras de eletricidade, bem como para a proteção da resiliência e da cibersegurança das infraestruturas energéticas críticas. Foi igualmente relançada a Rede Temática para a Proteção das Infraestruturas Energéticas Críticas, com prioridades e objetivos renovados, que se reuniu pela primeira vez em junho de 2020 com mais de cem participantes em linha.

---

5 Diretiva 2008/114/CE e Diretiva (UE) 2016/1148.

6 COM(2019) 546. A Comissão realizou também uma consulta pública (de 7 de julho a 2 de outubro de 2020) e visitas a todos os Estados-Membros com a finalidade de verificar a conformidade na aplicação da diretiva através de reuniões com os operadores e com as autoridades nacionais.

7 COM(2019) 546.

8 COM(2019) 2400.

Esta rede fornece uma plataforma com vista a fomentar a colaboração transfronteiras entre os operadores e os proprietários de infraestruturas energéticas críticas.

A fim de garantir uma base de partida comum para a colaboração entre os Estados-Membros na **preparação para os riscos no setor da eletricidade** a Rede Europeia dos Operadores das Redes de Transporte de Eletricidade definiu em setembro de 2020 os cenários regionais de crise de eletricidade mais relevantes, conforme previsto no regulamento de preparação para os riscos[9]. Esses cenários incluem os ciberataques, bem como as pandemias e os eventos meteorológicos extremos. Os Estados-Membros prepararão cenários nacionais de crise e planos de preparação para os riscos, a fim de prevenir e atenuar as crises de eletricidade (os anteprojetos estão previstos para abril de 2021). Para contribuir para este processo, foi emitido em junho de 2020 um conjunto de boas práticas[10], com base no acompanhamento rigoroso do impacto da COVID-19 no setor da energia através dos grupos de coordenação nos setores da eletricidade, do gás e do petróleo, bem como do Grupo de Reguladores Europeus em matéria de Segurança Nuclear e do Grupo de Autoridades do Petróleo e do Gás *Offshore* da União Europeia.

A crescente e sofisticada dependência dos processos digitais na prestação de serviços financeiros também exige o aumento do nível de cibersegurança no **setor financeiro**. Embora a segurança dos sistemas TIC seja reconhecida como parte integrante da gestão dos riscos para as entidades financeiras, tal ainda não se refletiu plenamente no quadro regulamentar dos serviços financeiros da UE. Em 24 de setembro de 2020, a Comissão adotou o seu pacote Estratégia de Financiamento Digital[11], com o claro objetivo claro de dar resposta aos desafios e aos riscos associados à transformação digital, promovendo a resiliência, a proteção de dados e uma supervisão prudencial adequada. O pacote incluiu uma proposta legislativa relativa à resiliência operacional digital[12], a fim de garantir que existam salvaguardas para atenuar os ciberataques e outros riscos[13]. Esta iniciativa contribui para um setor financeiro digital europeu robusto e dinâmico, reforçando assim a autonomia estratégica aberta da Europa nos serviços financeiros e, consequentemente, a sua capacidade para regulamentar e supervisionar o sistema financeiro de modo a proteger a estabilidade financeira na Europa.

Durante as emergências de grande escala, o elevado grau de interdependência entre os setores e os países exige uma ação coordenada para garantir uma resposta rápida e eficaz, bem como uma melhor prevenção e preparação para situações similares no futuro. Na revisão da Decisão relativa a um Mecanismo de Proteção Civil da União Europeia[14], a Comissão propôs[15] o desenvolvimento de **objetivos de resiliência a catástrofes** e um **planeamento da resiliência**, com um foco reforçado na construção de uma resiliência transetorial a longo prazo para as catástrofes transfronteiras. A nova abordagem proposta, de reforço da resiliência, complementa o trabalho de gestão dos riscos de catástrofes a nível nacional. Em 26 de novembro, o Conselho chegou a acordo sobre um mandato de

---

9 JO L 158 de 14.6.2019, p. 1.

10 «Energy security: good practices to address pandemic risks» [SWD(2020) 104].

11 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en.

12 COM(2020) 595.

13 A proposta estabelece uma linha de base coerente para os requisitos aplicáveis à gestão dos riscos das TIC, à comunicação de incidentes de TIC aos supervisores financeiros, aos testes digitais e à partilha de informações. Além disso, submete os prestadores de serviços terceiros de TIC críticos a um quadro de supervisão à escala europeia.

14 Decisão n.º 1313/2013/UE, de 17 dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia.

15 COM(2020) 220.

negociação para reforçar a prevenção, a preparação e a resposta em caso de catástrofe, com base na proposta da Comissão de 2 de junho de 2020[16].

A pandemia de COVID-19 demonstrou o impacto da crise sanitária na segurança a nível da UE e a nível mundial, e destacou a necessidade de intensificar o planeamento da preparação e da resposta em caso de epidemias e outras ameaças sanitárias transfronteiriças graves. O pacote da Comissão, de 11 de novembro de 2020, sobre «**Construir uma União Europeia da Saúde:** Reforçar a resiliência da UE» definiu as próximas medidas destinadas a fazer face às ameaças sanitárias transfronteiriças. O pacote criará um quadro reforçado para a cooperação transfronteiriça contra todas as ameaças para a saúde e incluirá três propostas legislativas: atualizar a legislação relativa às ameaças sanitárias transfronteiriças graves e reforçar o Centro Europeu de Prevenção e Controlo das Doenças (ECDC) e a Agência Europeia de Medicamentos (EMA). Em conjunto, estas propostas estabelecerão um quadro sólido e eficaz em termos de custos para colocar a UE e os Estados-Membros numa posição mais segura na resposta a futuras crises sanitárias.

Um elemento fundamental para proteger os principais ativos digitais da UE e nacionais é oferecer às infraestruturas críticas um canal para **comunicações seguras**. O desenvolvimento de uma infraestrutura de rede para comunicações governamentais por satélite seguras e resilientes, como componente do Programa Espacial da UE, contribuirá para esse processo.

[16] Proposta de alteração da Decisão n.º 1313/2013/UE relativa a um Mecanismo de Proteção Civil da União Europeia – Mandato para as negociações com o Parlamento Europeu.

2. *Cibersegurança*

Os benefícios da transformação digital são claros, mas também claro é o facto de que será inevitavelmente acompanhada por um aumento das potenciais vulnerabilidades[17]. A infraestrutura crítica é frequentemente alvo de ciberataques cada vez mais sofisticados[18]. Por conseguinte, a **cibersegurança** deve ser uma preocupação não só dos decisores políticos mas também de todas as pessoas que trabalham ou comunicam em linha.

Para aumentar a confiança e a segurança dos produtos, dos processos e dos serviços digitais, o ato legislativo relativo à cibersegurança, de junho de 2019, criou **um enquadramento da UE para a certificação da cibersegurança**. A Comissão solicitou à Agência da União Europeia para a Cibersegurança, ENISA, que preparasse dois sistemas de certificação da cibersegurança, estando essa preparação bem encaminhada. Este trabalho envolve igualmente as autoridades nacionais de certificação da cibersegurança, a indústria, os consumidores, os organismos de acreditação, os organismos de normalização e de certificação, bem como o Comité Europeu para a Proteção de Dados.

Inclui nomeadamente um sistema de **serviços de computação em nuvem** para apoiar um mercado de serviços de computação em nuvem seguro e fiável. Esse será um elemento essencial para a **estratégia para os dados da UE**, adotada em fevereiro de 2020[19]. Criaria uma linha de base de segurança comum para os serviços de computação em nuvem em todos os setores, com base no denominador comum mais elevado das normas, dos sistemas e das práticas existentes (europeus e internacionais). Este será um elemento essencial para

[17] ENISA Threat Landscape 2020: «Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected».

[18] Desde o início da pandemia, as agências da UE e os Estados-Membros detetaram um aumento significativo dos ciberataques, nomeadamente contra o setor dos cuidados de saúde.

[19] COM(2020) 66.

o livre fluxo de dados na UE[20]. O sistema promoverá igualmente a adoção de tecnologias de computação em nuvem, fornecendo aos utilizadores, em particular às pequenas e médias empresas e à administração pública, uma garantia alargada quanto ao nível de segurança quando utilizam a computação em nuvem.

Tal como salientado na Estratégia para a União da Segurança, e tendo em conta a introdução da infraestrutura 5G na UE e a potencial dependência de muitos serviços críticos das redes 5G, as consequências de perturbações sistémicas e generalizadas podem ser particularmente graves. O resultado tem sido um esforço comum envidado pelos Estados-Membros para desenvolver e pôr em prática medidas de segurança adequadas. Na sequência da recomendação da Comissão sobre a **cibersegurança das redes 5G**, de março de 2019[21], os Estados-Membros concluíram as suas avaliações nacionais dos riscos, que se traduziram num relatório de avaliação coordenada dos riscos da UE[22] que identifica os desafios em matéria de segurança associados às redes 5G. Nesta base, em 29 de janeiro de 2020, o grupo de cooperação SRI[23] publicou o **conjunto de medidas de atenuação dos riscos da UE**[24], estabelecendo as medidas estratégicas e técnicas necessárias. O conjunto de instrumentos inclui medidas para reforçar os requisitos de segurança aplicáveis aos operadores de redes móveis, garantir a diversidade dos fornecedores para os operadores de redes móveis individuais, avaliar o perfil de risco desses fornecedores e aplicar restrições aos fornecedores considerados de alto risco. A Comissão apoiará a aplicação do conjunto de instrumentos, utilizando plenamente as suas competências e os meios à sua disposição[25], incluindo as regras em matéria de telecomunicações e cibersegurança; coordenação em matéria de normalização e de certificação à escala da UE e o quadro da UE para os investimentos diretos estrangeiros[26].

Em julho de 2020, o grupo de cooperação SRI publicou um relatório intercalar sobre a aplicação das medidas do conjunto de instrumentos[27]. Este relatório salientou que a grande maioria dos Estados-Membros já adotou ou está em processo de aplicação das medidas recomendadas no conjunto de instrumentos. As medidas em que se verificou uma aplicação menos avançada incluíram a atenuação do risco de dependência dos fornecedores considerados de alto risco e o desenvolvimento de estratégias de diversificação dos fornecedores, tanto a nível das empresas como a nível nacional.

No decurso dos últimos meses, as instituições da UE e os Estados-Membros responderam ao aumento do nível de risco para a cibersegurança desencadeado pela **crise da COVID-19**, mediante a intensificação do intercâmbio de informações e o aumento do nível de preparação para uma potencial cibercrise. A cooperação da UE foi intensificada em fóruns importantes (grupo de cooperação SIR e rede de equipas de resposta a incidentes de

---

[20] Regulamento (UE) 2018/1807.

[21] COM(2019) 2335.

[22] Relatório sobre a avaliação coordenada pela UE dos riscos para a cibersegurança das redes 5G.

[23] O grupo de cooperação SRI foi criado para garantir a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros da UE sobre a cibersegurança.

[24] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[25] COM(2020) 50.

[26] Regulamento (UE) 2019/452. Contém igualmente referências explícitas a «infraestruturas críticas» (bem como a «tecnologias críticas»), de forma mais abrangente, enquanto «fatores que podem ser tomados em consideração pelos Estados-Membros ou pela Comissão», aquando da avaliação do impacto potencial de um investimento.

[27] Relatório sobre os progressos realizados pelos Estados-Membros na aplicação do conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G.

segurança informática [CSIRT]), bem como através de novas formas de coordenação e de instrumentos de partilha de informações[28]. Em setembro de 2020, houve um segundo exercício teórico a nível operacional para o plano pormenorizado (Blue OLEx)[29], em que foi lançada ainda a «Rede de Organizações de Ligação para a Cibercrise» (CyCLONe) dos Estados-Membros, a qual reforçará a aplicação do plano pormenorizado para as respostas rápidas de emergência a ciberincidentes ou a cibercrises transfronteiras em grande escala[30].

No ciberespaço global, os ciberataques e as ciberameaças têm frequentemente origem fora da UE. Para fazer face a estes desafios eficazmente, a UE e os Estados-Membros cooperam para promover a segurança e a estabilidade internacionais no ciberespaço, promover o comportamento responsável do Estado e aumentar a resiliência global e a sensibilização para as ciberameaças e para as ciberatividades maliciosas, inclusive com parceiros internacionais[31]. Em 30 de abril de 2020, o alto representante publicou uma declaração em nome da UE condenando o comportamento malicioso no ciberespaço e expressando solidariedade para com as vítimas[32].

Em 30 de julho de 2020, o Conselho adotou as **primeiras cibersanções da UE**, contra seis indivíduos e três entidades responsáveis ou envolvidas em ciberataques. Os casos incluem a tentativa de ciberataque contra a Organização para a Proibição de Armas Químicas (OPAQ) e aqueles publicamente conhecidos por «WannaCry», «NotPetya» e «Operation Cloud Hopper». Em 22 de outubro de 2020, o Conselho aplicou sanções a outros dois indivíduos e a uma entidade responsáveis ou envolvidos no ciberataque contra o Parlamento Federal alemão. Estas decisões seguiram-se à sinalização contínua da UE e dos Estados-Membros da necessidade de prevenir, desencorajar, dissuadir e dar resposta às ciberatividades maliciosas, nomeadamente ao fazer uso do seu regime de cibersanções como parte do seu conjunto de instrumentos de 2017 para a ciberdiplomacia[33].

As negociações entre os colegisladores sobre as novas regras em matéria de exportação que restringem a venda de bens de cibervigilância a regimes mundiais envolvidos na

---

[28] As instituições e os organismos da UE reuniram-se num grupo de missão para a cibersegurança no quadro da COVID-19 e lançaram um relatório semanal de sensibilização e de análise setorial da situação. A ENISA e a Europol lançaram campanhas sobre como manter a cibersegurança durante a COVID-19. A CERT-UE emitiu orientações sobre a forma de instalar RPV seguras. No verão de 2019, o grupo de cooperação estabeleceu um novo domínio de intervenção dedicado à cibersegurança na saúde e a Comissão e a ENISA lançaram o Centro da UE para a Análise e Partilha de Informações sobre a Saúde.

[29] https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone.

[30] COM(2017) 6100.

[31] A UE promove o quadro estratégico para a prevenção de conflitos, a estabilidade e a cooperação no ciberespaço, nomeadamente através da participação nos debates das Nações Unidas sobre as questões do ciberespaço. Dois processos importantes são o grupo de trabalho aberto sobre a evolução no domínio da evolução das tecnologias da informação e da comunicação no contexto da segurança internacional e o grupo de peritos governamentais encarregado de promover o comportamento responsável dos Estados no ciberespaço, no contexto da segurança internacional. As questões em causa incluem o impacto do direito internacional, a aplicação de normas voluntárias e não vinculativas de comportamento responsável dos Estados e de medidas de reforço de confiança, bem como o desenvolvimento da aplicação da regulamentação por meio do reforço de capacidades específicas.

[32] https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.

[33] Decisões do Conselho (PESC) 2020/1127, 2020/1537 e 2020/651 como parte do documento 9916/17.

repressão dos direitos humanos[34] também progrediram. Uma vez adotadas, estas regras conduzirão a um comércio mais responsável, concorrencial e transparente de produtos de dupla utilização[35]. As alterações propostas, tornadas necessárias pelos desenvolvimentos tecnológicos e pelos riscos de segurança crescentes, incluem novos critérios para conceder ou rejeitar licenças de exportação para certos produtos.

3. Proteção dos espaços públicos

Conforme reconhecido na agenda da UE de luta contra o terrorismo[36], a proteção dos espaços públicos, através do reforço da resiliência contra as ameaças à segurança, continua a ser uma componente crucial dos trabalhos para uma União da Segurança efetiva e genuína. A Comissão está a trabalhar com um leque abrangente de partes interessadas, públicas e privadas, a fim de desenvolver orientações e prestar apoio prático e financiamento[37], em conformidade com o **plano de ação de 2017 para apoiar a proteção dos espaços públicos**[38] e com a recolha de boas práticas para apoiar a proteção dos espaços públicos, de 2019[39]. Como consta da agenda da UE de luta contra o terrorismo, a Comissão intensificará o seu apoio às autoridades locais e regionais, que desempenham um papel fundamental na proteção dos espaços públicos e na prevenção da radicalização. Tal incluirá a elaboração de um protocolo da UE relativo à segurança urbana e à resiliência para as cidades, estabelecendo princípios e objetivos básicos para as autoridades locais nestes domínios.

Dado que os ataques terroristas têm cada vez mais como alvo os **locais de culto**, é colocado particular ênfase na cooperação entre as autoridades públicas e os líderes e as congregações religiosas, a fim de melhorar o nível de sensibilização para a segurança e ajudar a implementar boas práticas e formação nesses mesmos locais de culto. Há medidas simples que podem representar a diferença entre a vida e a morte. Em outubro de 2019, uma sinagoga em Halle foi alvo de um ataque terrorista. Uma porta blindada, um botão de pânico e câmaras de segurança, em conjunto, ajudaram a salvar vidas.

Para apoiar ainda mais o reforço da segurança nos espaços públicos, particularmente em locais de culto, a Comissão disponibilizou 20 milhões de EUR em 2020 para projetos liderados por partes interessadas.

A Comissão também está a trabalhar na resposta aos **riscos emergentes associados aos espaços públicos**, incluindo os **sistemas de aeronaves não tripuladas** (SANT). Embora os drones tragam oportunidades económicas e de emprego significativas, também representam um risco significativo para os espaços públicos, para as infraestruturas críticas e para outros locais sensíveis, como as prisões. As recentes regras da UE[40] neste domínio

---

34 COM(2016) 616. A proposta da Comissão visa alterar e reformular o Regulamento n.º 428/2009, que cria um regime comunitário de controlo das exportações, transferências, corretagem e trânsito de produtos de dupla utilização.

35 Trata-se de um vasto grupo de bens, materiais, *software* e tecnologia que pode ser utilizado para fins civis e militares.

36 COM (2020) 795.

37 O concurso público «ISF Protect», de 2019, incluiu o projeto «Secu4All», desenvolvendo um ciclo de formação abrangente destinado às autoridades locais para fornecer aos cidadãos um ambiente urbano seguro, e o projeto «DroneWISE», que visa reforçar a preparação dos elementos de primeira intervenção para combater veículos aéreos não tripulados hostis. Em 2020, haverá um novo concurso público com um orçamento de 12 milhões de EUR para a proteção dos espaços públicos.

38 COM(2017) 612.

39 SWD(2019) 140.

40 Regulamento de Execução (UE) 2019/947 da Comissão.

atenuam este risco, ao reforçarem a segurança das operações com drones. A partir de janeiro de 2021, os operadores de drones serão também obrigados a efetuar o seu registo junto das autoridades nacionais. Este regime pode ser complementado por um **quadro regulamentar para o espaço-U**, o sistema de gestão do tráfego não tripulado da Europa[41], para garantir operações com drones mais seguras e fiáveis. Em conjunto, estas medidas limitarão a possibilidade de os indivíduos colocarem em voo drones em áreas restritas e ajudarão a identificar e a responsabilizar os infratores.

A Comissão está igualmente a trabalhar no sentido de apoiar a aplicação da lei, os operadores de infraestruturas críticas, os organizadores de eventos de massa e outras partes interessadas, com vista a combater a utilização abusiva dos drones, por exemplo, trabalhando com a Agência da União Europeia para a Segurança da Aviação no desenvolvimento de **boas práticas para ajudar as partes interessadas aeroportuárias** a responder a incidentes não autorizados com drones, facilitando os **esforços para testes de contramedidas** mais harmonizados à escala da UE e desenvolvendo um manual prático destinado às partes interessadas, com foco no contexto urbano.

A **escola digital de outono da UE para a proteção dos espaços públicos**, organizada pelo Centro Comum de Investigação da Comissão em outubro de 2020, reuniu mais de 200 urbanistas e operadores públicos e privados dos espaços públicos. As sessões examinaram um vasto conjunto de temas, por exemplo a forma de se proteger contra as explosões e o atropelamento com veículos, atenuar as ameaças colocadas por drones hostis em ambientes urbanos e a utilização de tecnologias de vigilância e deteção.

A Comissão também continuou a apoiar ativamente a **Parceria para a Segurança nos Espaços Públicos**, lançada em janeiro de 2019 no âmbito da Agenda Urbana da UE, que publicou o seu novo plano de ação[42] para fazer face à segurança urbana em vários níveis de governação. As ações incluem a criação de um quadro para um instrumento de autoavaliação, recomendações para a elaboração de políticas, governação e financiamento a vários níveis, inovação por meio de soluções e tecnologias inteligentes, incluindo o conceito de segurança desde a conceção, a prevenção e a inclusão social. A parceria entrará agora na fase de implementação.

O apoio à melhoria da segurança dos espaços públicos a nível local também foi prestado através do 4.º convite à apresentação de propostas no domínio das Ações Urbanas Inovadoras. Foram selecionadas três cidades que estão a testar novas soluções no domínio da segurança urbana (Pireu, na Grécia, Tampere, na Finlândia, e Turim, na Itália), com financiamento do Fundo Europeu de Desenvolvimento Regional.

[41] A Comissão poderá apresentar um regulamento de execução para o efeito, que seria adotado no âmbito de um procedimento de exame envolvendo o Comité para a Segurança da Aviação.

[42] O plano de ação foi adotado e está disponível no Futurium, em: https://ec.europa.eu/futurium/en/security-public-spaces/security-public-spaces-partnership-final-action-plan-0.

Em termos de resposta, a Comissão desenvolveu igualmente um quadro europeu para melhorar a preparação e a resposta a incidentes resultantes de grandes incêndios, explorando a capacidade europeia global de cuidados a queimados para tratar doentes, através da cooperação a nível da UE. O Mecanismo de Proteção Civil da União Europeia pode ser utilizado para prestar apoio a um grande número de doentes com queimaduras graves, fornecendo acesso a camas para queimados em centros de tratamento especializados, peritos em avaliação de queimaduras e capacidades de evacuação médica.

III FAZER FACE ÀS AMEAÇAS EM PERMANENTE EVOLUÇÃO

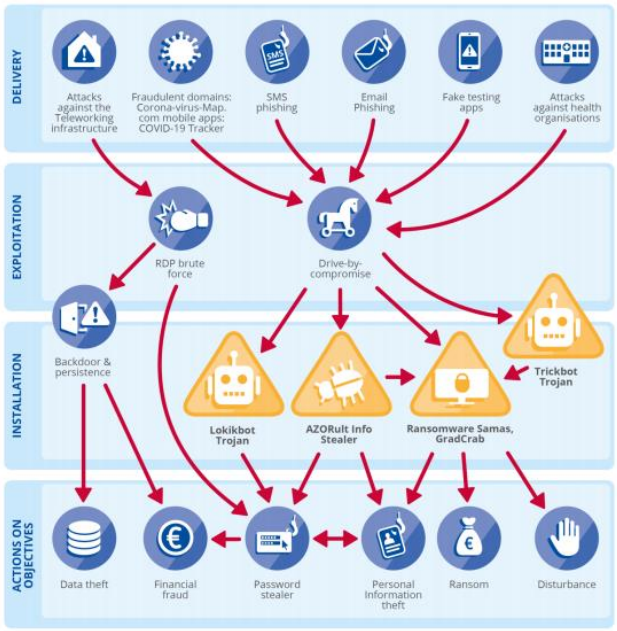
1. Cibercriminalidade

As deficiências na cibersegurança são frequentemente exploradas pelos criminosos. Esse facto ficou mais claro do que nunca durante a crise da COVID-19. Houve um aumento no cibercrime «clássico», utilizando programas maliciosos (*malware*) e programas sequestradores (*ransomware*) (ou seja, programas que tentam roubar os dados pessoais e de pagamento ou chantagear as vítimas), bem como uma proliferação de novos sítios Web que induzem os utilizadores a instalar programas maliciosos. Ocorreram ciberataques às infraestruturas de cuidados de saúde e de investigação, bloqueando os sistemas de TIC, que só podem ser desbloqueados mediante o pagamento de um resgate ou mediante o acesso a informações sobre o desenvolvimento de vacinas[43]. Também se observou um aumento significativo no abuso sexual de crianças e na pornografia infantil[44].

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

THREAT LANDSCAPE MAPPING

Exploitation by cybercriminals and advanced persistent threat (APT) groups of the current coronavirus (COVID-19) global pandemic.



Uma resposta eficaz ao cibercrime requer um quadro sólido para as investigações e as ações penais, e um primeiro passo importante é a plena transposição e aplicação da diretiva relativa a **ataques contra os sistemas de informação**[45]. A Comissão está a acompanhar as ações da Bulgária, da Itália, de Portugal e da Eslovénia na sequência da abertura de processos de infração em 2019. São também necessários progressos na aplicação da **diretiva relativa à luta contra a exploração sexual de crianças**[46], de 2011. Os domínios em que ainda são necessários esforços incluem: medidas de prevenção, de direito penal

[43] «Internet Organised Crime Threat Assessment (IOCTA) 2020», outubro de 2020.
[44] Relatório «Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic», Europol, 19.6.2020.
[45] Diretiva 2013/40/UE.
[46] Diretiva 2011/93/UE.

substantivo, de assistência e de apoio e proteção às crianças vítimas de crimes. Desde 2018, a Comissão iniciou procedimentos de infração contra 25 Estados-Membros[47].

Em 24 de julho de 2020, a Comissão adotou a **Estratégia da UE para uma luta mais eficaz contra o abuso sexual de crianças**[48], que visa dar uma resposta eficaz, a nível da UE, ao crime de abuso sexual de crianças. Surgiu também um desafio específico, uma vez que, a partir de 21 de dezembro de 2020, determinados serviços de comunicação em linha, como o correio Web ou os serviços de mensagens, passarão a ser abrangidos pelo âmbito de aplicação da Diretiva Privacidade Eletrónica e pelas definições revistas do Código Europeu das Comunicações Eletrónicas. Como resultado, existe um risco claro de que os prestadores desses serviços, que realizam certas atividades voluntárias importantes com o objetivo de detetar, combater e comunicar atualmente o abuso sexual de crianças em linha, tenham de deixar de o fazer. Por conseguinte, a Comissão propôs um **regulamento**[49] para permitir que estas atividades voluntárias continuem sob certas condições, até que se adote uma solução legislativa a longo prazo. A Comissão está a trabalhar numa proposta para tal solução, com adoção prevista para 2021.

A **Aliança para a Ciberdefesa no quadro da COVID-19** foi criada pela rede europeia de centros de cibersegurança e pelo centro de competências para a inovação e as operações para desenvolver abordagens inovadoras, com vista a combater os crimes relacionados com a COVID-19. Em abril de 2020, foi criada a plataforma dedicada EIC COVID-19[50], para ligar a sociedade civil, os inovadores, os parceiros e os investidores em toda a Europa, a fim de desenvolver soluções inovadoras.

A fim de assegurar um exercício da ação penal mais eficaz, e tendo em vista a importância da informação e das provas eletrónicas nas investigações penais, as autoridades policiais e judiciárias devem obter rapidamente o acesso a tais informações e provas para as suas investigações criminais. Essa necessidade foi reconhecida na declaração comum dos ministros dos Assuntos Internos da UE de 13 de novembro de 2020[51]. A Europol, a Eurojust e a Rede Judiciária Europeia publicaram, em 1 de dezembro de 2020, o seu segundo relatório «SIRIUS EU Digital Evidence Situation Report». O relatório destaca a relevância crescente das provas eletrónicas nas investigações criminais[52]. O Parlamento Europeu ainda não definiu a sua posição sobre as propostas da Comissão, de abril de 2018, relativas ao **acesso transfronteiras a provas eletrónicas**[53], pelo que as negociações entre os colegisladores ainda não começaram. Os atrasos na adoção destas propostas estão a travar o trabalho das autoridades policiais e judiciárias, bem como a complicar os esforços

---

47 Alemanha, Áustria, Bélgica, Bulgária, Chéquia, Croácia, Eslováquia, Eslovénia, Espanha, Estónia, Finlândia, França, Grécia, Hungria, Irlanda, Itália, Letónia, Lituânia, Luxemburgo, Malta, Países Baixos, Polónia, Portugal, Roménia e Suécia

48 COM(2020) 607.

49 COM(2020) 568.

50 A Comissão, em conjunto com o Conselho Europeu da Inovação e os Estados-Membros, organizou a iniciativa pan-europeia «EUvsVirus Hackathon + Matchathon», https://covid-eic.easme-web.eu/.

51 Declaração comum dos ministros dos Assuntos Internos da UE sobre os recentes ataques terroristas na Europa, 13.11.2020, 12634/20.

52 De acordo com o relatório, o volume de pedidos transfronteiras apresentados pelas autoridades da UE aos prestadores de serviços em linha aumentou significativamente em 2019, sendo a sua grande maioria emitida pela Alemanha (37,7 % dos pedidos), pela França (17,9 %) e pelo Reino Unido (16,4 %). Os pedidos de acesso a dados eletrónicos duplicaram na Polónia e quase triplicaram na Finlândia. Além disso, os pedidos de divulgação urgentes aumentaram em cerca de metade num ano.

53 COM(2018) 226 e COM(2018) 225.

em curso no sentido de estabelecer regras compatíveis para o acesso transfronteiras a provas eletrónicas através de negociações internacionais[54].

A nível internacional, a Comissão participa, em nome da UE, nas negociações em curso resultantes do segundo protocolo adicional à **Convenção de Budapeste sobre o Cibercrime, no quadro do Conselho da Europa**. Este protocolo forneceria às autoridades de aplicação da lei instrumentos reforçados e de longo alcance para a cooperação transfronteiras na investigação e na repressão da cibercriminalidade e de outras formas graves de criminalidade, nomeadamente por via da cooperação direta com os prestadores de serviços. Uma vez que a maioria destas formas de cooperação melhoradas e reforçadas dependerão do intercâmbio de dados pessoais, é essencial que o futuro protocolo preveja salvaguardas de proteção de dados adequadas, não só na perspetiva dos direitos fundamentais mas também para garantir a segurança jurídica, a confiança mútua e a eficácia da cooperação operacional na aplicação da lei.

As negociações deverão estar concluídas em 2021. Paralelamente, na sequência do mandato recebido pelo Conselho JAI no ano passado, a Comissão está a negociar um acordo **UE-EUA sobre o acesso transfronteiras a provas eletrónicas**. Um acordo desse tipo complementaria as regras internas da UE propostas para a cooperação transfronteiras direta com os prestadores de serviços, eliminando os conflitos entre diferentes normas legislativas e prevendo regras e salvaguardas comuns. As negociações formais tiveram início em 25 de setembro de 2019 e já foram realizadas várias rondas. No entanto, o resultado das negociações depende em grande parte dos progressos alcançados em matéria de regras internas para a utilização de provas eletrónicas.

No que diz respeito à **conservação e à utilização de dados para fins de aplicação da lei**, a Comissão deu seguimento ao acórdão *Tele2/Watson*[55] adotado em 2016, através de consultas de peritos com os prestadores de serviços pertinentes, as autoridades policiais e judiciais, a sociedade civil, as autoridades responsáveis pela proteção de dados, as universidades e as agências da UE. As reflexões foram ainda sustentadas por um estudo sobre as práticas de conservação de dados dos prestadores de serviços de comunicações eletrónicas e as necessidades e práticas das autoridades de aplicação da lei no acesso aos dados, a identificação dos desafios tecnológicos pertinentes e uma panorâmica dos quadros jurídicos nacionais[56]. Este trabalho destacou a necessidade de as autoridades de aplicação da lei terem acesso aos dados para realizarem as suas tarefas com mais eficácia.

Em 6 de outubro de 2020, o Tribunal de Justiça proferiu decisões[57] relativas à legislação nacional da Bélgica, da França e do Reino Unido em matéria de conservação, transmissão e acesso a dados relativos à comunicação, excluindo o respetivo conteúdo, para efeitos de

---

[54] A título de exemplo, a Assembleia Geral das Nações Unidas (AGNU) adotou, em 27 de dezembro de 2019, a Resolução n.º 74/247 relativa ao «combate à utilização das tecnologias da informação e comunicação para efeitos penais», que cria um comité intergovernamental *ad hoc* aberto composto por peritos encarregados de preparar uma convenção internacional abrangente sobre a cibercriminalidade. A UE não apoia a criação de um novo instrumento jurídico internacional sobre a cibercriminalidade, uma vez que a Convenção de Budapeste sobre o Cibercrime já fornece um quadro jurídico multilateral abrangente. Em julho de 2020, os Estados-Membros da ONU concordaram em adiar as primeiras etapas: a UE contribuiu para o processo com base numa posição comum (documento 7677/2/20).

[55] Acórdão nos processos apensos de 21 de dezembro de 2016, *Tele2 Sverige AB/Watson e outros*, C-203/15 e C-698/15.

[56] https://data.europa.eu/doi10.2837/26288

[57] Acórdãos no processo Privacy International, C-623/17, e processos apensos La Quadrature du Net e outros, C-511/18, French Data Network e outros, C-512/18, e Ordre des barreaux francophones et germanophone e outros, C-520/18.

aplicação da lei e de segurança nacional. A Comissão avaliará as opções disponíveis para garantir que os terroristas e outros criminosos possam ser identificados e localizados, respeitando, ao mesmo tempo o direito da UE tal como interpretado pelo Tribunal de Justiça e tendo igualmente em conta outros processos pendentes no Tribunal sobre esta matéria.

Outro elemento importante na luta contra a cibercriminalidade tem sido o trabalho para garantir a disponibilidade e a exatidão dos dados relativos às informações de registo de nomes de domínio («**informações WHOIS**»), em consonância com os esforços da Corporação da Internet para a Atribuição de Nomes e Números (ICANN). As discussões procuram garantir que os requerentes legítimos de acesso, incluindo os operadores de aplicação da lei e de cibersegurança, obtenham um acesso eficiente aos dados genéricos de registo de domínios de topo, no pleno respeito das regras aplicáveis em matéria de proteção de dados. As recomendações finais para uma nova política de WHOIS foram publicadas em 10 de agosto de 2020 e estão atualmente sob revisão, antes de ser tomada uma decisão por parte do conselho de administração da ICANN. A Comissão analisará as conclusões da revisão e considerará até que ponto refletem suficientemente a proteção de dados e as considerações de interesse público em fornecer acesso efetivo às autoridades de aplicação da lei e aos operadores de cibersegurança.

2. Serviços responsáveis pela aplicação da lei modernos

Uma vez que a tecnologia continua a reformular quase todos os setores da sociedade, incluindo a segurança, os serviços responsáveis pela aplicação da lei e o poder judiciário têm de conseguir acompanhar esta reformulação. É essencial integrar a inteligência artificial, os megadados e a computação de alto desempenho na política de segurança, sem enfraquecer simultaneamente a proteção efetiva dos direitos fundamentais, por forma a aumentar a proteção e a segurança.

A Comissão está a trabalhar em várias vertentes de trabalho importantes[58]. Em 25 de novembro de 2020, a Comissão propôs[59] o Regulamento Governação de Dados, um quadro para facilitar a partilha e a reutilização de dados pessoais e não pessoais para fins de inovação e desenvolvimento. O regulamento abrange a indústria e os organismos públicos, através de espaços de dados setoriais virtuais ou físicos. Permitiria o acesso das autoridades nacionais de aplicação da lei aos dados alojados noutros espaços de dados, para os seus fins de inovação particulares. Ao mesmo tempo, o acesso aos dados detidos pelas autoridades nacionais de aplicação da lei e de segurança não seria permitido, a menos que fosse autorizado pelo direito da UE ou nacional. As autoridades nacionais de aplicação da lei e de segurança também podem sair beneficiadas se os titulares de dados os disponibilizarem voluntariamente para o bem comum, exclusivamente para fins de investigação científica.

Estão ainda em curso trabalhos para preparar uma nova iniciativa em matéria de **inteligência artificial (IA)**, na sequência da publicação do Livro Branco sobre a IA[60]. Embora reconhecendo as oportunidades que a tecnologia de IA oferece no sentido de impulsionar a segurança e o bem-estar dos cidadãos e da sociedade em geral, o Livro Branco também identificou uma série de riscos – como as ciberameaças, os riscos associados à segurança pessoal ou a perda de conectividade. Na consulta pública, as

[58] Incluindo a estratégia da UE em matéria de dados (ver acima).
[59] COM(2020) 767.
[60] COM(2020) 65.

principais preocupações dos participantes relacionaram-se com a possibilidade de a IA violar os direitos fundamentais e com o risco de que possa conduzir a resultados discriminatórios[61]. Na comunicação «Aumentar a confiança numa inteligência artificial centrada no ser humano»[62], a Comissão salientou a necessidade de tornar os sistemas de IA resilientes contra os ataques não dissimulados e contra as tentativas mais subtis de manipular os dados ou os algoritmos, bem como de tomar medidas para atenuar este risco.

A **cifragem** desempenha um papel fundamental para garantir uma cibersegurança sólida e a proteção efetiva dos direitos fundamentais, como a privacidade, incluindo a confidencialidade das comunicações e a proteção de dados pessoais, bem como para assegurar a confiança nos produtos e serviços baseados nas tecnologias de cifragem, incluindo as soluções de identificação digital. Ao mesmo tempo, também pode ser utilizada para o encobrimento de delitos dos olhos dos serviços responsáveis pela aplicação da lei e do poder judiciário, dificultando assim a investigação, a deteção e a ação penal. Os Estados-Membros com assento no Conselho apelaram a soluções que permitam às autoridades de aplicação da lei e judiciárias obter acesso legal às provas digitais, no pleno respeito da privacidade, da proteção de dados e das garantias de um julgamento justo[63]. A Comissão trabalhará com os Estados-Membros para identificar soluções jurídicas, operacionais e técnicas de acesso legal à informação eletrónica em ambientes cifrados, que mantenham a segurança das comunicações.

As medidas práticas em curso incluem uma **plataforma de decifração** na Europol para ajudar os serviços responsáveis pela aplicação da lei a obter acesso legal a informações cifradas em dispositivos apreendidos no decurso de investigações criminais[64]. O Grupo Europeu de Formação e Educação em Cibercrime desenvolveu módulos de formação piloto, que contribuirão para o trabalho da Agência da União Europeia para a Formação Policial (CEPOL). Foi criada uma rede de pontos de perícia técnica em matéria de cifragem dos Estados-Membros, para partilhar as melhores práticas e os conhecimentos específicos e para apoiar o desenvolvimento de um conjunto de instrumentos técnicos e práticos.

O **sistema de intercâmbio digital de provas eletrónicas (eEDES)** fornecerá um instrumento para o intercâmbio transfronteiras seguro, célere e eficiente de decisões europeias de investigação, pedidos de assistência mútua e provas em formato digital. Deverá ser gradualmente enriquecido e alargado a outros instrumentos de cooperação judiciária em matéria penal, e o seu âmbito de aplicação futuro será definido numa proposta legislativa relativa à digitalização dos processos de cooperação judiciária prevista para 2021[65].

3. Combate aos conteúdos ilegais em linha

A radicalização que conduz ao extremismo violento e ao terrorismo é um fenómeno multidimensional e transfronteiras, que tem sido capaz de explorar o rápido crescimento da Internet. A Internet continua a ser utilizada para radicalizar e recrutar pessoas vulneráveis.

---

61 Respetivamente, 90 % e 87 % dos inquiridos consideram estas preocupações importantes ou muito importantes.

62 COM(2019) 168.

63 ST 13084 2020 – Regulamento do Conselho relativo à cifragem – Segurança através da cifragem e segurança apesar da cifragem

64 Este projeto no valor de 6 milhões de EUR também é apoiado pelo Centro Comum de Investigação da Comissão.

65 Comunicação sobre a digitalização da justiça na UE, COM(2020) 710 de 2 de dezembro de 2020.

Em julho, a Unidade de Sinalização de Conteúdos na Internet da Europol retirou duas mil ligações hipertexto para conteúdos terroristas – incluindo manuais e tutoriais sobre como realizar um ataque. A evidência do papel da Internet na radicalização e na publicidade dos delitos perpetrados pelos envolvidos nos ataques em França e na Áustria destaca ainda a necessidade de um quadro legislativo claro para prevenir a difusão de conteúdos terroristas em linha, mantendo ao mesmo tempo as salvaguardas eficazes de proteção dos direitos fundamentais. As negociações entre o Parlamento Europeu e o Conselho sobre a proposta de **Regulamento Conteúdos Terroristas em Linha**[66] intensificaram-se nas últimas semanas. A conclusão destas negociações, em particular com o estabelecimento de um novo e eficaz instrumento operacional de decisões de remoção para a eliminação transfronteiras de conteúdos terroristas no espaço de uma hora ou menos a partir da receção dessas decisões é fundamental para combater os conteúdos terroristas, incluindo aqueles que contribuem para a radicalização.

Entretanto, o **Fórum Internet da UE** continua a funcionar como um catalisador para a ação, fornecendo uma plataforma essencial que reúne os Estados-Membros e a indústria para prevenir a propagação de conteúdos terroristas em linha e combater as mensagens de radicalização. O fórum está a trabalhar no desenvolvimento de uma lista de referência de símbolos e de grupos proibidos nos Estados-Membros, que pode informar as políticas de moderação de conteúdos da plataforma.

O Fórum Internet da UE expandiu o seu âmbito de atividades para abranger igualmente o **abuso sexual de crianças em linha**. O fórum facultará um espaço comum para partilhar as melhores práticas e identificar os obstáculos colocados aos intervenientes públicos e privados, a fim de aumentar o entendimento mútuo e encontrar soluções em conjunto. Permite também uma coordenação política de alto nível para maximizar a eficiência e a eficácia da ação. Foi criado um processo de consulta pericial técnica no âmbito do Fórum Internet da UE, composto por universidades, indústria, autoridades públicas e organizações da sociedade civil, para identificar e avaliar previamente possíveis soluções técnicas para detetar e denunciar o abuso sexual de crianças em comunicações eletrónicas com cifragem de extremo a extremo. Tais soluções técnicas não devem enfraquecer a cifragem. Esta abordagem complementa outros elementos da luta contra o abuso sexual de crianças, tanto em linha como fora de linha, tal como descrito acima.

A Comissão também continuou a partilhar conhecimentos especializados e a experiência da UE, no quadro do comité consultivo independente do recém-criado **Fórum Mundial da Internet contra o Terrorismo** e como codiretora, em conjunto com a Microsoft, do Grupo de Trabalho para a Resposta a Situações de Crise. Em conjunto com a Europol, a Comissão continuou a apoiar os Estados-Membros na aplicação do **Protocolo de Crise da UE**. Em 23 de novembro de 2020, a Unidade da UE de Sinalização de Conteúdos na Internet organizou um segundo exercício teórico, para preparar orientações destinadas a melhorar as respostas operacionais e a coordenação em tempo real entre os Estados-Membros e os prestadores de serviços em linha.

Em junho de 2020, a Comissão publicou os resultados do último exercício de monitorização da aplicação do **código de conduta sobre discursos ilegais de incitação ao ódio em linha**[67]. Os resultados mostram que, em média, as empresas de TI avaliam 90 % dos conteúdos assinalados no prazo de 24 horas e eliminam 71 % dos conteúdos

[66] COM(2018) 640.

[67] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

considerados discursos ilegais de incitação ao ódio. No entanto, também identificou deficiências na transparência e nos elementos fornecidos aos utilizadores. A aplicação do código de conduta no decurso dos últimos quatro anos também foi integrada nas reflexões sobre como combater os conteúdos ilegais em linha sem pôr em causa a liberdade de expressão, com vista à proposta a apresentar em relação ao futuro ato legislativo sobre os serviços digitais. No seu discurso sobre o Estado da União em 2020, a presidente Ursula von der Leyen anunciou também que, até ao final de 2021, a Comissão irá propor um alargamento da lista dos crimes a nível da UE, ao abrigo do artigo 83.º, n.º 1, do TFUE, por forma incluir os crimes de ódio e o discurso de ódio[68].

4. ***Ameaças híbridas***

Em reconhecimento do caráter evolutivo das ameaças híbridas, o Conselho criou em julho de 2019 um **grupo de trabalho horizontal para reforçar a resiliência e combater as ameaças híbridas**. O seu principal objetivo é apoiar a coordenação estratégica e horizontal entre os Estados-Membros no domínio da resiliência do Estado e da sociedade, melhorando a comunicação estratégica e combatendo a desinformação. Os trabalhos incluíram o seguimento dado aos inquéritos sobre os riscos híbridos[69], bem como uma análise específica das ameaças híbridas e da desinformação nos países nossos parceiros da vizinhança. As atividades do grupo de trabalho horizontal foram apresentadas num relatório anual da presidência adotado em 14 de setembro de 2020.

Em dezembro de 2019, o Conselho adotou as «conclusões do Conselho sobre os esforços complementares para aumentar a resiliência e combater as ameaças híbridas»[70], apelando a uma abordagem abrangente para a segurança e para combater as ameaças híbridas e trabalhando em todos os setores políticos pertinentes de uma forma mais estratégica, mais coordenada e mais coerente. Em julho de 2020, foram tomadas duas medidas de acompanhamento importantes. Em primeiro lugar, os serviços da Comissão e o SEAE prepararam um **levantamento das medidas e documentos relacionados com a resposta da UE às ameaças híbridas**[71]. O levantamento propicia um inventário global das medidas no domínio do combate às ameaças híbridas a nível da UE e dos correspondentes documentos políticos. Servirá de ponto de partida para criar uma plataforma em linha restrita que possa servir de ponto único de contacto para todas as medidas relacionadas com o combate às ameaças híbridas e aos respetivos documentos políticos e legislativos, bem como para os estudos relevantes. Em segundo lugar, o **relatório anual mais recente sobre o combate às ameaças híbridas**[72] analisou a aplicação, abrangendo o conhecimento das situações, o reforço da resiliência, a preparação e a resposta a situações de crise, bem como a cooperação internacional e, em particular, a cooperação UE-NATO no combate às ameaças híbridas. Embora o relatório indique alguns progressos em termos de coordenação a nível da UE, a escala e a diversidade sem precedentes das ameaças híbridas atuais requerem medidas adicionais ao nível da abordagem da UE, por forma a integrar a

[68] Também estabelecido em maior pormenor na estratégia para a igualdade de tratamento das pessoas LGBTIQ 2020-2025 (COM(2020) 698).

[69] Ação 1 do quadro conjunto para o combate às ameaças híbridas, de 2016, ver o documento JOIN/2016/018.

[70] Conclusões do Conselho 14972/19.

[71] SWD(2020) 152, documento de trabalho conjunto dos serviços, Levantamento das medidas relacionadas com o reforço da resiliência e com a luta contra as ameaças híbridas.

[72] SWD(2020) 153, documento de trabalho conjunto dos serviços, relatório sobre a aplicação do quadro comum de 2016 em matéria de luta contra as ameaças híbridas e comunicação conjunta, de 2018, sobre o reforço da resiliência e das capacidades para fazer face às ameaças híbridas.

dimensão externa e interna num fluxo ininterrupto e apoiar os esforços dos Estados-Membros no combate às ameaças híbridas e no reforço da sua resiliência.

Paralelamente, estão em curso trabalhos sobre a aplicação das medidas estabelecidas na nova estratégia de segurança para integrar as considerações híbridas na elaboração de políticas, desenvolver uma plataforma em linha restrita, definir as linhas de base da resiliência da UE a nível setorial e facilitar os fluxos de informação de modo a aumentar o conhecimento das situações[73]. A ação será baseada na **célula de fusão da UE contra as ameaças híbridas**, estabelecida no quadro do Centro de Situação e de Informações da UE (INTCEN), que continuará a ser o +principal ponto focal na UE para a avaliação das ameaças híbridas. Já elaborou mais de 180 relatórios escritos sobre as ameaças híbridas e as ciberameaças. Um dos projetos da célula de fusão da UE contra as ameaças híbridas é a **análise de tendências híbridas**[74], que fornece dados relativos a assuntos como: análise recorrente das atividades híbridas dos intervenientes emergentes; atividades de serviços de informações externos contra os Estados-Membros, as instituições, os parceiros e os interesses da UE; e a exploração híbrida de intervenientes estatais e não estatais no quadro da pandemia de COVID-19.

A **cooperação UE-NATO** (no âmbito do quadro abrangente previsto nas declarações comuns de Varsóvia e de Bruxelas, de 2016 e 2018) intensificou-se ainda mais, tal como destacado no quinto relatório intercalar de junho de 2020, com a interação entre o pessoal de cada lado e resultados concretos nos domínios das ameaças híbridas, da ciberdefesa e do reforço das capacidades[75]. É crucial desenvolver uma metodologia única para todos os setores, a fim de desenvolver os trabalhos relacionados com as linhas de base em termos de resiliência híbrida, por forma a dar resposta ao risco de políticas, instrumentos e ações fragmentados e duplicados. O Centro Europeu de Excelência para o Combate às Ameaças Híbridas, em Helsínquia, também esteve envolvido nesta cooperação. A cooperação com a NATO foi intensificada no decurso da crise da COVID-19, nomeadamente quanto à desinformação relacionada com a pandemia e aso combate a atividades de informação hostis.

De um modo geral, a pandemia de COVID-19 tem evidenciado os riscos de uma **desinformação** em rápida evolução e o risco real para a vida das pessoas[76]. Em 10 de junho de 2020, a Comissão e o alto representante adotaram uma **comunicação conjunta sobre a COVID-19 e a desinformação**[77], para destacar os riscos específicos da desinformação sobre a COVID-19 e as medidas a tomar. Foi analisada a ação das principais plataformas em linha no desenvolvimento de políticas destinadas a combater a ameaça e a assegurar um acompanhamento intensificado da ação das plataformas, bem como uma cooperação dedicada através do sistema de alerta rápido gerido pelo SEAE. A

[73] Em 26 de novembro de 2020, por exemplo, o Centro Comum de Investigação propôs um novo quadro com vista a aumentar a sensibilização para as ameaças: https://ec.europa.eu/jrc/en/news/jrc-framework-against-hybrid-threats

[74] A análise de tendências híbridas é um instrumento a utilizar em paralelo com os sistemas nacionais, para acompanhar a escala e a intensidade das ameaças híbridas nos domínios político/diplomático, militar, económico, da informação, da inteligência, cibernético, social, da energia e das infraestruturas.

[75] A cooperação entre o pessoal no domínio da cibersegurança e da ciberdefesa intensificou-se ainda mais através de trabalhos realizados em conceitos e doutrinas consistentes, exercícios, intercâmbio de informações e sessões de informação cruzadas.

[76] As consequências reais incluíram casos de fogo posto em infraestruturas de telecomunicações e a difusão de informações deturpadas sobre a saúde, com consequências diretas.

[77] JOIN(2020) 8, comunicação conjunta, Combater a desinformação sobre a COVID-19: repor a verdade dos factos.

pandemia desencadeou mais esforços no combate à desinformação e uma maior sensibilização do público. No primeiro semestre de 2020, a base de dados pública **EUvsDisinfo** que contém exemplos de casos de desinformação, adicionou 1 963 novos casos pró-Kremlin, dos quais cerca de um terço estavam relacionados com a infodemia sobre a COVID-19. De meados de março ao final de abril de 2020, mais de 10 mil pessoas visitaram o sítio Web diariamente, e o número total de visitantes aumentou 400 %, quando comparado com o mesmo período de 2019. A resposta da UE incluiu campanhas de comunicação específicas[78] e o fornecimento de informações factuais sobre a pandemia.

Os ensinamentos colhidos foram integrados no desenvolvimento do **plano de ação para a democracia europeia**, adotado em 2 de dezembro de 2020[79]. O plano de ação define as principais medidas destinadas a reforçar a resiliência do tecido democrático da UE, promovendo eleições livres e justas, dando resposta às tensões com as quais os meios de comunicação social livres e independentes se confrontam e combatendo a desinformação. Este último aspeto utilizará o plano de ação de 2018 contra a desinformação[80] como base para uma maior ação da UE no combate à desinformação e para envolver as principais partes interessadas da sociedade civil e do setor privado. Aguarda igualmente com expectativa a próxima medida no âmbito do **Código de Conduta sobre Desinformação**, após a avaliação de setembro de 2020 da eficácia do código[81]. O código tem sido uma medida importante e necessária na criação de um ecossistema de plataformas em linha mais transparente e responsável, mas seria mais eficaz com definições mais uniformes, uma aplicação mais consistente e mais ações para dar resposta a domínios específicos, como o microdirecionamento. Outro instrumento importante atualmente à disposição da UE é o **Observatório Europeu dos Meios de Comunicação Digitais**, que ficou operacional em junho de 2020. Reúne as principais partes interessadas que trabalham no combate à desinformação, incluindo os verificadores de factos e os investigadores académicos.

IV PROTEGER OS EUROPEUS DO TERRORISMO E DA CRIMINALIDADE ORGANIZADA

1. *Terrorismo e radicalização*

Os ataques recentes demonstraram, uma vez mais, que a ameaça terrorista na UE continua a ser elevada. O homicídio de um professor em Conflans-Sainte-Honorine, em 16 de outubro de 2020, foi seguido pelo homicídio de três pessoas na basílica de Notre-Dame em Nice, em 29 de outubro. Em 2 de novembro, um ataque terrorista em Viena tirou a vida a quatro pessoas e provocou 23 feridos. Em 13 de novembro, o Conselho adotou uma declaração comum dos ministros dos Assuntos Internos da UE sobre os recentes ataques terroristas em França e na Áustria[82]. Esses recentes ataques de inspiração jihadista ocorreram num contexto de aumento da ameaça proveniente de grupos violentos de extrema-direita e de outras formas de terrorismo.

---

78 Foi lançada, por exemplo, a campanha «Pense antes de partilhar», para prestar aconselhamento sobre como limitar a propagação da desinformação ao público jovem e aos multiplicadores nos países da Parceria Oriental da UE, alcançando mais de 500 mil visualizações nas plataformas das redes sociais.

79 COM (2020) 790.

80 JOIN(2018) 36, comunicação conjunta, Plano de Ação contra a Desinformação.

81 SWD(2020) 180.

82 Declaração comum dos ministros dos Assuntos Internos da UE sobre os recentes ataques terroristas na Europa, 13.11.2020, 12634/20.

Para continuar a apoiar os Estados-Membros na luta contra o terrorismo e a radicalização, a Comissão adotou nessa data, a **Agenda da UE de Luta contra o Terrorismo**[83]. A agenda baseia-se nas políticas e nos instrumentos existentes e reforçará o quadro da UE para melhorar ainda mais a antecipação de ameaças e de riscos, a prevenção da radicalização e do extremismo violento e a proteção das pessoas e das infraestruturas, nomeadamente através da segurança nas fronteiras externas e de um acompanhamento eficaz após os ataques. Descreve também o caminho a seguir para melhorar a aplicação da lei e a cooperação judiciária, bem como a utilização de tecnologias e a partilha de informações pertinentes em toda a UE, nomeadamente em benefício dos responsáveis pelos controlos nas fronteiras externas. A aplicação e o cumprimento da legislação continuam a ser fundamentais.

A prevenção é fundamental no combate ao terrorismo. Os esforços da UE no domínio da **prevenção da radicalização** assentam na sólida experiência adquirida até ao momento no apoio aos profissionais da primeira linha e aos decisores políticos. Em 24 de novembro, a Comissão adotou um novo **plano de ação sobre a integração e a inclusão**[84]. É fundamental continuar a trabalhar na luta contra a radicalização e no sentido de aproximar as comunidades. Uma sociedade mais coesa e inclusiva pode também ajudar a impedir a propagação de ideologias extremistas que podem conduzir ao terrorismo e ao extremismo violento. O apoio à **Rede de Sensibilização para a Radicalização** incluiu a celebração em janeiro de 2020 de um novo contrato, no valor de 30 milhões de EUR para os próximos quatro anos, destinado à ajuda aos profissionais no terreno, bem como ao apoio suplementar aos decisores políticos e aos investigadores. Estes e outros instrumentos, como o **Fórum Internet da UE**, permitirão à Comissão dar resposta às ações prioritárias destacadas nas orientações estratégicas para 2021 relativas a uma abordagem coordenada da UE em matéria de prevenção da radicalização, desenvolvida com os Estados-Membros. As orientações são complementadas pelas ações previstas na agenda anti-terrorismo da UE para combater as ideologias extremistas em linha, intensificar os esforços nas prisões e no sentido da reabilitação e reintegração, nomeadamente dos combatentes terroristas estrangeiros, e para reforçar o apoio prestado aos intervenientes locais e construir comunidades mais resilientes.

A **Diretiva relativa à luta contra o terrorismo**[85], adotada em março de 2017, é o principal instrumento da justiça penal a nível da UE para combater o terrorismo. Estabelece normas mínimas para a definição de infrações terroristas ou ligadas ao terrorismo e a respetivas sanções, ao mesmo tempo que concede às vítimas do terrorismo direitos a proteção, apoio e assistência. Em 30 de setembro de 2020, a Comissão adotou um relatório[86] de avaliação das medidas adotadas pelos Estados-Membros para dar cumprimento à diretiva. O relatório conclui que a transposição para o direito nacional ajudou a reforçar a abordagem da justiça penal dos Estados-Membros ao terrorismo e aos direitos conferidos às vítimas do terrorismo, mas que subsistem lacunas. Por exemplo, nem todos os Estados-Membros criminalizam nas suas legislações nacionais todas as infrações indicadas na diretiva como infrações terroristas, nem aplicam integralmente as disposições destinadas a criminalizar as viagens para fins terroristas, a combater o financiamento do terrorismo e a prestar apoio às vítimas. No final de 2021, será adotado um relatório de avaliação sobre a diretiva.

[83] COM (2020) 795.
[84] COM(2020) 758.
[85] Diretiva (UE) 2017/541.
[86] COM (2020) 619.

A UE continua a trabalhar no sentido de apoiar os Estados-Membros a privarem os terroristas de meios de ataque e de apoiar a aplicação das regras. O regulamento sobre a comercialização e utilização de **precursores de explosivos**, adotado em junho de 2019[87], começará a ser aplicável a partir de 1 de fevereiro de 2021. Para ajudar as autoridades nacionais e o setor privado a aplicarem o regulamento, a Comissão publicou em junho de 2020 um conjunto de orientações[88]. Além disso, e também em junho de 2020[89], a Comissão estabeleceu um programa para acompanhar as realizações, os resultados e o impacto do regulamento.

Em novembro de 2019, a Comissão convidou os Estados-Membros a avaliar a aplicação do plano de ação de 2017 para melhorar a preparação para os riscos[90] em matéria de segurança **química, biológica, radiológica e nuclear (QBRN)**. A conclusão geral foi a de que a maioria das ações foram aplicadas. No início de 2020, a Comissão, em cooperação com os peritos nacionais, estabeleceu uma lista de substâncias químicas de elevado risco que suscitavam preocupação. Esta foi a base para o compromisso com os fabricantes de equipamentos, com vista a melhorar as capacidades de deteção. Recentemente, a Comissão lançou um estudo sobre a viabilidade de restringir o acesso a algumas destas substâncias químicas. Também estão em curso trabalhos no quadro do Mecanismo de Proteção Civil da União Europeia, ao mesmo tempo que estão a ser discutidas com os Estados-Membros capacidades de resposta QBRN adicionais nos domínios da descontaminação, deteção, vigilância e acompanhamento, bem como do armazenamento.

Em 12 de outubro de 2020, o Conselho decidiu prorrogar por um ano[91] o regime de sanções contra a proliferação e a utilização de armas químicas, permitindo à UE impor medidas restritivas a pessoas e a entidades envolvidas no desenvolvimento e na utilização de armas químicas. Em 14 de outubro de 2020, o Conselho adotou medidas restritivas contra seis indivíduos e uma entidade envolvidos na tentativa de homicídio de Alexei Navalny, que foi vítima de envenenamento por um agente neurotóxico do grupo «Novichok», em 20 de agosto de 2020, na Rússia[92].

As **informações financeiras** também são cruciais para permitirem a identificação de redes terroristas, uma vez que os terroristas dependem de financiamento para as viagens, a formação e o equipamento, pelo que os esforços de **combate ao financiamento do terrorismo** são essenciais para as investigações em matéria de luta contra o terrorismo. As principais questões incluem a exploração dos instrumentos e informações existentes em todo o seu potencial, a aplicação adequada das normas acordadas internacionalmente e a abordagem dos desafios em constante evolução causados pelas tecnologias emergentes e pelas plataformas das redes sociais[93] (ver abaixo).

A rede de **transportes** foi e continua a ser um alvo do terrorismo. Os esforços da UE incluem uma abordagem de avaliação baseada nos riscos para proteger o setor da

---

87 Regulamento (UE) 2019/1148.

88 Comunicação da Comissão – Orientações para a aplicação do Regulamento (UE) 2019/1148 sobre a comercialização e utilização de precursores de explosivos, JO C 210 de 24.6.2020, p. 1.

89 SWD(2020) 114 final.

90 COM(2017) 610 final.

91 Decisão (UE) 2020/1466 do Conselho, de 12 de outubro de 2020, que altera a Decisão (PESC) 2018/1544.

92 Decisão (PESC) 2020/1482 do Conselho, de 14 de outubro de 2020, e Regulamento de Execução (UE) 2020/1480 do Conselho.

93 Tal como previsto pela UE, em novembro de 2019, na conferência ministerial *No Money For Terror*, organizada pela Austrália, sobre a luta contra o financiamento do terrorismo.

aviação[94]. As zonas de conflito representam um sério risco para a aviação civil, e a partilha de informações e das avaliações dos riscos é fundamental para a respetiva atenuação[95]. O sistema da UE de informações de alerta e de **avaliação dos riscos em zonas de conflito** é reconhecido como melhor prática, e as normas internacionais relativas à partilha de informações foram incorporadas na legislação da UE[96]. Com base na experiência adquirida no domínio da aviação civil, a Comissão alargou a abordagem baseada na avaliação dos riscos a outros modos de transporte. A aplicação do **plano de ação para a segurança ferroviária**[97] da UE avança a bom ritmo e beneficia dos conhecimentos especializados da plataforma de passageiros dos serviços ferroviários da UE, um grupo de peritos dedicado criado pela Comissão. No domínio marítimo, a abordagem baseada na avaliação dos riscos é bem conhecida e aplicada, e a Comissão trabalha com os Estados-Membros e com as partes interessadas para reforçar a segurança dos passageiros. Esse processo está incorporado na **Estratégia de Segurança Marítima da UE** e no seu **plano de ação**, revisto em 2018, incluindo também uma dimensão de segurança e defesa, como indicado no último relatório de execução adotado e publicado em 23 de outubro de 2020[98].

A **Europol** presta apoio aos Estados-Membros nas investigações relacionadas com o terrorismo através do **Centro Europeu de Luta contra o Terrorismo (CELT)**. Os pedidos de apoio operacional dos Estados-Membros ao CELT continuaram a aumentar, com o centro a integrar hoje em dia quase todas as grandes investigações em matéria de luta contra o terrorismo. Durante o ano de 2019, a Europol apoiou um total de 632 operações diferentes no domínio do contra-terrorismo. Os investigadores dos Estados-Membros também demonstraram uma apreciação crescente deste trabalho, passando de um nível de satisfação de 8/10, em 2018, para 9,1/10, em 2019. O CELT coordenou um total de 18 Dias de Ação em 2019[99].

A **Eurojust** também apoiou 116 investigações em matéria de luta contra o terrorismo em 2019 e 2020. O trabalho atual conduzirá a uma proposta legislativa relativa ao intercâmbio de casos de terrorismo digital transfronteiras, por forma a desenvolver o Registo de Contraterrorismo lançado em 2019[100], bem como para expandir os trabalhos direcionados aos grupos de extrema-direita e de extrema-esquerda.

Em 30 de julho de 2020, o Conselho renovou pela última vez a lista da UE de pessoas, grupos e entidades sujeitos a medidas restritivas para o combate ao terrorismo. A lista mais recente integra 14 pessoas e 21 entidades. No mesmo dia, o Conselho impôs medidas restritivas a uma pessoa ao abrigo do regime de sanções contra o terrorismo do EIIL

---

94 O processo integrado de avaliação dos riscos para a segurança da aviação da UE apoia o processo de tomada de decisão nos domínios da segurança da carga aérea, das normas de segurança da aviação e dos riscos decorrentes da aviação civil em zonas de conflito.

95 A trágica queda do voo 752 da Ukraine International Airlines em 8 de janeiro de 2020 demonstrou ainda mais a importância da partilha de informações e da avaliação dos riscos para a segurança da aviação civil.

96 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R1583.

97 COM(2018) 470 final.

98 Relatório dos serviços da Comissão, do Serviço Europeu para a Ação Externa e da Agência Europeia de Defesa sobre a implementação do plano de ação revisto da Estratégia de Segurança Marítima da UE, SWD(2020) 252.

99 Relatório anual de atividades consolidado de 2019, Europol, 9.6.2020.

100 O Registo de Contraterrorismo é gerido pela Eurojust, funciona 24 horas por dia e fornece apoio pró-ativo às autoridades judiciárias nacionais. Esta informação centralizada deve ajudar os procuradores a coordenarem-se de forma mais ativa e a identificar os suspeitos ou as redes objeto de investigação em casos específicos com potenciais implicações transfronteiras.

(Daexe)/Alcaida. Atualmente, existem cinco pessoas autonomamente inscritas neste regime, que foi renovado por um ano em 19 de outubro de 2020[101].

Um elemento importante da política de luta contra o terrorismo diz respeito às ameaças representadas por **combatentes terroristas estrangeiros** atualmente na Síria e no Iraque. Embora respeitando plenamente a responsabilidade primária dos Estados-Membros nestas questões, o apoio e a cooperação a nível da UE ajudam os Estados-Membros a dar resposta aos desafios comuns: ação penal contra aqueles que cometeram crimes terroristas, prevenção da entrada não detetada no espaço Schengen e reintegração e reabilitação dos combatentes terroristas estrangeiros que regressaram. A Comissão está, por exemplo, a colaborar estreitamente com os Estados-Membros e com os principais países parceiros para garantir que as provas obtidas no campo de batalha são partilhadas e utilizadas de forma eficaz na identificação e na deteção nas fronteiras da UE, bem como para efeitos de ação penal. O memorando sobre as provas obtidas no campo de batalha[102] publicado em 2020 pela Eurojust mostra que embora a obtenção de tais dados e a garantia de que satisfaçam os critérios aplicáveis para que as provas sejam admissíveis coloquem muitos desafios, poderão ajudar a conduzir os suspeitos de terrorismo perante a justiça.

A Comissão também está a facilitar o diálogo com os Estados-Membros e com os intervenientes humanitários, a fim de fornecer uma visão global e factual da situação nos campos de refugiados sírios do nordeste, onde se encontram localizados familiares dos combatentes terroristas estrangeiros europeus. É colocada uma tónica particular na situação das crianças nos campos de refugiados sírios. A Comissão ajuda igualmente os Estados-Membros a partilharem experiências sobre as medidas e os mecanismos nacionais para gerir melhor **a reabilitação e a reintegração** dos combatentes terroristas estrangeiros que regressam, bem como das crianças. A Rede de Sensibilização para a Radicalização também realiza visitas de estudo e presta aconselhamento personalizado para dar uma melhor resposta aos desafios dos repatriados condenados, em particular após a libertação da prisão, bem como ao papel das famílias e das comunidades locais nos esforços de reintegração.

As **parcerias de luta contra o terrorismo e de cooperação com os países terceiros** e com os parceiros nos países vizinhos da UE são também fundamentais para melhorar a segurança dentro da UE e para estabelecer uma melhor ligação entre as dimensões interna e externa da política de segurança da UE. O Conselho apelou a um maior reforço do envolvimento externo da UE na luta contra o terrorismo[103], com ênfase nos Balcãs Ocidentais, no Norte de África e Médio Oriente, na região do Sael, no Corno de África e na Ásia. Este trabalho tem vindo a ser desenvolvido mediante um aproveitamento integral dos instrumentos de ação externa, incluindo diálogos de alto nível sobre o contra-terrorismo ou a rede de 17 **peritos em matéria de luta contra o terrorismo/segurança**[104] destacados nas delegações da UE, que continuou a prestar apoio, a facilitar a cooperação e a promover o reforço das capacidades. Está em curso uma reflexão sobre a possibilidade de reforçar e de expandir esta rede.

[101] Decisões do Conselho (PESC) 2020/1132, 2020/1126 e 2020/1516.

[102] https://www.eurojust.europa.eu/eurojust-memorandum-battlefield-evidence-0.

[103] Conclusões do Conselho (8868/20) sobre a ação externa da UE em matéria de prevenção e de luta contra o terrorismo e o extremismo violento (16 de junho de 2020).

[104] Arábia Saudita, Argélia, Bósnia-Herzegovina (regional para os Balcãs Ocidentais), Chade (regional para o Sael), Etiópia (ligação para a União Africana), Indonésia (regional para o Sudeste Asiático e ligação para a ASEAN-ARF), Iraque, Jordânia, Quénia (regional para o Corno de África), Quirguistão (regional para a Ásia Central), Líbano, Líbia, Marrocos, Nigéria, Paquistão, Tunísia e Turquia.

O plano de ação conjunto de 2018 para a luta contra o terrorismo nos **Balcãs Ocidentais** e os convénios bilaterais que o acompanham, assinados em 2019 com cada parceiro[105], proporcionarão um foco numa região de importância fundamental para a execução dos objetivos de segurança comuns e para a proteção das pessoas que vivem na UE. No Fórum Ministerial UE-Balcãs Ocidentais sobre Justiça e Assuntos Internos realizado em 22 de outubro de 2020, a UE e os parceiros dos Balcãs Ocidentais reafirmaram o seu compromisso de aplicar os objetivos do plano de ação conjunto para lá de 2020[106]. A cooperação com os Balcãs Ocidentais inclui a gestão do regresso em curso dos combatentes terroristas estrangeiros e dos seus familiares, bem como uma maior integração das atividades de luta contra a radicalização. A UE também mantém contactos regulares com os países do **Médio Oriente, do Norte de África e da Ásia Central** para efeitos de luta contra o terrorismo[107]. Os trabalhos na região da **Ásia Central** têm-se centrado no combate às ameaças químicas, biológicas, radiológicas e nucleares. A Comissão Mista de Cooperação do **Conselho de Cooperação UE-Golfo** reuniu-se em 25 de junho de 2020 e abordou questões como o combate à radicalização e o combate ao financiamento do terrorismo e ao branqueamento de capitais, bem como a cibersegurança e a cooperação com a Europol. A UE trabalhou com a NATO na primeira auditoria sobre as ameaças químicas, biológicas, radiológicas e nucleares num dos países do Golfo, no final de 2019. No geral, e até ao final de 2019, foram afetados cerca de 465 milhões de EUR em projetos em curso relacionados com a luta contra o terrorismo e na prevenção do extremismo violento fora da UE, um aumento de 15 % em relação ao ano anterior.

A UE também continuou a aprofundar a cooperação com as **Nações Unidas** em matéria de luta contra o terrorismo[108], nomeadamente com o Gabinete das Nações Unidas de Luta contra o Terrorismo e a direção executiva do Comité de Luta contra o Terrorismo, particularmente através de diálogos anuais de alto nível e, mais recentemente, através da participação ativa na semana virtual da ONU sobre a luta contra o terrorismo, no verão de 2020. A Comissão também acompanhou de perto as deliberações sobre a revisão da definição de infrações terroristas constante da Convenção do **Conselho da Europa** sobre a prevenção do terrorismo, incentivando o estreito alinhamento com as definições previstas no direito da UE. Prosseguiu a boa cooperação no domínio da luta contra o terrorismo e dos materiais químicos, biológicos, radiológicos e nucleares entre a **NATO** e a UE, que trocaram informações sobre o reforço das capacidades para evitar a duplicação e garantir a complementaridade.

2. Luta contra a criminalidade organizada

A criminalidade organizada está a aumentar, tornando-se cada vez mais transfronteiras, e a crescer em linha.

---

[105] Albânia, Bósnia-Herzegovina, Kosovo, Macedónia do Norte, Montenegro e Sérvia.

[106] Conferência de Imprensa conjunta: https://www.consilium.europa.eu/en/press/press-releases/2020/10/23/joint-press-statement-eu-western-balkans-ministerial-forum-on-justice-and-home-affairs/pdf.

[107] A ação de luta contra o terrorismo foi, por exemplo, destacada na nova estratégia da UE para a Ásia Central.

*Esta designação não prejudica as posições relativas ao estatuto, e está conforme com a RCSNU 1244/1999 e o parecer do TIJ sobre a declaração de independência do Kosovo.

[108] Em 2019 foi assinado um quadro para a cooperação entre a UE e a ONU em matéria de combate ao terrorismo. https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf.

Europol, Avaliação da Ameaça da Criminalidade Grave e Organizada (SOCTA), 2017.

A ação da Comissão incluiu a luta contra a droga, as armas de fogo ilícitas, a criminalidade financeira, a importação ilícita de bens culturais, o tráfico de seres humanos ou a criminalidade ambiental, apoiando as autoridades de aplicação da lei e judiciárias dos Estados-Membros, bem como os parceiros da vizinhança. A cooperação com os países terceiros, em particular na vizinhança, como os Balcãs Ocidentais, e com as organizações internacionais, incluindo o Gabinete das Nações Unidas contra a droga e a criminalidade[109], também foram fundamentais[110].

Em 2019, o **Centro de Luta contra a Criminalidade Grave e Organizada da Europol** recebeu e processou quase 55 mil contribuições operacionais, o que representa um aumento de 12 % relativamente a 2018. No que diz respeito ao número de operações apoiadas, o centro prestou assistência aos países em 726 casos[111]. É igualmente crucial que o quadro legislativo da UE para a criminalidade organizada[112], que visa harmonizar as legislações dos Estados-Membros relativas à criminalização das infrações relacionadas com a participação em organização criminosa e que estabelece sanções para estas infrações, seja plenamente transposto em todos os Estados-Membros. A Comissão lançou um estudo com vista a analisar as formas de melhorar esta legislação. Serão elaboradas outras medidas destinadas a intensificar a luta contra a criminalidade organizada na UE, em conjunto com a agenda da UE para combater a criminalidade organizada a adotar no primeiro trimestre de 2021.

O congelamento e a perda dos produtos do crime constituem um dos meios mais eficazes de combate à criminalidade organizada. O novo **Centro Europeu para a Criminalidade Económica e Financeira** (EFECC), criado em junho de 2020 no quadro da Europol, aumentará o apoio operacional prestado aos Estados-Membros e aos organismos da UE nos domínios da criminalidade financeira e económica e promoverá a utilização sistemática de investigações financeiras. Para apoiar os esforços da UE em matéria de uma identificação, congelamento e perda dos produtos do crime mais eficazes, o Conselho adotou conclusões, em junho de 2020, sobre o reforço das investigações financeiras para combater a criminalidade grave e organizada[113]. Em 2021, a Comissão procederá à revisão da

[109] Em 8 de dezembro de 2020, realizou-se um diálogo de alto nível entre a UE e o UNODC.
[110] No final de 2019, cerca de 830 milhões de EUR estavam afetados a ações em curso contra a criminalidade organizada fora da UE.
[111] Relatório anual consolidado de 2019, Europol, junho de 2020.
[112] Decisão- Quadro 2008/841.
[113] Conclusões do Conselho 8927/20.

legislação relativa ao congelamento e à perda dos produtos do crime[114] e aos gabinetes de recuperação de bens[115].

A luta contra a criminalidade organizada precisa de salvaguardas para garantir que os trabalhos dos serviços responsáveis pela aplicação da lei possam operar eficazmente mas assegurando o respeito de limites essenciais, como a proteção dos dados pessoais. A Diretiva Proteção de Dados na Aplicação da Lei, de 2016, que regulamenta a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais relacionados com infrações penais[116]. protege os direitos fundamentais à proteção de dados sempre que os dados pessoais são utilizados pelas autoridades penais responsáveis pela aplicação da lei e para esses fins. Assegura que os dados pessoais das vítimas, das testemunhas e dos suspeitos de crime sejam devidamente protegidos e facilita a cooperação transfronteiras na luta contra a criminalidade e o terrorismo. O prazo para a transposição da Diretiva Proteção de Dados na Aplicação da Lei expirou em 6 de maio de 2018. Até à data, a maioria dos Estados-Membros adotou legislação que transpõe a diretiva. Contudo, ainda estão em curso alguns procedimentos de infração[117]. A Comissão está atualmente a avaliar a conformidade das legislações nacionais de transposição com a diretiva.

Luta contra as drogas ilegais

Em julho de 2020, a Comissão adotou a nova **Agenda e Plano de Ação da UE de Luta contra a Droga 2021-2025**[118], na sequência das atuais estratégias da UE de luta contra a droga[119]. Estabelece o quadro político e as prioridades de ação para os próximos cinco anos. Os principais objetivos da agenda são: 1) reforçar as medidas de segurança centradas em todos os aspetos do tráfico ilícito de drogas, desde os grupos de criminalidade organizada à gestão das fronteiras externas e à distribuição e produção ilícitas; 2) melhorar a prevenção, incluindo a sensibilização para os efeitos nocivos das drogas, nomeadamente a intersecção entre o consumo de droga, a violência e outras formas de criminalidade; e 3) combater os danos resultantes da droga através do acesso a tratamentos, da redução dos riscos e dos danos e de uma abordagem equilibrada da questão da droga nas prisões. Em 30 de novembro de 2020, a Comissão também adotou a avaliação da política da UE em matéria de precursores de drogas, que conclui que são necessárias medidas adicionais para impedir o acesso dos grupos de criminalidade organizada na UE às substâncias químicas de que necessitam para produzirem drogas sintéticas ilegais[120].

A UE também financiou projetos concretos para reforçar a luta contra a droga, como o Fórum da Sociedade Civil sobre a Droga. O Relatório Europeu sobre Drogas de 2020 do Observatório Europeu da Droga e da Toxicodependência, publicado em 22 de setembro de 2020[121], mostra o consumo de droga nos tempos mais recentes e as tendências de mercado na UE, na Turquia e na Noruega. Verifica-se um aumento na disponibilidade de cocaína,

[114] Diretiva 2014/42/UE.
[115] Decisão do Conselho 2007/845/JAI.
[116] Diretiva (UE) 2016/680 relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais relacionados com infrações penais.
[117] Apesar dos procedimentos de infração, três Estados-Membros (XXX) ainda não notificaram a transposição integral. A Comissão apresentou um caso de não transposição ao Tribunal de Justiça e, em maio de 2020, dirigiu pareceres fundamentados complementares aos outros dois Estados-Membros, por não transposição integral da diretiva.
[118] COM(2020) 606.
[119] Estratégia da UE de Luta contra a Droga 2013-2020 e Plano de Ação da UE de Luta contra a Droga 2017-2020.
[120] COM(2020) 768, de 30 de novembro de 2020.
[121] Relatório Europeu sobre Drogas de 2020: Tendências e evoluções, EMCDDA, 22.9.2020.

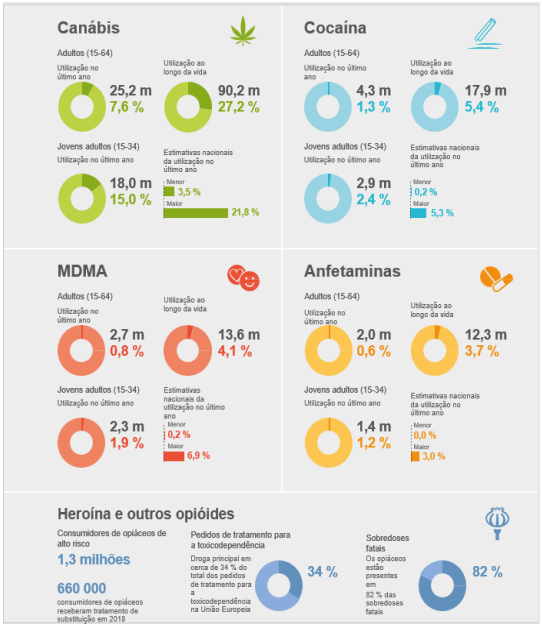
cujas apreensões totalizaram um recorde de 181 toneladas, quase o dobro das apreensões de heroína, que ascenderam a 9,7 toneladas, e uma grande disponibilidade de drogas de elevada pureza na UE. Explora igualmente o surgimento de novos opioides sintéticos, com preocupações específicas para a saúde, e aborda os desafios provocados pela pandemia de COVID-19.

Os trabalhos de luta contra a droga progridem em vários níveis diferentes. O **pacote legislativo relativo às novas substâncias psicoativas** (NSP) foi adotado no outono de 2017[122] e tornou-se plenamente aplicável em novembro de 2018. Cinco Estados-Membros continuam a ser objeto de procedimentos de infração[123]. Já foi adotado o primeiro ato delegado para definir como «droga» uma nova substância psicoativa (isotonitazeno)[124].

A **nível internacional**, a UE tem estado ativa na Comissão dos Estupefacientes das Nações Unidas[125], nomeadamente no que se refere à atualização relacionada com a inclusão das novas substâncias psicoativas[126], bem como para a reconsideração do caso da canábis e substâncias relacionadas[127]. Foram aprovados pelo Conselho dois novos processos de diálogo sobre as drogas, com a China e com o Irão[128], e o Observatório Europeu da Droga e da Toxicodependência avançou com protocolos para a colaboração com países terceiros[129].

Luta contra a criminalidade financeira

Foi adotada nova legislação com vista a reforçar a luta contra a criminalidade financeira, bem como o branqueamento de capitais. A diretiva que facilita a utilização de informações financeiras e de outro tipo para efeitos de prevenção, deteção, investigação ou repressão de determinadas infrações penais foi adotada em 2019, concedendo o acesso aos registos nacionais centralizados de contas bancárias por parte das autoridades de aplicação da lei e dos gabinetes de recuperação de bens para fins de combate à criminalidade grave. A diretiva visa igualmente melhorar a cooperação entre as autoridades de aplicação da lei e as Unidades de Informação Financeira (UIF) e facilitar o intercâmbio de informações entre as UIF. Em junho de 2020, a Comissão publicou o relatório intitulado «Recuperação e perda de bens: garantir que o crime não compensa»[130], que apontou para o potencial de uma maior harmonização dos regimes de



[122] Regulamento (UE) 2017/2101 e Diretiva (UE) 2017/2103.
[123] Áustria, Eslovénia, Finlândia, Irlanda e Portugal.
[124] C/2020/5897; JO L 379 de 13.11.2020, p. 55.
[125] Órgão de administração do Gabinete das Nações Unidas contra a Droga e a Criminalidade (UNODC).
[126] COM(2019) 631.
[127] COM(2019) 624 e COM(2020) 659.
[128] A cimeira UE-China de 16 a 17 de julho de 2018, em Pequim, resultou num acordo para lançar um diálogo anual sobre as drogas entre a UE e a China. Em 30 de outubro de 2019, as modalidades do futuro diálogo foram confirmadas pelo Coreper. Em 5 de março de 2020, o Conselho aprovou o lançamento de um novo diálogo sobre as drogas entre a UE e o Irão.
[129] Parecer da Comissão sobre o projeto de protocolo de colaboração com o Kosovo, adotado em 14 de abril de 2020, e sobre o protocolo de colaboração com a Sérvia, adotado em 16 de dezembro de 2019.
[130] COM(2020) 2017.

recuperação de bens[131] a fim de modernizar a legislação da UE na matéria e reforçar as capacidades das autoridades nacionais na luta contra a criminalidade organizada. Foi lançada, através de um estudo externo, uma análise mais aprofundada da recuperação de bens. O regulamento relativo ao reconhecimento mútuo das decisões de congelamento e de confisco[132] será aplicável a partir de 19 de dezembro de 2020 e reforçará significativamente a cooperação entre os Estados-Membros.

Em maio de 2020, a Comissão adotou **o plano de ação para uma política abrangente da União em matéria de luta contra o branqueamento de capitais e o financiamento do terrorismo**[133], a fim de reforçar o quadro da UE. Em 5 de novembro, o Conselho adotou as conclusões sobre a luta contra o branqueamento de capitais e o financiamento do terrorismo[134], nomeadamente solicitando à Comissão que trabalhasse na adoção de um conjunto único de regras, na criação de um supervisor independente e na coordenação das Unidades de Informação Financeira. Em consonância com as conclusões do Conselho sobre o reforço das investigações financeiras[135], a Comissão está a avaliar igualmente a necessidade de interligar os registos centralizados de contas bancárias, o que aceleraria significativamente o acesso às informações das contas bancárias por parte das Unidades de Informação Financeira e dos serviços responsáveis pela aplicação da lei. Paralelamente, prosseguem os esforços no sentido de garantir que as mais recentes normas da UE são aplicadas de forma eficaz pelos Estados-Membros. As regras da 5.ª Diretiva Antibranqueamento de Capitais visam assegurar um maior nível de transparência das estruturas de propriedade das empresas. O prazo de transposição expirou em 1 de janeiro de 2020 e a Comissão iniciou procedimentos de infração contra 16 Estados-Membros[136]. Outra medida importante é o novo Regulamento Controlo do Dinheiro Líquido[137], adotado em outubro de 2018 e aplicável a partir de 3 de junho de 2021. O regulamento melhorará os sistemas em vigor para o controlo do dinheiro líquido que entra ou sai da UE, e as disposições de execução estão em preparação.

Na frente externa, prosseguem os esforços no sentido de apoiar os países terceiros no combate ao branqueamento de capitais e ao financiamento do terrorismo. Neste contexto, o SEAE e as delegações da UE desempenham um papel primordial na promoção e apoio ao debate político com os países terceiros e com organizações internacionais como o Grupo de Ação Financeira (GAFI).

Para complementar estes trabalhos, a Comissão lançou um mecanismo global para prestar apoio aos países parceiros fora da UE na criação de quadros eficazes de combate ao branqueamento de capitais/financiamento do terrorismo em conformidade com as normas internacionais. A ação, no valor de 20 milhões de EUR, visa ainda incentivar a cooperação entre os intervenientes financeiros e da justiça a nível nacional, regional e internacional.

Combate à corrupção

A corrupção é um crime em si mesmo e constitui um vetor essencial que facilita a criminalidade organizada. A prevenção e o combate à corrupção serão objeto de um

[131] Incluindo a avaliação da Diretiva 2014/42/UE e da Decisão 2007/845/JAI do Conselho.
[132] Regulamento (UE) 2018/1805.
[133] COM(2020) 2800 final.
[134] Conclusões do Conselho 12608/20.
[135] Conclusões do Conselho 8927/20.
[136] Áustria, Bélgica, Chipre, Chéquia, Eslováquia, Eslovénia, Espanha, Estónia, Grécia, Hungria, Irlanda, Luxemburgo, Países Baixos, Polónia, Portugal e Roménia, bem como o Reino Unido
[137] Regulamento (UE) 2018/1672.

acompanhamento e avaliação regulares dos quadros jurídicos dos Estados-Membros, ao abrigo do **mecanismo de proteção do Estado de direito**[138] recentemente criado. Em 30 de setembro de 2020, foi adotado o primeiro relatório à escala da UE sobre o Estado de direito[139]. Este relatório demonstrou que muitos Estados-Membros possuem padrões elevados em matéria de Estado de direito, mas subsistem desafios importantes. O relatório abrange todos os Estados-Membros através de avaliações anuais objetivas e factuais, com o objetivo de desenvolver uma maior sensibilização e compreensão das evoluções ocorridas em cada Estado-Membro à medida que ocorrerem e de proporcionar condições que permitam identificar os riscos, conceber eventuais soluções e prestar um apoio direcionado numa fase precoce. A **Procuradoria Europeia** combaterá o crime contra o orçamento da UE, nesta fase nos 22 países participantes da UE. Terá poderes para investigar, instaurar uma ação penal e deduzir acusação aos responsáveis por infrações penais contra o orçamento da UE, como fraude, corrupção ou fraude grave transfronteiras em matéria de IVA. A Procuradoria Europeia deverá estar operacional no primeiro semestre de 2021[140].

A Comissão está atualmente a avaliar a transposição para o direito nacional das regras definidas na **Diretiva relativa à luta contra a fraude lesiva dos interesses financeiros da União** através do direito penal[141] e intentou procedimentos de infração contra os Estados-Membros que não notificaram a transposição integral[142]. Em 2021, a Comissão adotará um relatório que avaliará em que medida os Estados-Membros tomaram as medidas necessárias para dar cumprimento à diretiva.

Luta contra o tráfico de bens culturais

O principal objetivo do **Regulamento relativo à introdução e à importação de bens culturais**[143], adotado em junho de 2019, é interromper as importações para a União de bens culturais exportados ilicitamente do seu país de origem. Para assegurar a sua aplicação adequada, a Comissão está a preparar atualmente a adoção de disposições de execução, incluindo um sistema eletrónico centralizado para a importação de bens culturais, que permitirá o armazenamento e o intercâmbio de informações entre os Estados-Membros e as formalidades de importação necessárias[144]. Uma regra geral de proibição entrará em vigor no final de 2020, facultando às alfândegas dos Estados-Membros os meios legais para controlar e agir em relação a remessas que possam conter bens culturais exportados ilicitamente do seu país de origem.

Luta contra o tráfico de armas de fogo ilícitas

---

[138] O mecanismo de proteção do Estado de direito proporciona um processo de diálogo entre a Comissão e os Estados-Membros, bem como entre o Conselho e o Parlamento Europeu e os parlamentos nacionais, a sociedade civil e outras partes interessadas no Estado de direito. Os relatórios sobre o Estado de direito constituem o núcleo deste novo processo.

[139] COM(2020) 580.

[140] A decisão de execução do Conselho que nomeia os procuradores europeus entrou em vigor em 29 de julho de 2020. Os procuradores europeus do Colégio realizaram a sua primeira reunião em 28 de setembro de 2020. A Procuradoria Europeia concluirá em breve protocolos de colaboração com a Europol, com a Eurojust e com o OLAF.

[141] Diretiva (UE) 2017/1371.

[142] Continuam atualmente em curso processos de infração contra a Áustria, a Irlanda e a Roménia.

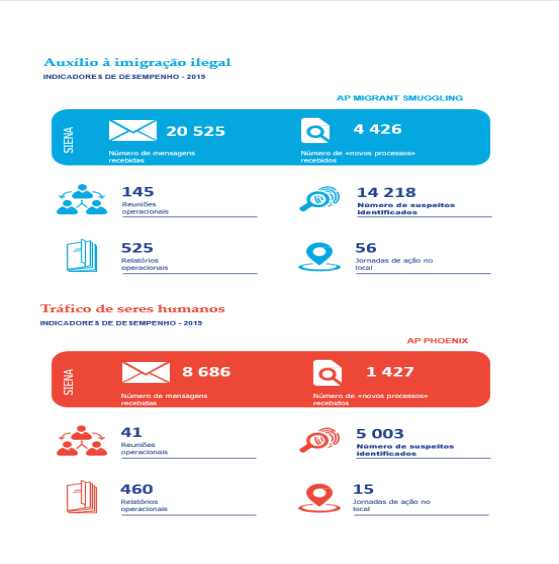
[143] Regulamento (UE) 2019/880

[144] O sistema para a importação de bens culturais tem de ser implementado antes de 28 de junho de 2025, o mais tardar. A Comissão adotou um primeiro relatório intercalar sobre o desenvolvimento do sistema para a importação de bens culturais. COM(2020) 342.

Em 24 de julho de 2020, a Comissão publicou **o novo Plano de Ação da UE sobre o Tráfico de Armas de Fogo para 2020-2025**[145]. A conferência ministerial de alto nível dos Ministérios dos Negócios Estrangeiros e dos Assuntos Internos da UE e dos Balcãs Ocidentais, que teve lugar em 31 de janeiro de 2020, sublinhou a necessidade de mais ações para combater o tráfico de armas de fogo ilícitas. O plano de ação inclui ações específicas para melhorar a legislação em matéria de controlo das armas de fogo, o conhecimento da ameaça relacionada com as armas de fogo, a cooperação policial e a cooperação internacional, com foco na Europa do Sudeste. A Comissão tomou medidas para garantir que a Diretiva relativa ao controlo da aquisição e da detenção de armas, adotada em maio de 2017[146], seja integralmente transposta pelos Estados-Membros. No entanto, 10 Estados-Membros ainda não notificaram a transposição integral da diretiva[147] e a grande maioria dos Estados-Membros não transpôs a legislação de execução que se seguiu. Consequentemente, a Comissão deu início a procedimentos de infração[148]. A Comissão está ainda a avaliar em pormenor as medidas de transposição notificadas e apresentará um relatório sobre a aplicação da diretiva no primeiro semest re de 2021. A Comissão também começou a avaliar a possível modernização do quadro jurídico para as autorizações de exportação e medidas de importação e de trânsito de armas de fogo[149].

Luta contra o tráfico de seres humanos

A Estratégia para a União da Segurança destacou a necessidade de desenvolver uma nova abordagem estratégica para erradicar o tráfico de seres humanos, no âmbito do programa de luta contra a criminalidade organizada. Além disso, tal como previsto no artigo 20.º da Diretiva Antitráfico[150], a Comissão publicou, em outubro de 2020, o seu terceiro relatório sobre os progressos realizados na luta contra o tráfico de seres humanos[151].



[145] COM(2020)608: este novo plano de ação integra a iniciativa franco-alemã para os Balcãs Ocidentais «Roadmap for a sustainable solution to the illegal possession, misuse and trafficking of small arms and light weapons (SALW) and their ammunition in the Western Balkans by 2024».

[146] Diretiva (UE) 2017/853. Também foram importantes duas diretivas de execução, de 16 de janeiro de 2019, que fornecem especificações técnicas para a marcação das armas de alarme e sinalização.

[147] São eles Chipre, Chéquia, Dinamarca, Eslováquia, Eslovénia, Espanha, Hungria, Luxemburgo, Polónia, e Suécia

[148] 25 processos em curso relacionados com esta diretiva (Alemanha, Áustria, Bélgica, Bulgária, Chéquia, Chipre, Dinamarca, Eslováquia, Eslovénia, Espanha, Estónia, Finlândia, França, Grécia, Hungria, Irlanda, Letónia, Lituânia, Luxemburgo, Malta, Países Baixos, Polónia, Portugal, Roménia e Suécia, bem como o Reino Unido) e 34 relacionados com as diretivas de execução (Diretiva 2019/68 - Alemanha, Áustria, Bélgica, Bulgária, Chéquia, Chipre, Croácia, Eslovénia, Espanha, Finlândia, Grécia, Hungria, Irlanda, Itália, Luxemburgo, Polónia, Roménia e Suécia, bem como o Reino Unido, e Diretiva 2019/69 - Bulgária, Chéquia, Chipre, Croácia, Eslovénia, Espanha, Finlândia, Grécia, Hungria, Irlanda, Itália, Luxemburgo, Países Baixos, Polónia, Roménia e Suécia, bem como o Reino Unido)

[149] Regulamentadas pelo Regulamento (UE) n.º 258/2012.

[150] JO L 101 de 15.4.2011, p. 1.

[151] COM(2020) 661 final, complementado por um estudo sobre a recolha de dados relativos ao tráfico de seres humanos na UE 2017-2018.

O relatório mostra avanços na cooperação transnacional, na aplicação da lei transfronteiras e nas ações operacionais judiciárias, na criação de mecanismos de orientação nacionais e transnacionais para as vítimas e no desenvolvimento da base de conhecimentos em matéria de tráfico de seres humanos. Os Estados-Membros cada vez mais fazem uso das agências da UE para trocar informações, realizar ações conjuntas e reunir equipas de investigação conjuntas para lutar contra o tráfico de seres humanos dentro e fora da UE[152]. A cooperação operacional trouxe resultados tangíveis, nomeadamente no âmbito da plataforma multidisciplinar europeia contra as ameaças criminosas: em 2019, estes trabalhos resultaram em 825 detenções, 8 824 suspeitos identificados e 1 307 potenciais vítimas, incluindo 69 crianças identificadas. Foram identificados ou desmantelados 94 grupos de criminalidade organizada envolvidos nestes crimes e foram congelados 1,5 milhões de EUR em ativos existentes em contas bancárias, empresas e domínios Web. No Dia Europeu de Luta contra o Tráfico de Seres Humanos, em 18 de outubro de 2020, a Comissão publicou um estudo sobre os custos associados ao tráfico de seres humanos e outro sobre os mecanismos de orientação nacionais e transnacionais[153].

Introdução clandestina de migrantes

O Centro Europeu contra a Introdução Clandestina de Migrantes comunicou um aumento contínuo das atividades de **introdução clandestina de migrantes**, principalmente nos Balcãs Ocidentais e nos países vizinhos, e dos movimentos secundários em toda a UE. Em 2019, a Europol contribuiu para a identificação de 14 218 suspeitos ativos no tráfico de migrantes[154]. Em maio de 2020, a Eurojust lançou o Grupo Focal para os Procuradores para a Introdução Clandestina de Migrantes como uma plataforma importante para ligar com regularidade entre si os principais intervenientes judiciários a nível nacional nos Estados-Membros da UE e para apoiar a sua resposta operacional conjunta[155].

Luta contra a criminalidade ambiental

A criminalidade ambiental abrange os atos que violam a legislação ambiental e causam ou podem causar danos ou riscos significativos para o ambiente e a saúde humana[156]. Entre os domínios mais importantes da **criminalidade ambiental** está a emissão ou a descarga ilegal de substâncias para o ar, a água ou o solo, o tráfico ilegal de espécies selvagens, o comércio ilegal de substâncias que empobrecem a camada de ozono e a transferência ou a descarga ilegais de resíduos. A avaliação recente da Diretiva Proteção do Ambiente[157] revelou que os progressos realizados no sentido de desenvolver um quadro europeu não foram acompanhados por um efeito significativo no terreno, nomeadamente em termos de uma melhor cooperação transfronteiras e de condições mais convergentes no que diz respeito às sanções nos Estados-Membros. Em particular, não conduziram a mais

[152] A título de exemplo, a Autoridade Europeia do Trabalho cooperou com a Europol para combater o tráfico de seres humanos na UE para todas as formas de exploração, incluindo a exploração sexual e laboral, bem como todas as formas de tráfico de crianças. Esta ação decorre também do Protocolo da Organização Internacional do Trabalho sobre o trabalho forçado (P29). Este protocolo representa uma norma fundamental no domínio do trabalho, que identifica o trabalho forçado como um crime e aborda as questões da prevenção, da proteção das vítimas, da compensação e da cooperação internacional em relação às formas conhecidas de trabalho forçado, incluindo a questão do tráfico.

[153] Estudos sobre os custos económicos, sociais e humanos do tráfico de seres humanos e revisão do funcionamento dos mecanismos de orientação nacionais e transnacionais dos Estados-Membros, disponíveis em: https://ec.europa.eu/anti-trafficking.

[154] Centro Europeu contra a Introdução Clandestina de Migrantes, 4.º relatório anual, 15.5.2020.

[155] http://www.eurojust.europa.eu/press/PressReleases/Pages/2020/2020-05-29.aspx.

[156] Diretiva 2008/99/CE relativa à proteção do ambiente através do direito penal.

[157] SWD(2020) 259 final.

condenações e à imposição de sanções mais dissuasivas nos Estados-Membros. Por conseguinte, foi decidido proceder-se a uma revisão da diretiva até ao final de 2021.

Entre 29 e 30 de outubro de 2019, a Eurojust realizou, em conjunto com a Rede Europeia de Procuradores para o Meio Ambiente (ENPE), a conferência «Colaboração e cooperação internacionais na luta contra a criminalidade ambiental», para sensibilizar e promover a cooperação transfronteiras entre os procuradores e outros profissionais, dentro e fora da UE, em matéria de criminalidade ambiental.

O Plano de Ação da UE contra o Tráfico de Animais Selvagens, adotado em 2016, está atualmente a ser avaliado. Uma ação específica é um projeto em execução até janeiro de 2021 orientada para o tráfico de espécies selvagens para a UE e através da UE utilizando a Internet e os serviços de entrega de encomendas, com o objetivo de neutralizar e desmantelar as redes de cibercriminalidade contra a vida selvagem[158].

V. UM SÓLIDO ECOSSISTEMA EUROPEU DE SEGURANÇA

A criação de uma União da Segurança genuína e eficaz deve ser o esforço comum de todos os setores da sociedade. Os governos, os serviços responsáveis pela aplicação da lei, o setor privado, o setor da educação e os próprios cidadãos devem ser mobilizados, equipados e conectados adequadamente para reforçar a preparação e a resiliência de todos, em especial dos mais vulneráveis, das vítimas e das testemunhas.

1. Cooperação e intercâmbio de informações

Um dos contributos mais importantes que a UE pode dar em matéria de proteção dos cidadãos consiste em ajudar os responsáveis pela segurança a colaborarem de forma eficaz. A cooperação e a partilha de informações são os instrumentos mais poderosos para combater a criminalidade e o terrorismo, lutar contra as ameaças, nomeadamente em termos de cibersegurança, e obter justiça. Foram implementados diversos instrumentos para apoiar o intercâmbio de informações entre as autoridades de aplicação da lei e judiciárias.

A Comissão está a adotar presentemente um mandato revisto para a **Europol**[159], a fim de introduzir uma série de melhorias específicas no seu trabalho. Esse processo permitirá à Europol lidar melhor com o caráter evolutivo dos crimes cometidos através da Internet e com os crimes financeiros. Reforçará a cooperação com o setor privado e alinhará as disposições em matéria de proteção de dados com as regras da UE em vigor.

A **Europol e outras agências da UE, como a Frontex, a CEPOL e a Eurojust**, com o apoio da Comissão, continuaram a desenvolver o ciclo político da UE relativo à criminalidade internacional organizada e grave, a chamada **Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas** (EMPACT[160]). A cooperação no âmbito da EMPACT continuou a revelar-se um instrumento eficaz contra a criminalidade organizada

[158] https://wwf.be/fr/wildlife-cybercrime/.

[159] COM(2020) 796.

[160] A EMPACT é o instrumento de cooperação policial da UE para combater as ameaças mais importantes à segurança da UE através do reforço da cooperação entre os serviços pertinentes dos Estados-Membros, as instituições da UE e as agências da UE, bem como com os países terceiros e as organizações internacionais. A EMPACT associa diferentes partes interessadas (abordagem multidisciplinar) para melhorar e reforçar a cooperação entre os Estados-Membros, as instituições da UE e as agências da UE, bem como com os países terceiros e as organizações internacionais, incluindo o setor privado.

em toda a Europa, por exemplo durante as jornadas de ação conjunta em setembro, outubro e novembro de 2020[161]. Essa é uma demonstração clara do valor da cooperação. Também apoiou objetivos menos quantificáveis: um quadro de informações melhorado, formação e reforço de capacidades, prevenção, cooperação com os parceiros de países terceiros e luta contra a criminalidade em linha[162]. A avaliação independente do ciclo político da UE 2018-2021/EMPACT, realizada em 2020[163], concluiu que este denotava cada vez mais relevância e eficácia no combate às ameaças mais urgentes colocadas pelos grupos de criminalidade organizada. O valor acrescentado advém da disponibilização de uma plataforma de cooperação que permite aos Estados-Membros obter melhores resultados contra a criminalidade grave e organizada do que se tivessem enfrentado estes problemas por si próprios. A avaliação também sinalizou oportunidades e apresentou recomendações no sentido de desenvolver ainda mais este instrumento de cooperação muito útil no próximo ciclo 2022-2025.

Em 2021, a Comissão lançará uma iniciativa para **um Código de Cooperação Policial da UE**a fim de simplificar, melhorar, desenvolver, modernizar e facilitar a cooperação policial entre as agências nacionais pertinentes. Este código será um importante apoio aos Estados-Membros na sua luta contra a criminalidade grave e organizada e o terrorismo.

A cooperação é igualmente necessária entre a **polícia e outras autoridades de aplicação da lei importantes**, bem como com agências como as alfândegas. As **alfândegas** da UE desempenham um papel fundamental para garantir a segurança das fronteiras externas e da cadeia de abastecimento, contribuindo assim para a segurança interna da União Europeia. As ameaças novas e em evolução afetam as principais interligações entre as autoridades aduaneiras e as autoridades de aplicação da lei, destacando particularmente o valor de «deteção/prevenção» dos controlos aduaneiros e o papel de liderança das alfândegas em relação às mercadorias. A Comissão tem apoiado e incentivado a cooperação entre as alfândegas e a Europol[164], com impacto direto na ação em domínios como as armas de fogo, a criminalidade ambiental, o financiamento da criminalidade e o crime cibernético. As autoridades aduaneiras participam atualmente em várias ações lideradas pela Europol contra a criminalidade internacional organizada e grave[165], bem como em formações da

[161] Jornadas de ação conjunta da EMPACT: Operação BÓSFORO, 1 776 armas de fogo apreendidas (2-11 novembro), Jornadas de ação conjunta «Mobile 3»: recuperados mais de 350 automóveis e mais de mil componentes automóveis furtados. (12-13 outubro), Jornadas de ação conjunta contra o tráfico de seres humanos para efeitos de exploração laboral, nas quais os agentes identificaram 715 potenciais vítimas de exploração laboral (14-20 setembro). Jornadas de ação conjunta contra a criminalidade na Europa do Sudeste, 51 armas de diferentes tipos e 47 quilogramas de uma variedade de drogas (setembro).

[162] Todas as fichas informativas detalhadas dos resultados, com valores e de acordo com as prioridades relativas à criminalidade da EMPACT da UE, podem ser consultadas em: https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf, documento 7623/20, de 5 de maio de 2020.

[163] Foi prevista uma avaliação independente nas conclusões do Conselho, de 27 de março de 2017, sobre a prossecução do ciclo político da UE para a criminalidade internacional grave e organizada para o período 2018-2021 (7704/17).

[164] Ver, por exemplo, o Plano de Ação do Grupo da Cooperação Aduaneira (GCA). Os principais domínios para 2020-2021 incluem: uma maior presença dos funcionários aduaneiros nos gabinetes de ligação da Europol, o acesso direto das autoridades aduaneiras à aplicação para a rede de intercâmbio seguro de informações da Europol (SIENA), uma melhor representação dos funcionários aduaneiros nas Unidades Nacionais Europol e a participação dos chefes de polícia e das alfândegas na Convenção Europeia de Chefes de Polícia.

[165] Fraude em matéria de impostos especiais de consumo/IVA, tráfico de armas de fogo, criminalidade ambiental, criminalidade financeira, luta contra o abuso sexual de crianças.

CEPOL. Estas atividades ajudam a promover e a desenvolver uma maior cooperação entre as agências e a melhorar a interação entre os principais participantes.

Os **sistemas de informação sólidos e eficientes** são indispensáveis para um melhor intercâmbio de informações entre as autoridades judiciárias e de aplicação da lei em toda a UE. O **Sistema de Informação Schengen (SIS)** também foi reforçado, mediante regras atualizadas que dão resposta a potenciais lacunas estabelecendo categorias adicionais de indicações, a expansão da lista de objetos relativamente aos quais podem ser emitidas indicações, bem como a autorização para a introdução de novos tipos de dados[166]. As novas regras entraram em vigor em 28 de dezembro de 2018 e deverão estar plenamente operacionais em dezembro de 2021[167].

Do mesmo modo, em 2019, o **Sistema Europeu de Informação sobre Registos Criminais (ECRIS)** foi complementado por um sistema adicional que permite um intercâmbio eficiente de informações sobre os registos criminais de nacionais de países terceiros condenados na UE (sistema ECRIS-TCN). Estão em curso os trabalhos de desenvolvimento técnico e de execução deste novo sistema centralizado, cuja entrada em vigor está prevista para 2023.

Em 24 de julho de 2020, a Comissão adotou o relatório de revisão da Diretiva Registos de Identificação dos Passageiros (PNR)[168], que revê os primeiros dois anos de aplicação da Diretiva PNR[169]. O relatório mostra que o desenvolvimento do sistema PNR à escala da UE avança a bom ritmo. A utilização de dados PNR é essencial na luta contra o terrorismo e a criminalidade grave e organizada, e já produziu resultados tangíveis. Só um Estado-Membro ainda não notificou a Comissão da transposição integral[170]. Em 3 de dezembro de 2020, a Comissão enviou um parecer fundamentado por não notificação da transposição integral da diretiva.

Em 9 de setembro de 2020, a Comissão publicou a avaliação da **Diretiva Informações Prévias sobre Passageiros** de 2004[171]. A avaliação destaca uma série de lacunas e de inconsistências, que serão tidas em conta na próxima revisão do atual quadro legislativo. Outro instrumento importante sob análise mais aprofundada são as **Decisões Prüm**[172], a considerar à luz dos desenvolvimentos operacionais, tecnológicos, forenses e de proteção de dados.

A cooperação também deve ultrapassar as fronteiras da UE para cooperar com os **principais países terceiros no combate ao terrorismo e à criminalidade organizada**. Em 13 de maio de 2020, o Conselho autorizou a abertura de negociações com a Nova Zelândia sobre o intercâmbio de dados pessoais entre a Europol e a Nova Zelândia. As negociações com a Turquia estão em curso, mas não foram conseguidos progressos nas negociações com a Argélia, o Egito, Israel, a Jordânia, o Líbano, Marrocos e a Tunísia sobre o intercâmbio de dados pessoais para a luta contra a criminalidade grave e o terrorismo. Além disso, a Comissão adotou em 19 de novembro de 2020 uma

[166] Regulamento (UE) 2018/1860, Regulamento (UE) 2018/1861, Regulamento (UE) 2018/1862.
[167] O SIS também será atualizado de acordo com as alterações propostas ao Regulamento Europol (COM(2020) XXX).
[168] COM(2020) 305.
[169] Diretiva (UE) 2016/681.
[170] Eslovénia
[171] SWD(2020) 174.
[172] O quadro jurídico de Prüm permite o intercâmbio automatizado de ADN, de impressões digitais e de dados de registo de veículos entre as autoridades de aplicação da lei. Foi publicada uma avaliação de impacto inicial.

recomendação de decisão do Conselho que autoriza a abertura de negociações para um acordo entre a União Europeia e dez países terceiros relativo à cooperação entre a Eurojust e esses países terceiros em matéria de intercâmbio de dados pessoais[173].

No que diz respeito à **cooperação internacional em matéria de intercâmbio de PNR** para fins de luta contra o terrorismo e a criminalidade grave, o Conselho autorizou a abertura de negociações com o Japão para a assinatura de um acordo PNR[174]. Entretanto, as **avaliações conjuntas dos acordos UE-EUA e UE-Austrália em vigor** *estão a ser finalizadas.* A Comissão lançou também um processo de revisão da sua abordagem geral atual em matéria de transferências de dados PNR para países terceiros[175].

A Comissão está a trabalhar igualmente com as Nações Unidas para aumentar a capacidade dos países parceiros no sentido de prevenir, detetar, investigar e reprimir as infrações terroristas e outros crimes graves, através da recolha e análise de dados de passageiros, tanto de informação antecipada sobre os passageiros como PNR.

A Comissão lançou o processo de facilitação das transferências de dados sob a forma de PNR em conformidade com os requisitos jurídicos da UE no quadro das novas normas PNR[176] adotadas pela Organização da Aviação Civil Internacional (OACI)[177].. Em 23 de junho de 2020, o Conselho da OACI adotou as novas normas e práticas recomendadas (SARP) em matéria de PNR[178], e as suas partes contratantes têm até 30 de janeiro de 2021 para informar a OACI de quaisquer diferenças entre as suas práticas regulamentares nacionais e as novas SARP em matéria de PNR.

2. Contributo das fronteiras externas sólidas

Uma gestão moderna e eficiente das fronteiras externas é fundamental para garantir a segurança dos cidadãos da UE. A mobilização de todos os intervenientes pertinentes para tirar o máximo partido da segurança nas fronteiras e disponibilizar-lhes os instrumentos adequados pode ter um impacto real na prevenção da criminalidade e do terrorismo transfronteiras. O Novo Pacto em matéria de Migração e Asilo[179] também destacou a necessidade de uma gestão robusta e equitativa das fronteiras externas, incluindo os controlos de identidade, de saúde e de segurança. Esse processo enquadra-se numa abordagem abrangente e mostra como a política de migração, asilo, integração e gestão das fronteiras depende de progressos em todas as frentes.

O novo pacto realçou que um espaço Schengen eficaz era indispensável para a política de migração e que tinha também profundas implicações em matéria de segurança. O tema foi discutido no primeiro Fórum Schengen, realizado em 30 de novembro de 2020. Os representantes dos Estados-Membros e do Parlamento Europeu concordaram com a importância de um espaço Schengen eficaz e que beneficie os cidadãos, tanto em termos de

[173] Os países terceiros propostos são os seguintes: Argélia, Arménia, Bósnia-Herzegovina, Egito, Israel, Jordânia, Líbano, Marrocos, Tunísia e Turquia, COM(2020) 743 final.
[174] 18 de fevereiro de 2020.
[175] Roteiro sobre a dimensão externa da política da UE em matéria de registo de identificação dos passageiros, disponível em: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-
[176] Decisão (UE) 2019/2107 do Conselho.
[177] Resolução 2396 do Conselho de Segurança das Nações Unidas (2017).
[178] Referida como a alteração 28 ao anexo 9 (facilitação) da Convenção sobre a Aviação Civil Internacional («Convenção de Chicago»).
[179] COM (2020) 609.

liberdade de circulação como também em termos de segurança. Este processo será integrado numa nova estratégia Schengen, a apresentar em 2021. O mecanismo de avaliação e controlo de Schengen é um instrumento fundamental para garantir a confiança mútua e garantir uma aplicação melhorada e coerente do acervo de Schengen, incluindo as suas implicações em matéria de segurança. Esse foi um tema importante constante do relatório aprovado em 25 de novembro[180], que apresenta o ponto da situação da aplicação do acervo de Schengen e faz o balanço do funcionamento do mecanismo de avaliação e controlo de Schengen.

Os **regulamentos relativos à interoperabilidade**[181] foram concebidos para que os sistemas de informação da UE existentes e novos ou atualizados trabalhem em conjunto de uma forma mais inteligente e eficiente para a gestão da segurança, das fronteiras e da migração. A interoperabilidade entre os sistemas de informação da UE melhorará a eficácia e a eficiência dos controlos nas fronteiras externas, contribuirá para a prevenção da imigração irregular e também para um elevado nível de segurança. Oferecerá um instrumento adicional valioso para as autoridades de aplicação da lei e para as autoridades responsáveis pelas fronteiras[182]. Os Estados-Membros, os países associados a Schengen e as agências pertinentes da União (a eu-LISA, a Agência Europeia da Guarda de Fronteiras e Costeira e a Europol) devem estar preparados, e a Comissão está a acompanhar a sua preparação e a prontidão para garantir que a aplicação plena seja alcançada até ao final de 2023.

Em 8 de dezembro de 2020, foi obtido um acordo provisório entre os colegisladores sobre a proposta de **atualização do Sistema de Informação sobre Vistos**[183].

No entanto, **ainda precisa de ser adotada alguma legislação fundamental**. O Parlamento Europeu deve concluir a sua disponibilidade para dialogar com o Conselho sobre as alterações[184] ao Sistema Europeu de Informação e Autorização de Viagem (ETIAS)[185].

As ligações entre os sistemas de informação pertinentes para a análise dos riscos de segurança são cruciais para reforçar a nossa segurança. Reforçar a **cooperação entre as autoridades aduaneiras e as autoridades responsáveis pela gestão das fronteiras** e as sinergias entre os seus **sistemas de informação**, em conformidade com os equilíbrios de poderes pertinentes, incluindo a proteção de dados pessoais e as legislações relativas à privacidade, é uma prioridade do plano de ação, de 28 de setembro de 2020[186], para fazer avançar a União Aduaneira para um novo patamar. A avaliação preliminar realizada pela Comissão com os peritos policiais e aduaneiros dos Estados-Membros recomenda, em particular, a concretização da ligação do Sistema de Informação Schengen (SIS) e dos dados da Europol ao sistema de controlo das importações 2 (ICS2)[187], para o que será agora lançado um estudo de viabilidade.

---

[180] SWD(2020) 327 final.

[181] Regulamento (UE) 2019/817 e Regulamento (UE) 2019/818.

[182] Sistemas existentes: Sistema de Informação Schengen (SIS), Sistema de Informação sobre Vistos (SIV), Eurodac e sistemas futuros: Sistema de Entrada/Saída, Sistema Europeu de Informação e Autorização de Viagem (ETIAS), Sistema Europeu de Informação sobre Registos Criminais de nacionais de países terceiros (ETIAS ECRIS-TCN).

[183] COM(2019) 12

[184] COM(2019) 3 final e COM(2019) 4 final.

[185] Regulamento (UE) 2018/1240 e Regulamento (UE) 2018/1241.

[186] COM(2020) 581.

[187] Sistema de informações antecipadas relativas à carga utilizado para a avaliação antecipada dos riscos de segurança de todas as movimentações de mercadorias que atravessam a fronteira externa.

O **Regulamento relativo à Guarda Europeia de Fronteiras e Costeira**[188] entrou em vigor em dezembro de 2019 e representa uma grande revisão das capacidades e dos instrumentos da UE para o reforço das suas fronteiras externas. O regulamento permitirá que a contribuição das fronteiras para a segurança seja significativamente reforçada. O novo mandato reforça a capacidade da Frontex para apoiar os Estados-Membros na gestão das fronteiras externas e das operações de regresso e alarga as possibilidades de cooperação com os países terceiros. Estão em curso trabalhos para assegurar a prontidão do corpo permanente da Guarda Europeia de Fronteiras e Costeira para o seu primeiro destacamento a partir de 1 de janeiro de 2021.

Em junho de 2019, a UE introduziu **normas de segurança mais rígidas em matéria de bilhetes de identidade**, a fim de facilitar a livre circulação dos cidadãos da UE e, ao mesmo tempo, reduzir a fraude de identidade[189]. A partir de agosto de 2021, os Estados-Membros são obrigados a iniciar a emissão de bilhetes de identidade e de títulos de residência em consonância com as novas normas de segurança. A maioria está atualmente a alinhar a conceção dos seus títulos em conformidade com os requisitos constantes do regulamento.

3. Reforçar a investigação e a inovação em matéria de segurança

A **investigação em matéria de segurança e de promoção da inovação** sustentam uma resposta coordenada da UE aos desafios complexos e permitem medidas concretas para atenuar os riscos. A União da Segurança é um dos quatro domínios de ação do programa de trabalho 2018-2020 para o **Horizonte 2020**[190], que representa 50 % do financiamento público total destinado à investigação em matéria de segurança na UE. A apresentação de propostas de investigação em matéria de segurança no âmbito dos convites à apresentação de propostas realizados em 2019 no âmbito do programa Horizonte 2020 conduziram à seleção de 42 projetos, aos quais foi alocado um total de 253 milhões de EUR de financiamento da UE. Os trabalhos abrangerão a proteção das infraestruturas, o aumento da resiliência a catástrofes, o combate à criminalidade e ao terrorismo e a proteção das fronteiras externas, bem como a melhoria da segurança digital. O orçamento indicativo disponível para os projetos em 2020 é de 265 milhões de EUR, o que inclui um convite à apresentação de candidaturas em matéria de inteligência artificial no valor de 20 milhões de EUR, que apoiará o aumento das capacidades de IA dos serviços europeus responsáveis pela aplicação da lei, colmatando as lacunas de competências a esse nível, e impulsionará a cooperação. Os trabalhos em preparação no âmbito do novo programa-quadro de investigação Horizonte Europa apoiarão a aplicação da Estratégia da UE para a União da Segurança, bem como a gestão das fronteiras e a dimensão da segurança do Novo Pacto em matéria de Migração e Asilo, as políticas da UE relativas à redução do risco de catástrofes e a Estratégia de Segurança Marítima da União Europeia[191].

A investigação em matéria de segurança financiada pela UE também se revelou eficaz na promoção da cooperação e no apoio aos profissionais de segurança durante a pandemia de

[188] Regulamento 2019/1896.
[189] Regulamento 2019/1157.
[190] A UE afetou cerca de 91 milhões de EUR ao financiamento de projetos que visam reforçar a proteção das infraestruturas, incluindo a associação das ciberameaças e das ameaças físicas, uma resposta melhorada e rápida a incidentes e uma melhor partilha de informações.
[191] No âmbito do Horizonte Europa, o agrupamento 3 apoiará, em particular, a prioridade política da Comissão «Promoção do modo de vida europeu», bem como o Pacto Ecológico Europeu e a iniciativa «Uma Europa Preparada para a Era Digital».

COVID-19[192]. O apoio inclui instrumentos para a avaliação e investigação epidemiológica e criminal conjunta em matéria dos riscos e das ameaças.

A fim de garantir a adoção de **projetos inovadores**, as agências da UE devem ser integradas no quadro em vigor para a investigação e a inovação em matéria de segurança. No seguimento do Conselho Justiça e Assuntos Internos de outubro de 2019, e com base nos seus mandatos legais vigentes, as agências da UE e o Centro Comum de Investigação da Comissão estão a criar, presentemente, o **polo europeu de inovação para a segurança interna**, que deverá servir como rede de colaboração para os seus laboratórios de inovação. O polo será um mecanismo de coordenação para apoiar as entidades participantes na partilha de informações e de conhecimento, na criação de projetos conjuntos e na divulgação de resultados e de soluções tecnológicas desenvolvidas que sejam relevantes para a segurança interna[193].

O **Centro Europeu Industrial, Tecnológico e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação** são a resposta da Europa no apoio à inovação e à política industrial em matéria de cibersegurança. Visam reforçar as capacidades europeias em matéria de cibersegurança, proteger a nossa economia e sociedade contra os ciberataques, manter a excelência da investigação e reforçar a competitividade da UE. Estão atualmente em curso os pertinentes diálogos tripartidos.

4. Competências e sensibilização

A sensibilização para as questões de segurança e a aquisição de competências para fazer face a potenciais ameaças são essenciais para construir uma sociedade mais resiliente, com empresas, administrações e indivíduos mais bem preparados. A garantia dos direitos das vítimas é também importante.

Profissionais da justiça e de aplicação da lei

As restrições relacionadas com a COVID-19 afetaram fortemente a CEPOL, que, a partir de março de 2020, foi obrigada a cancelar todas as atividades residenciais previstas. Estas circunstâncias especiais provocaram também uma procura crescente de serviços em linha; nos primeiros quatro meses do ano, a agência registou um aumento de 30 % nas atividades virtuais e uma duplicação dos utilizadores em linha. Entre os domínios de formação prioritários para 2019-2021[194] estão a luta contra a imigração ilegal, a luta contra o terrorismo, o tráfico de seres humanos e a cibercriminalidade e o abuso sexual de crianças. A Comissão está a preparar atualmente a avaliação da CEPOL, que ficará concluída em julho de 2021.

Público em geral

A **campanha «#SaferInternet4EU»** foi lançada no Dia por uma Internet mais Segura de 2018. As atividades tocaram cerca de 63 milhões de pessoas na UE nos últimos dois anos e incluem prémios, apoio a professores e ciber-higiene. A rede de centros Internet Segura forneceu mais de 1 800 novos recursos, abrangendo tópicos como as notícias falsas, o ciberassédio, as preocupações de privacidade, o aliciamento de menores e a ciber-higiene.

---

[192] As ações do Horizonte 2020 no apoio à resposta à pandemia encontram-se disponíveis em: https://www.researchgate.net/publication/341287556.

[193] Em 21 de fevereiro de 2020, o Comité Permanente para a Cooperação Operacional em matéria de Segurança Interna confirmou a declaração de missão e as principais características, tarefas e governação do polo europeu de inovação para a segurança interna.

[194] «European Union Strategic Training Needs Assessment 2018-2021», relatório UE-STNA, CEPOL.

Outubro de 2020 marcou o 8.º **Mês Europeu da Cibersegurança** da UE, promovendo a segurança em linha na UE. A campanha deste ano foi concebida para abordar as questões de segurança em torno da digitalização da vida quotidiana, acelerada pela pandemia de COVID-19. Incentivando as pessoas a «pensar antes de clicar», a campanha salientou diferentes temas em matéria de cibersegurança, para ajudar os utilizadores a identificarem e a estarem preparados para as ciberameaças. Encontra-se em fase de preparação o Desafio Europeu da Cibersegurança 2021, em Praga.

Uma ferramenta fundamental para ajudar as vítimas de cibercriminalidade é o «No More Ransom»[195], um repositório de instrumentos de decifragem gratuitos que ajuda as vítimas a contra-atacar sem pagar aos piratas informáticos. Apoiado pelo Centro da Cibercriminalidade da Europol, comemorou o seu quarto aniversário em julho de 2020 e, desde o seu lançamento, registou mais de 4,2 milhões de visitantes originários de 188 países, impedindo que cerca de 632 milhões de USD em pedidos de resgate fossem parar ao bolso dos criminosos.

Em 1 de julho de 2020, a Comissão apresentou a **Agenda de Competências para a Europa**[196] em prol da competitividade sustentável, da justiça social e da resiliência. Estabelece objetivos ambiciosos e quantitativos para melhorar as competências existentes e as formações em novas competências, que devem ser alcançados nos próximos cinco anos. Inclui ações específicas para aumentar o número de licenciados em ciências, tecnologia, engenharia, artes e matemática necessários em domínios de ponta como a cibersegurança. Em 10 de novembro de 2020, a Comissão lançou o Pacto para as Competências, durante a quinta edição da Semana Europeia da Formação Profissional 2020. O pacto promove ações conjuntas para maximizar o impacto do investimento na melhoria das competências existentes e na formação em novas competências. Em conjunto com o pacto, foram anunciadas as primeiras parcerias europeias de competências em três setores: automóvel, microeletrónica e indústria aeroespacial e da defesa.

Em 30 de setembro de 2020, a Comissão adotou um conjunto de estratégias políticas que terão um impacto importante no desenvolvimento da capacidade da UE em matéria de competências de segurança a longo prazo. O **Plano de Ação para a Educação Digital 2021-2027**[197] impulsionará um ecossistema de educação digital de alto desempenho, com competências reforçadas para a transformação digital[198]. No mesmo dia, foi adotada a comunicação sobre o **Espaço Europeu da Educação** até 2025[199], com particular incidência nas competências básicas e digitais. A comunicação sobre um novo **Espaço Europeu da Investigação para a Investigação e a Inovação**[200] definiu o caminho para melhorar o panorama de investigação e de inovação na Europa e acelerar a transição da UE para a liderança digital, bem como para combater a violência de género, em todas as suas formas, nas organizações de investigação e de inovação.

O **programa Erasmus+** também contribui para combater a radicalização, através de projetos de combate à radicalização, ao extremismo violento, à exclusão social, à

[195] https://www.nomoreransom.org/.
[196] COM(2020) 274.
[197] COM(2020) 624.
[198] https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-communication-sept2020_en.pdf.
[199] COM(2020) 625.
[200] COM(2020) 628.

desinformação e às notícias falsas[201]. Um exemplo é o projeto de prevenção da radicalização nas prisões, que visa melhorar as competências dos profissionais de primeira linha para identificar, comunicar e interpretar os sinais de radicalização e responder de forma adequada[202]. O projeto «No Hate BootCamp» ajudou os animadores de juventude a tornarem-se «embaixadores contra o discurso de ódio» nas suas comunidades locais.

A própria Comissão procura envolver o público nas reflexões sobre a política da UE em matéria de segurança. As ações a nível da UE tornaram-se mais visíveis e mais acessíveis aos cidadãos através do novo **sítio Web sobre a estratégia da UE em matéria de segurança**[203]. Foram lançadas várias **consultas públicas**, dando aos cidadãos a oportunidade de influenciar diretamente a elaboração de políticas.

Todas as vítimas da criminalidade têm direito ao apoio e à proteção, mas as vítimas dos crimes mais graves, como o terrorismo ou a exploração sexual de crianças, requerem atenção especial. Em 24 de junho de 2020, a Comissão adotou a sua primeira **Estratégia da UE sobre os direitos das vítimas (2020-2025)**[204]. A estratégia focaliza-se nas vítimas de todos os crimes, mas dá especial atenção aos mais vulneráveis, nomeadamente as vítimas do terrorismo, as crianças vítimas de exploração sexual e as vítimas de tráfico de seres humanos. Em 22 de setembro de 2020, a Comissão organizou uma conferência de alto nível sobre os direitos das vítimas, durante a qual inaugurou a **Plataforma para os Direitos das Vítimas**, para promover uma abordagem mais horizontal dos direitos das vítimas[205]. A Comissão também nomeou o seu primeiro **coordenador para os direitos das vítimas**, por forma a apoiar a consistência e a eficácia da política de direitos das vítimas.

No que diz respeito às **vítimas do terrorismo**, em janeiro de 2020 foi criado o Centro Especializado da UE para as Vítimas do Terrorismo, para disponibilizar conhecimentos específicos, orientações e apoio às autoridades nacionais e às organizações de apoio às vítimas. O centro promove o intercâmbio de melhores práticas e a partilha de conhecimentos especializados entre os profissionais e os especialistas transfronteiras. A sua conceção não se destina a prestar ajuda direta a vítimas específicas do terrorismo, mas a apoiar as estruturas nacionais na prestação de assistência e de apoio profissional, incluindo orientações a publicar em 2020. O centro da UE é um projeto-piloto que terá a duração de dois anos. A Presidência do Conselho está a trabalhar para apoiar esta ação mediante uma rede de pontos de contacto nacionais únicos para as questões relacionadas com as vítimas do terrorismo.

VI CONCLUSÃO

[201] Até à data, foram financiados cerca de 80 projetos que abrangem questões relacionadas com a radicalização, mais de uma centena de projetos sobre como prevenir e combater o ciberassédio e mais de uma centena em torno da educação para uma utilização crítica e ética da Internet, com vista a combater a desinformação em linha.

[202] http://www.r2pris.org/.

[203] https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union-strategy_en.

[204] COM(2020) 258.

[205] A plataforma reunirá, pela primeira vez, os principais intervenientes a nível da UE, incluindo a Rede Europeia dos Direitos das Vítimas, a Rede da UE de Pontos de Contacto Nacionais para a Indemnização, o Coordenador da UE da Luta Antiterrorista, as agências pertinentes, como a Eurojust, a Agência dos Direitos Fundamentais, a Agência da União Europeia para a Formação Policial, o Instituto Europeu para a Igualdade de Género e a sociedade civil.

A Estratégia para a União da Segurança foi implementada para favorecer uma abordagem abrangente e dinâmica. Os recentes ataques terroristas mostraram, uma vez mais, como a UE precisa de ser capaz de reagir, reforçando a nossa resiliência e reatividade através da modernização e da utilização eficaz dos principais instrumentos à nossa disposição. Mostraram também a necessidade de todos os intervenientes estarem plenamente envolvidos numa abordagem comum, de modo a que os Estados-Membros, as instituições da UE, o setor privado, as ONG e os próprios cidadãos possam desempenhar um papel na construção de uma base de segurança suficientemente sólida e flexível em termos de execução. Esta abordagem coerente e consistente será também a melhor forma de garantir que os nossos direitos fundamentais são protegidos no âmbito da promoção do nosso modo de vida europeu.

O presente relatório não só mostra os vários domínios de intervenção em curso como também de que forma se deve manter a dinâmica. O objetivo da Agenda da UE de Luta contra o Terrorismo hoje apresentada é reforçar o quadro europeu de combate ao terrorismo, definindo as próximas medidas necessárias: antecipar e prevenir o terrorismo, proteger os cidadãos e as infraestruturas e estar preparado para lhes responder, tendo em conta as ligações entre a segurança interna e a externa. Já temos mais cooperação, mais esforços envidados no combate à radicalização e mais instrumentos para privar os terroristas de meios para um ataque. Agora, há que ir mais longe nesta questão. Neste contexto, seria emblemático garantir a adoção de novas regras para combater os conteúdos terroristas em linha por via de um acordo a alcançar ainda este ano, que assume um caráter de máxima prioridade. A Comissão insta também os Estados-Membros a acelerarem a aplicação de toda a legislação acordada. Garantir a segurança dos cidadãos da UE é uma responsabilidade comum, pelo que avançar com uma ação comum tem de ser a ambição coletiva para uma Europa mais segura.