COMISSÃO
EUROPEIA

Bruxelas, 30.10.2019
COM(2019) 552 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO EUROPEU E AO CONSELHO

Vigésimo relatório sobre os progressos alcançados rumo a uma União da Segurança genuína e eficaz

I. INTRODUÇÃO

O presente vigésimo relatório sobre os progressos alcançados rumo a uma União da Segurança genuína e eficaz faz o ponto da situação sobre a evolução quanto a dois pilares principais: por um lado, a luta contra o terrorismo, a criminalidade organizada e os meios que os apoiam e, por outro, o reforço das nossas defesas e da nossa resiliência face a essas ameaças.

A Comissão Juncker atribuiu à segurança uma prioridade absoluta desde o início do seu mandato. Com base na Agenda Europeia para a Segurança[1], de abril de 2015, e na Comunicação da Comissão rumo à criação de uma União da Segurança genuína e eficaz, de abril de 2016[2], a UE respondeu com uma abordagem coordenada a uma série de ataques terroristas e a outros desafios crescentes em matéria de segurança, tendo alcançado progressos significativos em termos de reforço da segurança coletiva[3]. É cada vez mais evidente que os atuais desafios em matéria de segurança, nomeadamente o terrorismo, a criminalidade organizada, os ciberataques, a desinformação ou outras ameaças facilitadas pelo ciberespaço em evolução, são ameaças comuns. O nível de segurança coletiva que os nossos cidadãos procuram e esperam só pode ser alcançado se trabalharmos em conjunto. Este entendimento comum constituiu a base para os progressos alcançados rumo a uma União da Segurança genuína e eficaz. Impulsionado pela necessidade das autoridades nacionais que trabalham para garantir a segurança dos cidadãos, o apoio a nível da UE centrou-se em medidas legislativas e operacionais no âmbito das quais uma ação conjunta pode ter impacto na segurança dos Estados-Membros. Este trabalho foi realizado em estreita colaboração com o Parlamento Europeu e o Conselho, e com total transparência em relação ao público em geral. O pleno respeito dos direitos fundamentais esteve no cerne deste 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 UE envidou esforços para **lutar contra o terrorismo** limitando a margem de manobra dos terroristas, introduzindo novas regras que lhes dificultam o acesso a explosivos, a armas de fogo e a financiamento e restringem os seus movimentos. A UE intensificou o **intercâmbio de informações** com o objetivo de proporcionar aos agentes da primeira linha, aos agentes da polícia e aos guardas de fronteira um acesso eficiente a dados exatos e completos, utilizando da melhor forma as informações existentes, bem como colmatando as lacunas e eliminando os ângulos mortos. Uma proteção sólida das fronteiras externas constitui uma condição prévia para a segurança no espaço de livre circulação sem controlos nas fronteiras internas. Em março de 2019, o Parlamento Europeu e o Conselho chegaram a acordo para reforçar e equipar plenamente a **Guarda Europeia de Fronteiras e Costeira**, prevendo-se que o novo regulamento entre em vigor no início de dezembro de 2019. A UE criou uma plataforma e concedeu financiamento para que as pessoas que trabalham nas comunidades locais possam proceder ao intercâmbio de boas práticas em matéria de **luta contra a radicalização e de prevenção do extremismo violento**, e propôs novas regras para eliminar eficazmente os conteúdos terroristas em linha. O apoio da UE ajudou a **tornar as cidades mais resistentes** aos atentados, com planos de ação para apoiar a proteção dos espaços públicos e melhorar a preparação para os riscos de segurança químicos, biológicos, radiológicos e nucleares. A UE fez face às **ameaças à cibersegurança e às ameaças possibilitadas pelo ciberespaço** elaborando uma nova estratégia em matéria de cibersegurança adotando legislação pertinente e combatendo a **desinformação**, a fim de melhor proteger as nossas eleições. Prosseguem os esforços para reforçar a segurança das nossas **infraestruturas críticas digitais**, incluindo o reforço da cooperação no domínio da **cibersegurança das redes 5G** em toda a Europa.

Mais ainda há muito por fazer. O ataque a uma sinagoga, transmitido em direto, e o assassinato de dois

---

1 COM(2015) 185 final de 28.4.2015.
2 COM(2016) 230 final de 20.4.2016.
3 Os anteriores relatórios sobre os progressos alcançados rumo a uma União da Segurança genuína e eficaz podem ser consultados em: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

cidadãos em Halle, na Alemanha, em 9 de outubro de 2019, recordaram-nos de forma chocante a ameaça que o extremismo violento de direita e o antissemitismo representam. A UE salientou também, mais uma vez, a utilização abusiva da Internet para a propaganda terrorista e, por conseguinte, a necessidade de **regras à escala da UE para a supressão de conteúdos terroristas em linha**. O Conselho Justiça e Assuntos Internos de 7 e 8 de outubro de 2019 debateu o terrorismo e o extremismo violento de direita, salientando a necessidade de prosseguir os trabalhos, nomeadamente para combater a disseminação de conteúdos extremistas de direita ilegais em linha e fora de linha. Simultaneamente, o assassinato de três agentes da polícia e de outro membro do pessoal na sede da polícia de Paris, em 3 de outubro de 2019, demonstra que a ameaça do terrorismo inspirado no jiadismo continua a ser real e que é necessário prosseguir os esforços em curso para ajudar os Estados-Membros a fazer face a esta ameaça. A fuga de membros do EIIL/Daech detidos na sequência dos recentes acontecimentos no norte da Síria poderá ter graves repercussões na segurança na Europa. É importante que os Estados-Membros utilizem plenamente os sistemas de informação existentes para detetar e identificar os combatentes terroristas estrangeiros aquando da passagem das fronteiras externas. Estão também em curso trabalhos sobre a utilização de informações obtidas no campo de batalha para julgar os combatentes terroristas estrangeiros.

O presente relatório apresenta os progressos recentes nos trabalhos rumo a uma União da Segurança genuína e eficaz, salientando os domínios em que são necessárias novas medidas. Fornece informações atualizadas sobre a aplicação das medidas acordadas em matéria de **cibersegurança das redes de 5G**, em especial sobre o **relatório de avaliação de riscos da UE**, publicado em 9 de outubro de 2019, e sobre a **luta contra a desinformação**.

O presente relatório centra-se, em especial, na **dimensão externa** da cooperação na União da Segurança, com a assinatura de dois **acordos bilaterais de luta contra o terrorismo** com a Albânia e a República da Macedónia do Norte, bem como nos progressos realizados na cooperação com países terceiros parceiros no intercâmbio de **dados dos registos de identificação dos passageiros**. Além disso, juntamente com o presente relatório, a Comissão adotou um pedido de autorização para o início de negociações com vista à celebração de um acordo entre a UE e a **Nova Zelândia** sobre o intercâmbio de dados pessoais para combater a criminalidade grave e o terrorismo.

II. CONCRETIZAR AS PRIORIDADES LEGISLATIVAS

1. Prevenir a radicalização em linha e nas comunidades

A **prevenção da radicalização** constitui a pedra angular da resposta da União às ameaças que o terrorismo representa. A este respeito, a Internet tem sido o campo de batalha mais importante para a ação dos terroristas no século XXI. Os espaços em que os indivíduos radicalizados podem comunicar e partilhar conteúdos permitem o desenvolvimento de redes mundiais, alargando tanto as redes de extremistas violentos de direita como as redes de jiadistas. É por esta razão que a Comissão prossegue a sua abordagem em duas vertentes contra a radicalização em linha, no âmbito da qual as regras propostas para a eliminação de conteúdos terroristas ilegais em linha deverão reforçar a parceria voluntária com as plataformas em linha.

Para esse efeito, é fundamental **a proposta legislativa destinada a prevenir a difusão de conteúdos terroristas em linha**, com regras e salvaguardas claras que obriguem as plataformas na Internet a retirar os conteúdos terroristas no prazo de uma hora depois de terem recebido um pedido fundamentado das autoridades competentes, e a tomar medidas pró-ativas proporcionais ao nível de exposição a conteúdos terroristas[4]. Estão em curso negociações interinstitucionais entre o Parlamento Europeu e o Conselho, tendo sido realizada uma primeira reunião do trílogo em 17 de outubro de 2019. Dada a ameaça que os conteúdos terroristas em linha representam, a Comissão insta os colegisladores a chegarem a acordo sobre a legislação proposta até ao final de 2019.

[4] COM(2018) 640 final de 12.9.2018.

O ato legislativo proposto complementa a parceria voluntária com a indústria da Internet e outras partes interessadas no âmbito do **Fórum Internet da UE**. Desde a sua criação em 2015, tem sido um catalisador para as empresas da Internet agirem proativamente no sentido de identificar e remover conteúdos terroristas em linha, preparando desta forma a via para a iniciativa, liderada pelo setor, de uma «base de dados de valores de dispersão partilhada» (*database of hashes*)[5] e a criação do Fórum Mundial da Internet contra o Terrorismo. A Unidade da UE de Sinalização de Conteúdos na Internet, que faz parte da agência da UE responsável pela aplicação da lei, a Europol, tem sido fundamental para reforçar a cooperação com as empresas da Internet e contribuir para os objetivos gerais do Fórum Internet da UE. Na última reunião ministerial do Fórum Internet da UE, realizada em 7 de outubro de 2019, os Estados-Membros da UE e os altos representantes das empresas da Internet comprometeram-se a colaborar no âmbito do chamado **Protocolo de Crise da UE**. Este Protocolo identifica limiares para uma cooperação reforçada e estabelece novas formas de reforçar a resposta às crises. Estas medidas fazem parte dos esforços desenvolvidos a nível internacional para implementar o «apelo à ação de Christchurch»[6], que visa assegurar uma reação coordenada e rápida para conter a propagação de conteúdos terroristas e extremistas violentos em linha.

Para além destas medidas contra a radicalização em linha, a Comissão continua a apoiar os esforços a nível nacional e local para **prevenir e lutar contra a radicalização no terreno**. Com base na riqueza de experiências e de conhecimentos reunidos no âmbito da Rede de Sensibilização para a Radicalização, a UE oferece apoio específico aos intervenientes locais, incluindo as cidades[7], e proporciona oportunidades de intercâmbio entre profissionais, investigadores e decisores políticos. Por exemplo, a Rede emitiu orientações específicas e organizou seminários para ajudar as autoridades competentes a gerir os casos de crianças provenientes de zonas de conflito[8]. Tendo em vista assegurar a continuidade das atividades realizadas no âmbito da Rede de Sensibilização para a Radicalização, a Comissão lançou o procedimento para um novo contrato-quadro com um valor estimado de 61 milhões de EUR para um período de quatro anos, com início em 2020.[9]

A fim de combater a ameaça que representam os conteúdos terroristas em linha, a Comissão exorta o Parlamento Europeu e o Conselho a:

- concluírem as negociações sobre a proposta legislativa destinada a prevenir a difusão de **conteúdos terroristas em linha** antes do final do ano.

5 Instrumento criado por um consórcio de empresas para facilitar a cooperação, a fim de impedir a difusão de conteúdos terroristas em todas as plataformas.

6 Em resposta aos atentados perpetrados em Christchurch, na Nova Zelândia, em 15 de março de 2019, o presidente francês, Emmanuel Macron, e a primeira-ministra neozelandesa, Jacinda Ardern, convidaram os dirigentes e as plataformas em linha a reunirem-se em Paris, em 15 de maio de 2019, e a lançarem o «apelo à ação de Christchurch». O Presidente Juncker apoiou o apelo e anunciou a criação de um Protocolo de Crise da UE.

7 No que se refere à cooperação com as cidades em matéria de segurança, ver também a secção V.2 sobre preparação e proteção, nomeadamente sobre a proteção dos espaços públicos.

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf

9 O contrato-quadro é dividido em dois lotes: um montante de 29 000 000 EUR para apoiar as atividades da Rede de Sensibilização para a Radicalização durante os próximos quatro anos e um montante de 32 000 000 EUR para reforçar as capacidades dos Estados-Membros, das autoridades nacionais, regionais e locais e dos países terceiros prioritários para combater eficazmente a radicalização, em particular mediante a oferta de oportunidades de ligação em rede, serviços específicos e determinados pelas necessidades e investigação e análise.

2. *Sistemas de informação mais sólidos e mais inteligentes para a gestão da segurança, das fronteiras e da migração*

A UE intensificou o intercâmbio de informações, facilitando o combate à fraude de identidade[10], reforçando os controlos fronteiriços[11], modernizando as bases de dados policiais europeias[12], colmatando lacunas de informação[13] e reforçando a agência europeia para a cooperação policial, a Europol[14]. Para tal, é fundamental **a interoperabilidade dos sistemas de informação da UE**[15], o que significa tirar o máximo partido das informações existentes e eliminar os chamados «ângulos mortos». Respondendo às necessidades dos intervenientes no terreno, a interoperabilidade conduzirá a um acesso mais rápido e sistemático à informação por parte dos agentes responsáveis pela aplicação da lei, dos guardas de fronteira e dos funcionários dos serviços de migração, contribuindo assim para melhorar a segurança interna e a gestão das fronteiras.

No entanto, a interoperabilidade e toda a inovação que a mesma implica só será determinante para a gestão da segurança, das fronteiras e da migração no terreno se cada Estado-Membro aplicar plenamente a legislação na matéria. É por esta razão que a **aplicação** da interoperabilidade é uma prioridade máxima da União da Segurança, tanto a nível político como técnico. A Comissão e a Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA) apoiam os Estados-Membros com conhecimentos especializados e intercâmbio de boas práticas, utilizando uma rede de coordenadores nacionais e desenvolvendo um quadro de resultados para permitir mecanismos eficazes de acompanhamento e coordenação. A cooperação estreita entre as agências da UE, o conjunto dos Estados-Membros e os países associados de Schengen será crucial para alcançar o ambicioso objetivo da plena interoperabilidade dos sistemas de informação da UE para fins de gestão da segurança, das fronteiras e da migração até 2020.

---

[10] Regulamento (UE) 2019/1157, de 20 de junho de 2019, que visa reforçar a segurança dos bilhetes de identidade dos cidadãos da União e dos títulos de residência emitidos aos cidadãos da União e seus familiares que exercem o direito à livre circulação.

[11] Introdução de controlos sistemáticos de todos os cidadãos nas fronteiras externas utilizando o Sistema de Informação de Schengen. Todos os Estados Schengen, bem como a Roménia, a Bulgária, a Croácia e Chipre, aplicam as regras relativas aos controlos sistemáticos por confronto com as bases de dados pertinentes nas fronteiras externas, introduzidas em abril de 2017. Em conformidade com estas regras, são possíveis derrogações temporárias nas fronteiras terrestres ou marítimas, mas apenas em relação aos cidadãos da UE, tendo em conta o impacto desproporcionado no fluxo de tráfego. Atualmente, estas derrogações foram notificadas por seis Estados-Membros/países associados a Schengen (Croácia, Finlândia, Hungria, Letónia, Noruega e Eslovénia). No que diz respeito às fronteiras aéreas, a possibilidade de derrogação das regras relativas aos controlos sistemáticos terminou em abril de 2019.

[12] O Sistema de Informação de Schengen reforçado (Regulamento (UE) 2018/1860 de 28.11.2018, Regulamento (UE) 2018/1861 de 28.11.2018, Regulamento (UE) 2018/1862 de 28.11.2018) e o Sistema Europeu de Informação sobre Registos Criminais, alargado aos nacionais de países terceiros (Regulamento (UE) 2019/816 de 17.4.2019). O reforço do Sistema de Informação de Schengen inclui a obrigação geral de inserir no sistema indicações relacionadas com o terrorismo.

[13] O Sistema de Entrada/Saída da UE (Regulamento (UE) 2017/2226 de 30.11.2017) e o Sistema Europeu de Informação e Autorização de Viagem (Regulamento (UE) 2018/1240 de 12.9.2018 e Regulamento (UE) 2018/1241 de 12.9.2018).

[14] Nos últimos anos, o papel da Europol foi consideravelmente reforçado, tanto em termos de âmbito como de aprofundamento. A Agência foi reforçada graças à adoção do Regulamento Europol em 2016 (Regulamento (UE) 2016/794 de 11.5.2016). Os Estados-Membros aumentaram significativamente a quantidade de informações partilhadas com e através da Europol. A criação do Centro de Luta contra o Terrorismo (CELT) reforçou as capacidades analíticas da Europol nos casos de terrorismo. Nos últimos anos, o orçamento da Europol tem aumentado de modo constante, tendo passado de 82 milhões de EUR em 2014 para 138 milhões de EUR em 2019. Estão em curso as negociações sobre o orçamento para 2020.

[15] Regulamento (UE) 2019/817 de 20.5.2019 e Regulamento (UE) 2019/818 de 20.5.2019.

Entretanto, o Parlamento Europeu e o Conselho devem ainda **completar o trabalho legislativo** a este respeito. É essencial chegar rapidamente a acordo sobre todas as propostas legislativas pendentes para garantir a aplicação completa e atempada da interoperabilidade. Em primeiro lugar, no âmbito da implementação técnica do **Sistema Europeu de Informação e Autorização de Viagem**, é necessário introduzir alterações técnicas nos regulamentos conexos[16], a fim de implementar integralmente o sistema. A Comissão convida o Parlamento Europeu a acelerar os seus trabalhos sobre estas alterações técnicas, a fim de dar início às negociações interinstitucionais o mais rapidamente possível. Em segundo lugar, estão ainda em curso negociações interinstitucionais sobre a proposta de maio de 2018 para reforçar e modernizar o atual **Sistema de Informação sobre Vistos**[17]. Com base na primeira reunião do trílogo, que teve lugar em 22 de outubro de 2019, a Comissão apela a ambos os colegisladores para que concluam rapidamente as negociações. Em terceiro lugar, está ainda pendente um acordo sobre a proposta da Comissão de maio de 2016 que prevê o alargamento do âmbito de aplicação do **Eurodac**[18] para armazenar não só as impressões digitais e os dados pertinentes dos requerentes de asilo e das pessoas intercetadas por ocasião de uma passagem irregular da fronteira externa, mas também os dos nacionais de países terceiros em situação irregular. As alterações propostas também prolongariam o período de conservação das impressões digitais e dos dados pertinentes das pessoas que entram irregularmente na UE. A Comissão insta os colegisladores a procederem à adoção da proposta.

A fim de reforçar os sistemas de informação da UE para a gestão da segurança, das fronteiras e da migração, a Comissão insta o Parlamento Europeu e o Conselho a:

- avançarem nos trabalhos com vista a alcançar rapidamente um acordo sobre as alterações técnicas propostas que são necessárias para estabelecer o **Sistema Europeu de Informação e Autorização de Viagem**.
- realizarem e concluírem rapidamente as negociações sobre a proposta de reforço do atual **Sistema de Informação sobre Vistos**.
- adotarem a proposta legislativa relativa ao **Eurodac** *(prioridade da declaração conjunta)*.

3. Limitar a margem de manobra dos terroristas

A UE tomou medidas vigorosas para reduzir o espaço em que os terroristas operam, introduzindo novas regras que lhes dificultam o acesso a explosivos[19], a armas de fogo e a financiamento[20], bem como para restringir os seus movimentos.[21]

Para reforçar a resposta judicial ao terrorismo, a Agência Europeia para a Cooperação Judiciária Penal (Eurojust) criou, em 1 de setembro de 2019, um **Registo Europeu de Luta contra o Terrorismo**. O registo recolherá informações judiciais para estabelecer ligações entre os processos contra suspeitos de infrações terroristas, reforçando assim a coordenação entre os procuradores nas investigações em matéria de luta contra o terrorismo com potenciais implicações transfronteiras.

Contudo, são necessários esforços suplementares para apoiar e facilitar as investigações em processos transnacionais, nomeadamente no que se refere ao **acesso a provas eletrónicas** por parte das

16 Regulamento (UE) 2018/1240 de 12.9.2018 e Regulamento (UE) 2018/1241 de 12.9.2018.
17 COM(2018) 302 final de 16.5.2018.
18 COM(2016) 272 final de 4.5.2016.
19 Regulamento (UE) 2019/1148, de 20 de junho de 2019, sobre a comercialização e utilização de precursores de explosivos. O regulamento entrou em vigor em 31 de julho de 2019 e é aplicável 18 meses após essa data.
20 Diretiva (UE) 2019/1153 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, que estabelece normas destinadas a facilitar a utilização de informações financeiras e de outro tipo para efeitos de prevenção, deteção, investigação ou repressão de determinadas infrações penais.
21 Introdução de controlos sistemáticos de todos os cidadãos nas fronteiras externas utilizando o Sistema de Informação de Schengen.

autoridades de aplicação da lei. No que diz respeito às propostas legislativas de abril de 2018 destinadas a melhorar o acesso transfronteiras a provas eletrónicas em investigações criminais[22], o Parlamento Europeu deve ainda adotar a sua posição antes de os colegisladores poderem encetar negociações. A Comissão insta o Parlamento Europeu a avançar nesta proposta legislativa para que os colegisladores possam trabalhar para a sua rápida adoção. Com base na sua proposta de regras internas da UE, a Comissão está também a encetar **negociações internacionais** para melhorar o acesso transfronteiras às provas eletrónicas. Em 25 de setembro de 2019, a Comissão e as autoridades dos Estados Unidos realizaram a primeira ronda de negociações formais relativas a um **acordo UE-EUA sobre o acesso transfronteiras a elementos de prova eletrónicos**. Está prevista uma nova ronda para 6 de novembro de 2019. No contexto das negociações em curso de um **Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime do Conselho da Europa**, a Comissão participou, em nome da União, em três sessões de negociação, em julho, setembro e outubro de 2019. Embora se tenham registado progressos significativos nestas negociações, devem ainda ser tratados alguns temas importantes de interesse para a União, como as garantias em matéria de proteção de dados. A negociação de um Segundo Protocolo Adicional prosseguirá em novembro de 2019 e ao longo de 2020. É importante avançar rapidamente com ambas as negociações, a fim de reforçar a cooperação internacional em matéria de partilha de provas eletrónicas, assegurando simultaneamente a compatibilidade com o direito da UE e as obrigações dos Estados-Membros ao abrigo do mesmo, tendo igualmente em conta a futura evolução da legislação da UE.

Refletindo as atuais preocupações sobre o branqueamento de capitais, o Parlamento Europeu adotou, em 19 de setembro de 2019, uma **Resolução sobre o estado de aplicação da legislação da União relativa à luta contra o branqueamento de capitais**[23], em resposta ao pacote de quatro relatórios sobre a luta contra o branqueamento de capitais que a Comissão adotou em 24 de julho de 2019[24]. O Parlamento Europeu instou os Estados-Membros a garantirem a aplicação adequada e rápida das diretivas relativas ao branqueamento de capitais. O Parlamento Europeu instou igualmente a Comissão a avaliar se um regulamento relativo à luta contra o branqueamento de capitais seria mais adequado do que uma diretiva, bem como a examinar a necessidade de um mecanismo de coordenação e apoio para as unidades de informação financeira.

A fim de melhorar o acesso das autoridades de aplicação da lei às provas eletrónicas, a Comissão exorta o Parlamento Europeu e o Conselho a:

- chegarem rapidamente a acordo sobre as propostas legislativas em matéria de **provas eletrónicas** *(prioridade da declaração conjunta)*.

4. Reforçar a cibersegurança

O reforço da cibersegurança continua a ser um aspeto essencial do trabalho rumo a uma União da Segurança genuína e eficaz. Com a implementação da Estratégia da UE para a Cibersegurança, de 2017[25], a UE reforçou a sua resiliência, tendo-se tornado menos vulnerável aos ataques e mais rápida a recuperar; reforçou também a sua capacidade de dissuasão graças ao aumento das possibilidades de os atacantes serem capturados e punidos, nomeadamente através de um quadro para uma resposta diplomática conjunta da UE às ciberatividades mal-intencionadas. A União também apoia os

22 COM(2018) 225 final de 17.4.2018 e COM(2018) 226 final de 17.4.2018.

23 https://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_PT.html

24 Relatório sobre a avaliação dos riscos de branqueamento de capitais e de financiamento do terrorismo relacionados com atividades transnacionais a que está exposto o mercado interno [COM(2019) 370 de 24.7.2019]; Relatório sobre a interconexão dos mecanismos nacionais centralizados automatizados (registos centrais ou sistemas eletrónicos centrais de extração de dados) dos Estados-Membros sobre contas bancárias [COM(2019) 372 final de 24.7.2019]; Relatório sobre a avaliação de casos recentes de alegado branqueamento de capitais envolvendo instituições de crédito da UE [COM(2019) 373 final de 24.7.2019]; Relatório sobre a avaliação do quadro de cooperação entre as Unidades de Informação Financeira [COM(2019) 371 final de 24.7.2019].

25 JOIN(2017) 450 final de 13.9.2017.

Estados-Membros em matéria de ciberdefesa, implementando o Quadro Estratégico da UE para a Ciberdefesa.[26]

Com a entrada em vigor do Regulamento Cibersegurança[27] em junho de 2019, o **quadro europeu de certificação da cibersegurança** está a tomar forma. A certificação desempenha um papel essencial no aumento da confiança e da segurança dos produtos e serviços que são fulcrais para o Mercado Único Digital. O quadro de certificação proporcionará sistemas de certificação à escala da UE, sob a forma de um conjunto abrangente de regras, requisitos técnicos, normas e procedimentos. Envolve dois grupos de peritos, a saber, o Grupo Europeu para a Certificação da Cibersegurança, que representa as autoridades dos Estados-Membros, e o Grupo das Partes Interessadas para a Certificação da Cibersegurança, que representa a indústria. Este último reúne o lado da procura e da oferta de produtos e serviços das tecnologias da informação e da comunicação, incluindo as pequenas e médias empresas, os prestadores de serviços digitais, os organismos de normalização europeus e internacionais, os organismos nacionais de acreditação, as autoridades de controlo da proteção de dados e os organismos de avaliação da conformidade.

O Parlamento Europeu e o Conselho têm ainda de chegar a acordo sobre a iniciativa legislativa[28] tendo em vista a criação do **Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e da Rede de Centros Nacionais de Coordenação.** A proposta visa reforçar as capacidades da União no domínio da cibersegurança, estimulando o ecossistema tecnológico e industrial europeu neste domínio, bem como a coordenação e a partilha de recursos conexos. A Comissão exorta os dois colegisladores a retomarem e concluírem rapidamente as negociações interinstitucionais sobre esta iniciativa prioritária para reforçar a cibersegurança.

O trabalho com vista ao reforço da cibersegurança inclui o apoio aos níveis nacional e regional[29].

Para além das ciberameaças que visam os sistemas e os dados, a UE continua a fazer face aos desafios complexos e multifacetados que representam as **ameaças híbridas**. No Conselho, foi criado um grupo de trabalho horizontal em matéria de luta contra as ameaças híbridas, a fim de melhorar a resiliência da UE e dos seus Estados-Membros contra estas ameaças e apoiar as ações destinadas a reforçar a resiliência das sociedades em situações de crise. A Comissão e o Serviço Europeu para a Ação Externa apoiam estes esforços no âmbito do quadro comum de 2016 em matéria de luta contra as ameaças híbridas[30], bem como da Comunicação Conjunta de 2018[31] «Aumentar a resiliência e reforçar as capacidades para fazer face a ameaças híbridas». Além disso, o Centro Comum de Investigação está a elaborar um quadro de «modelo conceptual» para caracterizar as ameaças híbridas, com o objetivo de ajudar os Estados-Membros e as suas autoridades competentes a identificar o tipo de ataque híbrido com que podem ser confrontados. O modelo analisa a forma como um interveniente (estatal ou não estatal) utiliza uma série de instrumentos (desde a desinformação à espionagem ou às operações físicas) em vários domínios (económico, militar, social, político) para atingir um alvo a fim de alcançar uma série de objetivos.

A fim de reforçar a cibersegurança, a Comissão exorta o Parlamento Europeu e o Conselho a:

- chegarem rapidamente a acordo sobre a proposta legislativa relativa à criação do **Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e da Rede de Centros Nacionais de Coordenação**.

[26] Quadro Estratégico da UE para a Ciberdefesa (atualização de 2018), adotado pelo Conselho em 19 de novembro de 2018 (14413/18).
[27] Regulamento (UE) 2019/881 de 17.4.2019.
[28] COM(2018) 630 final de 12.9.2018.
[29] Por exemplo, a Comissão apoia uma parceria inter-regional de inovação sobre cibersegurança em que participam a Bretanha, Castela e Leão, a Renânia do Norte-Vestefália, a Finlândia Central e a Estónia, para desenvolver uma cadeia de valor da cibersegurança europeia centrada na comercialização e na expansão.
[30] JOIN(2016) 18 final de 6.4.2016.
[31] JOIN(2018) 16 final de 13.6.2018.

III. REFORÇAR A SEGURANÇA DAS INFRAESTRUTURAS DIGITAIS

As redes de quinta geração (5G) serão a futura espinha dorsal de economias e sociedades cada vez mais digitalizadas. Estão em causa milhares de milhões de objetos e sistemas conectados, nomeadamente em setores críticos como a energia, os transportes, a banca e a saúde, bem como sistemas de controlo industrial que transportam informações sensíveis e dão apoio aos sistemas de segurança. Por conseguinte, é essencial garantir a cibersegurança e a resiliência das redes 5G.

No âmbito de uma abordagem coordenada, os Estados-Membros publicaram, em 9 de outubro de 2019, um relatório sobre a **avaliação coordenada dos riscos em matéria de segurança das redes 5G a nível da UE** com o apoio da Comissão e da Agência Europeia para a Cibersegurança[32]. Este passo significativo faz parte da aplicação da Recomendação da Comissão Europeia de março de 2019 destinada a assegurar um elevado nível de cibersegurança das redes 5G em toda a UE[33]. O relatório baseia-se nos resultados das avaliações nacionais dos riscos de cibersegurança realizadas por todos os Estados-Membros. Identifica as principais ameaças e os seus principais autores, os ativos mais sensíveis, as principais vulnerabilidades (incluindo as vulnerabilidades técnicas e de outro tipo) e uma série de riscos estratégicos. Esta avaliação serve de base para identificar medidas de atenuação suscetíveis de ser aplicadas a nível nacional e europeu.

O relatório identifica uma série de importantes **desafios em matéria de cibersegurança** que poderão surgir ou tornar-se mais proeminentes nas redes 5G. Estes desafios em matéria de segurança estão principalmente relacionados com as principais *inovações* da tecnologia 5G, em especial a importância do *software* e a vasta gama de serviços e aplicações viabilizados pela 5G, bem como o papel dos *fornecedores* na construção e exploração das redes 5G e o grau de dependência dos fornecedores individuais. Isto significa que os produtos, serviços e operações dos fornecedores fazem cada vez mais parte da «superfície de ataque» das redes 5G. Além disso, o perfil de risco dos fornecedores individuais tornar-se-á particularmente importante, incluindo a probabilidade de o fornecedor estar sujeito a interferências de um país terceiro.

Em conformidade com o processo estabelecido na Recomendação da Comissão de março de 2019, os Estados-Membros devem chegar a acordo, até 31 de dezembro de 2019, sobre um **conjunto de medidas destinadas a atenuar** os riscos de cibersegurança identificados a nível nacional e da União. A Comissão e o Serviço Europeu para a Ação Externa continuarão também a trocar informações com os parceiros que partilham as mesmas ideias sobre cibersegurança e resiliência das redes 5G. A este respeito, a Comissão está em contacto com a NATO sobre a avaliação coordenada da UE dos riscos para a cibersegurança das redes 5G.

---

[32] A avaliação coordenada dos riscos em matéria de cibersegurança das redes 5G a nível da UE foi concluída pelo grupo de cooperação das autoridades competentes instituído no âmbito da Diretiva Segurança das Redes e da Informação (Diretiva (UE) 2016/1148 de 6.7.2016), com a ajuda da Comissão e da Agência Europeia para a Cibersegurança: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[33] C(2019) 2355 final de 26.3.2019.

IV. LUTAR CONTRA A DESINFORMAÇÃO E PROTEGER AS ELEIÇÕES DE OUTRAS AMEAÇAS POSSIBILITADAS PELO CIBERESPAÇO

A UE criou um **quadro para uma ação coordenada contra a desinformação**, no pleno respeito dos valores europeus e dos direitos fundamentais[34]. No âmbito do Plano de Ação contra a Desinformação[35], prosseguem os trabalhos para reduzir a margem para a desinformação, nomeadamente com vista a proteger a integridade das eleições.

Para este efeito, é fundamental o trabalho com o setor através do **Código de Conduta sobre Desinformação**, um instrumento de caráter autorregulador para as plataformas em linha e o setor da publicidade que entrou em vigor em outubro de 2018[36]. A Comissão avaliou a eficácia do Código após o seu primeiro ano de funcionamento, com base nos relatórios de autoavaliação anuais apresentados pelas plataformas em linha e pelos outros signatários do Código, publicados em 30 de outubro de 2019 juntamente com uma declaração da Comissão.[37] De um modo geral, os relatórios demonstram que os signatários envidaram esforços consideráveis para honrarem os seus compromissos.

As medidas tomadas pelas plataformas signatárias variam em termos de rapidez e de alcance entre os cinco pilares de compromissos do Código. Em geral, os progressos estão mais avançados no que diz respeito aos compromissos relativos às eleições europeias de 2019, nomeadamente interromper a publicidade e os incentivos monetários à desinformação (pilar 1), garantir a transparência da publicidade política e temática (pilar 2) e garantir a integridade dos serviços face às contas e comportamentos não autênticos (pilar 3). Em contrapartida, os progressos estão menos avançados ou são escassos no que diz respeito aos compromissos ligados à responsabilização dos consumidores (pilar 4) e à responsabilização da comunidade dos investigadores, nomeadamente através da disponibilização, pelas plataformas, de acesso pertinente e conforme com a privacidade a conjuntos de dados para fins de investigação (pilar 5). Existem também diferenças no âmbito das ações empreendidas por cada plataforma para assegurar o respeito dos seus compromissos, bem como diferenças entre os Estados-Membros no que diz respeito à aplicação das várias políticas. A Comissão continua a trabalhar com os signatários do Código e com outras partes interessadas para intensificar as medidas tomadas contra a desinformação.

No âmbito do Plano de Ação contra a Desinformação, a Comissão e a Alta Representante criaram, em cooperação com os Estados-Membros, um **sistema de alerta rápido** para combater as campanhas de desinformação. O sistema de alerta rápido permitiu às instituições da UE e aos Estados-Membros partilhar informações e análises antes das eleições para o Parlamento Europeu de 2019 e coordenar as respostas. Este trabalho intensificou-se após as eleições: estão em curso intercâmbios diários e foram organizadas três reuniões dos pontos de contacto do sistema de alerta rápido por diferentes Estados-Membros.

---

34 Ver o Plano de Ação contra a Desinformação (JOIN(2018) 36 final de 5.12.2018).

35 JOIN(2019) 12 final de 14.6.2019.

36 Nos termos do Código, as plataformas em linha Google, Facebook, Twitter e Microsoft assumiram o compromisso de impedir a utilização dos seus serviços para fins de manipulação por intervenientes mal-intencionados, garantir a transparência e a divulgação pública da publicidade de natureza política e tomar outras medidas para melhorar a transparência, a responsabilização e a fiabilidade do ecossistema em linha. As associações comerciais que representam o setor da publicidade também se comprometeram a cooperar com as plataformas para melhorar o controlo da colocação de anúncios e desenvolver instrumentos de segurança destinados a limitar a colocação de publicidade em sítios Web que divulgam desinformação.

37 https://ec.europa.eu/commission/presscorner/detail/pt/statement_19_6166. Para além da Google, do Facebook, do Twitter e da Microsoft, os outros signatários do Código incluem Mozilla, sete associações a nível europeu ou nacional que representam o setor da publicidade, e a EDiMA, uma associação europeia que representa plataformas e outras empresas de tecnologia ativas no setor em linha.

Outro passo concreto para identificar a desinformação consistiu no trabalho da **equipa de comunicação estratégica** («StratComms») e, em especial, o seu Grupo de Trabalho «East Stratcom», que gere o projeto «EUvsDisinfo» cujo objetivo consiste em monitorizar, analisar e dar resposta à desinformação pró-Kremlin[38]. Desde o início de 2019, o primeiro orçamento específico de 3 milhões de EUR permitiu intensificar e alargar este trabalho de modo a incluir a monitorização e a análise da desinformação pró-Kremlin na Web, nos serviços de radiodifusão e nas redes sociais em 19 línguas, desde o inglês até ao sérvio e ao árabe. O volume de atividades de desinformação exibidas mais do que duplicou graças à melhoria da capacidade de monitorização, com cerca de 2 000 casos de desinformação desmascarados até à data em 2019, em comparação com 765 casos durante o mesmo período de 2018. O Grupo de Trabalho «East Stratcom» desempenhou um papel fundamental na monitorização e exibição da desinformação pró-Kremlin visando as eleições para o Parlamento Europeu de 2019. A investigação foi acompanhada de uma campanha de sensibilização para a tentativa de interferência nos processos eleitorais em todo o mundo. A sua divulgação, realizada em estreita cooperação com o Parlamento Europeu e a Comissão, resultou em mais de 20 entrevistas nos meios de comunicação social, e a campanha envolveu mais de 300 jornalistas.

A Comissão tomou igualmente medidas para **reduzir a propagação da desinformação e de mitos sobre as instituições e as políticas da UE**. Criou uma rede de peritos em comunicação com um portal em linha que disponibiliza material informativo interativo sobre as políticas da UE, bem como sobre o problema da desinformação e o seu impacto na sociedade. Lançou também uma série de campanhas nas redes sociais centradas no combate à desinformação[39], em colaboração com o Parlamento Europeu e o Serviço Europeu para a Ação Externa.

V. EXECUÇÃO DE OUTROS DOSSIÊS PRIORITÁRIOS SOBRE SEGURANÇA

1. Aplicação de medidas legislativas no âmbito da União da Segurança

As medidas acordadas no quadro da União da Segurança só trarão plenos benefícios à segurança se todos os Estados-Membros assegurarem a sua aplicação rápida e completa. Com esse objetivo, a Comissão apoia ativamente os Estados-Membros na aplicação da legislação da UE, nomeadamente concedendo-lhes financiamento e facilitando o intercâmbio de boas práticas. Sempre que necessário, também faz pleno uso dos poderes que os Tratados lhe conferem para garantir a aplicação do direito da União, designadamente iniciando procedimentos de infração, quando apropriado.

O prazo para a aplicação da **Diretiva da UE relativa à utilização dos dados dos registos de identificação dos passageiros**[40] terminou em 25 de maio de 2018. Até à data, 25 Estados-Membros notificaram a sua transposição integral[41], o que representa um progresso significativo desde julho de 2018, data em que a Comissão deu início a procedimentos de infração contra 14 Estados-Membros[42]. Dois Estados-Membros ainda não notificaram a transposição integral apesar dos procedimentos de infração em curso lançados em 19 de julho de 2018.[43]. Paralelamente, a Comissão continua a apoiar todos os Estados-Membros nos seus esforços para concluir o desenvolvimento dos seus sistemas de registo de identificação dos passageiros, nomeadamente através da facilitação do intercâmbio de informações e de boas práticas.

---

38 www.euvsdisinfo.eu

39 https://europa.eu/euprotects/

40 Diretiva (UE) 2016/681 de 27.4.2016. A Dinamarca não participa na adoção da presente diretiva, não ficando por ela vinculada nem sujeita à sua aplicação.

41 As referências à notificação da transposição integral têm em conta as declarações dos Estados-Membros e não prejudicam a verificação dessa transposição pelos serviços da Comissão (situação em 17.10.2019).

42 Ver o décimo sexto relatório sobre os progressos alcançados rumo a uma União da Segurança genuína e eficaz [COM(2018) 690 final de 10.10.2018].

43 A Eslovénia notificou a transposição parcial. A Espanha não notificou qualquer medida de transposição (situação em 17.10.2019).

O prazo para a transposição da **Diretiva relativa à luta contra o terrorismo**[44] terminou em 8 de setembro de 2018. Até à data, 22 Estados-Membros notificaram a transposição integral, o que representa um progresso significativo desde novembro de 2018, data em que a Comissão deu início a procedimentos de infração contra 16 Estados-Membros[45]. Três Estados-Membros ainda não notificaram a transposição integral, apesar dos procedimentos de infração em curso[46]. Em 25 de julho de 2019, a Comissão enviou pareceres fundamentados a dois Estados-Membros por não terem notificado a transposição integral da diretiva[47]. Em resposta, ambos os Estados-Membros anunciaram que os trabalhos legislativos estarão concluídos antes do final do corrente ano.

O prazo para a transposição da **Diretiva relativa ao controlo da aquisição e da detenção de armas**[48] terminou em 14 de setembro de 2018. Até à data, 13 Estados-Membros notificaram a transposição integral. 15 Estados-Membros ainda não notificaram a transposição integral, apesar dos procedimentos de infração em curso lançados em 22 de novembro de 2018[49]. Em 25 de julho de 2019, a Comissão enviou pareceres fundamentados a 20 Estados-Membros por não terem notificado a transposição integral da diretiva. Em resposta, cinco Estados-Membros notificaram a transposição integral da diretiva[50].

O prazo para a transposição da **Diretiva sobre a Proteção de Dados na Aplicação da Lei**[51] terminou em 6 de maio de 2018. Até à data, 25 Estados-Membros notificaram a transposição integral, o que representa um progresso significativo desde julho de 2018, data em que a Comissão deu início a procedimentos de infração contra 19 Estados-Membros[52]. Três Estados-Membros ainda não notificaram a transposição integral, apesar dos procedimentos de infração em curso[53]. Em 25 de julho de 2019, a Comissão decidiu instaurar uma ação contra dois Estados-Membros[54] no Tribunal de Justiça da União Europeia por não transposição da diretiva e enviou uma carta de notificação para cumprir a um Estado-Membro[55] por não transposição integral da diretiva[56].

A Comissão está a avaliar a transposição da **Quarta Diretiva Branqueamento de Capitais**[57] e igualmente a verificar se as normas estão a ser corretamente aplicadas pelos Estados-Membros. Os Estados-Membros deviam transpor a diretiva para o direito nacional até 26 de junho de 2018. A Comissão iniciou procedimentos de infração contra 21 Estados-Membros, uma vez que considerou

---

44 Diretiva (UE) 2017/541 de 15.3.2017. Esta diretiva não é aplicável no Reino Unido, na Irlanda e na Dinamarca.

45 Ver o décimo sétimo relatório sobre os progressos realizados rumo a uma União da Segurança genuína e eficaz, COM(2018) 845 final de 11.12.2018.

46 A Grécia e o Luxemburgo não notificaram medidas nacionais de execução. A Polónia notificou medidas nacionais equivalentes a uma transposição parcial (situação em 17.10.2019).

47 Grécia e Luxemburgo.

48 Diretiva (UE) 2017/853 de 17.10.2019.

49 A Bélgica, a Chéquia, a Estónia, a Polónia, a Suécia, a Eslováquia e o Reino Unido notificaram medidas de transposição para parte das novas disposições. Chipre, a Alemanha, a Grécia, a Espanha, o Luxemburgo, a Hungria, a Roménia e a Eslovénia não notificaram quaisquer medidas de transposição (situação em 17.10.2019).

50 Finlândia, Irlanda, Lituânia, Países Baixos e Portugal (situação em 17.10.2019).

51 Diretiva (UE) 2016/680 de 27.4.2016.

52 Ver o décimo sexto relatório sobre os progressos alcançados rumo a uma União da Segurança genuína e eficaz, COM(2018) 690 final de 10.10.2018.

53 A Eslovénia notificou a transposição parcial. A Espanha não notificou a transposição. Embora a Alemanha tenha notificado a transposição integral, a Comissão considera que esta transposição não está completa (situação em 17.10.2019).

54 Grécia e Espanha.

55 Alemanha.

56 A Grécia notificou a transposição integral, que está a ser avaliada pela Comissão.

57 Diretiva (UE) 2015/849 de 20.5.2015.

que as comunicações que lhe foram transmitidas não eram uma transposição integral da diretiva.[58]

A Comissão avaliou a conformidade da transposição das **diretivas relativas à cibercriminalidade**. Em julho e em outubro de 2019, lançou procedimentos de infração contra 23 Estados-Membros[59] por ter considerado que a legislação nacional de execução notificada por esses Estados-Membros não representava uma transposição correta da **Diretiva relativa à luta contra o abuso sexual de crianças**[60]. A Comissão lançou igualmente, em julho e em outubro de 2019, procedimentos de infração contra quatro Estados-Membros[61] por ter considerado que a legislação nacional de execução notificada por esses Estados-Membros não representava uma transposição correta da **Diretiva relativa a ataques contra os sistemas de informação**[62].

A Comissão exorta os Estados-Membros a tomarem urgentemente as medidas necessárias para a transposição integral das seguintes diretivas para o direito nacional e a comunicarem a sua transposição à Comissão:

- A **Diretiva da UE relativa aos dados dos registos de identificação dos passageiros**, relativamente à qual um Estado-Membro ainda deve notificar a transposição para o direito nacional e um Estado-Membro deve completar a notificação da transposição[63];
- A **Diretiva Luta contra o Terrorismo**, relativamente à qual dois Estados-Membros ainda devem notificar a transposição para o direito nacional e um Estado-Membro deve completar a notificação da transposição[64];
- A **Diretiva relativa ao controlo da aquisição e da detenção de armas**, relativamente à qual oito Estados-Membros ainda devem notificar a transposição para o direito nacional e sete devem completar a notificação da transposição[65];
- A **Diretiva Proteção de Dados na Aplicação da Lei**, relativamente à qual um Estado-Membro deve ainda notificar a transposição para o direito nacional e dois Estados-Membros devem completar a notificação da transposição[66];
- A **Quarta Diretiva Branqueamento de Capitais**, relativamente à qual 21 Estados-Membros devem ainda completar a notificação da transposição[67];
- A **Diretiva relativa à luta contra o abuso sexual de crianças**, relativamente à qual foram iniciados procedimentos de infração contra 23 Estados-Membros por transposição incorreta[68];

58 Bélgica, Bulgária, Chéquia, Dinamarca, Alemanha, Estónia, Irlanda, França, Itália, Chipre, Letónia, Lituânia, Hungria, Países Baixos, Áustria, Polónia, Roménia, Eslováquia, Finlândia, Suécia e Reino Unido (situação em 17.10.2019). Antes, foram encerrados sete processos de infração relacionados com a diretiva.

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

60 Diretiva 2011/93/UE de 13.12.2011.

61 Bulgária, Itália, Portugal e Eslovénia.

62 Diretiva 2013/40/UE de 12.8.2013.

63 A Eslovénia notificou a transposição parcial. A Espanha não notificou qualquer medida de transposição (situação em 17.10.2019).

64 A Grécia e o Luxemburgo não notificaram qualquer medida de transposição. A Polónia notificou a transposição parcial (situação em 17.10.2019).

65 A Bélgica, a Chéquia, a Estónia, a Polónia, a Suécia, a Eslováquia e o Reino Unido notificaram medidas de transposição relativamente a parte das novas disposições. Chipre, a Alemanha, a Grécia, a Espanha, o Luxemburgo, a Hungria, a Roménia e a Eslovénia não notificaram quaisquer medidas de transposição (situação em 17.10.2019).

66 A Eslovénia notificou a transposição parcial. A Espanha não notificou a transposição. Embora a Alemanha tenha notificado a transposição integral, a Comissão considera que esta transposição não está completa (situação em 17.10.2019).

67 Bélgica, Bulgária, Chéquia, Dinamarca, Alemanha, Estónia, Irlanda, França, Itália, Chipre, Letónia, Lituânia, Hungria, Países Baixos, Áustria, Polónia, Roménia, Eslováquia, Finlândia, Suécia e Reino Unido (situação em 17.10.2019).

- A **Diretiva relativa a ataques contra os sistemas de informação**, relativamente à qual foram iniciados procedimentos de infração contra quatro Estados-Membros por transposição incorreta[69].

2. Preparação e proteção

Reforçar a resiliência face às ameaças à segurança constitui um aspeto importante dos trabalhos rumo a uma União da Segurança genuína e eficaz. A Comissão apoia os Estados-Membros e as autoridades locais no reforço da proteção dos espaços públicos, aplicando o Plano de Ação de outubro de 2017 e a Parceria para a Segurança nos Espaços Públicos, de janeiro de 2019, no âmbito da Agenda Urbana da UE. Este trabalho envolve as cidades que abordaram a Comissão e solicitaram apoio para fazer face aos desafios com que se depararam na proteção dos espaços públicos.

O intercâmbio de boas práticas entre as autoridades locais e com os operadores privados é fundamental para reforçar a segurança dos espaços públicos. Esta questão esteve no centro da **Semana Europeia da Segurança**, que decorreu em Nice, França, de 14 a 18 de outubro de 2019, e foi organizada pelo projeto financiado pela UE «Proteger as cidades aliadas contra o terrorismo garantindo a segurança das zonas urbanas». O evento, que reuniu 500 participantes de cidades de toda a Europa, autoridades nacionais e instituições de investigação, sublinhou a importância de uma estreita cooperação entre todas as partes interessadas, tanto públicas como privadas, e o papel das novas tecnologias na melhoria da proteção das cidades. A proteção dos espaços públicos fazia igualmente parte do programa da **Semana Europeia das Regiões e dos Municípios**, que se realizou em Bruxelas de 7 a 10 de outubro de 2019, tendo sido organizado um seminário sobre a Agenda Urbana da Parceria da UE para a Segurança nos Espaços Públicos. Centrou-se no papel das autoridades locais no domínio da política de segurança, na regulamentação e no financiamento da UE para fazer face aos principais desafios em matéria de segurança nos espaços públicos urbanos, bem como em temas fundamentais como a inovação através de soluções e tecnologias inteligentes, incluindo o conceito de segurança desde a conceção, a prevenção e a inclusão social. A Comissão está também a contribuir para promover a inovação das cidades nestes domínios através do seu último convite à apresentação de propostas para Ações Urbanas Inovadoras, cujos resultados foram anunciados em agosto de 2019. Entre os projetos selecionados, três cidades (Pireu na Grécia, Tampere na Finlândia e Turim em Itália) testarão novas soluções em matéria de segurança urbana[70].

Para melhor **proteger os locais de culto** e explorar as necessidades dos diferentes grupos religiosos, a Comissão organizou, em 7 de outubro de 2019, uma reunião com representantes das comunidades judaica, muçulmana, cristã e budista. A reunião, que se insere no quadro da execução do Plano de Ação da UE de 2017 para apoiar a proteção dos espaços públicos, mostrou que a sensibilização e a preparação para a segurança variam significativamente entre as diferentes comunidades religiosas, salientando a importância de um maior intercâmbio de boas práticas. A reunião revelou igualmente que a introdução de medidas de segurança de base e uma maior sensibilização para a segurança não são incompatíveis com a manutenção do caráter aberto e acessível dos locais de culto. A Comissão procederá à recolha de boas práticas e de material de sensibilização na sua plataforma eletrónica destinada aos peritos e submeterá a questão às autoridades de segurança dos Estados-Membros no fórum público-privado para a proteção dos espaços públicos.

Um domínio específico que requer maior atenção é a ameaça crescente que os **drones** representam para a segurança das infraestruturas críticas e dos espaços públicos. A fim de complementar a recente

---

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

69 Bulgária, Itália, Portugal e Eslovénia.

70 As Ações Urbanas Inovadoras são um instrumento cofinanciado pelo Fundo Europeu de Desenvolvimento Regional. Para mais informações, consultar: https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

legislação da UE[71] relativa a operações seguras de drones no espaço aéreo das aeronaves tripuladas e sem prejudicar as oportunidades de utilização benéfica dos drones, a Comissão apoia os Estados-Membros no seguimento das tendências da utilização mal-intencionadas de drones, financiando investigação pertinente e facilitando o teste de contramedidas. O intercâmbio de experiências e de boas práticas é crucial, conforme demonstrado na conferência internacional de alto nível sobre a luta contra as ameaças colocadas pelos sistemas de aeronaves não tripuladas, realizada em Bruxelas em 17 de outubro de 2019. Este evento organizado pela Comissão reuniu 250 participantes dos Estados-Membros, de organizações internacionais, de parceiros de países terceiros, da indústria, do meio académico e da sociedade civil, a fim de debater os problemas de segurança colocados pelos drones e as formas de os resolver. A reunião revelou a necessidade de avaliações periódicas dos riscos relacionados com os drones e de uma cooperação estreita entre o setor da aviação e as autoridades responsáveis pela aplicação da lei com o objetivo de reforçar a legislação europeia relativa a operações seguras de drones. É igualmente necessário testar novas contramedidas em resposta aos drones mediante uma abordagem europeia coordenada. Além disso, os participantes acordaram que, para que os «drones» sejam seguros, fiáveis do ponto de vista operacional e difíceis de utilizar para fins mal-intencionados, é essencial uma colaboração estreita entre as autoridades e a indústria.

3. Dimensão externa

Uma vez que a maior parte dos riscos de segurança que a União enfrenta ultrapassam as fronteiras da UE e representam ameaças globais, a cooperação com os países parceiros, as organizações e as partes interessadas relevantes desempenha um papel vital na construção de uma União da Segurança genuína e eficaz.

O intercâmbio de informações é fundamental para esta cooperação. Juntamente com o presente relatório, a Comissão adotou uma recomendação ao Conselho para que autorize a abertura de negociações com vista à celebração de um **acordo entre a UE e a Nova Zelândia sobre o intercâmbio de dados pessoais para combater a criminalidade grave e o terrorismo** entre a Europol e as autoridades neozelandesas competentes. Esse acordo reforçará as capacidades da Europol para cooperar com a Nova Zelândia para efeitos da prevenção e luta contra os crimes que fazem parte das competências da Europol. Embora o acordo de trabalho de abril de 2019 entre a Europol e a polícia neozelandesa preveja um quadro para a cooperação estruturada a nível estratégico, não oferece uma base jurídica para o intercâmbio de dados pessoais. O intercâmbio de dados pessoais no pleno respeito do direito da UE e dos direitos fundamentais é essencial para uma cooperação policial operacional eficaz. Anteriormente, a Comissão tinha identificado oito países prioritários na Região do Médio Oriente/Norte de África para encetar negociações, com base na ameaça terrorista, nos desafios relacionados com a migração e nas necessidades operacionais da Europol[72]. Tendo em conta as necessidades operacionais das autoridades responsáveis pela aplicação da lei em toda a UE e os potenciais benefícios de uma cooperação mais estreita neste domínio, conforme demonstrado pelas medidas tomadas na sequência do ataque de Christchurch de março de 2019, a Comissão considera necessário acrescentar a Nova Zelândia aos países prioritários com os quais devem ser encetadas negociações a curto prazo.

Outra pedra angular da cooperação da União com países terceiros em matéria de segurança é a transferência dos **dados dos registos de identificação dos passageiros**. Em 27 de setembro de 2019, a Comissão adotou uma recomendação ao Conselho para que autorize a abertura de negociações com vista à celebração de um acordo **UE-Japão** para a transferência dos dados dos registos de identificação

[71] Regulamento de Execução (UE) 2019/947 da Comissão, de 24 de maio de 2019, relativo às regras e aos procedimentos para a operação de aeronaves não tripuladas.

[72] Ver o décimo primeiro relatório sobre os progressos alcançados rumo a uma União da Segurança genuína e eficaz, COM(2017) 608 final de 18.10.2017. Os países prioritários são a Argélia, o Egito, Israel, a Jordânia, o Líbano, Marrocos, a Tunísia e a Turquia.

dos passageiros para fins de prevenção e luta contra o terrorismo e outros crimes transnacionais graves no pleno respeito das garantias em matéria de proteção de dados e dos direitos fundamentais.[73] A recomendação está a ser analisada pelo grupo de trabalho do Conselho, e a Comissão insta o Conselho a adotar rapidamente um mandato para as negociações com o Japão. Dispor de acordos a tempo para os Jogos Olímpicos de 2020 traria um verdadeiro valor acrescentado em matéria de segurança.

A nível mundial, a Comissão apoia o trabalho realizado pela **Organização da Aviação Civil Internacional** com o objetivo de estabelecer uma norma para o tratamento dos dados dos registos de identificação dos passageiros. Tal responde a um apelo da Resolução 2396 do Conselho de Segurança das Nações Unidas que insta todos os Estados membros das Nações Unidas a desenvolverem a capacidade de recolher, tratar e analisar os dados dos registos de identificação dos passageiros. Em 13 de setembro de 2019, a Comissão apresentou uma proposta[74] de decisão do Conselho relativa à posição a adotar, em nome da União Europeia, no Conselho da Organização da Aviação Civil Internacional no que diz respeito às normas e práticas recomendadas em matéria de dados dos registos de identificação dos passageiros. A proposta está a ser analisada pelo grupo de trabalho do Conselho, e a Comissão apela à rápida adoção da decisão do Conselho. A posição da União e dos seus Estados-Membros foi igualmente estabelecida num documento de informação intitulado «Normas e princípios aplicáveis à recolha, utilização, tratamento e proteção dos dados dos registos de identificação dos passageiros», que foi apresentado à 40.ª sessão da Assembleia da Organização da Aviação Civil Internacional.

No que diz respeito aos trabalhos com vista à celebração de um novo acordo sobre o registo de identificação dos passageiros com o **Canadá**, a Comissão pretende que esse acordo seja rapidamente finalizado. Entretanto, foram lançadas este verão a revisão conjunta e a avaliação conjunta do acordo sobre os registos de identificação dos passageiros com a **Austrália**, bem como a avaliação conjunta do acordo sobre o registo de identificação dos passageiros com os **Estados Unidos**, com visitas a Camberra e a Washington em agosto e setembro de 2019, respetivamente. Em 14 de outubro de 2019, a Comissão informou a Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu, numa sessão à porta fechada, sobre o ponto da situação dos trabalhos com o Japão, a Austrália e o Canadá relativamente aos dados dos registos de identificação dos passageiros.

Registaram-se igualmente progressos no domínio da cooperação em matéria de segurança com os parceiros dos **Balcãs Ocidentais**, em aplicação do plano de ação conjunto de combate ao terrorismo nos Balcãs Ocidentais, de outubro de 2018. Em 9 de outubro, a Comissão assinou dois acordos bilaterais não vinculativos de combate ao terrorismo com a Albânia e a República da Macedónia do Norte[75]. Estes acordos estabelecem as medidas prioritárias específicas a tomar pelas autoridades do país parceiro em causa, abrangendo os cinco objetivos do plano de ação conjunto[76] e indicando o apoio que a Comissão tenciona conceder. Prevê-se que nas próximas semanas sejam assinados acordos semelhantes com os restantes países parceiros dos Balcãs Ocidentais. Além disso, em 7 de outubro de 2019, a Comissão assinou um acordo com o Montenegro sobre a cooperação no domínio da gestão das fronteiras entre este país e a Agência Europeia da Guarda de Fronteiras e Costeira (Frontex). Esse acordo permite à Agência prestar assistência ao Montenegro na gestão das fronteiras, com o objetivo de combater a migração irregular e a criminalidade transfronteiriça, reforçando assim a segurança nas fronteiras externas da UE.

---

73 COM(2019) 420 final de 27.9.2019.

74 COM(2019) 416 final de 13.9.2019.

75 https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en

76 O plano de ação conjunto prevê ações relativas aos cinco objetivos seguintes: um quadro sólido de luta contra o terrorismo; a prevenção eficaz e a luta contra o extremismo violento; o intercâmbio efetivo de informações e a cooperação operacional; o reforço das capacidades de luta contra o branqueamento de capitais e o financiamento do terrorismo; o reforço da proteção dos cidadãos e das infraestruturas.

A fim de reforçar a cooperação com os países parceiros no combate às ameaças comuns à segurança, a Comissão insta o Conselho a:

- adotar a autorização para o início de negociações com vista à celebração de um acordo entre a UE e a **Nova Zelândia** sobre o intercâmbio de dados pessoais para combater a criminalidade grave e o terrorismo;
- adotar a autorização para o início de negociações com vista à celebração de um acordo entre a UE e o **Japão** sobre a transferência dos dados dos registos de identificação dos passageiros;
- adotar a proposta de **decisão do Conselho relativa à posição a adotar, em nome da União Europeia, na Organização da Aviação Civil Internacional** no que diz respeito às normas e práticas recomendadas em matéria de dados dos registos de identificação dos passageiros.

VI. CONCLUSÃO

O presente relatório expõe o vasto leque de medidas que a UE tem vindo a tomar para fazer face às ameaças comuns na Europa e reforçar a nossa segurança coletiva. Graças ao entendimento comum de que a forma mais eficaz de fazer face aos atuais desafios em matéria de segurança é a cooperação com os países terceiros, os progressos alcançados rumo a uma União da Segurança genuína e eficaz são o resultado da estreita cooperação entre um grande número de intervenientes, do estabelecimento de um clima de confiança, da partilha de recursos e da resposta conjunta às ameaças, em todos os níveis de governo, desde as cidades e outros intervenientes locais, as regiões e as autoridades nacionais até ao nível da UE, com o Parlamento Europeu e o Conselho; com a participação das autoridades públicas, das agências da UE, dos intervenientes privados e da sociedade civil, utilizando conhecimentos especializados, ferramentas e recursos em todos os domínios de intervenção, como a política de transportes, o mercado único digital ou a política de coesão. Desta forma, o trabalho para a União da Segurança está integrado na proteção dos direitos fundamentais, na salvaguarda e na promoção dos nossos valores.

Os trabalhos rumo a uma União da Segurança genuína e eficaz devem prosseguir. É preciso chegar rapidamente a acordo sobre importantes iniciativas pendentes, nomeadamente: (1) a proposta legislativa sobre a remoção de conteúdos terroristas em linha, (2) a proposta legislativa destinada a melhorar o acesso às provas eletrónicas pelas autoridades de aplicação da lei, (3) a proposta legislativa relativa à criação de um Centro Europeu Industrial, Tecnológico e de Investigação em Cibersegurança e da Rede de Centros Nacionais de Coordenação, e (4) as propostas legislativas pendentes sobre sistemas de informação mais sólidos e mais inteligentes para a gestão da segurança, das fronteiras e da migração. As medidas e os instrumentos acordados devem ser convertidos numa realidade operacional no terreno, com a aplicação atempada e integral da legislação da UE por todos os Estados-Membros, a fim de obter todos os seus benefícios para a segurança. Em especial, é essencial que todos os Estados-Membros apliquem a legislação recentemente acordada sobre a interoperabilidade dos sistemas de informação da UE para a gestão da segurança, das fronteiras e da migração, a fim de alcançar o objetivo ambicioso da plena interoperabilidade até 2020. Por último, a Europa deve permanecer vigilante face às ameaças emergentes e em evolução e continuar a trabalhar em conjunto para reforçar a segurança de todos os cidadãos.