COMISSÃO
EUROPEIA

Bruxelas, 24.7.2019
COM(2019) 353 final

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

Décimo nono relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz

I. INTRODUÇÃO

O presente décimo nono relatório trata dos progressos realizados no estabelecimento de uma União da Segurança genuína e eficaz e cobre a evolução da situação respeitante 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.

Os cidadãos europeus esperam muito justamente que a União assegure a sua segurança. Desde o início do seu mandato que a Comissão Juncker fez da segurança uma prioridade absoluta. No quadro da nova «Agenda Estratégica 2019-2024» do Conselho Europeu, o objetivo que consiste em «proteger os cidadãos e as liberdades» constitui a primeira das quatro prioridades principais da União[1]. O Conselho Europeu anunciou igualmente que irá desenvolver e reforçar as medidas União de luta contra o terrorismo e a criminalidade transfronteiras, nomeadamente através da melhoria da cooperação e da partilha de informações e do desenvolvimento de instrumentos comuns.

Graças a uma estreita cooperação entre o Parlamento Europeu, o Conselho e a Comissão, a UE registou progressos significativos no trabalho conjunto rumo à criação de uma União da Segurança genuína e eficaz, pondo em prática uma série de iniciativas legislativas prioritárias e aplicando uma vasta gama de medidas não legislativas para apoiar os seus Estados-Membros e aumentar a segurança para todos os cidadãos[2]. A União tomou medidas decisivas para reduzir a margem de manobra dos terroristas e dos criminosos, tendo para o efeito privado os terroristas dos meios de cometer atentados através da proibição da aquisição e utilização de determinadas armas de fogo e explosivos e limitando o acesso ao financiamento. A UE reforçou também o intercâmbio de informações entre os Estados-Membros e colmatou as lacunas e os ângulos mortos em matéria de informação, combatendo ao mesmo tempo a radicalização, protegendo os europeus em linha, lutando contra as ciberameaças e as ameaças possibilitadas pelo ciberespaço, reforçando a gestão das fronteiras externas da União e consolidando a cooperação internacional no domínio da segurança.

Paralelamente, diversas iniciativas prioritárias no quadro da União da Segurança ainda aguardam adoção por parte dos colegisladores. Na sequência da constituição da nona legislatura do Parlamento Europeu, em 2 de julho de 2019, o presente relatório:

- Define os casos em que os colegisladores devem tomar medidas para fazer face às ameaças imediatas. É particularmente urgente tomar medidas para **combater a propaganda terrorista e a radicalização em linha**;
- Apresenta as iniciativas prioritárias pendentes na União da Segurança que exigem novas medidas por parte dos colegisladores para reforçar a **cibersegurança**, facilitar o acesso às **provas eletrónicas** e concluir os trabalhos sobre sistemas de informação mais sólidos e mais inteligentes para efeitos da gestão da segurança, das fronteiras e da migração;
- Informa sobre os trabalhos conjuntos e urgentes lançados em março de 2019 para avaliar e reforçar **a segurança das redes 5G**, com base nas avaliações de risco nacionais apresentadas pelos Estados-Membros até 15 de julho de 2019;
- Examina um conjunto de quatro relatórios relacionados com a l**uta contra o branqueamento de capitais**, adotados pela Comissão em 24 de julho de 2019, que analisam os riscos e vulnerabilidades atuais em matéria de branqueamento de capitais e avaliam a forma como o quadro regulamentar pertinente da UE está a ser aplicado nos setores público e privado;

---

1 https://www.consilium.europa.eu/media/39965/a-new-strategic-agenda-2019-2024-pt.pdf

2 Para uma panorâmica geral, consultar a ficha de informação intitulada «União da Segurança: uma Europa que protege» (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_1.pdf e o décimo oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz [COM(2019) 145 final de 20.3.2019].

- Fornece informações atualizadas sobre os progressos alcançados desde março de 2019[3] na aplicação de medidas legislativas na União da Segurança, sendo a interoperabilidade dos sistemas de informação uma das principais prioridades para a aplicação rápida e completa pelos Estados-Membros;
- Faz o ponto da situação dos trabalhos em curso para combater a desinformação e proteger as eleições contra ameaças possibilitadas pelo ciberespaço, sobre os esforços para melhorar a preparação e a proteção contra ameaças à segurança e sobre a cooperação com os parceiros internacionais em questões de segurança.

II. CONCRETIZAR AS PRIORIDADES LEGISLATIVAS

1. Prevenir a radicalização em linha e nas comunidades

A prevenção da radicalização é o elemento central da resposta da UE ao terrorismo, tanto em linha como a nível das nossas comunidades.

O horrível ataque em Christchurch, na Nova Zelândia, em 15 de março de 2019, veio recordar, de forma terrível, como a Internet pode ser aproveitada para fins terroristas, quer seja alimentada pelo jiadismo, pela extrema-direita ou por qualquer outra ideologia extremista. A rapidez e a amplitude da difusão do vídeo de Christchurch nas plataformas Internet evidenciaram a importância crucial de essas plataformas disporem de medidas adequadas para bloquear a propagação rápida de tais conteúdos.

Na sequência desses acontecimentos, os Chefes de Estado ou de Governo de alguns Estados-Membros e de países terceiros, o Presidente Juncker e as plataformas em linha apoiaram, em 15 de maio de 2019, o «**apelo à ação de Christchurch**»[4] que estabelece ações coletivas com vista a eliminar conteúdos terroristas e extremistas violentos em linha. Foram assumidos compromissos adicionais a esse respeito no G7[5] e no G20[6].

A Comissão já abordou a questão da ameaça manifesta e atual que representam os conteúdos terroristas em linha com a **proposta legislativa** que o Presidente Juncker anunciou no seu discurso sobre o Estado da União de 2018, que propõe um quadro jurídico claro e harmonizado para prevenir a utilização abusiva dos prestadores de serviços de alojamento virtual para a difusão em linha de conteúdos terroristas[7]. As medidas propostas obrigariam as plataformas Internet a retirar os conteúdos terroristas no prazo de uma hora depois de terem recebido uma ordem de remoção emitida pelas autoridades competentes em qualquer Estado-Membro. Além disso, se uma plataforma estiver a ser utilizada de forma abusiva para a divulgação de conteúdos terroristas, tem a obrigação de adotar medidas pró-ativas para detetar esses conteúdos e impedir a sua repetição, estando previstas para o efeito regras e garantias claras. As autoridades dos Estados-Membros teriam de assegurar um serviço coercivo especializado dotado dos recursos necessários para detetar eficazmente os conteúdos terroristas e emitir decisões de remoção.

Tal permitirá dispor de um sistema rápido e eficaz, à escala da União, e estabelecerá garantias sólidas,

---

3 Ver o décimo oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz [COM(2019) 145 final de 20.3.2019].

4 https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. O Presidente francês, Emmanuel Macron, e a Primeira-Ministra neozelandesa, Jacinda Ardern, convidaram os dirigentes e as plataformas em linha a virem a Paris, em 15 de maio de 2019, para lançar esta iniciativa.

5 https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes

6 Na reunião do G20 em Osaca, em 28 e 29 de junho de 2019, os dirigentes reafirmaram a sua determinação em agir para proteger os cidadãos contra a exploração da Internet pelo terrorismo e o extremismo violento propício ao terrorismo (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf).

7 COM(2018) 640 final de 12.9.2018.

incluindo mecanismos efetivos de reclamação e a possibilidade de recurso judicial. As medidas propostas contribuirão para garantir o funcionamento harmonioso do Mercado Único Digital, aumentando simultaneamente a segurança e a confiança em linha e reforçando as garantias em matéria de liberdade de expressão e de informação.

A nível do Conselho, os Ministros da Justiça e dos Assuntos Internos aprovaram uma orientação geral sobre a proposta em dezembro de 2018. O Parlamento Europeu adotou a sua posição em primeira leitura em abril de 2019. **A Comissão exorta ambos os colegisladores a encetarem negociações interinstitucionais sobre esta iniciativa prioritária o mais rapidamente possível com o objetivo de eliminar os conteúdos terroristas em linha**, tendo em vista chegar a um rápido acordo sobre um quadro regulamentar da UE que inclua normas e garantias claras.

Paralelamente, a Comissão prossegue a cooperação com as plataformas em linha no âmbito do **Fórum Internet da UE**[8]. Tal como anunciado pelo Presidente Juncker na reunião realizada em Paris, em 15 de maio de 2019, sobre o «apelo à ação de Christchurch», a Comissão, juntamente com a Europol, começou a elaborar um **protocolo de crise da UE** que permita aos governos e às plataformas da Internet reagir rapidamente e de forma coordenada à difusão de conteúdos terroristas em linha, por exemplo, na sequência imediata de um atentado terrorista. Estes trabalhos fazem parte dos esforços desenvolvidos a nível internacional para implementar o «Apelo à ação de Christchurch». Para além de novos debates com os Estados-Membros e as empresas, e de um exercício de simulação de uma situação de emergência previsto para setembro de 2019, a Comissão organizará uma reunião ministerial do Fórum Internet da UE em 7 de outubro de 2019, com vista a aprovar o protocolo de crise da UE.

Além disso, a Comissão prossegue os seus esforços para **apoiar os Estados-Membros e os intervenientes locais na prevenção e luta contra a radicalização** no terreno em comunidades locais em toda a Europa. Para tal, são necessários esforços duráveis e de longo prazo, associando todos os intervenientes relevantes a nível local, nacional e da UE. O **comité diretor para as ações da União em matéria de prevenção e luta contra a radicalização**, criado em agosto de 2018 com o objetivo de aconselhar a Comissão sobre a forma de reforçar a resposta estratégica da UE neste domínio, realizou a sua segunda reunião em 17 de junho de 2019, a fim de explorar novas ações em domínios prioritários como a radicalização nas prisões e a luta contra as ideologias extremistas. Como os profissionais de primeira linha e no terreno estão muitas vezes mais bem colocados para identificar os sinais de alerta precoce de radicalização e as formas de os combater, a **Rede de Sensibilização para a Radicalização**[9], financiada pela UE, continua a apoiar os intervenientes da primeira linha, ligando cerca de 5 000 profissionais da sociedade civil, das escolas e da polícia, bem como os coordenadores nacionais e os decisores políticos.

A recente colaboração dos profissionais de primeira linha a nível da rede permitiu compreender melhor os desafios do extremismo de direita. Este ano, a Rede de Sensibilização para a Radicalização publicará fichas informativas para ajudar os decisores políticos e os profissionais a identificar as principais formas e manifestações do extremismo de direita e do extremismo islamista, tais como principais discursos, linguagem, formas, símbolos, tipologias e estratégias. Por último, uma vez que os

---

8 Lançado em 2015, o **Fórum Internet da UE** reúne os Ministros dos Assuntos Internos da UE, representantes do setor da Internet e outras partes interessadas que desejam colaborar no quadro de uma parceria voluntária para lutar contra a utilização abusiva da Internet por grupos terroristas e proteger os cidadãos.

9 Em 2011, a Comissão criou a **Rede de Sensibilização para a Radicalização** com o objetivo de reunir profissionais de primeira linha e do terreno. Em 2015, a Comissão reforçou essa rede através da criação do Centro de Excelência da Rede de Sensibilização para a Radicalização a fim de desenvolver serviços de orientação, de apoio e de aconselhamento mais direcionados destinados às partes interessadas nos Estados-Membros, e aumentar os conhecimentos especializados e as competências dos diferentes intervenientes. Para mais informações sobre as atividades da Rede de Sensibilização para a Radicalização, consultar: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

intervenientes locais e as **cidades** estão na primeira linha da prevenção e luta contra a radicalização, a Comissão apoia as iniciativas promovidas pelas cidades no domínio da luta contra a radicalização. No seguimento de uma conferência sobre o tema «Municípios da UE contra a radicalização», realizada em 26 de fevereiro de 2019, teve lugar em 8 de julho de 2019 a primeira reunião de um grupo-piloto composto por cerca de 20 cidades, organizada pelo Presidente da Câmara de Estrasburgo, com o objetivo de intensificar o intercâmbio de boas práticas e reforçar os esforços das cidades neste domínio.

Paralelamente, está a ser prestado apoio a países parceiros na luta contra a radicalização que pode conduzir ao terrorismo, nomeadamente nas prisões.

A fim de combater a ameaça representada pelos conteúdos terroristas em linha, a Comissão exorta o Parlamento Europeu e o Conselho:

- A encetarem negociações sobre a proposta legislativa destinada a prevenir a difusão de **conteúdos terroristas em linha**, com vista a obter rapidamente um acordo sobre um quadro regulamentar da UE que inclua normas e garantias claras.

2. Reforçar a cibersegurança

A cibersegurança continua a ser um grande desafio em matéria de segurança. A União realizou importantes progressos[10] na luta contra as ciberameaças «clássicas» direcionando a sua ação para os sistemas e dados, pondo em prática as medidas definidas na Comunicação Conjunta de setembro de 2017[11] intitulada «Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE». Trata-se, nomeadamente, do Regulamento da UE sobre cibersegurança[12] que confere um mandato permanente à Agência da União Europeia para a Cibersegurança, reforçando o seu papel e estabelecendo um quadro da UE para a certificação em matéria de cibersegurança. A Comissão também abordou os requisitos setoriais específicos, por exemplo, através da sua recomendação sobre a cibersegurança no setor da energia, adotada em 3 de abril de 2019[13]. No entanto, o aumento constante da atividade de agentes mal-intencionados no que diz respeito a uma série diversificada de alvos e vítimas significa que os esforços para combater a cibercriminalidade e reforçar a cibersegurança continuam a ser uma prioridade da ação da UE.

O Parlamento Europeu e o Conselho têm ainda de chegar a acordo sobre a iniciativa prioritária da Comissão 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**[14]. Essa proposta visa apoiar as capacidades tecnológicas e industriais em matéria de cibersegurança e aumentar a competitividade do setor da cibersegurança da União. Os dois colegisladores adotaram os respetivos mandatos de negociação em março de 2019. Dado que não foi possível concluir as negociações interinstitucionais antes do termo da anterior legislatura do Parlamento Europeu, este último adotou formalmente a sua posição em primeira leitura. Entretanto, prosseguem os debates entre os Estados-Membros a nível do Conselho, com especial destaque para a interação entre, por um lado, a

10 Para mais informações, consultar a brochura «Reforçar a cibersegurança na União Europeia: resiliência, dissuasão, defesa»: https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

11 JOIN(2017) 450 final de 13.9.2017.

12 O Regulamento da UE sobre a cibersegurança [Regulamento (UE) 2019/881 de 17 de abril de 2019] introduz, pela primeira vez, regras a nível da UE para a certificação da cibersegurança de produtos, processos e serviços. Além disso, confere um novo mandato permanente à Agência da União Europeia para a Cibersegurança e atribui-lhe mais recursos para que esta possa cumprir os seus objetivos. Para mais informações sobre o convite à apresentação de propostas, consultar: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

13 C(2019) 2400 final de 3.4.2019 e SWD(2019) 1240 final de 3.4.2019.

14 COM(2018) 630 final de 12.9.2018.

proposta de regulamento que estabelece o Centro e Rede de Competências em Cibersegurança e, por outro, os programas «Horizonte Europa» e «Europa Digital». **A Comissão exorta os dois colegisladores a retomarem e concluírem rapidamente as negociações interinstitucionais sobre esta iniciativa prioritária visando reforçar a cibersegurança.**

Paralelamente, a Comissão continua a **apoiar a investigação e a inovação** relacionadas com a cibersegurança, disponibilizando 135 milhões de EUR a título do atual quadro financeiro plurianual para projetos em domínios como a cibersegurança em infraestruturas críticas, a segurança inteligente e a gestão da privacidade, bem como ferramentas especificamente destinadas aos cidadãos e às pequenas e médias empresas[15]. Em julho de 2019, a Comissão publicou um novo convite à apresentação de propostas no âmbito do Mecanismo Interligar a Europa, disponibilizando 10 milhões de EUR para o financiamento da UE aos principais intervenientes identificados pela Diretiva relativa à segurança das redes e da informação (Diretiva SRI)[16], nomeadamente as equipas europeias de resposta a incidentes no domínio da segurança informática, os operadores de serviços essenciais (por exemplo, bancos, hospitais, prestadores de serviços de utilidade pública, caminhos de ferro, companhias aéreas, fornecedores de nomes de domínio) e várias autoridades públicas. Pela primeira vez, as autoridades europeias de certificação de cibersegurança são também elegíveis para se candidatarem a este programa a fim de lhes permitir aplicar o Regulamento Cibersegurança da UE.

Em 17 de maio de 2019, o Conselho aprovou um **regime de sanções** que permite à UE impor medidas restritivas direcionadas para dissuadir e responder a ciberataques que ameacem a UE e os seus Estados-Membros do exterior. O novo regime de sanções faz parte do **conjunto de instrumentos de ciberdiplomacia da UE**[17], um quadro para uma resposta diplomática conjunta da União às ciberatividades maliciosas[18] que permite à UE tirar pleno partido das medidas abrangidas pela Política Externa e de Segurança Comum a fim de desencorajar e responder a tais atos.

Para além das ciberameaças que visam sistemas e dados, a UE está igualmente a tomar medidas para fazer face aos desafios complexos e multifacetados que representam as **ameaças híbridas**[19]. O Conselho Europeu, nas suas conclusões de 21 de junho de 2019[20], sublinhou que *«A UE tem de assegurar uma resposta coordenada às ameaças híbridas e às ciberameaças e de reforçar a sua cooperação com os intervenientes internacionais relevantes»*. A Comissão congratula-se com o facto de a luta contra as ameaças híbridas ser também uma prioridade da Presidência finlandesa do Conselho, e de ter sido realizado um debate de orientação sobre este tipo de ameaças, com base em cenários, na reunião informal dos Ministros da Justiça e dos Assuntos Internos, de 18 e 19 de julho de 2019, em Helsínquia. Realizaram-se debates semelhantes, com base em cenários, sobre ameaças híbridas entre os diretores responsáveis pela política de defesa da UE, em 7 e 8 de julho de 2019, e entre os diretores políticos da UE, em 9 e 10 de julho de 2019, cujos resultados serão comunicados aos Ministros dos Negócios Estrangeiros e da Defesa numa sessão informal conjunta de 29 e 30 de agosto de 2019.

---

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

16 Diretiva (UE) 2016/1148 de 6.7.2016.

17 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/pt/pdf

18 Trata-se nomeadamente dos ciberataques, bem como das tentativas de ciberataques com um efeito potencialmente significativo, envolvendo, por exemplo, o acesso aos sistemas de informação ou a interceção de dados através de infraestruturas digitais, como as redes 5G (ver também a secção III sobre o reforço da segurança das infraestruturas digitais).

19 Ver o relatório sobre a aplicação do quadro comum de 2016 em matéria de luta contra as ameaças híbridas e a Comunicação Conjunta de 2018 sobre o reforço da resiliência e das capacidades para fazer face às ameaças híbridas [SWD (2019) 200 final de 28.5.2019]. Ver também a proposta legislativa de setembro de 2016 de um regulamento que cria um regime da União de controlo das exportações, transferências, corretagem, assistência técnica e trânsito de produtos de dupla utilização (reformulação) [COM (2016) 616 final de 28.9.2016].

20 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-pt.pdf

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 a um **Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e à Rede de Centros Nacionais de Coordenação**.

3. Melhorar o acesso das autoridades de aplicação da lei às provas eletrónicas

A UE aprovou medidas suplementares para privar os terroristas e os criminosos de meios de ação, dificultando-lhes o acesso aos precursores de explosivos[21], ao financiamento das suas atividades[22] e a viagens sem serem detetados[23].

As negociações sobre as propostas da Comissão, de abril de 2018, destinadas a melhorar o **acesso às provas eletrónicas** pelas autoridades de aplicação da lei deveriam ser concluídas o mais rapidamente possível, pois mais de metade do conjunto das investigações penais implicam atualmente um pedido transnacional de acesso a provas eletrónicas[24]. O Conselho adotou a sua posição de negociação sobre uma proposta de regulamento[25] visando melhorar o acesso transnacional às provas eletrónicas em investigações criminais e uma proposta de diretiva[26] que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal. Dada a importância crucial de um acesso eficaz a elementos de prova eletrónicos tendo em vista a investigação e repressão de crimes transnacionais como o terrorismo ou a cibercriminalidade, a Comissão exorta o Parlamento Europeu a avançar nos trabalhos sobre esta proposta, para que os colegisladores possam proceder à sua rápida adoção.

Paralelamente, a Comissão está a trabalhar no sentido de melhorar e assegurar as garantias necessárias em matéria de **intercâmbio internacional de provas eletrónicas** no quadro das negociações em curso de um Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime do Conselho da Europa, bem como das negociações com os Estados Unidos, em consonância com os mandatos de negociação conferidos pelo Conselho na reunião do Conselho Justiça e Assuntos Internos de 6 e 7 de junho de 2019[27]. A Comissão participou na última ronda de negociações sobre um Segundo Protocolo Adicional à Convenção de Budapeste sobre o Cibercrime do Conselho da Europa de 9 a 11 de julho de 2019. A Comissão e as autoridades dos Estados Unidos estão atualmente a preparar-se a nível técnico para o lançamento formal das negociações de um acordo entre a UE e os Estados Unidos sobre o acesso transnacional às provas eletrónicas.

---

21 Regulamento (UE) 2019/1148, de 20 de junho de 2019, sobre a comercialização e utilização de precursores de explosivos.

22 Diretiva (UE) 2019/1153, 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.

23 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.

24 As provas eletrónicas são necessárias em cerca de 85 % das investigações penais e, em dois terços destas investigações, é necessário solicitar provas aos prestadores de serviços em linha estabelecidos noutra jurisdição. Ver a avaliação de impacto que acompanha a proposta legislativa [SWD(2018) 118 final de 17.4.2018].

25 COM(2018) 225 final de 17.4.2018. O Conselho adotou o seu mandato de negociação sobre a proposta de regulamento no Conselho Justiça e Assuntos Internos de 7 de dezembro de 2018.

26 COM(2018) 226 final de 17.4.2018. O Conselho adotou a sua posição de negociação sobre a proposta de diretiva no Conselho Justiça e Assuntos Internos de 8 de março de 2019.

27 https://www.consilium.europa.eu/pt/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

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

- A adotar o seu mandato de negociação sobre as propostas legislativas relativas às **provas eletrónicas** com vista a encetar, sem demora, discussões em trílogo com o Conselho. *(Prioridade da Declaração Conjunta)*

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

Na sequência da adoção de regras sobre a **interoperabilidade dos sistemas de informação**[28], que colmatarão lacunas de informação e ângulos mortos, ajudando a detetar identidades múltiplas e combatendo a fraude de identidade, a Comissão lançou rapidamente uma série de iniciativas para apoiar os Estados-Membros tendo em vista a sua aplicação, nomeadamente com financiamento quando necessário, bem como com seminários destinados a facilitar o intercâmbio de conhecimentos especializados e boas práticas. A cooperação estreita entre as agências da UE, o conjunto dos Estados-Membros e os países associados de Schengen será crucial para alcançar o objetivo ambicioso da plena interoperabilidade dos sistemas de informação da UE para fins de gestão da segurança, das fronteiras e da migração até 2020.

Tal objetivo implica igualmente a implementação rápida e completa da legislação que foi recentemente adotada tendo em vista estabelecer novos sistemas de informação, ou seja, o Sistema de Entrada/Saída da UE[29] e o Sistema Europeu de Informação e Autorização de Viagem[30], bem como o reforço do Sistema de Informação de Schengen[31] e a extensão do Sistema Europeu de Informação sobre Registos Criminais[32] aos nacionais de países terceiros. A nova arquitetura destinada a estabelecer sistemas de informação mais sólidos e mais inteligentes para a gestão da segurança, das fronteiras e da migração só terá efeitos concretos no terreno se todos os elementos forem plenamente implementados a nível da União e por cada Estado-Membro, de acordo com o calendário acordado.

Paralelamente, é necessário que os colegisladores adotem novas medidas para completar os trabalhos iniciados sobre sistemas de informação mais sólidos e mais inteligentes para fins de gestão da segurança, das fronteiras e da migração.
No âmbito da implementação técnica do **Sistema Europeu de Informação e Autorização de Viagem**, a Comissão apresentou, em 7 de janeiro de 2019, duas propostas visando introduzir no regulamento correspondente as alterações técnicas necessárias ao estabelecimento do sistema na sua integralidade[33]. A Comissão exorta os colegisladores a avançarem nos seus trabalhos sobre essas alterações técnicas a fim de alcançar um acordo o mais rapidamente possível e permitir assim a implementação rápida e atempada do Sistema Europeu de Informação e Autorização de Viagem de modo a torná-lo operacional no início de 2021.

Em maio de 2018, a Comissão apresentou uma proposta destinada a **reforçar o atual Sistema de Informação sobre Vistos**[34], prevendo um controlo mais aprofundado dos antecedentes dos requerentes de visto e colmatando as lacunas de informação através de um melhor intercâmbio de dados entre os Estados-Membros.
O Conselho adotou o seu mandato de negociação em 19 de dezembro de 2018 e, em 13 de março de 2019, o Parlamento Europeu aprovou o seu relatório sobre a proposta em sessão plenária, concluindo

28 Regulamento (UE) 2019/817 de 20.5.2019 e Regulamento (UE) 2019/818 de 20.5.2019.
29 Regulamento (UE) 2017/2226 de 30.11.2017.
30 Regulamento (UE) 2018/1240 de 12.9.2018 e Regulamento (UE) 2018/1241 de 12.9.2018.
31 Regulamento (UE) 2018/1860 de 28.11.2018, Regulamento (UE) 2018/1861 de 28.11.2018, Regulamento (UE) 2018/1862 de 28.11.2018.
32 Regulamento (UE) 2019/816 de 17.4.2019.
33 COM(2019) 3 final e COM(2019) 4 final de 7.1.2019.
34 COM(2018) 302 final de 16.5.2018.

assim a primeira leitura dessa proposta. A Comissão exorta os colegisladores a iniciarem rapidamente as negociações após a recente constituição da legislatura do Parlamento Europeu.

Em maio de 2016, a Comissão propôs o alargamento do âmbito de aplicação do **Eurodac**[35], de modo a incluir não só a identificação dos requerentes de asilo, mas também a dos nacionais de países terceiros em situação irregular ou das pessoas que entram de forma irregular na UE. Em consonância com as conclusões do Conselho Europeu de dezembro de 2018[36] e com a Comunicação da Comissão, de 6 de março de 2019, sobre os progressos realizados na aplicação da Agenda Europeia da Migração[37], a Comissão exorta os colegisladores a adotarem a referida proposta. É necessário adotar esta proposta legislativa a fim de integrar o Eurodac na futura arquitetura dos sistemas de informação interoperáveis da UE, que incluirá desse modo os dados cruciais dos nacionais de países terceiros em situação irregular e das pessoas que entraram de forma irregular na União.

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

- A adotarem a proposta legislativa relativa ao **Eurodac** *(Prioridade da Declaração Conjunta)*;
- A avançarem nos trabalhos com vista a alcançar rapidamente um acordo sobre as alterações técnicas propostas que são necessárias para o estabelecimento do **Sistema Europeu de Informação e Autorização de Viagem.**

III. REFORÇAR A SEGURANÇA DAS INFRAESTRUTURAS DIGITAIS

A resiliência das nossas infraestruturas digitais é fundamental para os governos, as empresas, a segurança dos nossos dados pessoais e o funcionamento das nossas instituições democráticas. **As redes de quinta geração (5G)** que serão implantadas nos próximos anos constituirão a espinha dorsal digital das nossas sociedades e economias, ligando milhares de cidadãos, objetos e sistemas, incluindo em setores críticos como a energia, os transportes, os bancos e a saúde, bem como sistemas de controlo industrial que transmitirão informações sensíveis e darão suporte a dispositivos de segurança.

A tecnologia 5G, cujas receitas a nível mundial deverão atingir o equivalente a 225 mil milhões de EUR em 2025, é uma ferramenta essencial para assegurar a competitividade da Europa no mercado mundial e **a segurança das redes de 5G é crucial para garantir a autonomia estratégica da União**. A garantia de um elevado nível de cibersegurança exige medidas concertadas, tanto a nível nacional como europeu, uma vez que qualquer vulnerabilidade nas redes 5G num Estado-Membro afetaria a União no seu conjunto.

Na sequência do apoio manifestado pelos Chefes de Estado ou de Governo no Conselho Europeu de 22 de março[38], a Comissão apresentou, em 26 de março de 2019, uma **recomendação sobre a cibersegurança das redes 5G**[39], que expõe as medidas destinadas a avaliar os riscos em matéria de cibersegurança das redes 5G e a reforçar as medidas preventivas. As recomendações baseiam-se numa avaliação coordenada dos riscos e em medidas de gestão dos riscos a nível da UE, num quadro eficaz para a cooperação e o intercâmbio de informações, e o conhecimento comum da situação das redes de comunicação de importância crítica na UE.

Como **primeira fase** do processo lançado pela recomendação, em 15 de julho de 2019 todos os Estados-Membros tinham concluído a **avaliação nacional de riscos** e apresentaram as suas conclusões

35 COM(2016) 272 final de 4.5.2016.
36 https://www.consilium.europa.eu/pt/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/
37 COM(2019) 126 final de 6.3.2019.
38 https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/pt/pdf
39 C(2019) 2335 final de 26.3.2019.

à Comissão e à Agência da UE para a Cibersegurança ou anunciaram que o fariam em breve. As avaliações nacionais de riscos seguiram um conjunto de orientações e um modelo comum de relatório sobre as conclusões acordados pelos Estados-Membros e pela Comissão, a fim de promover a coerência e facilitar o intercâmbio de informações sobre os resultados nacionais a nível da UE. Os parâmetros avaliados em todos os Estados-Membros incluíram:

- As principais ameaças e os principais agentes maliciosos que afetam as redes 5G;
- O grau de sensibilidade dos componentes, funções e outros recursos da rede 5G; e
- Os diversos tipos de vulnerabilidades, técnicas e outras, como aquelas que poderiam decorrer da cadeia de fornecimento 5G.

Além disso, os trabalhos relativos às avaliações nacionais de riscos envolveram uma série de intervenientes responsáveis nos Estados-Membros, tais como, em função das responsabilidades nacionais, as autoridades em matéria de cibersegurança e de telecomunicações, bem como os serviços de segurança e de informações, que reforçaram a sua cooperação e coordenação. Paralelamente, e tendo em conta os calendários nacionais de implantação da tecnologia 5G, alguns Estados-Membros já tomaram medidas para reforçar os requisitos de segurança aplicáveis neste domínio, enquanto vários outros manifestaram a sua intenção de examinar novas medidas num futuro próximo.

Com base nos resultados da avaliação de riscos a nível nacional, as autoridades de cibersegurança dos Estados-Membros que integram o grupo de cooperação para as redes e os sistemas de informação[40], irão preparar uma **análise conjunta dos riscos a nível da UE** até 1 de outubro de 2019, que constituirá a segunda fase do processo iniciado no âmbito da recomendação. Tendo em conta esses resultados, e como terceira fase, o grupo de cooperação elaborará, até 31 de dezembro de 2019, um **conjunto de instrumentos comuns de medidas de atenuação a nível da União** para fazer face aos riscos identificados. A Comissão e a Agência da UE para a Cibersegurança continuarão a apoiar a aplicação da recomendação.

Os trabalhos a nível do grupo de cooperação para a segurança das redes e da informação são apoiados por várias outras instâncias. O organismo dos reguladores europeus de comunicações eletrónicas prepara atualmente um inquérito sobre todas as medidas de segurança existentes potencialmente relevantes para as redes 5G. Um novo grupo de peritos, especializado a nível da Agência da UE para a Cibersegurança, lançou os trabalhos para examinar o inventário das ameaças próprias às redes 5G. Além disso, na sequência da entrada em vigor do Regulamento sobre a cibersegurança, em 27 de junho de 2019, a Comissão e a Agência da UE para a Cibersegurança tomarão todas as medidas necessárias para estabelecer o quadro de certificação a nível da UE. Em junho de 2019, os Estados-Membros reuniram-se igualmente a nível do Comité das normas para debater a cibersegurança e a normalização em resposta à recomendação, que convida a examinar os futuros desafios para a normalização da cibersegurança, incluindo as redes 5G, e as iniciativas políticas adequadas a nível da UE.

Por último, a segurança das redes 5G reveste uma importância estratégica para a União. O investimento estrangeiro em setores estratégicos, a aquisição de ativos, tecnologias e infraestruturas de importância crítica na União e o fornecimento de equipamentos essenciais podem também representar riscos para a segurança da União.

[40] O referido grupo de cooperação é instituído por força da Diretiva (UE) 2016/1148, de 6 de julho de 2016, relativa à segurança das redes e da informação. Tal como previsto na recomendação, foi criada uma vertente de trabalho específica, dirigida por vários Estados-Membros, no âmbito do grupo de cooperação para a segurança das redes e da informação. O grupo já se reuniu três vezes, em abril, maio e julho de 2019, para partilhar informações sobre as abordagens nacionais e debater a forma de facilitar a preparação da avaliação coordenada dos riscos a nível da UE.

O novo **regime da UE de análise dos investimentos diretos estrangeiros**[41] entrou em vigor em 10 de abril de 2019. Nos próximos 18 meses, a Comissão e os Estados-Membros adotarão as medidas necessárias para garantir que a UE possa aplicar integralmente o Regulamento relativo à análise dos investimentos a partir de 11 de outubro de 2020.

IV. LUTA CONTRA O BRANQUEAMENTO DE CAPITAIS

A possibilidade de movimentar fundos entre contas bancárias em poucas horas permite aos criminosos e terroristas preparar mais facilmente atos terroristas ou branquear produtos do crime em diferentes Estados-Membros. Para fazer face a este problema, a União elaborou um sólido **quadro regulamentar para combater o branqueamento de capitais e o financiamento do terrorismo**, em conformidade com as normas internacionais adotadas pelo Grupo de Ação Financeira.

Dada a necessidade de acompanhar a evolução das tendências, os progressos tecnológicos e a capacidade de adaptação dos criminosos quando se trata de explorar lacunas ou deficiências do sistema, a Comissão adotou, em 24 de julho de 2019, um **pacote de quatro relatórios** que analisam os riscos e vulnerabilidades atuais relacionados com o branqueamento de capitais e avaliam a forma como o quadro é aplicado pelos intervenientes relevantes, tanto no setor privado como no setor público[42].

O pacote inclui uma **avaliação da interligação potencial dos registos nacionais centralizados das contas bancárias e dos sistemas de recuperação de dados** na UE. Estes sistemas nacionais centralizados permitem a identificação de qualquer pessoa singular ou coletiva titular ou gestor de contas de pagamento, contas bancárias e cofres-fortes, informações que são frequentemente cruciais para as autoridades competentes lutarem contra o branqueamento de capitais e o financiamento do terrorismo. A 5.ª Diretiva Branqueamento de Capitais[43] exige que os Estados-Membros estabeleçam esses sistemas nacionais centralizados e concedam às suas unidades nacionais de informação financeira acesso direto aos mesmos. As disposições recentemente adotadas visando facilitar a utilização de informações financeiras com o objetivo de combater a criminalidade grave[44] possibilitam às autoridades de aplicação da lei designadas e aos serviços de recuperação de bens um acesso direto aos respetivos registos nacionais centralizados de contas bancárias. Nessa base, e tal como exigido pela Diretiva Branqueamento de Capitais, o relatório avalia várias soluções informáticas a nível da UE, já operacionais ou em fase de desenvolvimento, que podem servir de modelo para uma possível interligação dos sistemas nacionais centralizados. Dado que uma futura interligação a nível da UE dos mecanismos centralizados aceleraria o acesso à informação financeira e facilitaria a cooperação transnacional das autoridades competentes, a Comissão tenciona voltar a consultar as partes interessadas, os governos, bem como as unidades de informação financeira, as autoridades de

41 Regulamento (UE) 2019/452, de 19 de março de 2019, que estabelece um regime de análise dos investimentos diretos estrangeiros na União. O novo quadro cria um mecanismo de cooperação com base no qual os Estados-Membros e a Comissão poderão trocar informações e exprimir as suas preocupações relacionadas com investimentos específicos. Também permite que a Comissão se pronuncie sempre que um investimento ameace a segurança ou a ordem pública de mais de um Estado-Membro, ou quando um investimento for suscetível de comprometer um projeto ou programa de interesse coletivo para a UE. O Estado-Membro onde o investimento é realizado tem a última palavra sobre a forma de tratar esse investimento.

42 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 final de 24.7.2019]; relatório sobre a interligação dos mecanismos automatizados centralizados nacionais (registos centrais ou sistemas eletrónicos centrais de extração de dados) dos Estados-Membros no respeitante a contas bancárias [COM (2019) 372 final de 24.7.2019]; relatório sobre a avaliação dos alegados casos de branqueamento de capitais que envolvem instituições de crédito da UE [COM (2019) 373 final de 24.7.2019]; relatório de avaliação do quadro de cooperação entre as unidades de informação financeira [COM (2019) 371 final de 24.7.2019].

43 Diretiva (UE) 2015/849 de 20.5.2015.

44 Diretiva (UE) 2019/1153 de 20.6.2019.

aplicação da lei e os serviços de recuperação de bens, enquanto potenciais utilizadores finais de um possível sistema de interligação.

No âmbito da reflexão da Comissão sobre os trabalhos das unidades de informação financeira, um relatório de avaliação da **cooperação entre as unidades de informação financeira** examina tanto a cooperação a nível da União como com os países terceiros[45]. Identifica algumas lacunas que poderão subsistir até que as missões e as obrigações de cooperação transnacional das unidades de informação financeira não estejam mais claramente definidas no quadro jurídico da UE em matéria de luta contra o branqueamento de capitais e o financiamento do terrorismo. A avaliação revela igualmente a necessidade de um mecanismo mais sólido para coordenar e apoiar a cooperação transnacional e a análise.

Para além dos trabalhos em curso no sentido de lutar contra o branqueamento de capitais e o financiamento do terrorismo, e também em resposta a um apelo do Parlamento Europeu[46], a Comissão continuará a avaliar a necessidade, a viabilidade técnica e a proporcionalidade de medidas adicionais para detetar o financiamento do terrorismo a nível da UE[47].

V. EXECUÇÃO DE OUTROS DOSSIÊS PRIORITÁRIOS EM MATÉRIA DE SEGURANÇA

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

A obtenção de um acordo sobre medidas no âmbito da União da Segurança não constitui a conclusão do processo; é fundamental assegurar posteriormente a sua aplicação rápida e completa pelos Estados-Membros de modo a que possam produzir plenamente os seus efeitos. Com esse objetivo, a Comissão apoia ativamente os Estados-Membros, nomeadamente concedendo-lhes financiamento e facilitando o intercâmbio das melhores práticas.
Porém, e sempre que necessário, a Comissão fará 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**[48] terminou em 25 de maio de 2018. Até à data, 25 Estados-Membros notificaram a plena transposição à Comissão[49]. A transposição integral ainda não foi efetuada em dois Estados-Membros apesar dos procedimentos de infração iniciados em 19 de julho de 2018[50]. 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 melhores práticas.

O prazo para a transposição da **Diretiva relativa à luta contra o terrorismo**[51] expirou em 8 de setembro de 2018. Até à data, 22 Estados-Membros notificaram a plena transposição à Comissão. Três

---

45 Esta avaliação é exigida pelo artigo 65.º, n.º 2, da 5.ª Diretiva (UE) 2018/843 relativa ao branqueamento de capitais (30.5.2018).

46 No seu relatório final, adotado em dezembro de 2018, a Comissão Especial sobre o Terrorismo do Parlamento Europeu apelou à criação de um sistema europeu de deteção do financiamento do terrorismo direcionado para as transações efetuadas por pessoas com ligações ao terrorismo e seu financiamento no espaço único de pagamentos em euros.

47 Ver o décimo oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz [COM(2019) 145 final de 20.3.2019].

48 Diretiva (UE) 2016/681 de 27.4.2016.

49 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.

50 A Eslovénia notificou a transposição parcial. A Espanha não notificou qualquer medida de transposição (situação em 24 de julho de 2019).

51 Diretiva (UE) 2017/541 de 15.3.2017.

Estados-Membros ainda não comunicaram a adoção de legislação nacional que transpõe integralmente a diretiva, apesar dos procedimentos de infração iniciados em 22 de novembro de 2018[52].

O prazo para a transposição da **Diretiva relativa ao controlo da aquisição e da detenção de armas**[53] expirou em 14 de setembro de 2018. Até à data, oito Estados-Membros notificaram a plena transposição à Comissão. Vinte Estados-Membros ainda não comunicaram a adoção das medidas nacionais que transpõem integralmente a diretiva, apesar dos procedimentos de infração iniciados em 22 de novembro de 2018[54].

No que diz respeito à transposição para o direito nacional da **Diretiva sobre a proteção de dados na aplicação da lei**[55], o prazo de transposição terminou em 6 de maio de 2018. Até à data, 20 Estados-Membros notificaram a plena transposição à Comissão[56]. Sete Estados-Membros ainda não comunicaram a adoção das medidas nacionais que transpõem integralmente a diretiva, apesar dos procedimentos de infração iniciados pela Comissão em 19 de julho de 2018[57].

Os Estados-Membros deveriam ter transposto até 9 de maio de 2018 a **Diretiva relativa à segurança das redes e da informação**[58] para a legislação nacional. Até à data, 26 Estados-Membros notificaram a transposição integral à Comissão e dois Estados-Membros transpuseram parcialmente a diretiva[59]. Além disso, em conformidade com a diretiva, os Estados-Membros eram obrigados a identificar os operadores de serviços essenciais até 9 de novembro de 2018. Até 9 de maio de 2019, a Comissão devia apresentar um relatório ao Parlamento Europeu e ao Conselho com a avaliação da coerência das abordagens adotadas pelos Estados-Membros na identificação dos operadores de serviços essenciais identificados no seu território. No entanto, dado que alguns Estados-Membros ainda tinham de apresentar informações completas sobre o processo de identificação, a Comissão teve de adiar o seu relatório.

A Comissão avalia atualmente a transposição da **4.ª Diretiva Branqueamento de Capitais**[60] e verifica se as normas estão a ser corretamente aplicadas pelos Estados-Membros. A Comissão iniciou procedimentos de infração contra 24 Estados-Membros, uma vez que considerou que as comunicações que lhe foram transmitidas não representavam uma transposição integral da diretiva[61].

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:

52 A Polónia notificou a transposição parcial. A Grécia e o Luxemburgo não notificaram qualquer medida de transposição (situação em 24 de julho de 2019).

53 Diretiva (UE) 2017/853 de 17.5.2017.

54 A Bélgica, a Chéquia, a Estónia, a Lituânia, a Polónia, Portugal, a Suécia e o Reino Unido notificaram a transposição parcial. A Alemanha, a Irlanda, a Grécia, a Espanha, Chipre, o Luxemburgo, a Hungria, os Países Baixos, a Roménia, a Eslovénia, a Eslováquia e a Finlândia não notificaram qualquer medida de transposição (situação em 24 de julho de 2019).

55 Diretiva (UE) 2016/680 de 27.4.2016.

56 Vinte Estados-Membros concluíram a transposição (situação em 24 de julho de 2019).

57 A Letónia, Portugal, a Eslovénia e a Finlândia notificaram a transposição parcial. A Grécia e Espanha não notificaram qualquer medida de transposição. Embora a Alemanha tenha notificado a transposição completa, a Comissão considera que esta transposição não está completa (ponto da situação em 24 de julho de 2019).

58 Diretiva (UE) 2016/1148 de 27.4.2016.

59 A Bélgica e a Hungria transpuseram parcialmente a diretiva (situação em 24 de julho de 2019).

60 Diretiva (UE) 2015/849 de 20.5.2015.

61 Bélgica, Bulgária, Chéquia, Dinamarca, Alemanha, Estónia, Irlanda, Espanha, França, Itália, Chipre, Letónia, Lituânia, Hungria, Países Baixos, Áustria, Polónia, Portugal, Roménia, Eslovénia, Eslováquia, Finlândia, Suécia e Reino Unido (situação em 11 de março de 2019).

- A **Diretiva Registos de Identificação dos Passageiros**, relativamente à qual um Estado-Membro ainda deve notificar a transposição para o direito nacional e outro Estado-Membro deve completar a notificação da transposição[62];
- 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[63];
- A **Diretiva Controlo da Aquisição e da Detenção de Armas**, relativamente à qual 12 Estados-Membros ainda devem notificar a transposição para o direito nacional e oito devem completar a notificação da transposição[64];
- A **Diretiva Proteção de Dados na Aplicação da Lei**, relativamente à qual dois Estados-Membros devem ainda notificar a transposição para o direito nacional e cinco Estados-Membros devem completar a notificação da transposição[65];
- A **Diretiva Segurança das Redes e da Informação**, relativamente à qual dois Estados-Membros devem ainda completar a notificação da transposição[66]; e
- A **4.ª Diretiva Branqueamento de Capitais**, relativamente à qual 24 Estados-Membros devem ainda completar a notificação da transposição[67].

2. Lutar contra a desinformação e proteger as eleições contra outras ameaças possibilitadas pelo ciberespaço

Proteger os processos democráticos e as instituições contra a desinformação e as ingerências conexas constitui um importante desafio para as sociedades de todo o mundo. Para resolver este problema, a UE criou um **quadro sólido para uma ação coordenada contra a desinformação**, no pleno respeito dos valores europeus e dos direitos fundamentais[68]. Tal como estabelecido na Comunicação Conjunta, de 14 de junho de 2019, sobre a execução do Plano de Ação contra a Desinformação[69], os trabalhos sobre várias vertentes complementares contribuíram para reduzir o espaço de influência da desinformação e preservar a integridade das eleições para o Parlamento Europeu.

O Conselho Europeu, nas suas conclusões de 21 de junho de 2019[70], saudou a intenção da Comissão de realizar uma avaliação aprofundada da execução dos compromissos assumidos pelas plataformas

62 A Eslovénia notificou a transposição parcial. A Espanha não notificou qualquer medida de transposição (situação em 24 de julho de 2019).

63 A Polónia notificou a transposição parcial. A Grécia e o Luxemburgo não notificaram qualquer medida de transposição (situação em 24 de julho de 2019).

64 A Bélgica, a Chéquia, a Estónia, a Lituânia, a Polónia, Portugal, a Suécia e o Reino Unido notificaram a transposição parcial. A Alemanha, a Irlanda, a Grécia, a Espanha, Chipre, o Luxemburgo, a Hungria, os Países Baixos, a Roménia, a Eslovénia, a Eslováquia e a Finlândia não notificaram qualquer medida de transposição (situação em 24 de julho de 2019).

65 A Letónia, Portugal, a Eslovénia e a Finlândia notificaram a transposição parcial. A Grécia e Espanha não notificaram qualquer medida de transposição. Embora a Alemanha tenha notificado a transposição completa, a Comissão considera que esta transposição não está completa (ponto da situação em 24 de julho de 2019).

66 A Bélgica e a Hungria transpuseram parcialmente a diretiva (situação em 24 de julho de 2019).

67 Bélgica, Bulgária, Chéquia, Dinamarca, Alemanha, Estónia, Irlanda, Espanha, França, Itália, Chipre, Letónia, Lituânia, Hungria, Países Baixos, Áustria, Polónia, Portugal, Roménia, Eslovénia, Eslováquia, Finlândia, Suécia e Reino Unido (situação em 24 de julho de 2019).

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

69 JOIN (2019) 12 final de 14.6.2019.

70 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-pt.pdf O apelo do Conselho Europeu tem por base os contributos da Presidência romena do Conselho, bem como da Comissão e da Alta Representante para os Negócios Estrangeiros e a Política de Segurança sobre os ensinamentos obtidos em matéria de desinformação e para garantir eleições livres e justas, incluindo a Comunicação Conjunta sobre a execução do Plano de Ação contra a Desinformação.

em linha e outros signatários no âmbito do **Código de Conduta sobre Desinformação**[71] e convidou a Comissão e a Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança a avaliar de forma contínua o *«caráter evolutivo das ameaças e o risco crescente de interferências mal-intencionadas e de manipulação em linha, associados ao desenvolvimento da inteligência artificial e das técnicas de recolha de dados»*, e a responder-lhes adequadamente.

A Comissão e a Alta Representante farão avançar os seus trabalhos neste domínio, em conformidade com as conclusões do Conselho Europeu. Em março de 2019, a Comissão e a Alta Representante criaram um **sistema de alerta rápido** entre as instituições da UE e os Estados-Membros para facilitar a partilha de pontos de vista relacionados com as campanhas de desinformação e coordenar as respostas. A primeira reunião dos pontos de contacto dos Estados-Membros na sequência das eleições para o Parlamento Europeu teve lugar em Taline, em 3 e 4 de junho de 2019. A fim de reforçar o sistema de alerta rápido, a Alta Representante e a Comissão, em estreita cooperação com os Estados-Membros, analisarão o funcionamento desse sistema no outono de 2019. Elaborarão igualmente uma metodologia comum para analisar e expor campanhas de desinformação, bem como para estabelecer parcerias reforçadas com parceiros internacionais como o G7 e a NATO.

Os trabalhos prosseguem também a nível da **rede europeia de cooperação para as eleições**[72], que realizou uma primeira reunião em 7 de junho de 2019, a fim de fazer o balanço das eleições para o Parlamento Europeu. Estas reflexões e o contributo das autoridades nacionais competentes, dos partidos políticos e das plataformas em linha contribuirão para o relatório abrangente da Comissão sobre as eleições para o Parlamento Europeu que será adotado em outubro de 2019. Os Estados-Membros utilizaram essa rede para outras eleições para além das do Parlamento Europeu, o que evidencia a sua utilidade geral para garantir a integridade da democracia na UE.

A Comissão continuará igualmente a acompanhar e a promover a execução dos compromissos assumidos pelas plataformas no âmbito do **Código de Conduta sobre Desinformação**. Os relatórios apresentados pelo Google, Twitter e Facebook no quadro do Código de Conduta revelam que todas as plataformas tomaram medidas antes das eleições para o Parlamento Europeu inserindo etiquetas nas publicidades de natureza política e permitindo a sua consulta pelo público através de pesquisas nas bibliotecas de anúncios. Paralelamente, há margem para melhorias, tal como identificadas pelo Grupo de reguladores europeus dos serviços de comunicação social audiovisual[73]. Continua a verificar-se, nomeadamente, um acesso insuficiente aos dados brutos pormenorizados necessários a uma monitorização completa. Por último, as plataformas devem permitir à comunidade científica um verdadeiro acesso aos dados, no respeito das regras de proteção de dados pessoais. Ainda este ano, a

---

71 O Código de Conduta foi assinado, em outubro de 2018, pelas plataformas em linha Facebook, Google e Twitter, Mozilla, bem como pelos anunciantes e o setor da publicidade e estabelece normas de autorregulação para lutar contra a desinformação. Visa alcançar os objetivos estabelecidos na Comunicação da Comissão de abril de 2018 intitulada «Combater a desinformação em linha» [COM/2018/236 final de 26.4.2018], definindo uma vasta gama de compromissos, que consistem em aumentar a transparência nas campanhas eleitorais, encerrar contas falsas e desmonetizar os transmissores de desinformação.

72 A rede europeia de cooperação para as eleições reúne os pontos de contacto das redes nacionais de cooperação eleitoral das autoridades competentes em matéria eleitoral e as autoridades responsáveis pelo controlo e aplicação das regras relativas às atividades em linha relevantes para o contexto eleitoral. A rede europeia de cooperação para as eleições serve para alertar sobre ameaças, trocar boas práticas entre redes nacionais, debater soluções comuns para os desafios identificados e incentivar projetos e exercícios comuns entre as redes nacionais.

73 O Grupo de reguladores europeus dos serviços de comunicação social audiovisual reúne responsáveis ou representantes de alto nível das entidades reguladoras nacionais independentes no domínio dos serviços audiovisuais, a fim de aconselhar a Comissão sobre a aplicação da Diretiva Serviços de Comunicação Social Audiovisual (Diretiva 2010/13/UE de 10.3.2010). Na sua última reunião de 20 e 21 de junho de 2019, em Bratislava, o referido grupo apresentou os resultados do trabalho realizado até à data sobre a desinformação, com destaque para as eleições de 2019 para o Parlamento Europeu e os domínios conexos da publicidade política e da publicidade temática.

Comissão procederá a uma avaliação exaustiva da execução de todos os compromissos assumidos no quadro do Código de Conduta durante o seu período inicial de 12 meses. Nesta base, a Comissão pode ponderar outras ações, nomeadamente de natureza regulamentar, para melhorar a resposta de longo prazo da UE perante a desinformação.

3. Preparação e proteção

Reforçar as defesas e criar resiliência face às ameaças contra a segurança constitui um aspeto importante dos trabalhos rumo a uma União da Segurança genuína e eficaz. Tal inclui o apoio prestado pela Comissão aos Estados-Membros e às respetivas autoridades locais com o objetivo de reforçar a **proteção dos espaços públicos**[74], bem como o apoio aos Estados-Membros no reforço da preparação contra os **riscos em matéria de segurança química, biológica, radiológica e nuclear**[75], na execução de dois planos de ação neste domínio e na análise das necessidades em matéria das capacidades de resposta a desenvolver no âmbito da rescEU[76]. No que diz respeito à evolução das ameaças químicas[77], a Comissão, em cooperação com os Estados-Membros e em consulta com os parceiros internacionais, elaborou uma lista de produtos químicos que suscitam maior preocupação em termos de utilização abusiva para fins terroristas. A lista da UE serve de base à continuação dos trabalhos destinados a reduzir o acesso a estes produtos químicos e à colaboração com os fabricantes no sentido de melhorar as capacidades de deteção.

As tecnologias para aeronaves não tripuladas permitem um largo espetro de possíveis operações. Com uma rápida expansão nos últimos anos no mercado de sistemas de aeronaves não tripuladas para fins militares, comerciais civis e de lazer, os **drones** representam uma oportunidade mas igualmente uma ameaça crescente para a segurança das infraestruturas críticas (incluindo a aviação), espaços públicos e eventos, sítios sensíveis e indivíduos. Na Europa, os drones têm sido utilizados para perturbar operações aéreas e policiais, vigiar infraestruturas críticas e introduzir mercadorias de contrabando em prisões e além-fronteiras.

A Comissão apoia os Estados-Membros na luta contra a ameaça crescente que os drones representam para os cidadãos e as funções societais críticas, sem excluir a sua utilização benéfica, por exemplo, em operações de resposta a emergências. A Comissão adotou recentemente **regras comuns à escala da UE sobre a segurança do funcionamento dos drones**[78], a fim de atenuar o risco da sua utilização maliciosa, que incluem disposições que exigem o registo do operador e permitem a identificação à distância. Além disso, a Comissão apoia os Estados-Membros no acompanhamento das tendências da evolução da ameaça que representam os «drones», financiando projetos de investigação relevantes e medidas de reforço das capacidades e facilitando os intercâmbios entre os Estados-Membros e outras

---

74 Ver as «Boas práticas destinadas às autoridades públicas e aos operadores privados para reforçar a segurança dos espaços públicos», tal como estabelecidas no décimo oitavo relatório sobre os progressos alcançados rumo à criação de uma União da Segurança genuína e eficaz [COM (2019) 145 final de 20.3.2019]. Estas medidas têm por base o Plano de ação para apoiar a proteção dos espaços públicos de outubro de 2017 [COM (2017) 612 final de 18.10.2017]. Em 5 de junho de 2019, realizou-se a terceira reunião dos operadores do Fórum da UE sobre a proteção dos espaços públicos. Reuniu representantes dos Estados-Membros da UE e operadores privados de espaços públicos, representados por 14 associações europeias, abrangendo o setor da hotelaria e restauração, espetáculos, música e entretenimento, parques de diversões e atrações turísticas, aviação, transporte ferroviário, centros comerciais e telecomunicações, bem como serviços de segurança privada e fabricantes de equipamentos de segurança.

75 Nomeadamente através da execução do Plano de ação de outubro de 2017 para melhorar a preparação para os riscos de segurança química, biológica, radiológica e nuclear [COM (2017) 610 final de 18.10.2017].

76 Ver o artigo 12.º, n.º 2, da Decisão 1313/2013/UE relativa a um Mecanismo de Proteção Civil da União Europeia (17.12.2013), com a redação que lhe foi dada pela Decisão (UE) 2019/420 de 13.3.2019.

77 Ver o reforço das ações contra as ameaças químicas, tal como estabelecido no décimo quinto relatório sobre os progressos alcançados rumo a uma União da Segurança genuína e eficaz [COM (2018) 470 final de 13.6.2018].

78 JO L 152 de 11.6.2019 - 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.

partes interessadas. Para melhorar esse apoio, a Comissão organizará, em 17 de outubro de 2019, uma conferência internacional de alto nível cujo tema será a luta contra os riscos decorrentes dos drones.

Em resposta à necessidade de ter uma visão abrangente da política da UE em matéria de **proteção de infraestruturas críticas**[79], a Comissão apresentou, em 23 de julho de 2019, uma avaliação da Diretiva relativa às infraestruturas críticas europeias[80], pois esta última constitui o quadro jurídico para a identificação e a designação das infraestruturas críticas europeias, bem como para a avaliação da necessidade de melhorar a sua proteção. A avaliação concluiu que o contexto em que se inscrevem as infraestruturas críticas na Europa se alterou consideravelmente desde a entrada em vigor da diretiva, designadamente com a evolução legislativa em setores especificamente visados pela diretiva, como a energia[81], e que a evolução da situação neste domínio tornou as disposições da diretiva apenas parcialmente relevantes. Ao mesmo tempo, os Estados-Membros continuam a apoiar a política da UE em matéria de proteção das infraestruturas críticas, que respeita a subsidiariedade e proporciona valor acrescentado.

4. Dimensão externa

Tendo em conta a natureza transnacional e mundial da maioria das ameaças contra a segurança na nossa União, a cooperação com as organizações internacionais e os países parceiros externos à UE faz parte integrante dos trabalhos com vista a uma União da Segurança genuína e eficaz.

Tirar partido das vantagens da cooperação multilateral é parte integrante deste esforço e inclui a cooperação entre a UE e a ONU, recentemente reforçada com a assinatura, em 24 de abril de 2019, do **Quadro entre as Nações Unidas e a União Europeia de luta contra o terrorismo**, em Nova Iorque, por ocasião do segundo diálogo político de alto nível ONU-UE sobre a luta contra o terrorismo[82]. Esse quadro promove a cooperação em matéria de reforço das capacidades para combater o terrorismo e prevenir e combater o extremismo violento em África, no Médio Oriente e na Ásia. Define domínios de cooperação e as prioridades entre a ONU e a UE até 2020.

A **cooperação em matéria de segurança com os Balcãs Ocidentais** representa uma prioridade regional específica que se traduz pela aplicação de uma série de ações prioritárias em matéria de segurança identificadas na Estratégia de 2018 para os Balcãs Ocidentais[83]. Para o efeito, a Comissão organizou, em 4 de abril de 2019, a primeira reunião do grupo de trabalho interserviços para os Balcãs Ocidentais, em que representantes de sete agências da UE partilharam a sua experiência e reforçaram a cooperação operacional com os parceiros da região, nomeadamente na luta contra a criminalidade organizada, o terrorismo, as armas de fogo, a droga, a introdução clandestina de migrantes e o tráfico de seres humanos. Foram lançados inquéritos sobre os riscos híbridos com os seis países dos Balcãs Ocidentais. Outro exemplo concreto da cooperação com esta região é o Acordo sobre o estatuto da Guarda Europeia de Fronteiras e Costeira entre a UE e a Albânia, que entrou em vigor em 1 de maio de 2019, a que se seguiu rapidamente um destacamento das equipas da Agência Europeia da Guarda de Fronteiras e Costeira para a fronteira com a Grécia. Este é o primeiro acordo desse tipo com um país terceiro e o primeiro destacamento num país terceiro. Em breve deverão ser assinados acordos semelhantes com outros países da região.

---

79 A avaliação global da política de segurança da UE, realizada em 2017 [SWD (2017) 278 final de 26.7.2017], apontou para a necessidade de se ter uma visão abrangente da política da UE em matéria de proteção das infraestruturas críticas.

80 A Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção visa reforçar a proteção das infraestruturas críticas na União Europeia.

81 Em especial, o Regulamento (UE) 2017/1938, de 25 de outubro de 2017, relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás, e o Regulamento (UE) 2019/941, de 5 de junho de 2019, relativo à preparação para riscos no setor da eletricidade.

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

83 COM(2018) 65 final de 6.2.2018.

Além disso, em julho de 2019, um agente de ligação da Europol foi destacado para a Albânia a fim de prestar assistência às autoridades albanesas nos seus esforços de prevenção e luta contra a criminalidade organizada. Tendo em vista intensificar a luta contra o tráfico de armas de fogo, a Comissão apresentou, em 27 de junho de 2019, uma avaliação do Plano de Ação 2015-2019 **em matéria de luta contra o tráfico de armas de fogo** entre a UE e a região do Sudeste da Europa[84]. A avaliação demonstra o valor acrescentado da cooperação, mas salienta que são necessários esforços adicionais, por exemplo, através da criação de centros de coordenação nacionais sobre armas de fogo que sejam eficazes, ou da harmonização da recolha de informações e comunicação de informações sobre apreensões de armas de fogo.

A UE dá igual prioridade ao desenvolvimento **da cooperação com os países do Médio Oriente e do Norte de África** no domínio da segurança. A UE lançou um diálogo sobre segurança com a Tunísia e a Argélia. A UE e a Tunísia realizaram a terceira sessão do diálogo sobre segurança e luta contra o terrorismo em 12 de junho, em Tunes, enquanto a segunda sessão do diálogo UE-Argélia sobre segurança e luta contra o terrorismo teve lugar em 12 de novembro de 2018, em Argel. Estão em curso conversações para lançar um diálogo estruturado sobre segurança com Marrocos, na sequência do recente Conselho de Associação de 27 de junho, em que a UE e Marrocos reconheceram a importância de aprofundar a cooperação em matéria de segurança para enfrentar desafios comuns. Paralelamente, estão em curso discussões sobre o desenvolvimento de um diálogo estruturado com o Egito em matéria de segurança, tal como confirmado pela última reunião de altos funcionários UE-Egito realizada em 10 de julho no Cairo.

Com base no mandato conferido pelo Conselho, a Comissão deu início a conversações informais com a maioria dos países **do Médio Oriente e do Norte de África** tendo em vista o lançamento de negociações formais para um acordo internacional de intercâmbio de dados pessoais entre a Agência da União Europeia para a Cooperação Policial (**Europol**) e as autoridades competentes nos países **do Médio Oriente e do Norte de África** a fim de combater a criminalidade grave e o terrorismo. Neste contexto, a Comissão está também a incentivar a celebração de acordos de trabalho diretamente entre a Europol e as autoridades parceiras dos países **do Médio Oriente e do Norte de África**, a fim de proporcionar um quadro formal para uma cooperação regular a nível estratégico.

A UE e os **Estados Unidos** são parceiros estratégicos privilegiados quando se trata de fazer face às ameaças comuns e de reforçar a segurança. Na reunião dos Ministros da Justiça e dos Assuntos Internos, de 19 de junho de 2019, a UE e os Estados Unidos reafirmaram que a luta contra o terrorismo figura entre as suas principais prioridades. No que diz respeito ao Acordo entre a UE e os EUA sobre os registos de identificação dos passageiros[85], ambas as partes reiteraram a importância do acordo e comprometeram-se a iniciar uma avaliação conjunta em setembro de 2019 para examinar a sua aplicação, em conformidade com as disposições do acordo. Ambas as partes se comprometeram igualmente a intensificar os seus esforços conjuntos na luta contra o terrorismo, nomeadamente alargando a partilha de informações recolhidas nas zonas de combate para utilização em investigações e procedimentos penais.

Para intensificar esta cooperação, a Comissão, juntamente com o Coordenador da UE da Luta Antiterrorista, organizou, em 10 de julho de 2019, em Bruxelas, um seminário de alto nível sobre as informações do campo de batalha. O seminário reuniu altos funcionários dos ministérios da defesa, dos assuntos internos e da justiça dos Estados-Membros, dos Estados Unidos, da Europol, da Eurojust e representantes de organizações internacionais, a fim de trocar pontos de vista sobre a utilização das informações do campo de batalha e refletir em conjunto sobre os problemas processuais, jurídicos e operacionais que enfrentam atualmente quando se trata de identificar terroristas e de os julgar. A UE e os Estados Unidos também realizaram um diálogo sobre reforço de capacidades no domínio químico,

[84] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_en.pdf

[85] JO L 215 de 11.8.2012, p. 5.

biológico, radiológico e nuclear em Bruxelas, em 14 e 15 de maio de 2019, a fim de coordenar os esforços e reduzir as ameaças das armas de destruição maciça e reforçar a segurança química, biológica, radiológica e nuclear a nível mundial.

O **Acordo UE-EUA sobre o Programa de Deteção do Financiamento do Terrorismo**[86] está em vigor desde 2010 e regula a transferência e o tratamento de dados a fim de identificar, vigiar e reprimir os terroristas e respetivas redes. Prevê garantias que asseguram a proteção de dados dos cidadãos da UE, bem como reexames regulares «das disposições em matéria de garantias, de controlos e de reciprocidade». Num relatório periódico de avaliação[87] publicado em 22 de julho de 2019, a Comissão manifestou a sua satisfação pelo facto de o Acordo, incluindo as suas garantias e controlos essenciais, estar a ser corretamente aplicado. Congratula-se com a transparência de que as autoridades dos Estados Unidos continuam a fazer prova na partilha de informações, ilustrando assim o valor do Programa de Deteção do Financiamento do Terrorismo no quadro dos nossos esforços conjuntos de luta contra o terrorismo. As informações fornecidas no âmbito do Acordo têm sido fundamentais para a realização de investigações específicas relativas a ataques terroristas em solo europeu, incluindo os atentados de Estocolmo, Barcelona e Turku em 2017. Os Estados-Membros e a Europol aumentaram o recurso ao mecanismo, e os dados do referido programa geraram sete vezes mais investigações do que no período de referência anterior. A próxima revisão conjunta do Acordo está prevista para 2021.

No que diz respeito à cooperação internacional em matéria de intercâmbio de **registos de identificação dos passageiros para efeitos de luta contra o terrorismo e a criminalidade grave**, na 17.ª Cimeira UE-Canadá, realizada em Montreal em 17 e 18 de julho de 2019, a UE e o Canadá congratularam-se com o facto de terem concluído as negociações com vista a um novo acordo sobre os registos de identificação dos passageiros. Embora o Canadá tenha tomado nota da sua obrigação de controlo jurisdicional, as partes, sob reserva dessa revisão, comprometem-se a finalizar o acordo o mais rapidamente possível, reconhecendo o papel crucial do mesmo no reforço da segurança, garantindo simultaneamente a privacidade e a proteção dos dados pessoais. No que diz respeito ao atual acordo UE-Austrália sobre os registos de identificação dos passageiros[88], a visita de uma equipa da UE a Camberra terá lugar em agosto de 2019, no contexto da revisão e avaliação conjuntas do acordo.

A Comissão está também a trabalhar com os Estados-Membros a nível do Conselho sobre a posição da UE na próxima 40.ª sessão da Assembleia da **Organização da Aviação Civil Internacional**, que terá lugar entre 24 de setembro e 4 de outubro de 2019. A Assembleia definirá a direção política e dará instruções ao Conselho da Organização da Aviação Civil Internacional sobre os trabalhos técnicos relativos às normas da OACI para o tratamento dos dados dos registos de identificação dos passageiros. O Conselho aprovou um documento de informação elaborado pela Comissão a fim de apresentar a posição da União sobre os princípios fundamentais que deverão estar na base de qualquer futuro sistema mundial relativo aos registos de identificação dos passageiros. O documento de informação será apresentado ao organismo em relação aos seus membros que não são Estados-Membros da UE.

VI. CONCLUSÕES

Graças a uma cooperação estreita entre o Parlamento Europeu, o Conselho, os Estados-Membros e a Comissão, a União realizou progressos consideráveis nos últimos anos no quadro dos trabalhos conjuntos rumo a uma União da Segurança genuína e eficaz, tendo chegado a acordo sobre uma série de iniciativas legislativas prioritárias. Os Estados-Membros, com o apoio da Comissão, estão também a aplicar uma série de medidas operacionais não legislativas para reforçar a segurança de todos os cidadãos. Ao mesmo tempo, há ainda algumas iniciativas prioritárias pendentes na União da

[86] JO L 195 de 27.7. 2010, p. 5.
[87] COM(2019) 342 final de 22.7.2019.
[88] JO L 186 de 14.7.2012, p. 4.

Segurança que requerem medidas adicionais por parte dos colegisladores para fazer face às ameaças imediatas. A Comissão exorta o Parlamento Europeu e o Conselho a tomarem as medidas necessárias para chegar rapidamente a acordo sobre as propostas legislativas que visam combater a propaganda terrorista e a radicalização em linha, reforçar a cibersegurança, facilitar o acesso a provas eletrónicas e concluir os trabalhos sobre sistemas de informação mais sólidos e mais inteligentes para a gestão da segurança, das fronteiras e da migração.

A Comissão exorta os Estados-Membros a aplicarem de forma rápida e integral o conjunto da legislação adotada no âmbito da União da Segurança, a fim de esta produza plenamente os seus efeitos. Além disso, a Comissão exorta os Estados-Membros a prosseguirem e a intensificarem os trabalhos cruciais sobre medidas concretas para reforçar a segurança das infraestruturas digitais, combater a desinformação e outras ameaças possibilitadas pelo ciberespaço, intensificar a preparação e a proteção, e reforçar a cooperação com parceiros externos à União contra as ameaças comuns. No seu conjunto, estas medidas deverão reforçar coletivamente a segurança de todos os cidadãos.