



Bruxelas, 20.3.2019
COM(2019) 145 final

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

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

{SWD(2019) 140 final}

I. INTRODUÇÃO

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

Antes das eleições para o Parlamento Europeu de maio de 2019, o presente relatório sublinha o importante trabalho desenvolvido a vários níveis para combater e prevenir as ciberameaças e a desinformação no contexto eleitoral. Em resposta ao apelo do Conselho Europeu no sentido de serem tomadas medidas para proteger os sistemas democráticos da União e combater a desinformação no período que antecede as próximas eleições, a União realizou progressos consideráveis com vista a uma ação mais coordenada em matéria de resiliência do sistema eleitoral. No entanto, tendo em conta que o tempo escasseia para garantir a preparação da União antes de os eleitores europeus irem às urnas em maio de 2019, a Comissão insta todas as partes envolvidas – autoridades governamentais, partidos políticos e, em particular, plataformas em linha – a redobram os esforços para aumentar a resiliência do sistema eleitoral a fim de combater a desinformação. Antes do próximo Conselho Europeu, que se realizará em 21 e 22 de março de 2019 e no qual serão debatidos os progressos neste domínio, a Comissão insta também os Estados-Membros a reforçarem a sua coordenação com vista a combater a desinformação e a assegurar a proteção das eleições para o Parlamento Europeu.

A UE realizou progressos consideráveis nos trabalhos rumo a uma União da Segurança genuína e eficaz graças ao acordo alcançado sobre uma série de iniciativas legislativas prioritárias que reforçarão a segurança de todos os cidadãos. Nos últimos meses¹, o Parlamento Europeu e o Conselho chegaram a acordo sobre a interoperabilidade dos sistemas de informação da UE em matéria de segurança, gestão das fronteiras e migração, bem como sobre as novas normas da UE para reduzir a margem de manobra dos terroristas e criminosos, que dificultarão o seu acesso aos precursores de explosivos, o financiamento das suas atividades e as viagens sem serem detetados. Graças ao acordo alcançado relativamente a 15 das 22 iniciativas legislativas apresentadas pela Comissão no domínio da União da Segurança (ver lista da totalidade das iniciativas neste domínio no *anexo I*), a UE está a cumprir o seu objetivo num domínio prioritário comum para o Parlamento Europeu, o Conselho e a Comissão².

No entanto, são necessários esforços suplementares. Em especial, no âmbito do atual mandato legislativo, os legisladores devem combater a ameaça premente dos conteúdos terroristas em linha, chegando a acordo sobre a proposta da Comissão. O Parlamento Europeu e o Conselho devem também chegar a acordo sobre a proposta da Comissão relativa ao reforço da Guarda Europeia de Fronteiras e Costeira a fim de aumentar a segurança graças à melhoria da proteção das fronteiras externas da União.

¹ Este acordo baseia-se nos progressos realizados anteriormente rumo a uma União da Segurança genuína e eficaz. Para uma panorâmica completa, ver os anteriores relatórios intercalares sobre a União da Segurança: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

² Ver a declaração conjunta sobre as prioridades legislativas da UE para o período 2018-2019: https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf.

Os trágicos acontecimentos ocorridos em Christchurch, na Nova Zelândia, em 15 de março de 2019, mostram que a ameaça do terrorismo continua a constituir um risco real e atual, quer seja alimentado pelo extremismo de extrema direita quer por outras ideologias extremistas. As dificuldades encontradas para remover das plataformas Internet os conteúdos transmitidos em direto e impedir o seu reaparecimento sublinham a importância vital da proposta da Comissão relativa aos conteúdos terroristas em linha. É fundamental que as normas propostas para a remoção de conteúdos terroristas em linha sejam acordadas pelos legisladores com a maior urgência. Igualmente importante para lutar contra o terrorismo sob todas as suas formas é a plena aplicação, por todos os Estados-Membros, da legislação adotada pela UE, nomeadamente em resposta aos atentados terroristas perpetrados na Europa, a fim de limitar a margem de manobra dos terroristas, em especial as diretivas relativas à luta contra o terrorismo e ao controlo da aquisição e da detenção de armas de fogo. No contexto da luta contra o extremismo, a Comissão também tem vindo a envidar esforços e a tomar medidas adequadas contra os discursos ilegais de incitação ao ódio em linha, a islamofobia e o antissemitismo.

O presente relatório descreve igualmente os progressos realizados na execução de outros dossiês prioritários em matéria de segurança, nomeadamente no que se refere às medidas de apoio à proteção dos espaços públicos. Deve ser dada a máxima prioridade à aplicação integral e correta das medidas acordadas, a fim de garantir a totalidade dos benefícios de uma União da Segurança genuína e eficaz. A Comissão apoia ativamente os Estados-Membros, nomeadamente concedendo-lhes financiamento e facilitando o intercâmbio das melhores práticas. Sempre que necessário, também 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 pano de fundo do presente relatório é a comemoração do 15.º Dia Europeu das Vítimas do Terrorismo, em 11 de março de 2019, quinze anos após os atentados bombistas cometidos em Madrid, em 11 de março de 2004, e três anos após os ataques mortíferos perpetrados em Bruxelas e em Zaventem, em 22 de março de 2016. O apoio às vítimas de ataques terroristas é uma parte importante dos esforços rumo a uma União da Segurança genuína e eficaz. Para intensificar este apoio, a Comissão adotou, em 31 de janeiro de 2019, uma decisão sobre o financiamento do projeto-piloto «Criação de um centro especializado da UE destinado às vítimas do terrorismo»³. O centro especializado da UE funcionará como um polo de competências e uma plataforma para os profissionais que lidam com estas vítimas.

A Comissão congratula-se com o relatório do Parlamento Europeu sobre as conclusões e recomendações da Comissão Especial sobre o Terrorismo⁴, um contributo valioso para o trabalho conjunto em prol de uma União da Segurança genuína e eficaz.

II. CONCRETIZAR AS PRIORIDADES LEGISLATIVAS

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

O intercâmbio de informações é um aspeto fulcral do apoio que a UE presta às autoridades nacionais no âmbito da luta contra o terrorismo e a criminalidade grave. Neste contexto, a

³ C(2019) 636 de 31.1.2019.

⁴ Resolução do Parlamento Europeu, de 12 de dezembro de 2018, sobre as conclusões e recomendações da Comissão Especial sobre o Terrorismo [2018/2044 (INI)].

interoperabilidade dos sistemas de informação a nível da UE constitui uma mudança radical na forma como os dados são disponibilizados às autoridades nacionais, assegurando o seu carácter exato e completo. Os legisladores chegaram a um acordo político sobre as propostas legislativas prioritárias relacionadas com este aspeto, a fim de alcançar a **interoperabilidade dos sistemas de informação da UE** para a gestão da segurança, das fronteiras e da migração⁵. As medidas propostas farão com que os sistemas de informação da UE funcionem em conjunto de forma mais inteligente e direcionada, no pleno respeito dos direitos fundamentais. Tirando o melhor partido dos dados existentes, a interoperabilidade irá colmatar as lacunas de informação e os «ângulos mortos», ajudando a detetar identidades múltiplas e a combater a fraude de identidade. Assim que os legisladores adotarem formalmente as novas normas, a Comissão estará pronta para ajudar os Estados-Membros a aplicá-las. Para alcançar o objetivo ambicioso da plena interoperabilidade dos sistemas de informação da UE para a gestão da segurança, das fronteiras e da migração até 2020, é necessária uma cooperação estreita com as agências da UE e com todos os Estados-Membros e países associados de Schengen. Para a preparar, em 5 de março de 2019 foi organizado um primeiro seminário com peritos dos Estados-Membros destinado a lançar um processo de coordenação eficaz.

Nesta fase, a futura arquitetura dos sistemas de informação interoperáveis da UE incluirá o **Sistema de Informação de Schengen**⁶ reforçado, o atual **Sistema de Informação sobre Vistos**⁷, a extensão recentemente acordada do **Sistema Europeu de Informação sobre Registos Criminais**⁸ aos nacionais de países terceiros, o recém-criado **Sistema de Entrada/Saída da UE**⁹ e o **Sistema Europeu de Informação e Autorização de Viagem (ETIAS)**¹⁰.

No âmbito da aplicação técnica do Sistema Europeu de Informação e Autorização de Viagem, a Comissão apresentou, em 7 de janeiro de 2019, uma proposta que estabelece alterações técnicas ao regulamento correspondente¹¹. As alterações propostas dizem respeito aos atos jurídicos relativos aos sistemas de informação da UE que o Sistema Europeu de Informação e Autorização de Viagem irá consultar no âmbito da avaliação dos riscos de segurança ou de migração irregular dos nacionais de países terceiros isentos da obrigação de visto antes da sua entrada no espaço Schengen. As alterações propostas são necessárias para a plena criação do Sistema Europeu de Informação e Autorização de Viagem. A Comissão insta os legisladores a avançarem com os seus trabalhos sobre as alterações técnicas, a fim de se alcançar um acordo o mais rapidamente possível e permitir assim a implementação rápida e

⁵ COM(2017) 793 final de 12.12.2017, COM(2017) 794 final de 12.12.2017, COM(2018) 478 final de 13.6.2018 e COM(2018) 480 final de 13.6.2018. O acordo político alcançado em 5 de fevereiro de 2019 foi aprovado pelo Comité dos Representantes Permanentes do Conselho em 13 de fevereiro de 2019, e pela Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu em 19 de fevereiro de 2019.

⁶ Regulamento (UE) 2018/1860 de 28.11.2018, Regulamento (UE) 2018/1861 de 28.11.2018, Regulamento (UE) 2018/1862 de 28.11.2018.

⁷ Regulamento (CE) n.º 767/2008 de 9.7.2008.

⁸ Os legisladores chegaram a um acordo político sobre esta proposta prioritária em 11 de dezembro de 2018 [COM(2017) 344 final de 29.6.2017]. O Comité dos Representantes Permanentes do Conselho aprovou o acordo em 19 de dezembro de 2018. A sessão plenária do Parlamento Europeu confirmou o acordo em 11 de março de 2019.

⁹ Regulamento (UE) 2017/2226 de 30.11.2017.

¹⁰ Regulamento (UE) 2018/1240 de 12.9.2018 e Regulamento (UE) 2018/1241 de 12.9.2018.

¹¹ COM(2019) 4 final de 7.1.2019.

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**¹², prevendo um controlo mais aprofundado dos antecedentes dos requerentes de visto e colmatando as lacunas de informação através de um melhor intercâmbio de informações 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 votou o seu relatório sobre a proposta em sessão plenária, concluindo assim a sua primeira leitura. A Comissão apela ao início rápido das negociações entre os legisladores durante a próxima legislatura do Parlamento Europeu.

Em maio de 2016, a Comissão propôs o alargamento do âmbito de aplicação do **Eurodac**¹³, de modo a incluir não só a identificação dos requerentes de asilo, mas também a dos nacionais de países terceiros em situação irregular ou daqueles que entram clandestinamente na UE. Em consonância com as conclusões do Conselho Europeu de dezembro de 2018¹⁴ e com a Comunicação da Comissão de 6 de março de 2019 sobre os progressos realizados na aplicação da Agenda Europeia da Migração¹⁵, a Comissão insta os legisladores a adotarem a proposta sem demora. A adoção desta proposta legislativa permitirá ao Eurodac tornar-se parte da futura arquitetura dos sistemas de informação interoperáveis da UE, integrando assim os dados essenciais dos nacionais de países terceiros em situação irregular e dos que entraram clandestinamente na UE.

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:

- Adotarem a proposta legislativa relativa ao **Eurodac**, em relação à qual estão perto de alcançar um acordo, antes das eleições para o Parlamento Europeu. (*Prioridade da Declaração Conjunta*)
- Avançarem nos trabalhos com vista a alcançar rapidamente um acordo sobre as alterações técnicas propostas necessárias para criar o **Sistema Europeu de Informação e Autorização de Viagem**.

2. Reforçar a segurança através de uma melhor gestão das fronteiras externas

Uma proteção sólida das fronteiras externas constitui uma condição prévia para a segurança no espaço de livre circulação sem controlos nas fronteiras internas. Trata-se de uma responsabilidade dos Estados-Membros, que devem assegurar a gestão das suas fronteiras internas, tanto no seu próprio interesse como no interesse de todos, com a ajuda da **Guarda Europeia de Fronteiras e Costeira**. Em resposta às conclusões do Conselho Europeu de junho de 2018¹⁶, a Comissão propôs, em setembro de 2018, reforçar as capacidades da Guarda Europeia de Fronteiras e Costeira¹⁷. A Agência passará assim para um novo nível operacional, dispondo de um corpo permanente de 10 000 guardas de fronteira que exercerão funções

¹² COM(2018) 302 final de 16.5.2018.

¹³ COM(2016) 272 final de 4.5.2016.

¹⁴ <https://www.consilium.europa.eu/pt/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/>.

¹⁵ COM(2019) 126 final de 6.3.2019.

¹⁶ <https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf>.

¹⁷ COM(2018) 631 final de 12.9.2018.

executivas com equipamentos próprios, no pleno respeito dos direitos fundamentais e da soberania dos Estados-Membros.

O trabalho legislativo sobre a proposta está a avançar bem, e as negociações entre os legisladores entraram na fase crucial. O Parlamento Europeu adotou o seu mandato de negociação em 11 de fevereiro de 2019, enquanto o Conselho recebeu o seu mandato em 20 de fevereiro de 2019. Realizaram-se duas reuniões do tríplice, em 27 de fevereiro de 2019 e em 12 de março de 2019. A Comissão saúda e apoia os progressos realizados sobre este dossiê prioritário, que demonstram que todas as instituições estão empenhadas em adotar esta proposta antes das eleições para o Parlamento Europeu de 2019.

A fim de reforçar a segurança através de uma melhor gestão das fronteiras externas, a Comissão insta o Parlamento Europeu e o Conselho a:

- Adotarem a proposta legislativa relativa ao reforço da **Guarda Europeia de Fronteiras e Costeira** durante o atual mandato do Parlamento Europeu. (*Iniciativa no âmbito do discurso sobre o estado da União de 2018*)

3. Prevenir a radicalização

A luta contra os conteúdos terroristas em linha continua a representar um desafio crucial para lutar contra o terrorismo e prevenir a radicalização. Estes conteúdos desempenharam um papel na maioria dos atentados perpetrados em solo europeu nos últimos dois anos, quer através do incitamento a cometer um atentado, quer de instruções sobre a forma de o cometer quer ainda da glorificação dos seus resultados mortíferos. A fim de combater o perigo claro e atual de tais conteúdos, juntamente com o discurso do Presidente Juncker sobre o estado da União de 2018, foi apresentada uma proposta¹⁸ de regulamento relativo aos **conteúdos terroristas em linha**, que estabelece um quadro jurídico para prevenir a utilização abusiva dos prestadores de serviços de alojamento virtual para a difusão de conteúdos terroristas em linha. Embora garantindo plenamente a liberdade de expressão e outros direitos fundamentais, é fundamental que as futuras normas prevejam medidas eficazes para remover os conteúdos terroristas em linha o mais rapidamente possível, dado que os potenciais danos causados por esses conteúdos aumentam a cada hora que permanecem em linha.

Enquanto o Conselho adotou o seu mandato de negociação em dezembro de 2018, os trabalhos no Parlamento Europeu ainda estão em curso, e espera-se que lhe permitam adotar o seu mandato de negociação em março de 2019¹⁹. A Comissão insta ambos os legisladores a chegarem a acordo sobre a legislação proposta durante o atual mandato do Parlamento Europeu, dada a importância vital de um quadro regulamentar da UE para a remoção dos conteúdos terroristas em linha que contenha normas e garantias claras.

Paralelamente, a Comissão continua a prestar apoio aos Estados-Membros nos esforços para **prevenir a radicalização**. Um mecanismo de cooperação específico da UE, que reúne representantes nacionais, ajuda a garantir que o apoio prestado a nível da UE dá resposta às

¹⁸ COM(2018) 640 final de 12.9.2018.

¹⁹ A Comissão do Mercado Interno e da Proteção dos Consumidores do Parlamento Europeu votou o seu parecer em 4 de março de 2019. A Comissão da Cultura e da Educação do Parlamento Europeu votou o seu relatório em 11 de março de 2019. A Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu deverá votar o seu relatório em 21 de março de 2019.

necessidades dos Estados-Membros²⁰. Entre os exemplos recentes contam-se uma conferência subordinada ao tema «Municípios da UE contra a radicalização», organizada conjuntamente com o Comité das Regiões, em 26 de fevereiro de 2019. Em 13 de março de 2019, a Comissão organizou uma reunião de peritos com decisores políticos nacionais com o objetivo de identificar medidas concretas para continuar a apoiar os serviços penitenciários e de liberdade condicional. Os resultados destes trabalhos integrarão um manual que a Rede de Sensibilização para a Radicalização está a preparar sobre a reabilitação e reintegração dos autores de atos terroristas, os combatentes terroristas estrangeiros que regressam aos seus países e os que se radicalizam na prisão (ver também secção IV.4).

A fim de prevenir a radicalização, a Comissão insta o Parlamento Europeu a:

- Adotar prioritariamente o seu mandato de negociação sobre a proposta legislativa relativa à prevenção da difusão de **conteúdos terroristas em linha**, de modo a que os colegisladores consigam alcançar um acordo durante a atual legislatura do Parlamento Europeu. (*Iniciativa no âmbito do discurso sobre o estado da União de 2018*)

4. Reforçar a cibersegurança

As ciberameaças clássicas aos sistemas e aos dados continuam a aumentar, tendo-se registado um recrudescimento da atividade dos agentes mal-intencionados relativamente a um amplo leque de alvos e de vítimas em 2018. Por conseguinte, a luta contra a cibercriminalidade e o reforço da cibersegurança continuam a constituir uma prioridade para a ação da UE. A União realizou progressos tangíveis no que diz respeito ao reforço da sua cibersegurança, pondo em prática as medidas definidas na Comunicação Conjunta de setembro de 2017 intitulada²¹ «Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE».

Em 12 de março de 2019, o Parlamento Europeu confirmou em sessão plenária o acordo político alcançado pelos colegisladores sobre o **Regulamento Cibersegurança**. Este regulamento, cuja entrada em vigor está prevista para maio de 2019, aumentará as capacidades de cibersegurança e o grau de preparação dos Estados-Membros e das empresas. O Regulamento Cibersegurança estabelecerá um quadro europeu de certificação da cibersegurança para produtos, sistemas e serviços das tecnologias da informação e comunicação. Melhorará também a cooperação e a coordenação entre os Estados-Membros e as instituições, agências e organismos da UE, nomeadamente a Agência da União Europeia para a Cibersegurança, com a sua nova designação.

No entanto, são necessários progressos suplementares relativamente à proposta da Comissão de setembro de 2018 que estabelece o **Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação**²². A proposta visa apoiar as capacidades tecnológicas e industriais em matéria de cibersegurança e aumentar a competitividade da indústria de cibersegurança da União. O Parlamento Europeu e o Conselho adotaram os seus mandatos de negociação em 13 de março

²⁰ As necessidades dos Estados-Membros no domínio da prevenção da radicalização foram identificadas, pela primeira vez, nas chamadas orientações estratégicas para as ações de prevenção da UE para 2019. As orientações estratégicas podem ser consultadas no seguinte endereço: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626&news=1&mod_groups=1&month=08&year=2018.

²¹ JOIN(2017) 450 final de 13.9.2017.

²² COM(2018) 630 final de 12.9.2018.

de 2019. A primeira reunião do tríplice realizou-se em 13 de março de 2019. A Comissão insta os legisladores a chegarem rapidamente a acordo sobre a legislação proposta.

A UE realizou progressos significativos no sentido da operacionalização da **resposta diplomática conjunta da UE às ciberatividades mal-intencionadas** («instrumentos de ciberdiplomacia»), em resposta ao apelo do Conselho Europeu²³ para prosseguir os trabalhos sobre a capacidade de resposta aos ciberataques e de os dissuadir através de medidas restritivas da UE. Em 8 de março de 2019, a Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança e a Comissão apresentaram uma proposta conjunta de regulamento do Conselho relativo a medidas restritivas para lutar contra os ciberataques que ameaçam a União ou os seus Estados-Membros. A Comissão e a Alta Representante apelam à rápida adoção desta proposta a fim de reforçar a resiliência da União contra os ciberataques.

A fim de reforçar a cibersegurança, a Comissão e a Alta Representante instam o Conselho a:

- Adotar o regulamento do Conselho relativo a **medidas restritivas destinadas a lutar contra os ciberataques** que ameaçam a União ou os seus Estados-Membros.

5. Limitar a margem de manobra dos terroristas

A UE tomou outras medidas para privar os terroristas e os criminosos de meios de ação, dificultando-lhes o acesso aos precursores de explosivos, ao financiamento das suas atividades e a viagens sem serem detetados.

Em 14 de fevereiro de 2019, o Parlamento Europeu e o Conselho alcançaram um acordo político sobre a proposta de regulamento relativo às **restrições à comercialização e utilização de precursores de explosivos**²⁴. Quando se tornar aplicável, o regulamento introduzirá melhorias significativas no atual quadro legislativo, restringindo o acesso aos precursores de explosivos perigosos suscetíveis de serem utilizados de forma abusiva para fabricar bombas artesanais. Colmatará as lacunas de segurança com medidas, como a proibição de produtos químicos adicionais, a realização de controlos obrigatórios dos registos criminais dos requerentes de uma licença para a compra de substâncias sujeitas a restrições e a indicação explícita de que as normas aplicáveis aos operadores económicos são igualmente aplicáveis às empresas que operam em linha.

Além disso, no âmbito dos esforços envidados para lutar contra o financiamento do terrorismo, os legisladores chegaram a acordo sobre a proposta de diretiva destinada a **facilitar a utilização de informações financeiras e de outro tipo** para prevenir, detetar, investigar ou reprimir infrações penais graves²⁵. Uma vez formalmente adotada e transposta, a diretiva proporcionará às autoridades designadas de aplicação da lei e aos serviços de recuperação de bens acesso direto às informações sobre contas bancárias constantes dos registos nacionais centralizados de contas bancárias. A diretiva reforçará igualmente a

²³ Ver conclusões dos Conselhos Europeus de junho de 2018 e de outubro de 2018.

²⁴ COM(2018) 209 final de 17.4.2018.

²⁵ Os legisladores chegaram a um acordo político sobre a proposta da Comissão em 12 de fevereiro de 2019 [COM(2018) 213 final de 17.4.2018]. O acordo político foi aprovado pelo Comité dos Representantes Permanentes do Conselho em 20 de fevereiro de 2019, e pela Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu em 26 de fevereiro de 2019.

cooperação entre as unidades de informação financeira nacionais e as autoridades de aplicação da lei e facilitará o acesso da Europol às informações financeiras.

Tendo em conta estes elementos, a Comissão continuará a refletir sobre a cooperação entre as unidades de informação financeira de vários Estados-Membros, nomeadamente no próximo relatório sobre a cooperação entre as unidades de informação financeira, como previsto na 5.^a Diretiva Branqueamento de Capitais²⁶. Além disso, conforme exigido por essa diretiva, a Comissão está a avaliar os aspetos relacionados com a eventual interligação entre os registos nacionais centralizados de contas bancárias e os sistemas de extração de dados na UE. A Comissão está também a analisar medidas de confisco não baseadas numa condenação na União. Por último, e também em resposta a um apelo do Parlamento Europeu,²⁷ a Comissão continuará a avaliar a necessidade, a viabilidade técnica e a proporcionalidade de medidas adicionais para detetar atividades de financiamento do terrorismo na UE.

No âmbito dos trabalhos destinados a reduzir a fraude documental, em 19 de fevereiro de 2019, os legisladores chegaram a um acordo provisório sobre o regulamento proposto que visa reforçar a **segurança dos bilhetes de identidade dos cidadãos da União e dos títulos de residência**²⁸, de modo a não poderem ser utilizados de forma fraudulenta por criminosos e terroristas. A Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu confirmou o acordo em 11 de março de 2019. Uma vez adotado, o regulamento introduzirá dispositivos de segurança mínimos nos bilhetes de identidade, incluindo identificadores biométricos (uma imagem facial e duas impressões digitais) que serão armazenados num chip sem contacto. A segurança dos bilhetes de identidade nacionais e dos títulos de residência será assim significativamente aumentada, dificultando aos terroristas e outros criminosos a utilização indevida ou a falsificação desses documentos para fins de entrada ou deslocação no interior da UE. A segurança acrescida dos documentos de identidade contribuirá para reforçar a gestão das fronteiras externas da UE. Ao mesmo tempo, o facto de os documentos serem mais seguros e mais fiáveis facilitará o exercício do direito à livre circulação dos cidadãos da UE.

Não obstante, são necessários progressos suplementares no que diz respeito às propostas da Comissão de abril de 2018 sobre o **acesso a provas eletrónicas**, dado que atualmente mais de metade de todas as investigações criminais envolvem um pedido transnacional de acesso a provas eletrónicas²⁹. O Conselho adotou o seu mandato de negociação sobre uma proposta de regulamento³⁰ para melhorar o acesso transnacional às provas eletrónicas em investigações

²⁶ O artigo 65.º, n.º 2, da Diretiva (UE) 2018/843 de 19.6.2018 estabelece que, até 1 de junho de 2019, a Comissão avalia o quadro de cooperação das UIF com países terceiros e os obstáculos e as oportunidades para reforçar a cooperação entre as UIF na União, incluindo a possibilidade de criar um mecanismo de coordenação e apoio.

²⁷ No seu relatório final, adotado em dezembro de 2018, a Comissão Especial sobre o Terrorismo do Parlamento Europeu apelou à criação de um sistema de deteção do financiamento do terrorismo da União Europeia direcionado para as transações de pessoas com ligações ao terrorismo e seu financiamento efetuadas no espaço único de pagamentos em euros.

²⁸ COM(2018) 212 final de 17.4.2018.

²⁹ Em cerca de 85 % das investigações criminais são necessárias provas eletrónicas, 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].

³⁰ 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.

criminais e uma proposta de diretiva³¹ que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal. No entanto, os progressos registados no Parlamento Europeu relativamente a estas propostas foram muito limitados desde a sua adoção pela Comissão em abril de 2018. Dada a importância crucial de um acesso eficiente às provas eletrónicas para a repressão de crimes transnacionais como o terrorismo ou a cibercriminalidade, a Comissão insta o Parlamento Europeu a avançarem nos trabalhos relativos a esta proposta.

Paralelamente, a Comissão está a trabalhar nas suas **iniciativas internacionais sobre o acesso a provas eletrónicas**, no contexto 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. Por conseguinte, em 5 de fevereiro de 2019, a Comissão adotou recomendações³² relativas aos mandatos de negociação para ambas as iniciativas internacionais. O Conselho está atualmente a debater os projetos de mandato, nomeadamente na reunião do Conselho Justiça e Assuntos Internos de 7 e 8 de março de 2019. A Comissão convida o Conselho a adotar a decisão que autoriza a participação nas negociações sobre um segundo protocolo adicional à Convenção de Budapeste sobre o Cibercrime do Conselho da Europa, bem como a decisão que autoriza a abertura de negociações com os Estados Unidos sobre o acesso transnacional a provas eletrónicas. É importante avançar rapidamente com 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 deste direito, tendo igualmente em conta a sua evolução futura.

A fim de limitar a margem de manobra dos terroristas, a Comissão insta:

- O **Parlamento Europeu** a adotar com urgência o seu mandato de negociação sobre as propostas legislativas relativas às **provas eletrónicas** com vista a encetar, sem demora, discussões do tríplice com o Conselho. (*Prioridade da Declaração Conjunta*)
- O **Conselho** a adotar a decisão que autoriza a participação nas negociações sobre um **segundo protocolo adicional à Convenção de Budapeste sobre o Cibercrime do Conselho da Europa**, bem como a decisão que autoriza a abertura de **negociações com os Estados Unidos** sobre o acesso transnacional a provas eletrónicas.

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

A capacidade de partes externas e internas interferirem nos debates públicos e manipularem as eleições é mais real do que nunca, e poderá aumentar ainda mais com as próximas eleições para o Parlamento Europeu. As possíveis consequências, a saber, o enfraquecimento ou a perda de legitimidade das instituições democráticas, são uma ameaça grave, estratégica e crescente. Constituem um elemento essencial dos desafios de segurança que a UE enfrenta atualmente, que ultrapassam as fronteiras nacionais e exigem uma resposta conjunta e transnacional.

As campanhas eleitorais que precedem as eleições para o Parlamento Europeu começarão verdadeiramente em março. Antes do Conselho Europeu de 21 e 22 de março de 2019, a

³¹ COM(2018) 226 final de 17.4.2018. O Conselho adotou o seu mandato de negociação sobre a proposta de diretiva no Conselho Justiça e Assuntos Internos de 8 de março de 2019.

³² COM(2019) 70 final de 5.2.2019 e COM(2019) 71 final de 5.2.2019.

Comissão insta os Estados-Membros a intensificarem a sua coordenação e o intercâmbio de informações com o objetivo de combater a desinformação e proteger as eleições contra as ameaças possibilitadas pelo ciberespaço. Os Estados-Membros devem utilizar plenamente os instrumentos e os canais de informação disponibilizados pela UE, nomeadamente o recém-criado Sistema de Alerta Rápido³³. Além disso, devido à preocupação com a situação atual, a Comissão insta as plataformas em linha a acelerarem os seus esforços em todos os Estados-Membros a fim de ajudarem a assegurar a integridade das eleições para o Parlamento Europeu em maio de 2019.

Para apoiar e incentivar estes esforços, a Comissão e a Alta Representante continuam a tomar medidas em duas vertentes complementares a fim de combater as ameaças possibilitadas pelo ciberespaço: combater a desinformação e assegurar a resiliência do sistema eleitoral.

1. Adoção de medidas contra a desinformação

A exposição dos cidadãos à desinformação em larga escala, incluindo informação comprovadamente falsa ou enganadora, pode constituir uma grave ameaça possibilitada pelo ciberespaço e é um importante desafio para as próximas eleições europeias. A Comissão está a acompanhar de perto a execução das ações anunciadas na sua **Comunicação «Combater a desinformação em linha», de abril de 2018**³⁴.

Além disso, a Comissão está a acompanhar de perto os progressos realizados no âmbito do **Código de Conduta sobre Desinformação**, assinado em outubro de 2018 por representantes das plataformas em linha, das principais redes sociais, dos anunciantes e do setor da publicidade (ver infra). A Comissão procederá a uma avaliação global da sua aplicação após um período inicial de doze meses. Caso a aplicação e o impacto do Código de Conduta se revelem insatisfatórios, a Comissão pode propor medidas adicionais, nomeadamente de natureza legislativa.

Com base nestes trabalhos, e respondendo ao apelo lançado pelos dirigentes no Conselho Europeu de junho de 2018 para proteger os sistemas democráticos da União, a Comissão e a Alta Representante apresentaram um **plano de ação conjunto contra a desinformação**³⁵ em dezembro de 2018. O plano de ação salienta que, de acordo com a **célula de fusão da UE contra as ameaças híbridas**, a desinformação originada pela Federação da Rússia constitui a maior ameaça para a UE. Trata-se de uma prática sistemática, que dispõe de bastantes recursos e é efetuada numa maior escala comparativamente a outros países. Para fazer face à ameaça que a desinformação representa, o plano de ação prevê um aumento dos recursos consagrados à luta contra a desinformação, mais especificamente para os **grupos de trabalho sobre comunicação estratégica** do Serviço Europeu para a Ação Externa (SEAE), nomeadamente o grupo de trabalho de comunicação estratégica para o Leste³⁶. O plano de

³³ No âmbito do Plano de Ação contra a Desinformação apresentado pela Comissão e pela Alta Representante em dezembro de 2018 (ver infra), o Sistema de Alerta Rápido constituirá uma plataforma para os Estados-Membros, as instituições da UE e os parceiros partilharem informações sobre as campanhas de desinformação em curso e para poderem coordenar as suas respostas. O sistema basear-se-á apenas em informações de fonte aberta e não classificadas.

³⁴ COM(2018) 236 final de 26.4.2018, seguida de um relatório de execução [COM(2018) 794 final de 5.12.2018].

³⁵ JOIN(2018) 36 final de 5.12.2018.

³⁶ Desde a sua criação em 2015, o grupo de trabalho de comunicação estratégica para o Leste catalogou, analisou e identificou quase 5 000 exemplos de desinformação por parte da Federação da Rússia, tendo

ação prevê igualmente um aumento dos recursos consagrados a esta questão e apela a um reforço dos mesmos ao longo dos próximos dois anos.

O plano de ação estabelece medidas concretas para combater a desinformação, incluindo a criação de um **Sistema de Alerta Rápido**. Na perspetiva das eleições para o Parlamento Europeu, o Sistema de Alerta Rápido foi criado em março de 2019 entre as instituições da UE e os Estados-Membros, a fim de facilitar a partilha de dados e avaliações de campanhas de desinformação e emitir alertas sobre ameaças de desinformação.

O plano de ação prevê igualmente um acompanhamento rigoroso da aplicação do Código de Conduta assinado pelas plataformas em linha referido supra. Em 29 de janeiro de 2019, a Comissão publicou os **relatórios apresentados pelos signatários do Código de Conduta** – Google, Facebook, Twitter, Mozilla e as associações comerciais que representam o setor da publicidade. Muito embora se tenha congratulado com os progressos realizados, a Comissão instou os signatários a intensificarem os seus esforços na perspetiva das eleições para o Parlamento Europeu de 2019³⁷.

Em 28 de fevereiro de 2019, a Comissão Europeia publicou os **relatórios do Facebook, Google e Twitter** sobre os progressos realizados em janeiro de 2019 respeitantes ao seu compromisso de lutar contra a desinformação. Nestes relatórios, as plataformas não comunicaram dados suficientes que provem que estão a aplicar novas políticas e ferramentas em tempo útil e que consagram recursos suficientes para esse efeito em todos os Estados-Membros. Há claramente margem para melhorias em relação a todos os signatários³⁸. Mais especificamente, a Comissão insta as plataformas a garantirem, até ao início da campanha para as eleições europeias, a transparência dos anúncios de cariz político em todos os Estados-Membros da UE, a permitirem um acesso adequado aos dados para fins de investigação e verificação de factos, e a assegurarem uma cooperação adequada com cada Estado-Membro através de pontos de contacto no Sistema de Alerta Rápido.

Em 20 de março de 2019, a Comissão apresentará um novo relatório sobre a aplicação do Código de Conduta supramencionado.

2. Reforçar a resiliência do sistema eleitoral

Em 12 de setembro de 2018, a Comissão adotou um pacote de medidas destinadas a reforçar a resiliência dos nossos sistemas eleitorais, dirigidas aos Estados-Membros e aos partidos políticos europeus e nacionais e fundações políticas nacionais e europeias, incluindo uma recomendação sobre as redes de cooperação eleitoral, a transparência em linha, a proteção contra os incidentes de cibersegurança e a luta contra as campanhas de desinformação, orientações sobre a aplicação do direito da União em matéria de proteção de dados³⁹, e uma alteração legislativa destinada a reforçar as disposições que regulam o financiamento dos partidos políticos europeus.

O Parlamento Europeu congratulou-se com o pacote na sua resolução adotada em 28 de outubro de 2018. O Conselho acolheu favoravelmente o pacote de medidas nas suas

desmontado vários discursos de desinformação, procedido à sensibilização do público e publicitado as ferramentas, técnicas e intenções das campanhas de desinformação.

³⁷ Para mais pormenores, ver: http://europa.eu/rapid/press-release_IP-19-746_pt.htm.

³⁸ Para mais pormenores, ver: http://europa.eu/rapid/press-release_STATEMENT-19-1379_pt.htm.

³⁹ COM(2018) 638 final de 12.9.2018.

conclusões de 19 de fevereiro de 2019 sobre a realização de eleições europeias livres e justas, que expressam um compromisso partilhado por todos os Estados-Membros no sentido de uma abordagem europeia coordenada para proteger a integridade das próximas eleições europeias. O Conselho Justiça e Assuntos Internos debateu o ponto da situação em 7 de março de 2019.

A alteração do regulamento relativo ao **estatuto e ao financiamento dos partidos políticos europeus e das fundações**⁴⁰ introduz a possibilidade de impor sanções contra a utilização ilegal de dados pessoais em caso de impacto deliberado nos resultados das eleições para o Parlamento Europeu. Na sequência de um acordo político⁴¹ alcançado em janeiro de 2019, o Parlamento Europeu aprovou o texto da alteração em sessão plenária, em 12 de março de 2019. Está previsto que a alteração seja incorporada na legislação antes das eleições para o Parlamento Europeu de 2019.

A Recomendação sobre **as redes de cooperação eleitoral, a transparência em linha, a proteção contra os incidentes de cibersegurança e as campanhas de desinformação no âmbito das eleições para o Parlamento Europeu**⁴² é dirigida aos Estados-Membros e aos partidos políticos nacionais e europeus e às fundações políticas nacionais e europeias, e apresenta medidas concretas para os atores pertinentes nestes domínios. Num esforço para aplicar a recomendação, as redes eleitorais nacionais nomearam pontos de contacto para participar numa **rede europeia de cooperação para as eleições**, cuja missão é lançar alertas sobre ameaças, proceder ao intercâmbio de boas práticas entre as redes nacionais, discutir soluções comuns para os desafios identificados e encorajar projetos e exercícios comuns entre as redes nacionais. Na primeira reunião da rede, realizada em 21 de janeiro de 2019, os participantes concordaram que é essencial uma abordagem global para garantir a integridade das eleições e preservar simultaneamente um debate democrático aberto e condições equitativas a nível político. A segunda reunião da rede europeia de cooperação para as eleições teve lugar em 27 de fevereiro de 2019, tendo-se centrado em temas relevantes no contexto eleitoral relacionados com a monitorização e a execução, incluindo a proteção de dados, a regulamentação dos meios de comunicação social, a aplicação da lei, a transparência e as redes sociais, e a participação das diferentes partes interessadas nas atividades de monitorização. Lançou as bases para a sua participação num exercício de ciber-resiliência imediatamente após a próxima reunião antecipada da rede, que terá lugar em 5 de abril de 2019.

Em 19 de fevereiro de 2019, realizou-se um **seminário sobre o tema «Reforçar a ciber-resiliência das eleições»**, organizado conjuntamente pelo Parlamento Europeu e pela Comissão com o objetivo de melhorar a segurança e a resiliência dos sistemas e infraestruturas eleitorais contra as ameaças em constante evolução. As autoridades nacionais responsáveis pela cibersegurança dos Estados-Membros, a Agência da União Europeia para a Segurança das Redes e da Informação e as plataformas em linha discutiram medidas centradas em ações urgentes e relevantes para assegurar a integridade das eleições para o Parlamento Europeu de 2019.

As instituições da UE e os Estados-Membros estão também a cooperar estreitamente noutras **atividades de sensibilização** destinadas a proteger a integridade do processo eleitoral e no

⁴⁰ COM(2018) 636 final de 12.9.2018.

⁴¹ Os legisladores alcançaram um acordo político em 16 de janeiro de 2018, que foi aprovado pelo Comité dos Representantes Permanentes do Conselho em 25 de janeiro de 2019, e pela Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos do Parlamento Europeu em 29 de janeiro de 2019.

⁴² C(2018) 5949 final de 12.9.2018.

envolvimento de intervenientes do setor privado e público, incluindo os meios de comunicação social, as plataformas em linha e a sociedade civil.

A fim de combater a desinformação e assegurar a resiliência do sistema eleitoral, a Comissão e a Alta Representante instam os Estados-Membros a:

- Executarem rapidamente e com determinação as ações do **plano de ação conjunto contra a desinformação** de dezembro de 2018.

IV. EXECUÇÃO DE OUTROS DOSSIÊS PRIORITÁRIOS EM MATÉRIA DE SEGURANÇA

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

Deve ser dada a máxima prioridade à aplicação integral e correta das medidas acordadas, a fim de garantir a totalidade dos benefícios de uma União da Segurança genuína e eficaz. A Comissão apoia ativamente os Estados-Membros, nomeadamente concedendo-lhes financiamento e facilitando o intercâmbio das melhores práticas. Sempre que necessário, também 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.

No que se refere à aplicação da **Diretiva da UE relativa à utilização dos dados dos registos de identificação dos passageiros**⁴³, a Comissão lançou, em 19 de julho de 2018, procedimentos de infração contra 14 Estados-Membros por não terem comunicado a adoção de legislação nacional que transponha integralmente a diretiva⁴⁴ – um instrumento essencial na luta contra o terrorismo e a criminalidade grave. Desde então, nove desses Estados-Membros notificaram a transposição integral⁴⁵. Os Estados-Membros que ainda não procederam à transposição integral receberam pareceres fundamentados (Espanha, em 24 de janeiro de 2019, Países Baixos e Finlândia, em 7 de março de 2019). 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**⁴⁶ expirou em 8 de setembro de 2018. Em 22 de novembro de 2018, a Comissão lançou procedimentos de infração contra 16 de Estados-Membros por não terem comunicado a adoção de legislação nacional que transponha integralmente a diretiva. Desde então, nove desses Estados-Membros notificaram a transposição integral⁴⁷. A Comissão insta os restantes sete Estados-Membros a tomarem as medidas necessárias o mais rapidamente possível⁴⁸.

⁴³ Diretiva (UE) 2016/681 de 27.4.2016.

⁴⁴ Bulgária, Chéquia, Estónia, Grécia, Espanha, França, Chipre, Luxemburgo, Países Baixos, Áustria, Portugal, Roménia, Eslovénia e Finlândia.

⁴⁵ Bulgária, Estónia, Grécia, França, Chipre, Luxemburgo, Áustria, Portugal e Roménia (ponto da situação em 11 de março de 2019).

⁴⁶ Diretiva (UE) 2017/541 de 15.3.2017.

⁴⁷ A Bulgária, Chéquia, Alemanha, Estónia, Espanha, França, Croácia, Itália, Letónia, Lituânia, Hungria, Malta, Países Baixos, Áustria, Portugal, Eslováquia, Finlândia e Suécia notificaram a transposição (situação em 11 de março de 2019).

⁴⁸ A Bélgica, Polónia, Roménia e Eslovénia notificaram a transposição parcial. A Grécia, Chipre e o Luxemburgo não notificaram qualquer transposição (situação em 11 de março de 2019).

O prazo para a transposição da **Diretiva relativa ao controlo da aquisição e da detenção de armas**⁴⁹ expirou em 14 de setembro de 2018. Até à data, seis Estados-Membros notificaram a transposição integral⁵⁰ e cinco a transposição parcial⁵¹. 22 Estados-Membros⁵², incluindo os que notificaram uma transposição parcial, receberam cartas de notificação para cumprir da Comissão em 22 de novembro de 2018.

No que diz respeito à transposição para o direito nacional da **Diretiva relativa à proteção de dados**⁵³, a Comissão iniciou procedimentos de infração contra 19 Estados-Membros, em 19 de julho de 2018, por não terem comunicado a adoção de legislação nacional que assegure a plena transposição da diretiva⁵⁴. Até à data, 17 Estados-Membros notificaram a transposição integral e cinco notificaram uma transposição parcial⁵⁵. Até ao momento, foram encerrados os procedimentos contra seis Estados-Membros⁵⁶, enquanto nove Estados-Membros receberam um parecer fundamentado em 25 de janeiro de 2019⁵⁷.

A Comissão deverá apresentar um relatório sobre a coerência da identificação dos operadores de serviços essenciais até 9 de maio de 2019. De acordo com as notificações dos Estados-Membros, a **Diretiva relativa à segurança das redes e da informação**⁵⁸ foi integralmente transposta em 25 Estados-Membros e parcialmente transposta num Estado-Membro⁵⁹. Em janeiro de 2019, a Comissão encerrou procedimentos de infração por não comunicação contra seis Estados-Membros⁶⁰. Nove Estados-Membros⁶¹ são objeto de um procedimento de infração por não comunicação da transposição integral da diretiva. No âmbito da transposição da Diretiva relativa à segurança das redes e da informação, os Estados-Membros deviam apresentar à Comissão, até 9 de novembro de 2018, informações

⁴⁹ Diretiva (UE) 2017/853 de 17.5.2017.

⁵⁰ Dinamarca, França, Croácia, Itália, Malta e Áustria (situação em 11 de março de 2019).

⁵¹ Chéquia, Estónia, Lituânia, Portugal e Reino Unido (situação em 11 de março de 2019).

⁵² Bélgica, Bulgária, Chéquia, Alemanha, Estónia, Irlanda, Grécia, Espanha, Chipre, Letónia, Lituânia, Luxemburgo, Hungria, Países Baixos, Polónia, Portugal, Roménia, Eslovénia, Eslováquia, Finlândia, Suécia e Reino Unido (situação em 11 de março de 2019).

⁵³ Diretiva (UE) 2016/680 de 27.4.2016.

⁵⁴ Bélgica, Bulgária, Chéquia, Estónia, Grécia, Espanha, França, Croácia, Chipre, Letónia, Lituânia, Luxemburgo, Hungria, Países Baixos, Polónia, Portugal, Roménia, Eslovénia e Finlândia. A Comissão está a receber respostas dos Estados-Membros, incluindo notificações da legislação em causa, que estão atualmente a ser analisadas (situação em 11 de março de 2019).

⁵⁵ A Bélgica, Alemanha, Estónia, Irlanda, França, Croácia, Itália, Lituânia, Luxemburgo, Hungria, Malta, Áustria, Polónia, Roménia, Eslováquia, Suécia e Reino Unido notificaram a transposição integral. A Chéquia, Portugal, Finlândia, Eslovénia e Países Baixos notificaram uma transposição parcial. Além disso, a Dinamarca concluiu a transposição (situação em 11 de março de 2019).

⁵⁶ Bélgica, França, Croácia, Lituânia, Luxemburgo e Hungria (situação em 11 de março de 2019).

Greece, Cyprus, Spain, Slovenia, Portugal, Czechia, Bulgaria, Latvia and the Netherlands (state of play as of 11 March 2019). Grécia, Chipre, Espanha, Eslovénia, Portugal, Chéquia, Bulgária, Letónia e Países Baixos (situação em 11 de março de 2019).

⁵⁸ Diretiva (UE) 2016/1148 de 27.4.2016.

⁵⁹ A Bulgária, Chéquia, Dinamarca, Alemanha, Grécia, Estónia, Irlanda, Espanha, França, Croácia, Itália, Chipre, Letónia, Lituânia, Malta, Países Baixos, Áustria, Polónia, Portugal, Roménia, Eslovénia, Eslováquia, Finlândia, Suécia e Reino Unido notificaram a transposição integral. A Hungria notificou uma transposição parcial. A Bélgica e o Luxemburgo não notificaram qualquer medida nacional de transposição à Comissão (situação em 11 de março de 2019).

⁶⁰ Irlanda, Espanha, França, Croácia, Países Baixos e Portugal (situação em 11 de março de 2019).

⁶¹ Bulgária, Bélgica, Dinamarca, Letónia, Lituânia, Luxemburgo, Hungria, Áustria e Roménia (situação em 11 de março de 2019).

sobre os operadores dos serviços essenciais identificados no seu território. A Comissão está atualmente a avaliar as informações apresentadas pelos Estados-Membros⁶².

A Comissão está também a avaliar a transposição da **Quarta Diretiva Branqueamento de Capitais**⁶³ e a verificar se as normas são aplicadas nos Estados-Membros. A Comissão iniciou procedimentos de infração contra os 28 Estados-Membros, uma vez que considerou que as comunicações recebidas dos mesmos não representam uma transposição integral da diretiva⁶⁴. Continuará a utilizar os seus poderes quando apropriado para garantir a aplicação integral desta diretiva.

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

- **Diretiva Registos de Identificação dos Passageiros da UE**, relativamente à qual três Estados-Membros ainda devem notificar a transposição para a legislação nacional e dois Estados-Membros devem completar a notificação da transposição⁶⁵;
- **Diretiva Segurança das Redes e da Informação**, relativamente à qual dois Estados-Membros ainda devem notificar a transposição para o direito nacional e um Estado-Membro deve completar a notificação da transposição⁶⁶;
- **Diretiva Luta contra o Terrorismo**, relativamente à qual três Estados-Membros ainda devem notificar a transposição para o direito nacional e quatro Estados-Membros devem completar a notificação da transposição⁶⁷;
- **Diretiva relativa ao controlo da aquisição e da detenção de armas**, relativamente à qual 17 Estados-Membros ainda devem notificar a transposição para o direito nacional e cinco devem completar a notificação da transposição⁶⁸;
- **Diretiva sobre a Proteção de Dados na Aplicação da Lei**, relativamente à qual cinco Estados-Membros ainda devem notificar a transposição para o direito nacional e cinco

⁶² Bulgária, Chipre, Chéquia, Alemanha, Dinamarca, Estónia, Espanha, Finlândia, França, Croácia, Hungria, Irlanda, Itália, Lituânia, Malta, Países Baixos, Polónia, Portugal, Eslováquia, Suécia e Reino Unido (situação em 11 de março de 2019).

⁶³ Diretiva (UE) 2015/849 de 20.5.2015.

⁶⁴ A Comissão iniciou procedimentos de infração contra todos os Estados-Membros por não terem comunicado a legislação nacional de transposição integral da diretiva, uma vez que, de acordo com a avaliação, a Comissão concluiu que algumas disposições da diretiva não tinham sido transpostas.

⁶⁵ Espanha, Países Baixos e Finlândia ainda têm de comunicar a transposição. Chéquia e Eslovénia comunicaram a transposição parcial e devem ainda completar a notificação da transposição (situação em 11 de março de 2019). As referências à notificação da transposição integral têm em conta as declarações dos Estados-Membros e não prejudicam a verificação da transposição efetuada pelos serviços da Comissão.

⁶⁶ A Bélgica e o Luxemburgo ainda não comunicaram a transposição. A Hungria comunicou uma transposição parcial e deve ainda completar a notificação da transposição (situação em 11 de março de 2019).

⁶⁷ A Grécia, Chipre e o Luxemburgo ainda não comunicaram a transposição. Bélgica, Polónia, Roménia e Eslovénia comunicaram a transposição parcial e devem ainda completar a notificação da transposição (situação em 11 de março de 2019).

⁶⁸ Bélgica, Bulgária, Alemanha, Irlanda, Grécia, Espanha, Chipre, Letónia, Luxemburgo, Hungria, Países Baixos, Polónia, Roménia, Eslovénia, Eslováquia, Finlândia e Suécia ainda têm de comunicar a transposição. Chéquia, Estónia, Lituânia, Malta, Portugal e Reino Unido comunicaram a transposição parcial e devem ainda completar a notificação da transposição (situação em 11 de março de 2019). As referências à notificação da transposição integral têm em conta as declarações dos Estados-Membros e não prejudicam a verificação da transposição efetuada pelos serviços da Comissão.

Estados-Membros devem completar a notificação da transposição⁶⁹; e

- **Quarta Diretiva Branqueamento de Capitais**, relativamente à qual um Estado-Membro deve completar a notificação da transposição⁷⁰.

2. *Proteção dos espaços públicos: boas práticas recomendadas*

No âmbito dos trabalhos práticos destinados a melhorar a proteção e a resiliência contra o terrorismo, a Comissão continua a apoiar os Estados-Membros e as suas autoridades locais na **proteção dos espaços públicos**. No âmbito da aplicação do plano de ação para apoiar a proteção dos espaços públicos de outubro de 2017,⁷¹ os trabalhos centram-se no desenvolvimento e na recolha de orientações e boas práticas. Trabalhando em conjunto com as autoridades públicas e os operadores privados de espaços públicos no chamado Fórum dos responsáveis por espaços públicos⁷², a Comissão identificou boas práticas relativas a várias medidas que todos os operadores e autoridades públicas envolvidos na proteção dos espaços públicos podem aplicar para reforçar a segurança⁷³. Preveem as medidas básicas para orientar os trabalhos futuros em todos os setores relevantes para a proteção dos espaços públicos (ver quadro infra).

Boas práticas destinadas às autoridades públicas e aos operadores privados para reforçar a segurança dos espaços públicos

Avaliação e planeamento

- Preparar e realizar avaliações de vulnerabilidade para identificar potenciais vulnerabilidades contra ataques cometidos por terceiros ou pessoas com acesso a informação privilegiada;
- Conceber e aplicar um plano de segurança para instalações ou eventos, incluindo medidas de preparação, emergência e recuperação, e identificar as medidas de segurança adequadas para a instalação ou evento em causa. As medidas de segurança devem ser eficazes, discretas, proporcionadas e adaptadas a diferentes ambientes, tendo em conta o seu funcionamento específico;
- Nomear e formar uma pessoa responsável pela coordenação e aplicação das medidas de segurança previstas no plano de segurança; e

⁶⁹ A Bulgária, Grécia, Espanha, Chipre e Letónia ainda não comunicaram a transposição. Chéquia, Portugal, Países Baixos, Finlândia e Eslovénia comunicaram a transposição parcial e devem ainda completar a notificação da transposição (situação em 11 de março de 2019).

⁷⁰ Até à data, a Roménia apenas comunicou uma transposição parcial e ainda não completou a notificação de transposição. Os restantes Estados-Membros notificaram a transposição integral. No entanto, de acordo com a avaliação da Comissão, ainda há algumas disposições da diretiva cuja transposição não parece estar inteiramente concluída (situação em 11 de março de 2019).

⁷¹ COM(2017) 612 final de 18.10.2017.

⁷² O fórum dos operadores público-privados, criado ao abrigo do plano de ação de outubro de 2017 para apoiar a proteção dos espaços públicos, reúne decisores políticos dos Estados-Membros e operadores de vários setores, tais como os eventos de massa e entretenimento, a hotelaria, os centros comerciais, os espaços desportivos e culturais, as interfaces de transportes e outros.

⁷³ Para mais informações sobre as boas práticas, consultar o documento de trabalho dos serviços da Comissão intitulado «Boas práticas para apoiar a proteção dos espaços públicos» [SWD (2019) 140 de 20.3.2019].

- Conceber e aplicar um plano de gestão de crises.

Sensibilização e formação

- Dar início a campanhas de sensibilização do público sobre a comunicação de comportamentos suspeitos e sobre a forma de reagir em caso de ataque que ponha em perigo a segurança de uma instalação ou de um evento;
- Conceber e aplicar um programa de sensibilização para a segurança interna destinado a todos os trabalhadores;
- Conceber e aplicar um programa de sensibilização para as ameaças internas, que ajude a proteger as instalações ou os eventos contra diferentes tipos de ameaças internas, tais como a sabotagem, o roubo comercial ou os atentados terroristas;
- Conceber programas de formação de base em matéria de segurança destinados a todo o pessoal e realizar formações específicas em matéria de segurança, contribuindo assim para o desenvolvimento de uma cultura de segurança nas empresas; desenvolver atividades que motivem os trabalhadores a aplicar boas práticas em matéria de segurança e a manter um elevado nível de vigilância em matéria de segurança; e
- Realizar regularmente exercícios de segurança que contribuam para identificar o nível de preparação necessário para dissuadir e responder a ataques.

Proteção física

- Avaliar os problemas ligados à segurança e à proteção física desde o início do processo de conceção de uma nova instalação ou de um novo evento;
- Determinar os controlos de acesso e barreiras necessários, evitando ao mesmo tempo criar novas vulnerabilidades. Os controlos de acesso e as barreiras não devem transferir os riscos e criar novos alvos;
- Avaliar a tecnologia mais adequada para detetar explosivos, armas de fogo, armas brancas, bem como agentes químicos, biológicos, radiológicos e nucleares.

Cooperação

- Nomear pontos de contacto e clarificar as respetivas funções e responsabilidades a nível da cooperação entre os setores público e privado em matéria de segurança (por exemplo, entre operadores, segurança privada e autoridades de aplicação da lei) para uma melhor comunicação e cooperação numa base regular;
- Estabelecer uma comunicação e cooperação fiáveis e atempadas que permitam o intercâmbio específico de informações sobre riscos e ameaças entre as autoridades públicas responsáveis, as autoridades policiais locais e o setor privado;
- Coordenar os trabalhos sobre a proteção dos espaços públicos a nível local, regional e nacional e participar em atividades de comunicação e de intercâmbio de boas práticas a todos os níveis, incluindo a nível da UE; e
- As autoridades públicas, juntamente com os operadores, devem conceber e disponibilizar recomendações práticas e documentos de orientação para detetar, atenuar ou dar resposta às ameaças à segurança.

3. Vulnerabilidades das infraestruturas digitais

A resiliência digital é crucial para proteger as vastas atividades dos nossos governos, a investigação industrial, a propriedade intelectual, os planos empresariais, as nossas eleições, as instituições democráticas e os nossos próprios dados pessoais. Uma das principais questões ligadas à cibersegurança que suscita uma atenção generalizada no debate público em toda a UE diz respeito às redes de quinta geração (5G). No recente Conselho de Ministros das Telecomunicações informal, realizado em Bucareste em 1 de março de 2019, os ministros

manifestaram o seu apoio a uma abordagem europeia coordenada para reforçar a resiliência digital na UE em relação às redes 5G. A infraestrutura das redes 5G constitui uma base importante para a economia digital. Para além dos serviços ao consumidor, a tecnologia 5G foi concebida e deverá prestar serviços de importância crítica a setores verticais, tais como a mobilidade, a energia e a saúde. As normas relativas às redes 5G são globais e o equipamento e os dispositivos serão disponibilizados por vários fornecedores mundiais.

A implantação de redes 5G nos próximos anos constitui uma mudança radical em relação às redes anteriores. O armazenamento de dados na nuvem permitirá a milhares de milhões de dispositivos da «Internet das coisas» passar a estar conectados, e alimentará as novas inovações no domínio da inteligência artificial, criando assim oportunidades para os cidadãos e as empresas. Por conseguinte, a cibersegurança é particularmente importante, dado que as vulnerabilidades podem ser exploradas e causar danos muito graves. Dado que a Internet não conhece fronteiras, uma violação da segurança num Estado-Membro pode ter repercussões em muitos outros.

A fim de proteger as infraestruturas digitais críticas contra potenciais implicações graves para a segurança, impõe-se uma abordagem comum da UE no tocante à segurança das redes 5G. Para o efeito, na sequência do Conselho Europeu de 21 e 22 de março de 2019, a Comissão formulará uma recomendação em prol de uma abordagem europeia comum dos riscos de segurança das redes 5G, com base numa avaliação coordenada dos riscos na UE e das medidas de gestão dos riscos, um quadro eficaz de cooperação e intercâmbio de informações e uma apreciação comum da situação na UE que abranja as redes de comunicação de importância crítica. O debate sobre as eventuais medidas deve abranger a implantação de tecnologias quânticas para a segurança das redes, bem como para a proteção dos dados armazenados⁷⁴.

Em 12 de março de 2019, o Parlamento Europeu adotou uma resolução sobre as ameaças à segurança no contexto do aumento da presença tecnológica da China na UE e possíveis medidas a tomar a nível da UE para as reduzir.

4. *Questões externas*

As negociações entre a UE e o Canadá relativas à **revisão do Acordo sobre os Registos de Identificação dos Passageiros** estão a avançar a bom ritmo. A próxima Cimeira UE-Canadá, que se realizará em Montreal de 11 a 12 de abril de 2019, poderá dar um impulso positivo às negociações.

A Comissão está a trabalhar com as autoridades dos Estados Unidos na preparação da próxima avaliação conjunta do **Acordo UE-EUA sobre os Registos de Identificação dos Passageiros**⁷⁵, em conformidade com as disposições desse acordo. Estão já em curso trabalhos no âmbito da quinta revisão conjunta do Acordo entre a UE e os EUA relativo ao **Programa de Detecção do Financiamento do Terrorismo**⁷⁶. A revisão conjunta, que inclui a revisão das cláusulas relativas às garantias, controlos e reciprocidade do acordo, servirá igualmente para avaliar o valor do programa enquanto instrumento de luta contra o terrorismo tanto para a UE como para os Estados Unidos.

⁷⁴ Ver também a Comunicação intitulada «Iniciativa Europeia para a Nuvem – Construir uma economia de dados e conhecimento competitiva na Europa» [COM(2016) 178 final de 19.4.2016].

⁷⁵ JO L 215 de 11.8.2012, p. 5.

⁷⁶ JO L 195 de 27.7.2010, p. 5.

A evolução da situação na Síria chamou ainda mais a atenção para o debate sobre os **combatentes terroristas estrangeiros** atualmente presentes ou detidos em zonas de conflito. A UE pode prestar apoio aos Estados-Membros quando estes o solicitarem, nomeadamente no que diz respeito ao intercâmbio de informações e à ajuda no domínio das investigações criminais, em especial a cooperação com parceiros internacionais e através da Europol, bem como com base na experiência e nas melhores práticas em matéria de reabilitação e reintegração desenvolvidas no contexto da Rede de Sensibilização para a Radicalização. A UE pode também ajudar a desenvolver capacidades nos países terceiros particularmente afetados pelos combatentes terroristas estrangeiros que regressam ao país de origem. A decisão de repatriar ou não os combatentes terroristas estrangeiros e as suas famílias das zonas de conflito deve ser tomada pelos Estados-Membros em causa.

A UE e o Egito copresidiram o **Fórum Mundial Contra o Terrorismo** na reunião plenária do Grupo de Trabalho da África Oriental, realizada em Nairobi em 20 de fevereiro de 2019, que contou com uma elevada participação dos setores judiciário e policial da Somália, Quênia, Sudão, Uganda, Jibuti, Etiópia, Iémen e Tanzânia.

V. CONCLUSÃO

A UE realizou progressos consideráveis nos trabalhos conjuntos desenvolvidos rumo a uma União da Segurança genuína e eficaz, graças a uma série de iniciativas legislativas prioritárias adotadas pelo Parlamento Europeu e pelo Conselho ao longo das últimas semanas e meses. No entanto, é necessário envidar mais esforços antes das eleições para o Parlamento Europeu, em maio de 2019, a fim de responder às necessidades de segurança mais urgentes. A Comissão convida os legisladores a encetarem negociações sobre as normas propostas para a remoção de conteúdos terroristas em linha logo que o Parlamento Europeu adote o seu mandato de negociação, com vista a alcançar um acordo ainda durante o presente mandato do Parlamento Europeu. No que se refere à proposta de reforço da Guarda Europeia de Fronteiras e Costeira, as negociações já estão na fase do trílogo, o que demonstra que todas as instituições estão empenhadas em adotar esta proposta antes das eleições para o Parlamento Europeu. A Comissão insta igualmente os Estados-Membros a aplicarem todas as medidas acordadas no âmbito da União da Segurança a fim de garantirem o seu pleno efeito para a segurança de todos os cidadãos.

Além disso, tendo em conta que o tempo urge para garantir a preparação da União antes de os eleitores europeus se dirigirem às urnas, em maio de 2019, a Comissão insta todas as partes envolvidas a redobram esforços para reforçar a resiliência do sistema eleitoral com vista a combater a desinformação. Antes do Conselho Europeu de 21 e 22 de março de 2019, os Estados-Membros devem intensificar a sua coordenação e o intercâmbio de informações para combater a desinformação e proteger as eleições contra outras ameaças possibilitadas pelo ciberespaço, utilizando plenamente os instrumentos que a UE disponibiliza para o efeito. Simultaneamente, as plataformas em linha devem acelerar os seus esforços em todos os Estados-Membros para ajudarem a garantir a integridade das eleições para o Parlamento Europeu em maio de 2019. Com o objetivo de proteger a integridade das referidas eleições, a Comissão continuará a apoiar e a incentivar este trabalho nas próximas semanas e meses.