COMISSÃO
EUROPEIA

Bruxelas, 25.1.2017
COM(2017) 41 final

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

Quarto relatório sobre os progressos alcançados na criação de uma União da Segurança genuína e eficaz

Quarto relatório sobre os progressos alcançados na criação de uma União da Segurança genuína e eficaz

I. INTRODUÇÃO

O presente quarto relatório mensal sobre os progressos alcançados na criação de uma União da Segurança genuína e eficaz traça a evolução da situação no respeitante a dois pilares principais: *lutar contra o terrorismo e a criminalidade organizada e os meios que os apoiam; reforçar as nossas defesas e a resiliência contra tais ameaças*. O presente relatório centra-se em quatro domínios fundamentais: sistemas de informação e interoperabilidade, proteção dos alvos vulneráveis, ciberameaças e proteção de dados no âmbito de investigações criminais.

O atentado contra o mercado de Natal em Berlim, no mês de dezembro, veio uma vez mais pôr a descoberto as graves insuficiências dos nossos sistemas de informação, que temos de resolver urgentemente, em especial a nível da UE, para ajudar as autoridades de fronteira e policiais nacionais no terreno a desempenharem a sua difícil missão de forma mais eficaz. O facto de os diferentes sistemas de informações não estarem interligados — permitindo aos atacantes utilizar múltiplas identidades para circular sem serem detetados, incluindo quando atravessam as fronteiras — e de tais informações não serem sistematicamente descarregadas pelos Estados-Membros para as bases de dados da UE constituem insuficiências de implementação na prática que urge corrigir. Além disso, importa ainda prosseguir o trabalho no que respeita à aplicação de medidas coercivas nas fronteiras e ao regresso de requerentes de asilo cujos pedidos tenham sido rejeitados.[1]

Em termos de proteção de alvos vulneráveis, a Comissão intensificará os trabalhos em curso para reunir peritos dos Estados-Membros com vista a partilhar boas práticas e definir orientações normalizadas.

A ciberameaça com que a UE se depara tem sido objeto de ampla cobertura mediática e o presente relatório analisa as diferentes vertentes do trabalho já em curso neste domínio. Tal abrange quer a prevenção — através da colaboração com a indústria para promover a segurança desde a fase de projeto e da implementação da Diretiva «Segurança das Redes e da Informação» — quer a promoção da cooperação entre os Estados-Membros e com as organizações e parceiros internacionais para reagir a ciberataques no momento em que se produzem. Nos próximos meses, a Comissão e a Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança identificarão as medidas necessárias para assegurar uma resposta eficaz da UE a estas ameaças, com base na Estratégia da UE para a Cibersegurança, de 2013.

A proteção da privacidade e dos dados pessoais é um direito fundamental e, por conseguinte, uma pedra angular de qualquer ação em prol de uma genuína União da Segurança. A Diretiva relativa à proteção de dados destinados às autoridades policiais e judiciais, adotada em abril de 2016, garante um elevado nível de proteção de dados, pelo que facilitará o intercâmbio de dados entre as autoridades com funções coercivas dos Estados-Membros. A Comissão lançou igualmente uma revisão da Diretiva «Privacidade

[1] A Comissão apresentará nas próximas semanas um Plano de Ação revisto em matéria de Regresso; ver relatório da Comissão ao Parlamento Europeu, ao Conselho Europeu e ao Conselho sobre a operacionalização da Guarda Europeia de Fronteiras e Costeira, COM(2017) 42.

e Comunicações Eletrónicas», como parte do seu pacote de medidas sobre dados, a fim de alargar o âmbito de aplicação da diretiva a todos os prestadores de serviços de comunicações eletrónicas e alinhar as suas disposições pelo Regulamento Geral sobre a Proteção de Dados. A proposta pretende assegurar a privacidade das comunicações eletrónicas, definindo, simultaneamente, os fundamentos em que poderão assentar eventuais restrições do âmbito de aplicação do Regulamento relativo à proteção da privacidade nas comunicações eletrónicas, nomeadamente por motivos de segurança nacional ou investigação criminal.

II. REFORÇAR OS SISTEMAS DE INFORMAÇÃO E A INTEROPERABILIDADE

O discurso do Presidente Jean-Claude Juncker sobre o estado da União, de setembro de 2016, e as conclusões do Conselho Europeu de dezembro de 2016 referem a necessidade de corrigir as atuais deficiências da gestão da informação e de melhorar a **interoperabilidade e a interconexão dos sistemas de informação existentes**. Os acontecimentos recentes puseram uma vez mais em evidência a necessidade urgente de ligar as diferentes bases de dados existentes na UE, designadamente para proporcionar às autoridades de fronteira e policiais no terreno os instrumentos necessários para detetar a fraude de identidade. Por exemplo, o autor do atentado terrorista de Berlim, em dezembro de 2016, utilizou pelo menos 14 identidades diferentes e conseguiu passar entre Estados-Membros sem ser detetado. Há que poder efetuar pesquisas em simultâneo nos sistemas de informação existentes e futuros da UE utilizando identificadores biométricos para bloquear esta possibilidade aos terroristas e criminosos.

Nesta perspetiva, a Comissão iniciou os trabalhos em abril de 2016 com as suas propostas relativas a «sistemas de informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a segurança»[2]. Assim, foi possível detetar as deficiências nas funcionalidades dos sistemas existentes, as lacunas na arquitetura de gestão dos dados da UE, os problemas decorrentes de um mosaico complexo de sistemas de informação regidos de formas diferentes e uma fragmentação causada pelo facto de os sistemas existentes terem sido concebidos para funcionar individualmente, e não para se articularem. No âmbito deste processo, a Comissão criou o **Grupo de Peritos de Alto Nível em matéria de Sistemas de Informação e Interoperabilidade** com as agências da UE, os Estados-Membros e as partes interessadas. Em 21 de dezembro de 2016[3], num relatório do seu presidente, o Grupo expôs as suas **conclusões intercalares** que incluíam, como opção prioritária, a criação de um portal único para permitir que as autoridades de fronteira e policiais nacionais efetuem pesquisas em simultâneo nas bases de dados e nos sistemas de informação existentes na UE. O relatório intercalar sublinha igualmente a importância da qualidade dos dados — pois a eficácia dos sistemas de informação depende da qualidade e do formato dos dados que neles são introduzidos — e formula recomendações para melhorar a qualidade dos dados nos sistemas da UE utilizando dispositivos automatizados de controlo da qualidade.

[2] Comunicação «Sistemas de informação mais sólidos e mais inteligentes para controlar as fronteiras e garantir a segurança» COM(2016) 205 final

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

A Comissão dará rapidamente seguimento à opção de criar um portal único de pesquisa e, juntamente com a Agência Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala, eu-LISA, iniciará os seus trabalhos sobre um portal que permita interrogar simultaneamente todos os sistemas existentes na UE. Em junho, deverá estar concluído um estudo que servirá de base para a conceção e ensaio de um protótipo do portal antes do final do ano. A Comissão considera que, em paralelo, a Europol deverá prosseguir os seus trabalhos sobre uma interface de sistemas que permita aos agentes de primeira linha dos Estados-Membros consultar automaticamente e em simultâneo as bases de dados da Europol quando estiverem a consultar os seus próprios sistemas nacionais.

O trabalho com vista à interoperabilidade dos sistemas de informação tem por objetivo superar a atual fragmentação da arquitetura de gestão dos dados para o controlo das fronteiras e a segurança da UE, bem como os ângulos mortos daí decorrentes. Quando as bases de dados utilizam um repositório comum de dados de identificação — tal como previsto para o Sistema de Entrada/Saída da UE e para o Sistema Europeu de Informação e Autorização de Viagem (ETIAS) propostos — uma pessoa só pode estar inscrita com uma única identidade nas diferentes bases de dados, o que impede a utilização de diferentes identidades falsas. Como primeiro passo, tal como sugerido nas conclusões intercalares do grupo de peritos de alto nível, a Comissão pediu à eu-LISA que analisasse os aspetos técnicos e operacionais da aplicação de um serviço partilhado de correspondências biométricas. Tal serviço permitiria efetuar pesquisas em diferentes bases de dados com dados biométricos, que poderiam expor as falsas identidades utilizadas pela pessoa em questão noutro sistema. Além disso, o grupo de peritos de alto nível deve agora apreciar se é necessário, tecnicamente exequível e proporcionado alargar a outros sistemas o **repositório comum de dados de identificação** previsto para o Sistema de Entrada/Saída da UE e o ETIAS. Para além de dados biométricos armazenados no serviço de correspondências biométricas, o repositório comum de dados de identificação incluiria igualmente dados alfanuméricos de identificação. O Grupo deverá apresentar conclusões a este respeito no seu relatório final até ao fim de abril de 2017.

Os recentes acontecimentos no domínio da segurança sublinham a necessidade de reexaminar a questão da **partilha obrigatória de informações** entre Estados-Membros. A proposta da Comissão, de dezembro de 2016, no sentido de se reforçar o **Sistema de Informação de Schengen** prevê, pela primeira vez, a obrigação de os Estados-Membros emitirem alertas relativos a pessoas relacionadas com crimes de terrorismo. É importante que os colegisladores se empenhem agora no sentido da rápida adoção das medidas propostas. A Comissão está pronta a examinar se convém introduzir a partilha obrigatória de informações relativamente a outras bases de dados.

III. PROTEGER OS NOSSOS ALVOS VULNERÁVEIS CONTRA ATENTADOS TERRORISTAS

O atentado de Berlim foi o ataque mais recente contra os chamados alvos vulneráveis da UE, que normalmente são zonas civis onde se junta um grande número de pessoas (espaços públicos, hospitais, escolas, centros culturais, recintos desportivos, cafés e restaurantes, centros comerciais e plataformas de transporte, por exemplo). Estes locais são, pela sua própria natureza, vulneráveis e difíceis de proteger e caracterizam-se igualmente pela forte probabilidade de se verificar um elevado número de vítimas em caso de ataque. É por todas estas razões que são privilegiados pelos terroristas. A ameaça

de futuros ataques contra alvos vulneráveis, nomeadamente transportes, continua a ser elevada, como confirmado pelas avaliações disponíveis, incluindo o relatório da Europol sobre a evolução do *modus operandi*[4] do Daexe.

A Agenda Europeia para a Segurança de 2015 e a comunicação de 2016 sobre a União da Segurança sublinharam a necessidade de intensificar os esforços para melhorar a segurança e utilizar instrumentos e tecnologias de deteção inovadores na proteção de alvos vulneráveis. A Comissão tem-se esforçado por apoiar os Estados-Membros e incentivar a partilha de boas práticas entre Estados-Membros em matéria de desenvolvimento de melhores instrumentos para prevenir e dar resposta a ataques a alvos vulneráveis. Este trabalho permitiu elaborar manuais operacionais e material de orientação. A Comissão está atualmente a desenvolver, em estreita cooperação com peritos dos Estados-Membros, um manual geral sobre os procedimentos e os modelos de segurança aplicáveis a diferentes alvos vulneráveis (centros comerciais, hospitais, instalações desportivas e eventos culturais, por exemplo). O objetivo é formular, no início de 2017, orientações sobre a proteção de alvos vulneráveis destinadas aos Estados-Membros, com base nas melhores práticas nos Estados-Membros.

Em paralelo, a Comissão organizará em fevereiro o primeiro seminário com autoridades nacionais sobre proteção de alvos vulneráveis, com vista a trocar informações e desenvolver as melhores práticas sobre a questão complexa da proteção destes alvos e a ordem e a segurança públicas. A Comissão está também a financiar um projeto-piloto executado pela Bélgica, os Países Baixos e o Luxemburgo ao abrigo do Fundo para a Segurança Interna a fim de estabelecer um centro de excelência regional para intervenções especiais das forças de segurança que ministrará formação a agentes de polícia, que são muitas vezes os primeiros a intervir em caso de atentado.

A resposta aos ataques a alvos vulneráveis é uma componente fundamental do trabalho da Comissão no âmbito da proteção civil. Em dezembro, a Comissão anunciou as ações que tenciona desenvolver com os Estados-Membros para proteger os cidadãos da UE e reduzir a vulnerabilidade imediatamente após um atentado terrorista. Estas ações permitirão reforçar a coordenação entre todos os intervenientes na gestão das consequências de atentados e a Comissão comprometeu-se a apoiar os esforços dos Estados-Membros, facilitando a organização de ações de formação e exercícios conjuntos e assegurando um diálogo permanente através dos pontos de contacto e de grupos de peritos. A Comissão apoiará ainda o desenvolvimento de módulos especializados para reagir a atentados terroristas no âmbito do Mecanismo de Proteção Civil da União e de iniciativas de partilha dos ensinamentos retirados e de sensibilização da opinião pública.

Juntamente com os Estados-Membros, a Comissão irá igualmente analisar que tipo de apoio a UE poderá mobilizar para ajudar a criar resiliência e reforçar a segurança em torno de potenciais alvos vulneráveis. Os Estados-Membros também podem solicitar um financiamento do Banco Europeu de Investimento (BEI), incluindo o Fundo Europeu para Investimentos Estratégicos, em conformidade com o direito da UE e as políticas do Grupo BEI. Os projetos serão sujeitos aos procedimentos normais de tomada de decisões previstos na legislação.

---

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited*, novembro de 2016 — publicação Europol, disponível em: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

No tocante aos alvos vulneráveis específicos em locais públicos de transportes, tais como partes públicas de aeroportos ou estações de caminho de ferro, o seminário que a Comissão consagrou a esta questão, em novembro de 2016, e que reuniu uma vasta gama de partes interessadas, realçou a necessidade de manter o equilíbrio entre as necessidades de segurança, a comodidade dos passageiros e as operações de transporte. As conclusões sublinham a importância de construir uma cultura de segurança que englobe não só o pessoal mas também os passageiros, a importância de avaliações de risco a nível local, como base para definir as medidas de correção adequadas, e a necessidade de melhorar a comunicação entre todas as partes envolvidas.

IV. ENFRENTAR AS AMEAÇAS À CIBERSEGURANÇA

A cibercriminalidade e os ciberataques são os principais desafios que se colocam à União e um domínio em que uma ação a nível da UE pode ajudar a reforçar a nossa resiliência coletiva. Todos os dias se verificam incidentes a nível da cibersegurança que prejudicam gravemente a vida das pessoas, provocando prejuízos económicos consideráveis para a economia e as empresas europeias. Os ciberataques são uma componente essencial das ameaças híbridas que, se combinados de forma precisa com as ameaças físicas, relacionadas com o terrorismo, por exemplo, podem ter um impacto devastador. Podem também contribuir para desestabilizar um país ou pôr em causa as suas instituições políticas e processos democráticos fundamentais. À medida que a dependência das tecnologias em linha vai aumentando, as nossas infraestruturas críticas (desde os hospitais às centrais nucleares) tornam-se cada vez mais vulneráveis.

A estratégia da UE para a Cibersegurança de 2013 faz parte do núcleo de medidas adotadas para dar resposta aos desafios em matéria de cibersegurança. O elemento central é a Diretiva «Segurança das Redes e da Informação» (SRI)[5], adotada em julho. Estabelece as bases para melhorar a cooperação e a ciber-resiliência a nível da UE através do apoio à cooperação e intercâmbio de informações entre Estados-Membros e à promoção da cooperação operacional aquando de incidentes de cibersegurança específicos e da partilha de informações sobre os riscos. Para assegurar a aplicação coerente nos diferentes setores e além-fronteiras, a Comissão organizará a primeira reunião do grupo de cooperação em matéria de SRI com os Estados-Membros em fevereiro.

Em abril de 2016, a Comissão e a Alta Representante adotaram um quadro comum em matéria de luta contra as ameaças híbridas[6] que propunha 22 ações operacionais destinadas a aumentar a sensibilização, reforçar a resiliência, melhorar a resposta às crises e reforçar a cooperação entre a UE e a NATO. Tal como solicitado pelo Conselho, a Comissão e a Alta Representante apresentarão até julho de 2017 um relatório de avaliação dos progressos realizados.

A Comissão está também a promover e apoiar a inovação tecnológica, nomeadamente através do recurso a fundos de investigação da UE, para encontrar novas soluções e criar

[5] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

[6] JOIN (2018)18.

novas tecnologias que possam contribuir para reforçar a nossa resiliência face a ciberataques (por exemplo, incorporando a segurança desde a fase de projeto). No verão passado, lançou uma parceria público-privada no valor de 1800 milhões de euros com a indústria no domínio da cibersegurança[7].

No setor dos transportes, a digitalização está a tornar-se um dos principais elementos da tão necessária transformação do sistema de transportes atual. O ritmo acelerado da digitalização traz muitas vantagens, mas torna também os transportes mais vulneráveis a riscos de cibersegurança. Estão a ser empreendidas numerosas ações destinadas a atenuar as ameaças a diferentes níveis, especialmente do domínio da aviação, mas também nos setores dos transportes marítimos, fluviais, ferroviários e rodoviários[8]. O desafio consiste em continuar a clarificar, harmonizar e completar as atividades dos diferentes intervenientes empenhados no reforço dos diferentes aspetos da ciber-resiliência.

Em termos mais gerais, e tendo em conta a natureza rapidamente evolutiva da ameaça, nos próximos meses a Comissão e a Alta Representante da UE identificarão as medidas necessárias para dar uma resposta eficaz a estas ameaças a nível da UE, com base na Estratégia da União Europeia para a Cibersegurança, de 2013.

V. PROTEGER OS DADOS PESSOAIS, CONTRIBUINDO SIMULTANEAMENTE PARA A EFICÁCIA DAS INVESTIGAÇÕES CRIMINAIS

A diretiva relativa à proteção de dados no domínio da polícia e da justiça penal[9] é uma componente essencial da luta contra o terrorismo e a criminalidade grave. Com base numa norma comum de proteção de dados estabelecida na diretiva, as autoridades policiais dos Estados-Membros poderão trocar regularmente informações pertinentes, enquanto os dados de vítimas, testemunhas e suspeitos de crimes serão devidamente protegidos.

Além disso, a fim de garantir elevado nível de confidencialidade das comunicações, tanto para particulares como para empresas, e condições equitativas para todos os intervenientes no mercado, como previsto na Estratégia para o Mercado Único Digital, de abril de 2015, a Comissão adotou a proposta de **Regulamento «Privacidade e**

---

7 Anunciada na Comunicação sobre ciber-resiliência de 2016, COM(2016) 410 final.

8 Por exemplo, as diretrizes internacionais, tais como as elaboradas pela Organização Marítima Internacional ou através de uma resolução da OACI, recentemente adotada, por iniciativa conjunta da UE e dos EUA; comunicação de incidentes, domínio em que está atualmente a ser desenvolvida uma modalidade mais reativa pela Agência Europeia para a Segurança da Aviação, bem como cibersegurança desde a fase de projeto, aplicável aos novos sistemas que estão a ser desenvolvidos, como o Plano Diretor Europeu de Gestão do Tráfego Aéreo da empresa comum SESAR.

9 Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de crimes ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. A Diretiva, que entrou em vigor em 5 de maio de 2016, deve ser transposta pelos Estados-Membros até 6 de maio de 2018. A Comissão criou um grupo de peritos dos Estados-Membros para a troca de pontos de vista sobre a transposição da Diretiva «Cooperação Policial».

Comunicações Eletrónicas» (que substitui a Diretiva 2002/58/CE), em 11 de janeiro[10]. Tal como no caso da Diretiva em vigor, o Regulamento «Privacidade e Comunicações Eletrónicas» revisto precisa as disposições do Regulamento Geral de Proteção de Dados[11] e estabelece o quadro que rege a proteção da privacidade e dos dados pessoais no setor das comunicações eletrónicas.

Na sequência desta revisão, todos os dados de comunicações eletrónicas, mesmo quando a comunicação é acessória, serão considerados confidenciais/respeitados, quer a comunicação se efetue através dos serviços de telecomunicações tradicionais ou dos chamados serviços OTT (*over-the-top*), que são funcionalmente equivalentes (por exemplo, Skype e WhatsApp) e que, para muitos utilizadores, podem frequentemente substituir os operadores de telecomunicações normais[12]. As obrigações impostas aos prestadores de serviços — para além do respeito pelas opções de privacidade dos seus clientes na utilização, armazenagem e tratamento dos respetivos dados — incluem também a obrigação de os prestadores de serviços sediados fora da UE designarem um representante no território de um Estado-Membro. Tal proporcionará também aos Estados-Membros a possibilidade de facilitar a cooperação entre as autoridades policiais e judiciais e os prestadores de serviços no que respeita ao acesso a provas eletrónicas (ver *infra*).

Tal como acontece ao abrigo das normas em vigor em matéria de privacidade e comunicações eletrónicas, o acesso por parte das autoridades policiais e judiciais às informações eletrónicas necessárias para investigar crimes é regido pela exceção prevista no artigo 11.º da proposta de Regulamento «Privacidade e Comunicações Eletrónicas»[13]. Esta disposição confere a possibilidade, no direito da UE ou no direito nacional, de restringir a confidencialidade das comunicações, quando necessário e proporcionado, para salvaguardar a segurança nacional, a defesa e a segurança pública, bem como para efeitos de prevenção, investigação, deteção e repressão de crimes ou de execução de sanções penais. Esta disposição é especialmente pertinente no que respeita às normas nacionais em matéria de **conservação de dados**, ou seja, para obrigar os prestadores de serviços de telecomunicações a conservarem os dados das comunicações por período determinado com vista ao eventual acesso por parte das autoridades policiais, na sequência da anulação da Diretiva «Conservação de Dados» pelo Tribunal de Justiça, em 2014[14]. Desde então, não foi adotado nenhum instrumento da UE relativo à conservação de dados e alguns Estados-Membros adotaram a sua própria legislação nesta matéria. As leis da Suécia e do Reino Unido em matéria de conservação de dados foram contestadas

---

10 Regulamento «Privacidade e Comunicações Eletrónicas», COM(2017) 10.

11 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados – RGPD), aplicável a partir de 25 de maio de 2018.

12 Trata-se da mesma abordagem seguida na proposta de Diretiva que estabelece o Código Europeu das Comunicações Eletrónicas, apresentada pela Comissão em 14 de setembro de 2016 (Pacote «telecomunicações»), COM(2016) 590 final.

13 Ver artigo 11.º, n.º 1, a cláusula sobre «conservação de dados», que se mantém inalterada em relação ao artigo 15.º da Diretiva «Privacidade e Comunicações Eletrónicas» e está alinhada pelos requisitos do Regulamento Geral sobre a Proteção de Dados. Essas restrições têm de respeitar o conteúdo essencial dos direitos fundamentais e ser necessárias, adequadas e proporcionadas.

14 Acórdão do Tribunal de Justiça nos processos apensos C-293/12 e C-594/12, *Digital Rights Ireland*, de 8 de abril de 2014.

junto do Tribunal de Justiça, que proferiu o acórdão do processo *Tele2* em 21 de dezembro[15]. O Tribunal de Justiça da União Europeia considerou incompatível com o direito da União a legislação nacional que, para combater o crime, preveja a conservação geral e indiscriminada de todos os dados de tráfego e de localização dos assinantes e utilizadores de todos os meios de comunicação eletrónicos. As implicações do acórdão estão a ser analisadas e a Comissão tenciona elaborar orientações sobre a forma de redigir legislação nacional em matéria de conservação de dados em conformidade com o acórdão.

O crime deixa um rasto digital que pode servir como prova em processos judiciais; as comunicações eletrónicas entre suspeitos são frequentemente os únicos indícios que as autoridades policiais e os procuradores podem recolher. No entanto, o acesso a **elementos de prova eletrónicos** — especialmente se estiverem armazenados no estrangeiro ou num serviço de computação em nuvem — pode revelar-se complexo do ponto de vista técnico e jurídico e, muitas vezes, moroso em termos processuais, impedindo os investigadores de avançar com a celeridade necessária. Para ultrapassar estes obstáculos, a Comissão está atualmente a ponderar soluções para permitir aos investigadores obter provas eletrónicas transfronteiras, designadamente através de assistência jurídica mútua mais eficaz e de modalidades de cooperação direta com fornecedores de serviços Internet, e propor critérios para a determinação e aplicação da competência jurisdicional no ciberespaço, em plena conformidade com as normas aplicáveis em matéria de proteção de dados.[16]A Comissão apresentou um relatório sobre os progressos realizados ao Conselho «Justiça e Assuntos Internos», em 9 de dezembro de 2016[17].

O vasto processo de consulta de peritos (ainda em curso) permitiu à Comissão identificar os diferentes problemas, muitas vezes complexos, suscitados pelo acesso a elementos de prova eletrónicos, compreender melhor as atuais regras e práticas nos Estados-Membros e identificar os meios de ação possíveis. O relatório apresenta uma panorâmica das ideias que surgiram até à data durante o processo de recolha de informações e de consulta de peritos, e que a Comissão, em consulta com as partes interessadas, analisará mais pormenorizadamente nos próximos meses. Tal como anunciado no programa de trabalho, a Comissão apresentará uma iniciativa em 2017.

VI. CONCLUSÃO

O próximo relatório, previsto para 1 de março, representará uma oportunidade para analisar os progressos realizados na implementação destas e de outras importantes vertentes de trabalho.

---

15 Acórdão do Tribunal de Justiça nos processos apensos C−203/15 e C−698/15, *Tele 2*, de 21 de dezembro de 2016.

16 Tal como anunciado na Agenda Europeia para a Segurança, COM(2015) 185 final, e na Comunicação da Comissão «Dar cumprimento à Agenda Europeia para a Segurança para combater o terrorismo e abrir caminho à criação de uma União da Segurança genuína e eficaz», COM(2016) 230 final.

17 Nas conclusões sobre a melhoria da justiça penal no ciberespaço, de 9 de junho de 2016, o Conselho convidou a Comissão a tomar medidas concretas, a desenvolver uma abordagem comum da UE e a produzir resultados até junho de 2017.