COMISSÃO
EUROPEIA

Bruxelas, 24.7.2020
COM(2020) 605 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

sobre a Estratégia da UE para a União da Segurança

I. Introdução

As orientações políticas da Comissão deixaram bem claro que não podemos poupar esforços quando se trata de proteger os nossos cidadãos. A segurança não apenas é a base da proteção pessoal, mas protege também direitos fundamentais e constitui os alicerces da confiança e do dinamismo da nossa economia, da nossa sociedade e da nossa democracia. Os europeus enfrentam hoje um panorama fluido no que toca à segurança, afetado por ameaças em permanente evolução, bem como por outros fatores, designadamente as alterações climáticas, as tendências demográficas e a instabilidade política fora das nossas fronteiras. A globalização, a livre circulação e a transformação digital continuam a trazer prosperidade, a tornar as nossas vidas mais fáceis e a estimular a inovação e o crescimento. Mas estes benefícios comportam riscos e custos. Podem ser manipuladas pelo terrorismo, pela criminalidade organizada, pelo tráfico de droga e pelo tráfico de seres humanos, que constituem ameaças diretas aos cidadãos e ao nosso modo de vida europeu. Os ciberataques e a cibercriminalidade continuam a aumentar. As ameaças à segurança estão, por outro lado, a tornar-se mais complexas: valem-se das potencialidades do trabalho transfronteiriço e da interconectividade; exploram a indefinição das fronteiras entre o mundo físico e o mundo digital; aproveitam-se dos grupos vulneráveis e das divergências sociais e económicas. Os ataques podem ocorrer sem aviso prévio e podem deixar poucos ou nenhuns vestígios; os intervenientes tanto estatais, como não estatais, podem recorrer a uma grande variedade de ameaças híbridas[1] e o que acontece fora da UE pode ter repercussões particularmente graves na segurança da UE.

A crise provocada pela pandemia de COVID-19 também modificou a nossa conceção de ameaças à segurança e as políticas correspondentes. Assinalou a necessidade de garantir a segurança tanto no contexto físico como digital. Sublinhou a importância de uma autonomia estratégica aberta das nossas cadeias de aprovisionamento em termos de produtos, serviços, infraestruturas e tecnologias críticos. Reforçou a necessidade de mobilizar todos os setores e todos os cidadãos num esforço comum para garantir que a UE está, à partida, mais preparada e resiliente e dispõe de melhores instrumentos para responder, quando necessário.

A proteção dos cidadãos não pode ser alcançada através de ações isoladas dos Estados-Membros. Tirar partido dos nossos pontos fortes para trabalhar em conjunto nunca foi tão essencial, e a UE nunca teve tanto potencial para fazer a diferença. Pode dar o exemplo, reforçando o seu sistema global de gestão de crises e trabalhando dentro e fora das suas fronteiras para contribuir para a estabilidade mundial. Embora a responsabilidade pela segurança caiba em primeiro lugar aos Estados-Membros, os anos mais recentes mostraram de forma cada vez mais evidente que a segurança de um Estado-Membro depende da segurança de todos. A UE pode dar uma resposta multidisciplinar e integrada, ajudando os intervenientes no domínio da segurança nos Estados-Membros com os instrumentos e as informações de que necessitam[2].

A UE pode também assegurar que a política de segurança continua assente nos nossos valores comuns europeus - respeitando e defendendo o Estado de direito, a igualdade[3] e os direitos fundamentais e garantindo a transparência, a responsabilização e o controlo democrático - para dar às políticas a base correta da confiança. Pode criar uma União da Segurança genuína e eficaz, na qual os direitos e liberdades das pessoas são bem protegidos. A segurança e o respeito dos direitos fundamentais não são objetivos incompatíveis, mas sim coerentes e complementares. Os nossos valores e direitos fundamentais devem constituir a base das políticas de segurança, assegurando o

[1] Embora as definições de ameaças híbridas variem, em geral, estas visam captar a combinação de atividades coercivas e atividades subversivas, de métodos convencionais e não convencionais (isto é, diplomáticos, militares, económicos, tecnológicos), que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para alcançar objetivos específicos (permanecendo a um nível inferior ao limiar de uma guerra formalmente declarada). Ver JOIN(2016) 18 (final).

[2] Por exemplo, através dos serviços prestados pelo programa espacial da UE, como o Copernicus, que fornece dados de observação da Terra e aplicações para a vigilância das fronteiras, a segurança marítima, a aplicação da lei, a luta contra a pirataria e o contrabando de droga, bem como a gestão de emergências.

[3] Uma União da Igualdade: Estratégia para a Igualdade de Género 2020-2025, COM (2020) 152.

respeito dos princípios da necessidade, da proporcionalidade e da legalidade, com as salvaguardas adequadas em termos de responsabilização e de recursos judiciais, permitindo simultaneamente uma resposta eficaz de proteção das pessoas, em especial das mais vulneráveis.

Já existem instrumentos jurídicos, práticos e de apoio significativos, mas estes têm de ser reforçados e aplicados de forma mais eficaz. Foram realizados muitos progressos no sentido de melhorar o intercâmbio de informações e a cooperação com os Estados-Membros em matéria de serviços de informação e de restringir o perímetro de ação dos terroristas e dos criminosos. Mas os esforços continuam a ser fragmentados.

A nossa ação deve ultrapassar as fronteiras da UE. Proteger a União e os seus cidadãos já não é apenas garantir a segurança dentro das fronteiras da UE, mas também abordar a dimensão externa da segurança. A abordagem da UE em matéria de segurança externa no âmbito da Política Externa e de Segurança Comum (PESC) e da Política Comum de Segurança e Defesa (PCSD) continuará a ser uma componente essencial dos esforços da UE para reforçar a segurança na União. A cooperação com os países terceiros e a nível mundial para fazer face a desafios comuns é fundamental para uma resposta eficaz e abrangente, sendo a estabilidade e a segurança das zonas vizinhas da UE crucial para a própria segurança da UE.

Com base nos trabalhos anteriores do Parlamento Europeu[4], do Conselho[5] e da Comissão[6], esta nova estratégia mostra que uma União da Segurança genuína e eficaz tem de combinar um núcleo de políticas e instrumentos sólidos para garantir a segurança na prática com o reconhecimento de que a segurança tem implicações para todos os setores da sociedade e em todas as políticas públicas. A UE deve assegurar um ambiente seguro para todos, independentemente da sua raça ou origem étnica, religião, crença, género, idade ou orientação sexual.

A presente estratégia abrange o período 2020-2025 e centra-se no reforço das capacidades e recursos para garantir um ambiente de segurança a longo prazo. Estabelece uma abordagem da segurança que mobiliza toda a sociedade suscetível de responder eficazmente a um cenário de ameaça em rápida mutação de uma forma coordenada. Define as prioridades estratégicas e as ações correspondentes para fazer face aos riscos digitais e físicos de uma forma integrada em todo o ecossistema da União da Segurança, concentrando-se nos domínios em que a UE pode acrescentar valor. O seu objetivo é proporcionar um dividendo de segurança para proteger todas as pessoas na UE.

II. Um cenário europeu de ameaças à segurança em rápida mutação

A proteção, a prosperidade e o bem-estar dos cidadãos dependem da segurança. As ameaças à segurança dos cidadãos dependem do grau de vulnerabilidade das suas vidas e dos seus meios de subsistência. Quanto maior for a vulnerabilidade, maior é o risco de alguém se aproveitar. Tanto as vulnerabilidades como as ameaças estão em constante evolução e a UE tem de se adaptar.

A nossa vida quotidiana depende de uma grande variedade de serviços, como a energia, os transportes, as finanças ou a saúde. Estes dependem de infraestruturas físicas e digitais, o que aumenta a vulnerabilidade e o potencial de perturbação. Durante a pandemia de COVID-19, as novas tecnologias mantiveram em funcionamento muitas empresas e serviços públicos, quer mantendo os cidadãos conectados para poderem trabalhar à distância, quer mantendo a logística das cadeias de aprovisionamento. Mas esta situação também abriu a porta a um aumento extraordinário de ataques

[4] Por exemplo, os trabalhos da Comissão TERR do Parlamento Europeu, que apresentou um relatório em novembro de 2018.

[5] Desde as conclusões do Conselho de junho de 2015 sobre uma «estratégia renovada de segurança» até às mais recentes conclusões do Conselho de dezembro de 2019.

[6] «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. Ver a recente avaliação da aplicação da legislação no domínio da segurança interna: Aplicação da legislação relativa aos assuntos internos no domínio da segurança interna - 2017-2020 (SWD(2020) 135).

maliciosos, tentando aproveitar a perturbação da pandemia e a transição para o trabalho digital em casa para fins criminosos[7]. A escassez de bens criou novas oportunidades para a criminalidade organizada. As consequências poderiam ter sido fatais, podendo ter criado interrupções nos serviços de saúde essenciais no momento de máxima pressão.

O aumento constante dos benefícios que as tecnologias digitais trazem às nossas vidas também tornou a **cibersegurança** das tecnologias uma questão de importância estratégica[8]. As casas, os bancos, os serviços financeiros e as empresas (nomeadamente as pequenas e médias empresas) são fortemente afetados por ciberataques. Os danos potenciais são ainda multiplicados pela interdependência dos sistemas físicos e digitais: qualquer impacto físico afeta os sistemas digitais, e os ciberataques aos sistemas de informação e às infraestruturas digitais podem causar interrupções nos serviços essenciais[9]. O aumento da Internet das coisas e o aumento da utilização da inteligência artificial trarão novos benefícios, bem como novos riscos.

O nosso mundo assenta em infraestruturas e tecnologias digitais e em sistemas em linha, que nos permitem criar oportunidades de negócio, consumir produtos e usufruir de serviços. Todos estas atividades dependem da comunicação e da interação. A dependência da atividade em linha abriu as portas a uma vaga de **cibercriminalidade**[10]. A «cibercriminalidade como serviço» e a economia cibercriminosa subterrânea concedem um acesso fácil aos produtos e serviços da cibercriminalidade em linha. Os criminosos adaptam-se rapidamente à utilização das novas tecnologias para fins próprios. Por exemplo, medicamentos contrafeitos e falsificados foram introduzidos na cadeia de abastecimento legal de produtos farmacêuticos[11]. O crescimento exponencial do material em linha com imagens de abusos sexuais de crianças[12] revelou as consequências sociais da evolução das atividades da criminalidade. Um inquérito recente revelou que a maioria das pessoas na UE (55 %) está preocupada com o facto de criminosos e autores de fraudes terem acesso aos seus dados[13].

O **contexto a nível mundial** também acentua estas ameaças. As políticas industriais assertivas adotadas por países terceiros, combinadas com o roubo continuado dos direitos de propriedade intelectual possibilitado pelo ciberespaço, estão a alterar o paradigma estratégico de proteção e promoção dos interesses europeus. Esta situação é acentuada pelo aumento das aplicações de dupla utilização, fazendo com que a existência de um forte setor tecnológico civil seja um valioso ativo para a capacidade de defesa e segurança. A espionagem industrial tem um impacto significativo na economia, no emprego e no crescimento da UE: estima-se que o ciberfurto de segredos comerciais

---

7 Europol: *Beyond the pandemic*. *How COVID-19 will shape the serious and organised crime landscape in the EU* - Para além da pandemia. Como a COVID-19 transformará o panorama da criminalidade grave e organizada na UE (abril de 2020).

8 Recomendação da Comissão intitulada: «Cibersegurança das redes 5G», C(2019) 2335; Comunicação intitulada: «Implantação segura de redes 5G na UE – Aplicação do conjunto de instrumentos da UE», COM(2020) 50.

9 Em março de 2020, o Hospital Universitário de Brno, na Chéquia, foi vítima de um ciberataque que o obrigou a reencaminhar doentes e a adiar cirurgias (Europol: *Pandemic Profiteering*. *How criminals exploit the COVID-19 crisis* - Aproveitar-se da pandemia: Como a criminalidade explora a crise da COVID-19). A inteligência artificial pode ser utilizada de forma abusiva para ataques digitais, políticos e físicos, bem como para efeitos de vigilância. A recolha de dados da Internet das coisas pode ser utilizada para a vigilância de pessoas (relógios inteligentes, assistentes virtuais, etc.).

10 De acordo com algumas projeções, os custos das violações de dados atingirão os 5 biliões de dólares anuais até 2024, contra 3 biliões de dólares em 2015 (Juniper Research, *The Future of Cybercrime & Security*).

11 Um estudo de 2016 (Legiscript) estimou que, a nível mundial, apenas 4 % das farmácias Internet operam de forma lícita, sendo os consumidores da UE os alvos mais importantes das 30 000-35 000 farmácias ilícitas ativas em linha.

12 Estratégia da UE a favor de uma luta mais eficaz contra o abuso sexual de crianças, COM (2020) 607.

13 Agência dos Direitos Fundamentais da União Europeia (2020), *Your rights matter*: *Security concerns and experiences*, *Fundamental Rights Survey* - Os seus direitos: Preocupações e experiências em matéria de segurança, Luxemburgo, Serviço das Publicações.

custa à UE 60 mil milhões de EUR[14]. Tal exige uma reflexão profunda sobre a forma como as dependências e o aumento da exposição às ciberameaças afetam a capacidade da UE de proteger tanto as pessoas como as empresas.

A crise da COVID-19 pôs também em evidência a forma como as fraturas e as incertezas sociais criam vulnerabilidade em termos de segurança. Este facto aumenta o potencial de **ataques** mais sofisticados e **híbridos** por parte de intervenientes estatais e não estatais, com vulnerabilidades exploradas através de uma combinação de ciberataques, danos em infraestruturas críticas[15], campanhas de desinformação e radicalização do discurso político[16].

Ao mesmo tempo, as ameaças tradicionais continuam a evoluir. Em 2019, verificou-se uma tendência decrescente nos **atentados terroristas** na UE. No entanto, a ameaça para os cidadãos da UE de ataques jiadistas pelo Daexe e pela Alcaida e seus membros, ou inspirados por estas organizações, continua a ser elevada[17]. Paralelamente, está também a aumentar a ameaça do extremismo violento de direita[18]. Os ataques inspirados pelo racismo são motivo de grande preocupação: os atentados terroristas antissemitas mortais em Halle recordam a necessidade de intensificar a resposta, em conformidade com a Declaração do Conselho de 2018[19]. Uma em cada cinco pessoas na UE está muito preocupada com um ataque terrorista nos próximos 12 meses[20]. A grande maioria dos recentes ataques terroristas foram ataques de «baixa tecnologia», cometidos por elementos isolados visando pessoas em espaços públicos, enquanto a propaganda terrorista em linha adquiriu um novo significado com a transmissão em direto dos ataques de Christchurch.[21]. A ameaça representada por elementos radicalizados continua a ser elevada - potencialmente reforçada pelo regresso de combatentes terroristas estrangeiros e por extremistas libertados das prisões[22].

A crise demonstrou também a forma como as ameaças existentes podem evoluir em novas circunstâncias. Os grupos de **criminalidade organizada** exploraram a escassez de bens que proporcionou uma oportunidade para a criação de novos mercados ilícitos. O comércio de drogas ilícitas continua a ser o maior mercado criminoso na UE, com um valor mínimo estimado de 30 mil milhões de EUR por ano de vendas a retalho na UE.[23]. O tráfico de seres humanos persiste: as estimativas mostram um lucro global anual relativamente a todas as formas de exploração de quase 30 mil milhões de EUR[24]. O comércio internacional de produtos farmacêuticos falsificados atingiu o

---

14 A escala e o impacto da espionagem industrial e o roubo de segredos comerciais através do ciberespaço, 2018.

15 As infraestruturas críticas são essenciais para as funções vitais da sociedade, como a saúde, a segurança e o bem-estar económico ou social, cuja perturbação / destruição tem um impacto significativo (Diretiva 2008/114/EC do Conselho).

16 97 % dos cidadãos da UE têm sido confrontados com notícias falsas, 38 % numa base diária. Ver JOIN (2020) 8 final.

17 13 Estados-Membros da UE comunicaram um total de 119 ataques terroristas levados a cabo, falhados ou evitados, com dez mortes e 27 feridos (Europol, Situação e tendências do terrorismo na União Europeia, 2020).

18 Em 2019, foram perpetrados seis atentados terroristas de extrema direita (um levado a cabo, um falhado e quatro evitados, em três Estados-Membros), em comparação com apenas um em 2018, com outras mortes em casos não classificados como terrorismo (Europol, 2020).

19 Ver também a Declaração do Conselho sobre o combate ao antissemitismo e o desenvolvimento de uma abordagem de segurança comum para melhor proteger as comunidades e instituições judaicas na Europa.

20 Agência dos Direitos Fundamentais da UE: *Your rights matter*: *Security concerns and experiences*, 2020.

21 Desde julho de 2015 até ao final de 2019, a Europol encontrou conteúdos terroristas em 361 plataformas (Europol, 2020).

22 Europol: *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism* - Uma análise das melhores práticas transatlânticas de combate à radicalização nas prisões e da reincidência do terrorismo, 2019.

23 OEDT e Europol, *EU Drugs Market Report 2019* (Relatório sobre os mercados de droga na UE, 2019).

24 Relatório da Europol de 2015 sobre o modelo económico financeiro do tráfico de seres humanos.

montante de 38,9 mil milhões de EUR[25]. Ao mesmo tempo, as baixas taxas de confisco permitem que os criminosos continuem a expandir as suas atividades criminosas e a infiltrar a economia legal[26]. Os criminosos e os terroristas têm mais facilidade em ter acesso a armas de fogo no mercado em linha e através de novas tecnologias, como a impressão 3-D[27]. A utilização da inteligência artificial, das novas tecnologias e da robótica aumentará ainda mais o risco de os criminosos explorarem os benefícios da inovação com maus intuitos[28].

Estas ameaças abrangem várias categorias e atingem diferentes partes da sociedade de formas diferentes. Todos elas representam uma grande ameaça para os indivíduos e as empresas e exigem uma resposta abrangente e coerente a nível da UE. Quando as vulnerabilidades a nível da segurança podem provir de pequenos artigos domésticos interligados, como um frigorífico ou uma máquina de café ligados à Internet, já não podemos contar apenas com os organismos tradicionais do Estado para garantir a nossa segurança. Os operadores económicos devem assumir uma maior responsabilidade pela cibersegurança dos produtos e serviços que colocam no mercado; por outro lado, as pessoas também precisam de ter, pelo menos, uma compreensão básica da cibersegurança para poderem proteger-se a si próprios.

III. Uma resposta coordenada da UE englobando o conjunto da sociedade

A UE já demonstrou como pode acrescentar valor. Desde 2015, a União da Segurança trouxe novas ligações na forma como as políticas de segurança são abordadas a nível da UE. Mas há ainda muito a fazer para mobilizar toda a sociedade, incluindo os governos a todos os níveis, as empresas de todos os setores e as pessoas em todos os Estados-Membros. A crescente sensibilização para os riscos de dependência[29] e a necessidade de uma estratégia industrial europeia forte[30] apontam para uma UE com massa crítica em termos de indústria, de produção de tecnologia e de resiliência da cadeia de aprovisionamento. A solidez significa também o pleno respeito dos direitos fundamentais e dos valores da UE: estes constituem um pré-requisito para políticas de segurança legítimas, eficazes e sustentáveis. A presente estratégia da União da Segurança estabelece planos de trabalho concreto a realizar. Articula-se em torno dos seguintes objetivos comuns:

- ***Criar aptidões e capacidades de deteção precoce, prevenção e resposta rápida a situações de crise:*** A Europa precisa de ser mais resiliente para prevenir, proteger e resistir a choques futuros. Precisamos de criar aptidões e capacidades de deteção precoce, prevenção e resposta rápida a situações de crise através de uma abordagem integrada e coordenada, tanto globalmente como mediante iniciativas setoriais específicas (tais como as iniciativas para os setores financeiro, da energia, judiciário, policial, da saúde, marítimo e dos transportes) e construir a partir de instrumentos e iniciativas já existentes[31]. A Comissão também apresentará propostas

[25] Instituto da Propriedade Intelectual da UE e relatório da OCDE sobre o comércio de produtos farmacêuticos falsificados

[26] Relatório intitulado «Recuperação e perda de bens: garantir que o crime não compensa, COM (2020) 217.

[27] Em 2017, foram utilizadas armas de fogo em 41 % de todos os ataques terroristas (Europol, 2018).

[28] Em julho de 2020, as autoridades policiais e judiciais francesas e neerlandesas, juntamente com a Europol e a Eurojust, apresentaram uma investigação conjunta para desmantelar EncroChat, uma rede telefónica cifrada utilizada por redes criminosas envolvidas em ataques violentos, corrupção, tentativas de homicídios e grandes transportes de droga.

[29] Os riscos de dependência externa implicam uma maior exposição a potenciais ameaças, desde a exploração das vulnerabilidades das infraestruturas informáticas suscetíveis de comprometer as infraestruturas críticas (por exemplo, energia, transportes, banca, saúde) ou a apropriação dos sistemas de controlo industrial, até um aumento da capacidade de roubo de dados ou de espionagem.

[30] Comunicação da Comissão - Uma nova estratégia industrial para a Europa, COM (2020) 102.

[31] Como o Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR), o Centro de Coordenação de Resposta de Emergência, a Recomendação da Comissão sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (C(2017)6100) e o Protocolo operacional da UE para fazer face às ameaças híbridas, «EU Playbook», SWD(2016) 227.

para um sistema de gestão de crises mais ambicioso e abrangente na UE, que poderá ter igualmente incidência na segurança.

- ***Centrar-se nos resultados***: Uma estratégia centrada no desempenho deve basear-se numa avaliação cuidadosa das ameaças e dos riscos, a fim de orientar os nossos esforços para a obtenção dos melhores resultados. Tem de definir e aplicar as regras e os instrumentos adequados e precisa de informações estratégicas fiáveis como base para as políticas de segurança da UE. Nos casos em que é necessária legislação da UE, esta deve ser acompanhada de forma a que seja aplicada na íntegra, a fim de evitar a fragmentação e as lacunas suscetíveis de serem exploradas. A execução eficaz desta estratégia dependerá também da garantia de um financiamento adequado no próximo período de programação 2021-2027, incluindo para as agências da UE envolvidas.
- ***Associar todos os intervenientes dos setores público e privado num esforço comum:*** Os principais intervenientes dos setores público e privado têm mostrado relutância em partilhar informações relevantes para a segurança por receio de comprometer a segurança nacional ou a sua competitividade.[32] No entanto, somos mais eficazes quando canalizamos os nossos esforços para nos apoiarmos uns aos outros. Em primeiro lugar, tal significa uma cooperação mais estreita entre os Estados-Membros, envolvendo as autoridades policiais, judiciais e outras autoridades públicas, e com as instituições e agências da UE, a fim de desenvolver a compreensão e o intercâmbio necessários para a consecução de soluções comuns. A cooperação com o setor privado é também fundamental, tanto mais que a indústria detém uma parte importante das infraestruturas digitais e não digitais essenciais para combater eficazmente a criminalidade e o terrorismo. As próprias pessoas também podem contribuir através, por exemplo, do desenvolvimento das competências e da sensibilização para combater a cibercriminalidade ou a desinformação. Por último, este esforço comum deve estender-se para além das nossas fronteiras, criando laços mais estreitos com os parceiros que partilham as mesmas ideias.

IV. Proteger todos na UE: prioridades estratégicas para a União da Segurança

A UE está excecionalmente bem colocada para responder a estas novas ameaças e desafios globais. A análise das ameaças acima referidas aponta para quatro prioridades estratégicas interdependentes a apresentar a nível da UE, no pleno respeito dos direitos fundamentais: i) um ambiente de segurança a longo prazo, ii) fazer face à evolução das ameaças, iii) proteger os europeus do terrorismo e da criminalidade organizada, iv) um sólido ecossistema de segurança.

1. Um ambiente de segurança a longo prazo

Proteção e resiliência das infraestruturas críticas

As pessoas dependem de infraestruturas essenciais na sua vida quotidiana para se deslocar, trabalhar, beneficiar de serviços públicos essenciais, como hospitais, transportes, fornecimentos de energia, ou para exercer os seus direitos democráticos. Se estas infraestruturas não estiverem suficientemente protegidas e não forem resilientes, os ataques podem causar enormes perturbações - físicas ou digitais - tanto num Estado-Membro como, potencialmente, em toda a UE.

O atual enquadramento da UE para a proteção e a resiliência das infraestruturas críticas[33] não tem acompanhado a evolução dos riscos. O aumento das interdependências significa que as perturbações

[32] Comunicação conjunta intitulada «Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE», JOIN(2017) 450.

[33] Diretiva (UE) 2016/1148 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, JO L 194 de 19.7.2016; Diretiva 2008/114/CE do Conselho

num setor podem ter uma repercussão imediata nas atividades de outros: um ataque à produção de eletricidade pode afetar as telecomunicações, os hospitais, os bancos ou os aeroportos, e um ataque a infraestruturas digitais pode causar perturbações nas redes de energia ou financeiras. À medida que a nossa economia e a nossa sociedade evoluem cada vez mais para atividades em linha, os riscos como estes aumentam. O quadro legislativo deve abordar esta maior interconexão e interdependência, com medidas eficazes para proteger e dar mais resiliência às infraestruturas críticas, tanto cibernéticas como físicas. Os serviços essenciais, incluindo os baseados em infraestruturas espaciais, devem ser adequadamente protegidos contra ameaças atuais e previsíveis, mas também devem ser resilientes. Isto implica a capacidade de um sistema de preparar e planear, de absorver, de recuperar e de se adaptar a eventualidades adversas.

Ao mesmo tempo, os Estados-Membros exerceram a sua margem de discricionariedade aplicando a legislação existente de diferentes formas. A fragmentação decorrente deste facto pode comprometer o mercado interno e tornar a coordenação transnacional mais difícil - sobretudo nas regiões fronteiriças. Os operadores que prestam serviços essenciais em diferentes Estados-Membros têm de observar diferentes regimes de comunicação de informações. A Comissão está a analisar se os **novos enquadramentos para as infraestruturas físicas e digitais** poderão estabelecer uma abordagem mais consistente e mais coerente de modo a garantir a prestação fiável de serviços essenciais. Os referidos enquadramentos devem ser acompanhados de **iniciativas setoriais específicas** para fazer face aos riscos específicos com que se deparam as infraestruturas críticas, como os transportes, a infraestrutura espacial, a energia, as finanças e a saúde[34]. Dada a elevada dependência do setor financeiro dos serviços informáticos e tendo em conta a sua elevada vulnerabilidade aos ciberataques, um primeiro passo será a adoção de uma iniciativa sobre a resiliência operacional digital dos setores financeiros. Devido às sensibilidades particulares e ao impacto do sistema energético, uma iniciativa específica apoiará uma maior resiliência das infraestruturas energéticas críticas contra ameaças físicas, cibernéticas e híbridas, garantindo condições de concorrência equitativas para os operadores energéticos transfronteiriços.

Os efeitos relevantes para a segurança dos investimentos diretos estrangeiros suscetíveis de afetar infraestruturas ou tecnologias críticas serão também sujeitos às avaliações efetuadas pelos Estados-Membros da UE e pela Comissão no âmbito do novo quadro europeu para a análise dos investimentos diretos estrangeiros.[35].

A UE pode também criar novos instrumentos para apoiar a resiliência das infraestruturas críticas. A Internet global demonstrou até agora um elevado nível de resiliência, em especial no que diz respeito à capacidade de suportar o aumento do volume de tráfego. No entanto, precisamos de estar preparados para eventuais crises futuras que ameacem a segurança, a estabilidade e a resiliência da Internet, assegurando que esta continua a ser um instrumento sólido contra os ciberincidentes e as atividades maliciosas em linha e limita a dependência em relação a infraestruturas e serviços localizados fora da Europa. Tal implicará adotar nova legislação e rever as regras existentes para garantir um elevado nível comum de segurança das redes e dos sistemas de informação na UE;

---

relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção.

[34] Tendo em conta que o setor da saúde tem estado sob pressão, em especial durante a crise da COVID-19, a Comissão irá também ponderar a adoção de iniciativas destinadas a reforçar o quadro de segurança do setor da saúde da UE e das agências competentes da UE para dar resposta a ameaças sanitárias transfronteiriças graves.

[35] Com a sua entrada em vigor em 11 de outubro de 2020, o Regulamento (UE) 2019/452 do Parlamento Europeu e do Conselho, de 19 de março de 2019, que estabelece um quadro para a análise dos investimentos diretos estrangeiros na União, dotará a UE de um novo mecanismo de cooperação para investimentos diretos provenientes de países terceiros suscetíveis de afetar a segurança ou a ordem pública. Nos termos do referido regulamento, os Estados-Membros e a Comissão avaliarão os riscos potenciais associados a esse investimento direto estrangeiro e, sempre que adequado e relevante para mais do que um Estado-Membro, propõem os meios adequados para atenuar esses riscos.

investir mais na investigação e na inovação; e prever a implantação ou o reforço de infraestruturas e recursos fundamentais da Internet, nomeadamente o Sistema de Nomes de Domínio[36].

Um elemento fundamental para proteger os principais ativos digitais da UE e nacionais é oferecer às infraestruturas críticas um canal para comunicações seguras. A Comissão está a trabalhar com os Estados-Membros para criar uma infraestrutura quântica de extremo a extremo, segura e certificada, terrestre e espacial, em combinação com o sistema de comunicações por satélite seguras para entidades governamentais previsto no regulamento relativo ao programa espacial[37].

Cibersegurança

O número de ciberataques continua a aumentar[38]. Estes ataques são mais sofisticados do que nunca, provêm de uma vasta gama de fontes dentro e fora da UE e visam áreas de maior vulnerabilidade. Envolvem frequentemente intervenientes estatais ou protegidos por um Estado, visam infraestruturas digitais essenciais, como os principais prestadores de serviços de computação em nuvem[39]. Os riscos cibernéticos surgiram como uma ameaça significativa também para o sistema financeiro. O Fundo Monetário Internacional estimou as perdas anuais resultantes de ciberataques em 9 % do rendimento líquido dos bancos a nível mundial, ou seja, cerca de 100 mil milhões de dólares[40]. Apesar de a mudança para dispositivos conectados trazer grandes benefícios para os utilizadores, com menos dados armazenados e tratados em centros de dados e mais dados tratados próximo do utilizador («na periferia da rede»)[41], a cibersegurança deixará de poder concentrar-se na proteção dos pontos centrais[42].

Em 2017, a UE apresentou uma abordagem à cibersegurança, tendo como base o reforço da resiliência, uma resposta rápida e uma dissuasão eficaz[43]. A UE deve agora certificar-se de que as suas capacidades de cibersegurança acompanham a realidade, a fim de garantir a resiliência e a capacidade de resposta. Tal exige uma verdadeira abordagem que mobilize toda a sociedade, de modo que as instituições, agências e organismos da UE, os Estados-Membros, a indústria, o meio académico e as pessoas deem à cibersegurança a prioridade necessária[44]. Esta abordagem horizontal deve igualmente ser complementada com abordagens setoriais em matéria de cibersegurança para domínios como a energia, os serviços financeiros, os transportes ou a saúde. Os trabalhos realizados pela UE na próxima fase devem ser congregados numa Estratégia Europeia de Cibersegurança revista.

A exploração de novas e mais estreitas de formas de cooperação entre os serviços de informação, o INTCEN da UE e outras organizações envolvidas na segurança deve fazer parte dos esforços para

---

[36] Um Sistema de Nomes de Domínio (DNS) é um sistema de atribuição de nomes hierárquico e descentralizado para computadores, serviços, ou outros recursos conectados à Internet ou a uma rede privada. Traduz nomes de domínio para os endereços IP necessários para localizar e identificar serviços e dispositivos informáticos.

[37] Proposta de regulamento que cria o programa espacial da União e a Agência da União Europeia para o Programa Espacial. COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Um ataque distribuído de negação de serviço continua a constituir uma ameaça permanente: em fevereiro de 2020, os principais prestadores de serviços tiveram de enfrentar ataques distribuídos de negação de serviço, como, por exemplo, um ataque aos serviços Web da Amazon.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

[41] A computação periférica é uma arquitetura informática aberta e distribuída que inclui capacidade computacional descentralizada, permitindo tecnologias de computação móvel e de Internet das Coisas (IdC). Na computação periférica, os dados são tratados pelo próprio dispositivo ou por um computador ou servidor locais, em vez de serem transmitidos a um centro de dados.

[42] Comunicação intitulada «Uma estratégia europeia para os dados», COM(2020) 66 final.

[43] Comunicação conjunta intitulada «Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE», JOIN(2017) 450.

[44] O relatório «Cibersegurança - a nossa âncora digital» do Centro Comum de Investigação fornece informações multidimensionais sobre o crescimento da cibersegurança nos últimos 40 anos.

intensificar a cibersegurança, bem como para combater o terrorismo, o extremismo, o radicalismo e as ameaças híbridas.

Tendo em consideração a introdução da **infraestrutura 5G** na UE e a potencial dependência de muitos serviços críticos das redes 5G, as consequências de perturbações sistémicas e generalizadas seriam particularmente graves. O processo criado pela Recomendação da Comissão de 2019 sobre a cibersegurança das redes 5G[45] levou agora a uma ação específica dos Estados-Membros sobre as principais medidas previstas num conjunto de instrumentos 5G[46].

Uma das necessidades mais importantes a longo prazo é desenvolver uma cultura de **cibersegurança desde a conceção**, com base na construção de produtos e serviços desde o início. Um importante contributo para este objetivo será o novo quadro de certificação da cibersegurança ao abrigo do Regulamento Cibersegurança[47]. O quadro já está em vias de realização, com dois sistemas de certificação em preparação e prioridades para outros regimes a definir ainda este ano. A cooperação entre a Agência da UE para a Cibersegurança (ENISA), as autoridades responsáveis pela proteção de dados e o Comité Europeu para a Proteção de Dados[48] é de importância fundamental neste domínio.

A Comissão já identificou a necessidade de uma **Ciberunidade Conjunta** que proporcione uma cooperação operacional estruturada e coordenada. Tal poderá incluir um mecanismo de assistência mútua em tempos de crise a nível da UE. Com base na aplicação do recomendação «Plano de Ação»[49], a ciberunidade conjunta pode estabelecer a confiança entre os diferentes intervenientes do ecossistema europeu de cibersegurança e oferecer um serviço fundamental aos Estados-Membros. A Comissão lançará debates com as partes interessadas pertinentes (começando pelos Estados-Membros) e estabelecerá um processo claro, com etapas e um calendário até ao final de 2020.

É igualmente importante estabelecer regras comuns em matéria de segurança da informação e de cibersegurança para todas as instituições, organismos e agências da UE. O objetivo deve ser o de criar normas obrigatórias e rigorosas para o intercâmbio seguro de informações e a segurança das infraestruturas e sistemas digitais em todas as instituições, organismos e agências da UE. Este novo quadro deverá estar na base de uma cooperação operacional forte e eficaz em matéria de cibersegurança em todas as instituições, organismos e agências da UE, centrada no papel da equipa de resposta a emergências informáticas (CERT-UE) para as instituições, os organismos e as agências da UE.

Dada a natureza global dos ciberataques, a criação e a manutenção de **parcerias internacionais** sólidas é fundamental para prevenir, dissuadir e responder mais eficazmente a este tipo de ataques. O quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas («conjunto de instrumentos de ciberdiplomacia»[50]) estabelece medidas no âmbito da Política Externa e de Segurança Comum, incluindo medidas restritivas (sanções), que podem ser utilizadas contra atividades que prejudiquem os seus interesses políticos, económicos e de segurança. A UE deve também aprofundar o seu trabalho através de fundos de desenvolvimento e de cooperação para reforçar as capacidades de apoio aos Estados parceiros no reforço dos seus ecossistemas digitais, na adoção de reformas legislativas nacionais e no cumprimento das normas internacionais. Tal aumenta

---

45 Recomendação da Comissão intitulada: «Cibersegurança das redes 5G», C(2019) 2335 final. A recomendação prevê a sua revisão no último trimestre de 2020.

46 Ver o relatório do grupo de cooperação Segurança das Redes e da Informação sobre a aplicação do conjunto de instrumentos, de 24 de julho de 2020.

47 Regulamento 2019/881 relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação («Regulamento Cibersegurança»).

48 Comunicação intitulada «A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital - dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados, COM(2020) 264.

49 Recomendação 2017/1584 da Comissão sobre a resposta coordenada da União a incidentes e crises de cibersegurança de grande escala.

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

a resiliência da comunidade em geral e a sua capacidade para combater e responder eficazmente às ciberameaças. Trata-se designadamente de trabalhos específicos para promover as normas da UE e a legislação pertinente para aumentar a cibersegurança dos países parceiros na vizinhança da UE[51].

Proteção dos espaços públicos

Os recentes ataques terroristas centraram-se em **espaços públicos**, incluindo locais de culto e plataformas de transporte, explorando a sua natureza aberta e acessível. O aumento do terrorismo desencadeado por extremismo político ou ideológico tornou esta ameaça ainda mais premente, requerendo uma maior proteção física desses locais e sistemas de deteção adequados, sem prejudicar as liberdades dos cidadãos[52]. A Comissão reforçará a cooperação entre os setores público e privado para a proteção dos espaços públicos, com financiamento, intercâmbio de experiências e boas práticas, assim como orientações[53] e recomendações específicas[54]. O aumento da sensibilização, os requisitos de desempenho e os testes dos equipamentos de deteção, bem como o reforço da verificação dos antecedentes para fazer face às ameaças internas farão também parte da abordagem. Um aspeto importante a ter em conta é o facto de as minorias e as pessoas vulneráveis poderem ser afetadas de forma desproporcionada, nomeadamente as pessoas visadas devido à sua religião ou ao seu género, exigindo, por conseguinte, uma atenção especial. As autoridades públicas regionais e locais têm um papel importante a desempenhar no reforço da segurança dos espaços públicos. A Comissão está também a ajudar a promover a inovação das cidades em matéria de segurança dos espaços públicos[55]. O lançamento, em novembro de 2018, de uma nova parceria da Agenda Urbana[56] sobre «segurança dos espaços públicos» reflete o forte empenho dos Estados-Membros, da Comissão e das cidades em enfrentar com mais eficácia as ameaças à segurança no espaço urbano.

O mercado dos **drones** continua a expandir-se, com muitas utilizações valiosas e legítimas. No entanto, estes dispositivos também têm potencial para serem utilizados de forma abusiva por criminosos e terroristas, ameaçando particularmente os espaços públicos. Os alvos podem incluir pessoas, encontros de pessoas, infraestruturas críticas, autoridades policiais, fronteiras ou espaços públicos. Os conhecimentos adquiridos sobre a utilização de veículos aéreos não tripulados («drones») nos conflitos poderiam ser utilizados na Europa diretamente (através do regresso dos combatentes terroristas estrangeiros) ou ser disponibilizados em linha. As regras já desenvolvidas pela Agência Europeia para a Segurança da Aviação constituem um primeiro passo importante em domínios como o registo dos operadores de drones e a identificação remota obrigatória de drones. Dado que os drones se estão a tornar cada vez mais disponíveis, mais acessíveis e mais capazes, é necessário tomar medidas adicionais. Tal poderá incluir a partilha de informações, orientações e boas práticas para todos, incluindo a aplicação da lei, bem como mais testes de contramedidas contra o

---

51 Ver as diretrizes da UE para o reforço das cibercapacidades externas, adotadas nas conclusões do Conselho de 26 de junho de 2018.

52 Os sistemas de identificação biométrica à distância merecem um exame específico. Os pontos de vista iniciais da Comissão são apresentados no Livro Branco da Comissão, de 19 de fevereiro de 2020, sobre a inteligência artificial, COM (2020) 65.

53 Como, por exemplo, orientações sobre a forma de selecionar soluções adequadas de barreiras de segurança destinadas à proteção de espaços públicos (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

54 Orientações sobre boas práticas são fornecidas no documento SWD(2019) 140, incluindo uma secção relativa à cooperação entre os setores publico e privado. O financiamento ao abrigo do FSI-Polícia tem uma incidência especial no reforço da cooperação entre os setores público e privado.

55 Três cidades (Pireu na Grécia, Tampere na Finlândia e Turim em Itália) testarão novas soluções no âmbito das Ações Urbanas Inovadoras, cofinanciadas pelo Fundo Europeu de Desenvolvimento Regional (FEDER).

56 A Agenda Urbana da UE representa um novo método de trabalho a vários níveis que promove a cooperação entre os Estados-Membros, as cidades, a Comissão Europeia e outras partes interessadas para estimular o crescimento, a qualidade de vida e a inovação nas cidades da Europa e identifica e enfrenta com êxito os desafios sociais.

uso de drones.[57]. Por outro lado, as implicações em termos de proteção da privacidade e dos dados na sequência do uso de drones devem ser objeto de análises e de medidas mais pormenorizadas.

Principais ações
• Legislação em matéria de proteção e resiliência das infraestruturas críticas • Revisão da Diretiva relativa à segurança das redes e da informação • Uma iniciativa sobre a resiliência operacional do setor financeiro • Proteção e cibersegurança das infraestruturas críticas da energia e código de rede para a cibersegurança dos fluxos transfronteiriços de eletricidade • Uma estratégia europeia para a cibersegurança • Próximas etapas para a criação de uma Ciberunidade Conjunta • Regras comuns em matéria de segurança da informação e cibersegurança para as instituições, organismos e agências da UE • Reforço da cooperação em matéria de proteção dos espaços públicos, incluindo locais de culto • Partilha de boas práticas em matéria de utilização abusiva dos drones

2. Fazer face às ameaças em permanente evolução

Cibercriminalidade

A tecnologia proporciona novas oportunidades à sociedade. Oferece igualmente novos instrumentos ao sistema judicial e aos serviços repressivos. Mas, ao mesmo tempo, abre portas a criminosos. A presença de programas informáticos maliciosos (*malware*), o furto de dados pessoais ou empresariais por meio de pirataria informática e a interrupção da atividade digital, causando danos financeiros ou à reputação, estão todos a aumentar. O ambiente resiliente criado por uma cibersegurança forte é a primeira defesa. As autoridades responsáveis pela aplicação da lei devem poder trabalhar no âmbito das investigações digitais com regras claras para investigar e julgar crimes, oferecendo às vítimas a proteção necessária. Esse trabalho deverá basear-se no Grupo de Ação Conjunto contra a Cibercriminalidade da Europol e no Protocolo relativo à resposta de emergência dos serviços repressivos, criado para coordenar a resposta a ciberataques em grande escala. São também fundamentais mecanismos eficazes que permitam parcerias e cooperação entre os setores público e privado.

Paralelamente, a luta contra a cibercriminalidade deve tornar-se uma prioridade estratégica da comunicação em toda a UE, a fim de alertar os europeus para os riscos e indicar as medidas preventivas que poderão tomar. Tal deve fazer parte de uma abordagem proativa. Um passo essencial é também a plena implementação do atual quadro jurídico[58]: a Comissão está pronta a recorrer a processos por infração, se for caso disso, bem como a manter o quadro sob exame, a fim de garantir que este continua a ser adequado à sua finalidade. A Comissão irá também explorar, em conjunto com a Europol e a Agência da União Europeia para a Cibersegurança, ENISA, a viabilidade de um sistema de alerta rápido da UE relacionado com o cibercrime que possa assegurar o fluxo de informações e reações rápidas no caso de um surto de cibercrimes.

A cibercriminalidade é um desafio mundial em que é necessária uma cooperação internacional eficaz. A UE apoia a Convenção de Budapeste sobre a cibercriminalidade do Conselho da Europa, que constitui um modelo eficaz e bem estabelecido que permite a todos os países identificar os sistemas e os canais de comunicação necessários para poderem comunicar eficazmente entre si.

[57] Foi criado recentemente um programa de testes plurianual para apoiar os Estados-Membros no desenvolvimento de uma metodologia e de uma plataforma de ensaio comuns neste domínio.

[58] Diretiva 2013/40/UE relativa a ataques contra os sistemas de informação.

Cerca de metade dos cidadãos da UE estão preocupados com a utilização abusiva de dados[59] e com a **usurpação de identidade**[60]. A utilização fraudulenta da identidade para obter ganhos financeiros é apenas um aspeto, mas pode também haver um grande impacto pessoal e psicológico, com publicações ilegais realizadas pelo ladrão da identidade que podem permanecer em linha durante anos. A Comissão irá explorar possíveis medidas práticas para proteger as vítimas contra todas as formas de usurpação de identidade, tendo em conta a futura iniciativa relativa à identidade digital europeia.[61].

Combater a cibercriminalidade significa olhar para o futuro. Uma vez que a sociedade utiliza novos desenvolvimentos tecnológicos para reforçar a economia e a sociedade, os criminosos também procuram explorar esses instrumentos para fins negativos. Por exemplo, os criminosos podem utilizar a inteligência artificial para detetar e identificar senhas ou para simplificar a criação de *software* malicioso (*malware*), a fim de explorar ficheiros de imagens e de áudio que podem ser utilizados para usurpação de identidade ou para o cometimento de fraudes.

Serviços repressivos modernos

Os profissionais da justiça e os serviços repressivos têm de se adaptar às novas tecnologias. Os progressos tecnológicos e as ameaças emergentes exigem que as autoridades repressivas tenham acesso a novos instrumentos, adquiram novas competências e desenvolvam técnicas de investigação alternativas. Para complementar as ações legislativas destinadas a melhorar o acesso transfronteiriço a elementos de prova eletrónicos para investigações criminais, a UE pode ajudar as autoridades repressivas a desenvolver a capacidade necessária para identificar, proteger e ler os dados necessários para investigar crimes e utilizar esses dados como elementos de prova em tribunal. A Comissão estudará medidas destinadas a **reforçar a capacidade dos serviços repressivos nas investigações digitais**, definindo a melhor forma de utilizar a investigação e o desenvolvimento para criar novos instrumentos de aplicação da lei e precisando a maneira como a formação pode proporcionar as competências adequadas aos serviços repressivos e judiciais. Tratar-se-á também de propor avaliações científicas rigorosas e métodos de ensaio através do Centro Comum de Investigação da Comissão.

As abordagens comuns podem igualmente assegurar que a **inteligência artificial, as capacidades espaciais, os megadados** e a **computação de alto desempenho são integrados** na política de segurança de forma eficaz tanto na luta contra os crimes como na garantia dos direitos fundamentais. A inteligência artificial pode funcionar como um instrumento poderoso de luta contra a criminalidade, criando enormes capacidades de investigação através da análise de grandes quantidades de informações e da identificação de padrões e anomalias[62]. Pode também fornecer instrumentos concretos, como ajudar a identificar conteúdos terroristas em linha, detetar transações suspeitas na venda de produtos perigosos ou prestar assistência aos cidadãos em situações de emergência. Concretizar este potencial significa reunir a investigação, a inovação e os utilizadores da inteligência artificial com a governação e as infraestruturas técnicas adequadas, mobilizando ativamente o setor privado e os meios académicos. Significa também garantir os mais elevados padrões de conformidade com os direitos fundamentais, assegurando simultaneamente uma proteção eficaz dos cidadãos. Em especial, as decisões que afetam as pessoas devem ser sujeitas a controlo humano e respeitar o direito da UE aplicável[63].

---

[59] 46 % (Eurobarómetro sobre as atitudes dos europeus em relação à cibersegurança, janeiro de 2020).

[60] A grande maioria dos inquiridos no Eurobarómetro de 2018 «Atitudes dos europeus face à segurança da Internet» (95%) viram a usurpação de identidade como um crime grave e sete em cada dez afirmam que se trata de um crime muito grave. O Eurobarómetro, publicado em janeiro de 2020, confirmou as preocupações com a cibercriminalidade, a fraude em linha e a usurpação de identidade: dois terços dos inquiridos estavam preocupados com a fraude bancária (67 %) ou com a usurpação de identidade (66 %).

[61] Comunicação de 19 de fevereiro de 2020 intitulada «Construir o futuro digital da Europa, COM (2020) 67.

[62] Por exemplo, em matéria de crimes financeiros.

[63] Tal significa a conformidade com a legislação em vigor, incluindo o Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679), bem como a Diretiva sobre a proteção de dados na aplicação da

As informações e os elementos de prova eletrónicos são necessários em cerca de 85 % das investigações relativas a crimes graves, enquanto 65 % do total dos pedidos destinam-se a prestadores estabelecidos noutra jurisdição[64]. O facto de os vestígios físicos tradicionais terem passado a estar em linha aumenta ainda mais o fosso entre os serviços repressivos e as capacidades dos criminosos. É essencial estabelecer regras claras para o acesso transfronteiriço a provas eletrónicas em investigações criminais. É por esta razão que a rápida adoção pelo Parlamento Europeu e pelo Conselho das propostas relativas às provas eletrónicas é fundamental para proporcionar aos profissionais um instrumento eficiente. O acesso transfronteiriço a provas eletrónicas através de negociações internacionais multilaterais e bilaterais é também essencial para estabelecer regras compatíveis a nível internacional[65].

O **acesso a elementos de prova digitais** depende também da disponibilidade de informações. Se os dados forem apagados demasiado rapidamente, podem desaparecer elementos de prova importantes, de modo a que já não exista a possibilidade de identificar e localizar os suspeitos e as redes criminosas (bem como as vítimas). Por outro lado, os sistemas de conservação de dados levantam questões de proteção da privacidade. Em função do resultado dos processos pendentes no Tribunal de Justiça Europeu, a Comissão avaliará o caminho a seguir em matéria de conservação de dados.

O acesso a informações de registo de nomes de domínio («dados WHOIS»)[66] é importante para as investigações criminais, a cibersegurança e a proteção dos consumidores. Contudo, o acesso a estas informações está a tornar-se mais difícil, na pendência da adoção de uma nova política WHOIS pela Sociedade Internet para os Nomes e Números Atribuídos (ICANN). A Comissão continuará a trabalhar com a ICANN e a comunidade multilateral para assegurar que os requerentes legítimos de acesso, incluindo os serviços repressivos, possam obter um acesso eficiente aos dados WHOIS em conformidade com os regulamentos da UE e internacionais em matéria de proteção de dados. Tal implicará a avaliação de possíveis soluções, incluindo a eventual necessidade de legislação para clarificar as regras de acesso a essas informações.

As autoridades policiais e judiciais também precisam de estar equipadas para obter os dados e elementos de prova necessários, quando a **arquitetura 5G para as telecomunicações móveis** estiver plenamente implantada na UE, de forma a respeitar a confidencialidade das comunicações. A Comissão apoiará uma abordagem reforçada e coordenada na elaboração de normas internacionais, definindo as melhores práticas, o processo e a interoperabilidade técnica em áreas tecnológicas fundamentais como a IA, a Internet das coisas ou as tecnologias de cadeia de blocos (*blockchain*).

Atualmente, uma parte substancial das investigações contra todas as formas de criminalidade e terrorismo envolve **informações encriptadas**. A encriptação é essencial para o mundo digital, protegendo sistemas e transações digitais e protegendo também uma série de direitos fundamentais, incluindo a liberdade de expressão, a privacidade e a proteção de dados. No entanto, se utilizado para fins criminosos, pode ocultar a identidade dos criminosos e esconder o conteúdo das suas comunicações. A Comissão explorará e apoiará soluções técnicas, operacionais e jurídicas equilibradas para os obstáculos e promoverá uma abordagem que mantenha a eficácia da encriptação na proteção da privacidade e da segurança, dando simultaneamente uma resposta eficaz à criminalidade e ao terrorismo.

Combate aos conteúdos ilegais em linha

Garantir a segurança dos ambientes em linha e físicos significa continuar a ajustar o combate aos conteúdos ilegais em linha. Cada vez mais as ameaças principais para os cidadãos, como o

---

lei (Diretiva (UE) 2016/680) que regulam o tratamento de dados pessoais para efeitos de deteção, prevenção, investigação e repressão de infrações penais ou de execução de sanções penais.

64 Documento da Comissão SWD(2018) 118 final.

65 Em especial, o segundo protocolo adicional à Convenção de Budapeste sobre a Cibercriminalidade e um acordo entre a UE e os Estados Unidos sobre o acesso transnacional a provas eletrónicas.

66 Armazenados em bases de dados mantidos por 2 500 operadores de registo e agentes de registo baseados em todo o mundo.

terrorismo, o extremismo ou o abuso sexual de crianças, dependem do ambiente digital: este facto exige medidas concretas e um enquadramento apto a garantir o respeito pelos direitos fundamentais. Um primeiro passo essencial é concluir rapidamente as negociações sobre a legislação proposta em matéria de conteúdos terroristas em linha[67] e assegurar a sua aplicação. O reforço da cooperação voluntária entre os serviços repressivos e o setor privado no **Fórum Internet da UE** é também fundamental para combater a utilização abusiva da Internet por parte de terroristas, extremistas violentos e criminosos. A Unidade da UE de Sinalização de Conteúdos na Internet da Europol continuará a desempenhar um papel crucial no acompanhamento da atividade em linha dos grupos terroristas e das medidas tomadas pelas plataformas[68], bem como no desenvolvimento do **Protocolo de Crise da UE**[69]. Além disso, a Comissão continuará a colaborar com os parceiros internacionais, nomeadamente através da participação no **Fórum Mundial da Internet contra o Terrorismo**, a fim de fazer face a estes desafios a nível global. Os trabalhos continuarão a apoiar o desenvolvimento de narrativas alternativas e contrárias ao ódio através do Programa de Capacitação da Sociedade Civil[70].

Para prevenir e combater a propagação de discursos ilegais de incitação ao ódio em linha, a Comissão lançou, em 2016, o código de conduta da UE sobre discursos ilegais de incitação ao ódio em linha, com um compromisso voluntário das plataformas em linha para eliminar os conteúdos de incitamento ao ódio. A última avaliação mostra que as empresas avaliam 90 % dos conteúdos assinalados no prazo de 24 horas e eliminam 71 % dos conteúdos considerados ilegais de incitação ao ódio. No entanto, as plataformas devem melhorar a transparência e as respostas aos utilizadores e assegurar uma avaliação coerente dos conteúdos assinalados[71].

O Fórum Internet da UE facilitará também o intercâmbio de tecnologias existentes e em desenvolvimento para enfrentar os desafios relacionados com o abuso sexual de crianças em linha. A luta contra o abuso sexual de crianças em linha está no centro de uma nova estratégia para intensificar a **luta contra o abuso sexual de crianças**[72], que procurará maximizar a utilização dos instrumentos disponíveis a nível da UE para combater esse tipo de crimes. As empresas devem estar em condições de prosseguir o seu trabalho de deteção e remoção de material relacionado com o abuso sexual de crianças em linha, e os danos causados por este material exigem um quadro que estabeleça obrigações claras e permanentes para resolver o problema. A referida estratégia anunciará igualmente que a Comissão começará também a preparar legislação setorial específica para combater o abuso sexual de crianças em linha de forma mais eficaz, no pleno respeito dos direitos fundamentais.

De um modo mais geral, o próximo ato legislativo sobre os serviços digitais irá também clarificar e melhorar as regras em matéria de responsabilidade e segurança dos serviços digitais e eliminar os desincentivos que travam ações destinadas a combater os conteúdos, os bens ou os serviços ilegais.

Além disso, a Comissão continuará a colaborar com os parceiros internacionais e com o **Fórum Mundial da Internet contra o Terrorismo**, designadamente através o comité consultivo independente, a fim de debater a forma de fazer face a estes desafios a nível global, preservando ao mesmo tempo os valores e direitos fundamentais da UE. Devem também ser abordados novos temas, como os algoritmos ou os jogos em linha[73].

Ameaças híbridas

---

67 Proposta relativa à prevenção da difusão de conteúdos terroristas em linha, COM(2018) 640 de 12 de setembro de 2018.

68 Europol, novembro de 2019.

69 Uma Europa que protege - Protocolo de Crise da UE: responder aos conteúdos terroristas em linha. (outubro de 2019).

70 Ligado aos trabalhos do programa de sensibilização para a radicalização, ver secção IV.3.

71 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

72 Estratégia da UE a favor de uma luta mais eficaz contra o abuso sexual de crianças, COM(2020) 607.

73 Os terroristas estão a utilizar cada vez mais frequentemente os sistemas de mensagens das plataformas de jogos em linha para o intercâmbio de mensagens e jovens terroristas também replicam ataques violentos vistos em jogos de vídeo.

A escala e a diversidade das ameaças híbridas atuais não têm precedentes. A crise da COVID-19 trouxe mais provas deste facto, com vários intervenientes estatais e não estatais a tentar instrumentalizar a pandemia, em especial através da manipulação do ambiente de informação e do ataque às infraestruturas de base. Esta situação é suscetível de enfraquecer a coesão social e de minar a confiança nas instituições da UE e nos governos dos Estados-Membros.

A abordagem da UE em relação às ameaças híbridas é estabelecida no quadro comum de 2016[74] e na Comunicação Conjunta de 2018 «Aumentar a resiliência e reforçar as capacidades para fazer face a ameaças híbridas»[75]. A ação a nível da UE é sustentada por um importante conjunto de instrumentos que abrange o nexo entre a segurança interna e a segurança externa, baseado numa abordagem que mobilize toda a sociedade e numa estreita cooperação com os parceiros estratégicos, nomeadamente a NATO e o G7. Juntamente com a presente estratégia, é publicado um relatório sobre a aplicação da abordagem da UE em matéria de ameaças híbridas.[76]. Com base no levantamento[77] apresentado em paralelo com a presente estratégia, os serviços da Comissão e o Serviço Europeu para a Ação Externa criarão uma **plataforma em linha restrita** na qual os Estados-Membros encontrarão referência dos instrumentos e medidas contra as ameaças híbridas à escala da UE.

Considerando que a responsabilidade pela luta contra as ameaças híbridas cabe, em primeiro lugar, aos Estados-Membros - devido às ligações intrínsecas com as políticas nacionais de segurança e defesa - algumas vulnerabilidades são comuns a todos os Estados-Membros e algumas ameaças ultrapassam as fronteiras, como os ataques a redes ou infraestruturas transfronteiriças. A Comissão e o Alto Representante definirão uma abordagem da UE em relação às ameaças híbridas que integre as dimensões externa e interna num fluxo contínuo e que congregue os interesses nacionais e da UE. A referida abordagem deve abranger toda a gama de ações - desde a deteção precoce, a análise, a sensibilização, o reforço da resiliência e a prevenção até à resposta às crises e à gestão das consequências.

Para além de uma implementação reforçada, com as ameaças híbridas em constante evolução, será dada especial atenção à **integração das considerações sobre as ameaças híbridas no quadro mais geral da elaboração de políticas**, a fim de acompanhar a dinâmica da evolução e de garantir que nenhuma iniciativa potencialmente relevante será ignorada. Os efeitos das novas iniciativas serão igualmente avaliados do ponto de vista das ameaças híbridas, incluindo iniciativas em domínios que, até à data, se mantiveram fora do âmbito da luta contra as ameaças híbridas, como a educação, a tecnologia e a investigação. A abordagem beneficiará do trabalho realizado sobre a conceptualização das ameaças híbridas, que proporciona uma visão abrangente dos vários instrumentos que os adversários podem utilizar.[78]. O objetivo deve ser o de assegurar que o processo de tomada de decisões sé sustentado por uma comunicação regular e abrangente baseada em informações sobre a evolução das ameaças híbridas. Tal dependerá fortemente da informação dos Estados-Membros e do reforço da cooperação em matéria de informações com os serviços competentes dos Estados-Membros através do INTCEN da UE.

Para desenvolver o **conhecimento situacional**, os serviços da Comissão e o Serviço Europeu para a Ação Externa irão estudar opções para racionalizar os fluxos de informação de diferentes fontes, incluindo dos Estados-Membros, bem como das agências da UE, como a ENISA, a Europol e a Frontex. A célula de fusão da UE contra as ameaças híbridas continuará a ser o ponto focal da UE

[74] Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia, JOIN (2016) 18.

[75] Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas, JOIN (2018) 16.

[76] SWD(2020) 153, Relatório sobre a aplicação do quadro comum de 2016 em matéria de luta contra as ameaças híbridas e Comunicação Conjunta de 2018 sobre o reforço da resiliência e das capacidades para fazer face às ameaças híbridas.

[77] SWD(2020) 152, Levantamento das medidas relacionadas com o reforço da resiliência e a luta contra as ameaças híbridas.

[78] *The Landscape of Hybrid Threats*: *A conceptual Model* (O panorama das ameaças híbridas: Um modelo conceptual), JRC117280, desenvolvido conjuntamente pelo Centro Comum de Investigação e pelo Centro de Excelência de Luta contra as Ameaças Híbridas.

para as avaliações das ameaças híbridas. O **reforço da resiliência** é fundamental para a prevenção e a proteção contra as ameaças híbridas. Por conseguinte, é crucial acompanhar sistematicamente e medir objetivamente os progressos realizados neste domínio. Um primeiro passo será a identificação das exigências de base setoriais em matéria de resiliência contra as ameaças híbridas, tanto dos Estados-Membros como das instituições e organismos da UE. Por último, a fim de intensificar a **preparação para a resposta a situações de crise provocadas por ameaças híbridas,** deve ser revisto o protocolo existente, definido no protocolo operacional da UE para fazer face às ameaças híbridas de 2016 («EU Playbook»)[79], refletindo uma análise mais ampla e reforçando o sistema de resposta a situações de crise da UE atualmente em estudo.[80]. O objetivo é maximizar o efeito da ação da UE, conjugando rapidamente respostas setoriais e assegurando uma cooperação sem descontinuidades com os nossos parceiros, a NATO em primeiro lugar.

Principais ações
• Assegurar que a legislação em matéria de cibercriminalidade é aplicada e adequada ao fim a que se destina • Uma estratégia da UE a favor de uma luta mais eficaz contra o abuso sexual de crianças • Propostas sobre a deteção e a retirada de material relativo ao abuso sexual de crianças • Uma abordagem da UE em matéria de luta contra as ameaças híbridas • Revisão do protocolo operacional da UE para fazer face às ameaças híbridas (EU Playbook) • Avaliação da forma de reforçar a capacidade dos serviços repressivos nas investigações digitais

3. Proteger os europeus do terrorismo e da criminalidade organizada

Terrorismo e radicalização

A ameaça terrorista continua a ser elevada na UE. Apesar da diminuição global do seu número, os atentados podem ainda ter efeitos devastadores. A radicalização pode também conduzir a uma maior polarização e desestabilização da coesão social. Os Estados-Membros continuam a ser os principais responsáveis pela luta contra o terrorismo e a radicalização. No entanto, a dimensão cada vez mais transnacional e intersetorial da ameaça exige novas medidas de cooperação e coordenação na UE. A aplicação efetiva da legislação da UE em matéria de luta contra o terrorismo, incluindo as medidas restritivas[81], constitui uma prioridade. A ampliação do mandato da Procuradoria Europeia aos crimes terroristas transfronteiriços continua a ser um objetivo a atingir.

Par lutar contra o terrorismo é necessário estudar primeiro as suas causas profundas. A polarização da sociedade, as discriminações reais ou percebidas e outros fatores psicológicos e sociológicos podem aumentar a vulnerabilidade das pessoas face ao discurso radical. Neste contexto, a luta contra a **radicalização** é indissociável da promoção da coesão social a nível local, nacional e europeu. Na última década, foram desenvolvidas várias iniciativas e políticas com impacto, nomeadamente através da Rede de Sensibilização para a Radicalização e da iniciativa «Cidades da UE contra a Radicalização»[82]. Chegou o momento de ponderar as ações destinadas a integrar as políticas, as

[79] Protocolo operacional da UE para fazer face às ameaças híbridas (EU Playbook), SWD(2016) 227.

[80] Na sequência da sua videoconferência de 26 de março de 2020, os membros do Conselho Europeu adotaram uma declaração sobre as ações da UE em resposta ao surto de COVID-19, convidando a Comissão a apresentar propostas para um sistema de gestão de crises mais ambicioso e abrangente na UE.

[81] O Conselho adotou medidas restritivas contra o EIIL (Daexe) e a Alcaida, bem como medidas restritivas específicas contra determinadas pessoas e entidades com o objetivo de combater o terrorismo. Ver o mapa das sanções impostas pela UE (https://www.sanctionsmap.eu/#/main) para uma panorâmica de todas as medidas restritivas.

[82] A iniciativa-piloto «Cidades da UE contra a Radicalização» tem o duplo objetivo de promover o intercâmbio de experiências entre as cidades da UE e de recolher opiniões sobre a melhor forma de apoiar as comunidades locais a nível da UE.

iniciativas e os fundos da UE para combater a radicalização. Estas ações podem apoiar o desenvolvimento de capacidades e competências, reforçar a cooperação, reforçar a base factual e contribuir para a avaliação dos progressos alcançados, associando todas as partes interessadas, incluindo os profissionais de primeira linha, os decisores políticos e os meios académicos.[83]. As políticas designadas por não vinculativas ou flexíveis (*soft policies*), como a educação, a cultura, a juventude e o desporto, podem contribuir para a prevenção da radicalização, oferecendo perspetivas aos jovens em risco e proporcionando uma certa coesão dentro da UE.[84]. Os domínios prioritários incluem ações no âmbito da deteção precoce e da gestão dos riscos, do reforço da resiliência e da desmobilização, bem como da reabilitação e reintegração na sociedade.

Terroristas procuraram adquirir materiais químicos, biológicos, radiológicos e nucleares (QBRN)[85] e transformá-los em armas, bem como desenvolver os conhecimentos e a capacidade para os utilizar[86]. O possível recurso a ataques QBRN ocupa lugar de destaque na propaganda terrorista. Tendo em conta os potenciais danos muito elevados de tais ataques, é necessário conceder uma atenção especial a uma eventualidade deste tipo. Com base na abordagem utilizada para regulamentar o acesso a precursores de explosivos, a Comissão analisará a possibilidade de restringir o acesso a determinados produtos químicos perigosos, suscetíveis de serem utilizados para realizar atentados. O desenvolvimento das capacidades de resposta da proteção civil da UE (rescEU) no domínio químico, biológico, radiológico e nuclear será igualmente determinante. A cooperação com países terceiros é igualmente importante para reforçar uma cultura comum de segurança e proteção no domínio QBRN, tirando pleno partido da ação dos Centros de Excelência QBRN da UE de nível internacional. A referida cooperação incluirá a avaliação de lacunas e de riscos a nível nacional, apoio a planos de ação nacionais e regionais em matéria de QBRN, intercâmbios de boas práticas e atividades de reforço das capacidades no domínio QBRN.

A UE desenvolveu a legislação mais avançada do mundo para restringir o acesso a **precursores de explosivos**[87] e detetar transações suspeitas destinadas à construção de engenhos explosivos improvisados. Mas a ameaça da utilização de explosivos artesanais continua a ser elevada, tendo-se recorrido a este tipo de explosivos em múltiplos ataques em toda a UE[88]. A primeira medida a tomar deve ser a aplicação das regras, bem como a garantia de que o ambiente em linha não permite contornar os controlos.

A ação penal efetiva contra as pessoas que cometeram crimes terroristas, incluindo os **combatentes terroristas estrangeiros** atualmente na Síria e no Iraque, é também um elemento importante da política de luta contra o terrorismo. Embora estas questões sejam essencialmente tratadas pelos Estados-Membros, a coordenação e o apoio da UE podem ajudar os Estados-Membros a enfrentar desafios comuns. As medidas em curso para aplicar integralmente a legislação em matéria de segurança das fronteiras[89] e utilizar plenamente todas as bases de dados pertinentes da UE para partilhar informações sobre os suspeitos conhecidos constituirão um passo importante. Para além de identificar indivíduos de alto risco, é necessária uma política de reintegração e reabilitação. A cooperação interprofissional, associando nomeadamente o pessoal penitenciário e os agentes de

---

83 Por exemplo, o financiamento ao abrigo do Fundo Europeu da Segurança e do programa «Direitos, Igualdade e Cidadania».

84 Ações da UE, como os intercâmbios virtuais Erasmus+ e a geminação eletrónica.

85 Nos últimos dois anos, registaram-se, por exemplo, vários casos na Europa (França, Alemanha e Itália) e fora da Europa (Tunísia e Indonésia) de utilização de agentes biológicos (geralmente toxinas de origem vegetal).

86 O Conselho adotou medidas restritivas contra a proliferação e a utilização de armas químicas.

87 Produtos químicos que podem ser utilizados para fabricar explosivos artesanais. Estes produtos são regulamentados pelo Regulamento (UE) 2019/1148 sobre a comercialização e utilização de precursores de explosivos.

88 Podem citar-se como exemplos desses ataques devastadores os de Oslo (2011), Paris (2015), Bruxelas (2016) e Manchester (2017). Um atentado cometido com um explosivo artesanal em Lyon (2019) feriu 13 pessoas.

89 Incluindo o novo mandato da Agência Europeia da Guarda de Fronteiras e Costeira (Frontex).

liberdade condicional, reforçará a compreensão judicial dos processos de radicalização conducentes ao extremismo violento e consolidará a abordagem do setor judicial em matéria de sanções e de recurso a soluções alternativas à detenção.

O desafio dos combatentes terroristas estrangeiros é emblemático da ligação entre a segurança interna e a **segurança externa**. A cooperação em matéria de luta contra o terrorismo e de prevenção e combate à radicalização e ao extremismo violento é fundamental para a segurança no interior da UE[90]. São necessárias novas medidas para estabelecer parcerias no domínio da luta contra o terrorismo e desenvolver a cooperação com os países vizinhos e para além destes, tirando partido dos conhecimentos da rede de peritos em matéria de luta contra o terrorismo/segurança. O Plano de Ação conjunto de combate ao terrorismo nos Balcãs Ocidentais constitui uma boa referência para esse género de cooperação específica. Em especial, devem ser envidados esforços para apoiar a capacidade dos países parceiros de identificar e localizar os combatentes terroristas estrangeiros. A UE continuará também a promover a cooperação multilateral, em colaboração com os principais intervenientes mundiais neste domínio, como as Nações Unidas, a NATO, o Conselho da Europa, a Interpol e a OSCE. A UE colaborará igualmente com o Fórum Mundial contra o Terrorismo e com a coligação internacional contra o Daexe, bem como com os intervenientes da sociedade civil envolvidos. Os instrumentos de política externa da União, nomeadamente em matéria de desenvolvimento e cooperação, também desempenham um papel importante na cooperação com os países terceiros com vista à prevenção do terrorismo e da pirataria. A cooperação internacional é também essencial para eliminar todas as fontes de **financiamento do terrorismo**, por exemplo, por meio do Grupo de Ação Financeira.

Criminalidade organizada

A criminalidade organizada tem enormes custos económicos e pessoais. Estima-se que a perda económica devida à criminalidade organizada e à corrupção represente entre 218 e 282 mil milhões de EUR por ano[91]. Mais de 5 000 grupos de criminalidade organizada estavam a ser investigados na Europa em 2017 - um aumento de 50 % em relação a 2013[92]. A criminalidade organizada opera cada vez mais a nível transfronteiriço, nomeadamente a partir dos países vizinhos mais próximos da UE, o que exige uma intensificação da cooperação operacional e do intercâmbio de informações com os parceiros da vizinhança.

Novos desafios estão a surgir e o crime em linha assume novas formas: a pandemia de COVID-19 registou um enorme aumento das fraudes em linha tendo como alvo os grupos vulneráveis e os produtos sanitários e do setor da saúde foram objeto de roubos e assaltos[93]. A UE tem de intensificar o seu trabalho contra a criminalidade organizada, nomeadamente a nível internacional, com mais instrumentos para desmantelar o modelo de negócio da criminalidade organizada. A luta contra a criminalidade organizada exige também uma estreita cooperação com as administrações locais e regionais, bem como com a sociedade civil, que são parceiros fundamentais na prevenção da criminalidade e na prestação de assistência e apoio às vítimas, sendo as mais afetadas as administrações das regiões fronteiriças. As ações neste domínio serão reunidas num **programa de luta contra a criminalidade organizada**.

Mais de um terço dos grupos de criminalidade organizada ativos na UE estão envolvidos na produção, tráfico ou distribuição de drogas. Em 2019, a toxicodependência provocou mais de oito mil mortes por *overdose* na UE. A maior parte do **tráfico de droga** atravessa as fronteiras e uma

[90] As conclusões do Conselho de 16 de junho de 2020 sublinharam a necessidade de proteger os cidadãos da UE contra o terrorismo e o extremismo violento, em todas as suas formas e independentemente da sua origem, e apelaram ao reforço da atuação e das medidas da UE, na ação externa, em matéria de luta contra o terrorismo em determinados domínios geográficos e temáticos prioritários.

[91] Em termos de Produto Interno Bruto (PIB); Relatório da Europol: "*Does crime still pay?*" – *Criminal asset recovery in the EU*, 2016.

[92] Europol, *Serious and Organised Threat Assessments* (SOCTA), 2013 e 2017.

[93] Europol, 2020.

percentagem muito importante dos seus lucros é investido na economia legal[94]. Um novo programa antidroga da UE[95] potenciará os esforços da UE e dos Estados-Membros nos domínios da redução da procura e da oferta de droga, definindo ações conjuntas para resolver um problema comum e reforçando o diálogo e a cooperação entre a UE e os parceiros externos sobre questões relacionadas com a droga. Na sequência de uma avaliação do Observatório Europeu da Droga e da Toxicodependência, a Comissão avaliará se o mandato deste deve ser atualizado para responder aos novos desafios.

Os grupos da criminalidade organizada e os terroristas são também intervenientes fundamentais no comércio de **armas de fogo ilegais**. Entre 2009 e 2018, ocorreram 23 incidentes de massacres com armas de fogo na Europa, em que foram mortas mais de 340 pessoas[96]. As armas de fogo são frequentemente objeto de tráfico para a UE através dos países vizinhos mais imediatos[97], o que aponta para a necessidade de reforçar a coordenação e a cooperação tanto dentro da UE como com os parceiros internacionais, em especial a Interpol, a fim de harmonizar a recolha e a comunicação de informações sobre as apreensões de armas de fogo. É igualmente essencial melhorar a rastreabilidade das armas, nomeadamente na Internet, e assegurar o intercâmbio de informações entre as autoridades responsáveis pela concessão de licenças e as autoridades responsáveis pela aplicação da lei. A Comissão apresentará um novo **plano de ação da UE contra o tráfico de armas de fogo**[98] e avaliará também se as regras em matéria de autorização de exportação, de importação e de trânsito de armas de fogo continuam a ser adequadas à sua finalidade[99].

As organizações criminosas tratam os migrantes e as pessoas com necessidade de proteção internacional como mercadoria. 90 % dos migrantes irregulares chegam à UE através de uma rede criminosa[100]. A introdução clandestina de migrantes está muitas vezes interligada a outras formas de criminalidade organizada, nomeadamente o tráfico de seres humanos.[101]. Para além do enorme custo humano do tráfico, a Europol estima que, globalmente, o lucro anual gerado por todas as formas de exploração resultante do tráfico de seres humanos ascende a 29,4 mil milhões de EUR. Trata-se de um crime transnacional que se alimenta da procura ilegal gerada dentro e fora da UE e que afeta todos os Estados-Membros. O balanço pouco brilhante de identificação, julgamento e condenação destes crimes revela a necessidade de uma nova abordagem para reforçar a ação neste domínio. Uma nova **abordagem global do tráfico de seres humanos** permitirá congregar as linhas de ação. Além disso, a Comissão apresentará um **novo Plano de Ação da UE contra o tráfico de migrantes** para 2021-2025. Ambas as vertentes se centrarão no combate às redes criminosas, no reforço da cooperação e no apoio à ação dos serviços repressivos.

Os grupos da criminalidade organizada - bem como os terroristas - procuram também oportunidades noutros domínios, especialmente nos que geram lucros elevados com um baixo risco de deteção, como os **crimes contra o ambiente**. A caça ilícita e o comércio ilegal de espécies selvagens, a mineração ilegal, a exploração florestal, assim como a eliminação e expedição ilegais de resíduos tornaram-se na quarta maior atividade criminosa a nível mundial.[102]. Os regimes de comércio de

---

94 OEDT e Europol, *EU Drug Markets Report* (Relatório sobre os mercados de droga na UE), (novembro de 2019).

95 Programa e plano de ação antidroga da UE (2021-2025), COM(2020) 606.

96 Flemish Peace Institute, Armed to kill, (outubro de 2019).

97 A UE financiou a luta contra a proliferação e o tráfico de armas ligeiras e de pequeno calibre na região desde 2002; financiou, designadamente a Rede de Peritos em Armas de Fogo da Europa do Sudeste (SEEFEN). Desde 2019, os parceiros dos Balcãs Ocidentais estão plenamente envolvidos na prioridade relativa às armas de fogo da Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas (EMPACT).

98 COM(2020) 608.

99 Regulamento (UE) n.º 258/2012 que aplica o artigo 10.º do Protocolo das Nações Unidas contra o fabrico e o tráfico ilícitos de armas de fogo.

100 Fonte: Europol.

101 Europol, EMSC, 4.º relatório anual.

102 UNEP-INTERPOL *Rapid Response Assessment*: *The Rise of Environmental Crime*, junho de 2016.

licenças de emissão e os sistemas de certificação energética também foram aproveitados para fins criminosos; por outro lado, registaram-se desvios nos fundos atribuídos à resiliência ambiental e ao desenvolvimento sustentável. Para além de promover a ação da UE, dos Estados-Membros e da comunidade internacional para intensificar os esforços contra a criminalidade ambiental[103], a Comissão está atualmente a avaliar se a Diretiva Criminalidade Ambiental[104] continua adequada à sua finalidade. O **tráfico de bens culturais** está a aumentar e também se tornou uma das atividades criminosas mais lucrativas, constituindo uma fonte de financiamento para os terroristas e para a criminalidade organizada. Deve ser estudada a possibilidade de melhorar a rastreabilidade em linha e fora de linha dos bens culturais no mercado interno e a cooperação com países terceiros onde os bens culturais são saqueados, bem como de prestar apoio ativo aos serviços repressivos e às comunidades académicas.

Os **crimes económicos e financeiros** são altamente complexos, mas afetam todos os anos milhões de cidadãos e milhares de empresas na UE. A luta contra a fraude é crucial e exige uma ação a nível da UE. A Europol, juntamente com a Eurojust, a Procuradoria Europeia e o Organismo Europeu de Luta Antifraude apoiam os Estados-Membros e a UE na proteção dos mercados económicos e financeiros e na salvaguarda do dinheiro dos contribuintes da UE. A Procuradoria Europeia irá tornar-se plenamente operacional no final de 2020 e irá investigar, instaurar a ação penal e deduzir acusação e sustentá-la na instrução e no julgamento contra os autores de crimes contra o orçamento da UE, como a fraude, a corrupção e o branqueamento de capitais. Combaterá igualmente a fraude transfronteiriça ao IVA que custa aos contribuintes, pelo menos, 50 mil milhões de EUR por ano.

A Comissão apoiará igualmente o desenvolvimento de competências e de um quadro legislativo em matéria de riscos emergentes, como os criptoativos e os novos sistemas de pagamento. Em especial, a Comissão está a planear a resposta face ao aparecimento dos criptoativos, como a bitcoin, e o efeito que estas novas tecnologias terão na emissão, na troca e na partilha de ativos financeiros, bem como no acesso a tais ativos.

Na União Europeia, deve haver tolerância zero para o dinheiro ilícito. Ao longo de trinta anos, a UE estabeleceu um quadro regulamentar sólido para a prevenção e o combate ao **branqueamento de capitais**, bem como para o financiamento do terrorismo, no pleno respeito da necessidade de proteger os dados pessoais. Não obstante, existe um consenso crescente quanto à necessidade de melhorar significativamente a aplicação do quadro atual. É necessário sanar as grandes divergências quanto à forma como é aplicado, mas também as graves deficiências na aplicação das regras. Tal como indicado no plano de ação de maio de 2020[105], estão em curso trabalhos para avaliar as possibilidades de reforçar o quadro da UE no domínio da luta contra o branqueamento de capitais e o financiamento do terrorismo. As áreas a explorar incluem a interligação dos registos centralizados de contas bancárias nacionais, que poderá acelerar significativamente o acesso à informação financeira das Unidades de Informação Financeira e das autoridades competentes.

Os **lucros dos grupos da criminalidade organizada** são estimados em 110 mil milhões de EUR por ano na UE. A resposta atual inclui legislação harmonizada em matéria de confisco e recuperação de bens[106], a fim de melhorar o congelamento (apreensão) e o confisco de bens de origem criminosa na UE e fomentar a confiança mútua e uma cooperação eficaz transfronteiriça entre os Estados-Membros. No entanto, apenas cerca de 1 % desses lucros são confiscados[107], o que permite que os grupos da criminalidade organizada invistam na expansão das suas atividades criminosas e se infiltrem na economia legal, em especial, nas pequenas e médias empresas, que têm dificuldades de acesso ao crédito, constituindo um alvo para o branqueamento de capitais. A Comissão analisará a

[103] Ver o Pacto Ecológico Europeu, COM(2019) 640 final.
[104] Diretiva 2008/99/CE relativa à proteção do ambiente através do direito penal.
[105] Plano de ação de luta contra o branqueamento de capitais e o financiamento do terrorismo C(2020) 2800.
[106] A legislação da UE exige que sejam criados em todos os Estados-Membros gabinetes de recuperação de bens.
[107] Relatório intitulado «Recuperação e perda de bens: garantir que o crime não compensa, COM (2020) 217 final.

aplicação da legislação[108] e a eventual necessidade de novas regras comuns, nomeadamente sobre a perda (confisco) não baseada em condenação. Os gabinetes de recuperação de bens[109], intervenientes importantes no processo de recuperação de ativos, poderiam também estar equipados com melhores instrumentos para identificar e rastrear os bens de uma forma mais rápida em toda a UE, a fim de aumentar as taxas de perda (confisco).

Existe uma forte ligação entre a criminalidade organizada e a **corrupção**. Segundo as estimativas, a corrupção, por si só, custa à economia da UE cerca de 120 mil milhões de EUR por ano[110]. A prevenção e a luta contra a corrupção continuarão a ser objeto de um acompanhamento regular no âmbito do mecanismo de proteção do Estado de direito e do Semestre Europeu. O Semestre Europeu avaliou os desafios na luta contra a corrupção, como os contratos públicos, a administração pública, o ambiente empresarial ou os cuidados de saúde. O novo relatório anual da Comissão sobre o Estado de direito abrangerá a luta contra a corrupção e permitirá um diálogo preventivo com as autoridades nacionais e as partes interessadas a nível nacional e da UE. As organizações da sociedade civil podem também desempenhar um papel fundamental na promoção da ação das autoridades públicas em matéria de prevenção e luta contra a criminalidade organizada e a corrupção, podendo estas organizações participar num fórum comum. Em razão da natureza transnacional da criminalidade organizada e da corrupção, a cooperação e assistência em matéria de luta contra estes fenómenos com as regiões vizinhas da UE constitui um aspeto de grande importância.

Principais ações
• Programa da UE de luta contra o terrorismo, incluindo novas ações contra a radicalização na União • Nova cooperação com os principais países terceiros e organizações internacionais contra o terrorismo • Programa de luta contra a criminalidade organizada, incluindo o tráfico de seres humanos • Programa e plano de ação antidroga da UE, 2021-2025 • Avaliação do Observatório Europeu da Droga e da Toxicodependência • Plano de Ação da UE sobre o Tráfico de Armas de Fogo para 2020-2025 • Revisão da legislação em matéria de congelamento (apreensão) e confisco e de gabinetes de recuperação de bens • Avaliação da Diretiva Criminalidade Ambiental • Plano de Ação da UE contra o tráfico de migrantes, 2021-2025

4. Um sólido ecossistema europeu da segurança

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

Todas as políticas devem incluir uma vertente de segurança e a UE pode contribuir a todos os níveis. Nos lares, a violência doméstica é um dos riscos mais graves em matéria de segurança. Na UE, 22 % das mulheres foram vítimas de violência familiar.[111]. A adesão da UE à Convenção de Istambul para

[108] Diretiva 2014/42/UE sobre o congelamento e a perda dos instrumentos e produtos do crime.

[109] Decisão 2007/845/JAI do Conselho relativa à cooperação entre os gabinetes de recuperação de bens dos Estados-Membros no domínio da deteção e identificação de produtos ou outros bens relacionados com o crime.

[110] É difícil estimar o montante total dos custos económicos da corrupção, embora alguns organismos tenham envidado esforços nesse sentido, nomeadamente a Câmara de Comércio Internacional, Transparência Internacional, o Pacto Global das Nações Unidas e o Fórum Económico Mundial, sugerindo que a corrupção ascenda a 5 % do PIB mundial.

[111] Uma União da Igualdade: Estratégia para a Igualdade de Género 2020-2025, COM (2020) 152.

a Prevenção e o Combate à Violência Contra as Mulheres e a Violência Doméstica continua a ser uma prioridade fundamental. Caso as negociações permaneçam bloqueadas, a Comissão tomará outras medidas para alcançar os mesmos objetivos que a Convenção, nomeadamente propondo acrescentar a violência contra as mulheres à lista de crimes da UE definidos no Tratado.

Cooperação e intercâmbio de informações

Um dos contributos mais importantes que a UE pode dar em matéria de proteção dos cidadãos consiste em ajudar os responsáveis pela segurança a colaborarem de forma eficaz. A cooperação e a partilha de informações são os instrumentos mais poderosos para combater a criminalidade e o terrorismo e obter justiça. Para serem eficientes, têm de ser direcionadas e atempadas. Para serem fiáveis, devem ser acompanhadas de garantias e controlos comuns.

Foram criados vários instrumentos e estratégias setoriais específicas da UE[112] para reforçar a **cooperação operacional entre os serviços repressivos** dos Estados-Membros. Um dos principais instrumentos da UE de apoio à cooperação policial entre os Estados-Membros é o Sistema de Informação de Schengen, utilizado para o intercâmbio de dados sobre pessoas e objetos procurados e desaparecidos em tempo real. Os resultados traduziram-se na detenção de criminosos, em apreensões de drogas e no resgate de potenciais vítimas[113]. No entanto, o nível de cooperação poderá ainda ser reforçado através da racionalização e modernização dos instrumentos disponíveis. A maior parte do quadro jurídico da UE subjacente à cooperação operacional entre os serviços repressivos foi concebida há 30 anos. Uma rede complexa de acordos bilaterais entre Estados-Membros, muitos desatualizados ou subutilizados, corre o risco de fragmentação. Nos países mais pequenos ou sem litoral, os agentes dos serviços repressivos que exercem as suas atividades além-fronteiras têm de levar a cabo ações operacionais observando, em alguns casos, até sete conjuntos de regras diferentes: consequentemente, algumas operações, como a perseguição de suspeitos para além das fronteiras internas, simplesmente não se pode verificar. A cooperação operacional em novas tecnologias, como os drones, também não é abrangida pelo atual quadro legislativo da UE.

A eficácia operacional pode ser apoiada por uma cooperação específica entre serviços repressivos, que pode igualmente contribuir para fornecer apoio essencial a outros objetivos estratégicos - como a prestação de informações em matéria de segurança para a nova avaliação do investimento direto estrangeiro. A Comissão analisará a forma este processo poderá ser apoiado por um Código de Cooperação Policial. Os serviços repressivos dos Estados-Membros recorrem cada vez mais ao apoio e aos conhecimentos especializados a nível da UE, enquanto o INTCEN da UE tem desempenhado um papel fundamental na promoção do intercâmbio de informações estratégicas entre os serviços de informações e de segurança dos Estados-Membros, fornecendo um conhecimento da situação às instituições da UE[114]. A **Europol** pode também desempenhar um papel fundamental no alargamento da sua cooperação com países terceiros no domínio da luta contra a criminalidade e o terrorismo, em consonância com outras políticas e instrumentos externos da UE. No entanto, a Europol enfrenta hoje uma série de graves restrições - nomeadamente no que se refere ao intercâmbio direto de dados pessoais com entidades privadas - que a impedem de apoiar eficazmente os Estados-Membros na luta contra o terrorismo e a criminalidade. O mandato da Europol está agora a ser avaliado para determinar a forma como deve ser melhorado, a fim de assegurar que este organismo pode desempenhar cabalmente as suas funções. Neste contexto, as autoridades competentes a nível da UE (como o OLAF, a Europol, a Eurojust e a Procuradoria Europeia) devem também cooperar mais estreitamente e melhorar o intercâmbio de informações.

Outro elemento fundamental é o desenvolvimento da **Eurojust**, a fim de maximizar as sinergias entre a cooperação policial e a cooperação judiciária. A UE beneficiaria também de uma maior

[112] Como o Plano de Ação para a Estratégia de Segurança Marítima da UE, que permitiu alcançar importantes resultados com a cooperação no domínio das funções de guarda costeira entre as agências competentes da UE.

[113] A luta da UE contra a criminalidade organizada em 2019 (Conselho, 2020).

[114] O INTCEN da UE serve como ponto de acesso único para que os serviços de informação e segurança dos Estados-Membros possam proporcionar à UE uma apreciação da situação com base em informações.

coerência estratégica: a **EMPACT**[115], o ciclo político da UE lutar contra a grande criminalidade internacional organizada, fornece às autoridades uma metodologia baseada nas informações criminais que lhes permite enfrentar conjuntamente as ameaças criminosas mais importantes que afetam a UE. Esta plataforma produziu resultados operacionais importantes[116] na última década. Com base na experiência dos profissionais, o mecanismo existente deve ser racionalizado e simplificado para melhor responder às ameaças criminosas mais prementes e em permanente evolução num novo ciclo político 2022-2025.

É essencial dispor de **informações** pertinentes e em tempo útil para o trabalho quotidiano dos serviços repressivos. Apesar do desenvolvimento de novas bases de dados a nível da UE para a segurança e a gestão das fronteiras, muitas informações estão ainda localizadas em bases de dados nacionais ou são intercambiadas fora destes instrumentos. O resultado é uma carga de trabalho adicional significativa, atrasos e um risco acrescido de perda de informações fundamentais. Processos mais eficazes, mais rápidos e mais simples, que envolvam toda a comunidade de segurança, permitiriam a obtenção de resultados mais satisfatórios. Dispor dos instrumentos adequados é fundamental para que o intercâmbio de informações seja utilizado de acordo com todas as suas potencialidades no quadro de uma luta eficaz contra a criminalidade, com todas as garantias necessárias, para que a partilha de dados respeite a legislação em matéria de proteção de dados e os direitos fundamentais. À luz da evolução tecnológica, forense e de proteção de dados, e tendo em conta as necessidades operacionais, a UE poderá ponderar a necessidade de modernizar instrumentos como as **Decisões Prüm de 2008**, estabelecendo o intercâmbio automatizado de dados de ADN, impressões digitais e dados de registo de veículos, a fim de permitir o intercâmbio automatizado de outras categorias de dados já disponíveis nos Estados-Membros em bases de dados criminais ou outras para efeitos de investigações criminais. Por outro lado, a Comissão analisará a possibilidade de proceder ao intercâmbio de registos criminais a fim de ajudar a determinar se existe um registo criminal de uma pessoa noutros Estados-Membros e facilitar o acesso a esses registos uma vez identificados, com todas as garantias necessárias.

As **informações sobre os viajantes** contribuíram para melhorar os controlos nas fronteiras, reduzir a migração irregular e identificar pessoas que representam riscos de segurança. As informações antecipadas sobre os passageiros são os dados biográficos de cada passageiro recolhidos pelas transportadoras aéreas durante o registo (*check-in*) e enviados antecipadamente às autoridades de controlo das fronteiras no destino. A revisão do quadro jurídico[117] poderá permitir uma utilização mais eficaz das informações, assegurando simultaneamente o cumprimento da legislação em matéria de proteção de dados e facilitando o fluxo de passageiros. Os registos de identificação dos passageiros (PNR) são os dados fornecidos pelos passageiros aquando da reserva dos voos. A implementação da Diretiva PNR[118] é fundamental e a Comissão continuará a apoiar e a velar pela sua aplicação. Além disso, como ação a médio prazo, a Comissão lançará uma revisão da atual abordagem em matéria de **transferência de dados PNR para países terceiros**.

A **cooperação judicial** é um complemento necessário dos esforços dos serviços de polícia para combater a criminalidade transnacional. A cooperação neste domínio sofreu uma profunda evolução nos últimos 20 anos. Organismos como a **Procuradoria Europeia** e a **Eurojust** devem dispor dos meios necessários para poder exercer cabalmente as suas funções ou devem ser reforçados. A cooperação entre os profissionais da justiça poderá também ser reforçada, através de novas medidas relativas ao reconhecimento mútuo das decisões judiciais, à formação judiciária e ao intercâmbio de informações. O objetivo deve ser aumentar a confiança mútua entre os juízes e os magistrados do Ministério Público, essencial para agilizar os processos transfronteiriços. A utilização de **tecnologias**

[115] EMPACT - Plataforma multidisciplinar europeia contra as ameaças criminosas.
[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.
[117] Diretiva 2004/82/CE do Conselho relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras.
[118] Diretiva (UE) 2016/681 relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.

digitais pode também melhorar a eficiência dos nossos sistemas judiciários. Está a ser criado um novo sistema de intercâmbio digital para a transmissão de decisões europeias de investigação, de pedidos de auxílio judiciário mútuo, bem como de comunicações relacionadas com estas atividades entre Estados-Membros, com o apoio da Eurojust. A Comissão colaborará com os Estados-Membros para acelerar a implantação dos sistemas informáticos necessários a nível nacional.

A cooperação internacional é também fundamental para a eficácia dos serviços repressivos e para a cooperação judicial. Os acordos bilaterais com os principais parceiros desempenham um papel-chave na obtenção de informações e elementos de prova provenientes de países terceiros. A **Interpol**, uma das maiores organizações intergovernamentais de polícia criminal, desempenha um papel importante neste domínio. A Comissão estudará formas possíveis de reforçar a cooperação com a Interpol, incluindo o eventual acesso às bases de dados da Interpol e a intensificação da cooperação operacional e estratégica. Os serviços repressivos da UE também dependem dos principais países parceiros para detetar e investigar criminosos e terroristas. As **parcerias em matéria de segurança entre a UE e os países terceiros** poderão ser reforçadas, a fim de estreitar a cooperação na luta contra as ameaças comuns, como o terrorismo, a criminalidade organizada, a cibercriminalidade, o abuso sexual de crianças e o tráfico de seres humanos. Esta abordagem tem por base os interesses comuns em matéria de segurança e assenta nos diálogos estabelecidos em matéria de cooperação e segurança.

Como a informação, o intercâmbio de conhecimentos especializados pode ser particularmente útil para aumentar o grau de preparação dos serviços repressivos face às **ameaças não tradicionais**. Para além de incentivar o intercâmbio de boas práticas, a Comissão irá estudar um possível **mecanismo de coordenação a nível da UE para as forças policiais** em caso de acontecimentos de força maior como, por exemplo, pandemias. A pandemia provou também que o policiamento da comunidade digital, assente num enquadramento jurídico suscetível de agilizar o policiamento em linha, será fundamental para combater a criminalidade e o terrorismo. As parcerias entre comunidades policiais, fora de linha e em linha, podem ser úteis na prevenção da criminalidade e atenuar o impacto da criminalidade organizada, da radicalização e das atividades terroristas. O estabelecimento de ligações entre as soluções policiais de âmbito local e regional e as soluções policiais de âmbito nacional e europeu é um fator de sucesso fundamental para a União da Segurança da UE no seu conjunto.

O contributo das fronteiras externas sólidas

Uma gestão moderna e eficiente das fronteiras externas tem a dupla vantagem de manter a integridade de Schengen e de garantir a segurança dos nossos cidadãos. A mobilização de todos os intervenientes pertinentes para tirar o máximo proveito da segurança nas fronteiras pode ter um impacto real na prevenção da criminalidade e do terrorismo transfronteiriço. As atividades operacionais conjuntas da recentemente reforçada Guarda Europeia de Fronteiras e Costeira[119] contribuem para a prevenção e a deteção da criminalidade transnacional nas **fronteiras externas** e para além das fronteiras da UE. As atividades aduaneiras de deteção de riscos de segurança em todas as mercadorias antes da sua chegada à UE e de controlo das mercadorias quando chegam são cruciais na luta contra a criminalidade e o terrorismo transfronteiriço. O futuro Plano de Ação sobre a União Aduaneira anunciará medidas destinadas a reforçar a gestão dos riscos e a reforçar a segurança interna, nomeadamente através da avaliação da viabilidade de uma ligação entre os sistemas de informação pertinentes para a análise dos riscos em matéria de segurança.

O quadro para a **interoperabilidade entre os sistemas de informação da UE** no domínio da justiça e dos assuntos internos foi adotado em maio de 2019. Esta nova arquitetura visa melhorar a eficiência e a eficácia dos sistemas de informação novos ou modernizados[120]. O referido quadro

[119] Constituído pela Agência Europeia da Guarda de Fronteiras e Costeira (Frontex) e pelas autoridades dos Estados-Membros de guarda das fronteiras e de guarda costeira.

[120] O Sistema de Entrada/Saída (SES), o Sistema Europeu de Informação e Autorização de Viagem (ETIAS), Sistema europeu alargado de informação sobre os registos criminais de nacionais de países (ECRIS-TCN), o Sistema de Informação de Schengen, o Sistema de Informação sobre Vistos e o futuro Eurodac atualizado.

permitirá que os agente de polícia, os guardas de fronteira e os funcionários dos serviços de migração tenham uma informação mais rápida e sistemática. Contribuirá para uma identificação correta das pessoas e para combater a fraude de identidade. Para que tal seja uma realidade, a implementação da interoperabilidade deve ser uma prioridade, tanto a nível político como técnico. A cooperação estreita entre os organismos da UE e todos os Estados-Membros será fundamental para alcançar o objetivo da plena interoperabilidade até 2023.

A **falsificação de documentos de viagem** é considerada um dos crimes mais frequentemente cometidos. Facilita o movimento clandestino de criminosos e terroristas e desempenha um papel fundamental no tráfico de seres humanos e no comércio de droga[121]. A Comissão examinará as possibilidades de ampliar os trabalhos em curso sobre as normas de segurança aplicáveis aos documentos de residência e de viagem da UE, nomeadamente através da digitalização. A partir de agosto de 2021, os Estados-Membros começarão a emitir bilhetes de identidade e documentos de residência de acordo com normas de segurança harmonizadas, incluindo um chip que contenha identificadores biométricos que possam ser verificados por todas as autoridades de fronteira da UE. A Comissão acompanhará a aplicação destas novas normas, incluindo a substituição gradual dos documentos atualmente em circulação.

Reforçar a investigação e a inovação em matéria de segurança

Os trabalhos destinados a garantir a cibersegurança e a combater a criminalidade organizada, a cibercriminalidade e o terrorismo dependem em grande medida do desenvolvimento futuro de instrumentos destinados a contribuir para criar novas tecnologias mais protegidas e seguras, a enfrentar os desafios tecnológicos e a sustentar a atividade dos serviços repressivos, com o apoio de parceiros privados e do setor industrial.

A inovação deve ser vista como um instrumento estratégico para combater as ameaças atuais e antecipar tanto os riscos como as oportunidades futuras. As tecnologias inovadoras podem trazer novos instrumentos para ajudar os serviços repressivos e outros intervenientes no domínio da segurança. A inteligência artificial e a análise de megadados poderão tirar partido da computação de alto desempenho, a fim de permitir uma melhor deteção e uma análise rápida e exaustiva[122]. Uma condição prévia essencial para o desenvolvimento de tecnologias fiáveis é o estabelecimento de conjuntos de dados de alta qualidade, que permitam às autoridades competentes formar, testar e validar algoritmos.[123]. De um modo mais geral, o risco de dependência tecnológica é hoje elevado - a UE é, por exemplo, um importador líquido de produtos e serviços de cibersegurança, com tudo o que isso representa para a economia e as infraestruturas críticas. Para dominar a tecnologia e garantir a continuidade do aprovisionamento também em caso de acontecimentos e crises adversos, a Europa deve estar presente e dispor de capacidades nas áreas críticas das cadeias de valor pertinentes.

A **investigação, a inovação e o desenvolvimento tecnológico** da UE oferecem a oportunidade de ter em conta a dimensão da segurança na fase de desenvolvimento e aplicação destas tecnologias. A próxima geração das propostas de financiamento da UE pode funcionar como um estímulo importante neste sentido[124]. As iniciativas relativas aos espaços europeus de dados e às infraestruturas de computação em nuvem integram desde o princípio a vertente da segurança. O Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a

[121] A ligação entre a fraude documental e o tráfico de seres humanos é estabelecida no segundo relatório sobre os progressos realizados na luta contra o tráfico de seres humanos, COM(2018) 777, e no documento de trabalho dos serviços da Comissão que o acompanha (SWD(2018) 473), bem como no relatório da Europol de 2016 intitulado «*Situation Report Trafficking in human beings in the EU*» (Relatório sobre a situação relativa ao tráfico de seres humanos na UE).

[122] Tal deveria basear-se na estratégia da Comissão em matéria de inteligência artificial.

[123] Uma estratégia europeia para os dados, COM(2020) 66 final.

[124] As propostas da Comissão relativas ao Horizonte Europa, ao Fundo para a Segurança Interna, ao Fundo de Gestão Integrada das Fronteiras, ao Programa EUInvest, ao Fundo Europeu de Desenvolvimento Regional e ao Programa Europa Digital apoiarão o desenvolvimento e a implantação de tecnologias e soluções inovadoras em matéria de segurança ao longo da cadeia de valor da segurança.

Rede de Centros Nacionais de Coordenação[125] visam criar uma estrutura eficaz e eficiente para reunir e partilhar as capacidades de investigação e os resultados no domínio da cibersegurança. O programa espacial da UE presta serviços de apoio à segurança da UE, dos seus Estados-Membros e dos seus cidadãos[126].

Com mais de 600 projetos lançados num valor total próximo dos 3 mil milhões de EUR desde 2007, a investigação no domínio da segurança financiada pela UE é um instrumento fundamental para impulsionar a tecnologia e o conhecimento em benefício de soluções no domínio da segurança. No âmbito da revisão do mandato da Europol, a Comissão analisará a criação de uma **polo europeu de inovação para a segurança interna**[127] que terá como objetivo procurar soluções comuns para os desafios e oportunidades partilhados em matéria de segurança, que os Estados-Membros poderiam não estar em condições de explorar isoladamente. A cooperação é fundamental para concentrar o investimento da forma mais eficiente e para desenvolver tecnologias inovadoras com benefícios tanto em termos de segurança como económicos.

Competências e sensibilização

A sensibilização para as questões de segurança e a aquisição de competências para fazer face a potenciais ameaças são essenciais para construir uma sociedade mais resiliente, com empresas, administrações e indivíduos mais bem preparados. Os desafios em termos de infraestruturas informáticas e sistemas eletrónicos revelaram a necessidade de melhorar a nossa capacidade de preparação e resposta em matéria de cibersegurança. A pandemia também pôs em evidência a importância da digitalização em todos os domínios da economia e da sociedade da UE.

Mesmo um **conhecimento básico das ameaças à segurança** e da forma de as combater podem ter um impacto real na resiliência da sociedade. A consciência dos riscos ligados à cibercriminalidade e a necessidade de proteger-se a si próprios podem reforçar a proteção fornecida dos prestadores de serviços para combater os ciberataques. As informações sobre os perigos e os riscos ligados ao tráfico de drogas podem dificultar o êxito dos criminosos. A UE pode encorajar a divulgação das melhores práticas, nomeadamente através da rede de centros para uma Internet mais segura[128], e assegurar que esses objetivos são integrados nos seus próprios programas.

O futuro Plano de Ação para a Educação Digital deve incluir medidas específicas para reforçar as competências informáticas de toda a população no domínio da segurança. A Agenda de Competências[129], recentemente adotada, apoia o desenvolvimento de competências ao longo da vida. Inclui ações específicas para aumentar o número de licenciados em ciências, tecnologia, engenharia, artes e matemática necessários em domínios de ponta, como a cibersegurança. Ações complementares, financiadas pelo programa Europa Digital, permitirão aos profissionais acompanhar a evolução das ameaças à segurança e, ao mesmo tempo, colmatar as lacunas neste domínio do mercado de trabalho da UE. O objetivo geral será o de permitir que as pessoas adquiram competências para fazer face às ameaças à segurança e que as empresas encontrem os profissionais de que necessitam neste domínio. Os futuros Espaço Europeu da Investigação e Espaço Europeu da

[125] Proposta de 12 de setembro de 2018 de regulamento do Parlamento Europeu e do Conselho que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação, COM(2018) 630.

[126] Por exemplo, o Copernicus presta serviços que permitem a vigilância das fronteiras externas e a vigilância marítima da UE, contribuindo para combater a pirataria e o contrabando e apoiar infraestruturas críticas. Quando estiver plenamente operacional, Copernicus constituirá um fator determinante nas missões e operações civis e militares.

[127] O polo trabalhará igualmente com a Frontex, a CEPOL, a eu-LISA e o Centro Comum de Investigação.

[128] Ver www.betterinternetforkids.eu: o portal central e os centros nacionais para uma Internet mais segura são atualmente financiados no âmbito da vertente telecomunicações do Mecanismo Interligar a Europa (MIE) e um financiamento futuro foi proposto no âmbito do Programa Europa Digital.

[129] Agenda de Competências para a Europa em prol da competitividade sustentável, da justiça social e da resiliência, COM(2020) 274 final.

Educação irão também promover carreiras nos domínios da ciência, da tecnologia, da engenharia, das artes e da matemática.

O acesso das **vítimas** aos seus direitos é também importante; as vítimas devem receber a assistência e o apoio de que necessitam tendo em conta a sua situação específica. Devem ser envidados esforços especiais no que diz respeito às minorias e às vítimas mais vulneráveis, como as crianças ou as mulheres vítimas de tráfico para fins de exploração sexual ou expostas à violência doméstica[130].

O reforço das **competências necessárias para as funções policiais** desempenha um papel especial. As atuais e as novas ameaças tecnológicas exigem mais investimentos a favor da melhoria das competências dos membros dos serviços repressivos, desde o início da carreira e ao longo desta. A CEPOL é um parceiro essencial para assistir os Estados-Membros nesta tarefa. A formação dos serviços repressivos em matéria de racismo e a xenofobia e, de um modo mais geral, dos direitos dos cidadãos, deve ser uma componente essencial de uma cultura de segurança da UE. Os sistemas de justiça nacionais e os profissionais da justiça devem também estar equipados para se adaptarem e responderem a desafios sem precedentes. A formação é, assim, fundamental para permitir às autoridades no terreno explorarem esses instrumentos em situação operacional. Além disso, devem ser envidados todos os esforços para reforçar a integração da perspetiva de género e reforçar a participação das mulheres nos serviços repressivos.

Principais ações
• Reforço do mandato da Europol • Estudo de um «Código de Cooperação Policial» da UE e de uma coordenação policial em tempos de crise • Consolidação da Eurojust a fim de assegurar uma ligação entre as autoridades judiciárias e os serviços repressivos • Revisão da Diretiva relativa a Informações Prévias sobre Passageiros • Comunicação sobre a dimensão externa dos registos de identificação dos passageiros • Reforço da cooperação entre a UE e a Interpol • Definição de um quadro de negociação com os principais países terceiros sobre a partilha de informações • Melhoria das normas de segurança aplicáveis aos documentos de viagem • Estudo de um polo de inovação europeu para a segurança interna

V. Conclusões

Num mundo cada vez mais turbulento, a União Europeia é ainda amplamente considerada como um dos locais mais seguros e protegidos. Contudo, não podemos dar este dado por adquirido.

A nova estratégia da União da Segurança estabelece as bases para um ecossistema de segurança que abrange todo o espetro da sociedade europeia. A referida estratégia assenta na constatação de que a segurança é uma responsabilidade partilhada. A questão da segurança afeta todos os cidadãos. Todos os organismos governamentais, as empresas, as organizações sociais, as instituições e os cidadãos devem assumir as suas próprias responsabilidades, a fim de tornar as nossas sociedades mais seguras.

As questões de segurança têm agora de ser encaradas numa perspetiva muito mais ampla do que no passado. Há que superar as falsas distinções entre meio físico e meio digital. A estratégia da UE sobre a União da Segurança reúne toda a gama de necessidades em matéria de segurança e centra-se nas áreas que serão as mais críticas para a segurança da UE nos próximos anos. Reconhece igualmente que as ameaças à segurança não respeitam as fronteiras geográficas e dá conta da

[130] Ver Estratégia para a Igualdade de Género, COM(2020) 152; Estratégia sobre os direitos das vítimas, COM(2020) 258; e Estratégia europeia para uma Internet melhor para as crianças, COM(2012) 196.

interligação crescente entre a segurança interna e a segurança externa[131]. Neste contexto, será importante que a UE coopere com os parceiros internacionais para a proteção de todos os cidadãos da UE e mantenha uma estreita coordenação com a ação externa da UE na implementação da presente estratégia.

A nossa segurança está ligada aos nossos valores fundamentais. Todas as ações e iniciativas propostas na presente estratégia respeitarão plenamente os direitos fundamentais e os nossos valores europeus. Estes constituem os alicerces do nosso modo de vida europeu e devem permanecer no centro de toda a nossa atividade.

Por último, a Comissão está plenamente consciente do facto de que qualquer política ou ação vale o que vale a sua execução. Por conseguinte, é necessário insistir sem descanso na aplicação e execução adequadas da legislação existente e futura. Serão elaborados relatórios periódicos sobre a União da Segurança e a Comissão manterá o Parlamento Europeu, o Conselho e as partes interessadas devidamente informados e envolvidos em todas as ações pertinentes. Por outro lado, a Comissão está pronta a participar e a organizar debates conjuntos com as instituições sobre a estratégia da União da Segurança, a fim de fazer um balanço dos progressos alcançados e analisar os desafios futuros.

A Comissão convida o Parlamento Europeu e o Conselho a aprovarem a presente estratégia da União da Segurança como base para a cooperação e a ação conjunta em matéria de segurança nos próximos cinco anos.

[131] Ver a Estratégia global da UE