Conselho da
União Europeia

Bruxelas, 18 de outubro de 2023
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	18 de outubro de 2023
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2023) 665 final
Assunto:	COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO relativa ao sexto relatório intercalar sobre a execução da Estratégia da UE para a União da Segurança

Envia-se em anexo, à atenção das delegações, o documento COM(2023) 665 final.

Anexo: COM(2023) 665 final

COMISSÃO
EUROPEIA

Bruxelas, 18.10.2023
COM(2023) 665 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

relativa ao sexto relatório intercalar sobre a execução da Estratégia da UE para a União da Segurança

I. Introdução

Há três anos, a Comissão adotou a Estratégia para a União da Segurança 2020-2025[1], que define as principais prioridades da União no domínio da segurança. Desde então, realizámos grandes progressos no âmbito dos quatro pilares da estratégia, adotando legislação histórica em todos os domínios, desde a proteção das entidades críticas ao reforço da ciber-resiliência. O conjunto das ameaças à segurança na Europa e na nossa vizinhança tem continuado, contudo, a evoluir. Os ataques terroristas recentemente perpetrados numa escola em França e nas ruas de Bruxelas recordam-nos de formal brutal da urgência de continuar a adaptar e a reforçar a nossa arquitetura de segurança. Os riscos suscitados pelos ciberataques têm vindo a aumentar, estimulados pela intervenção nos conflitos em curso de terceiros mal-intencionados. As ameaças híbridas continuam a multiplicar-se, nomeadamente a desinformação. A Europol identificou a guerra de agressão da Rússia contra a Ucrânia como estando na origem de um forte aumento dos ciberataques contra alvos da UE, alguns dos quais de grandes proporções, politicamente motivados e coordenados por grupos de piratas informáticos pró-russos[2]. Esses ataques causaram bloqueios do acesso à Internet e a interrupção de serviços essenciais, como as redes de energia[3].

A Estratégia para a União da Segurança foi concebida a fim de equipar a UE para enfrentar melhor uma grande variedade de ameaças em rápida evolução. À medida que enfrentámos as crises colocadas pela pandemia e pela guerra, os acontecimentos demonstraram a importância da abordagem adotada na Estratégia – a nossa determinação em estabelecer elos em todo o ecossistema de segurança da UE e em quebrar a compartimentação entre as dimensões cibernética e física da segurança, incluindo a luta contra a criminalidade organizada e o terrorismo, bem como a luta contra a radicalização.

No entanto, a vigilância exige que continuemos a avaliar continuamente o que tem falhado nos nossos esforços para manter os cidadãos seguros. A estratégia centra-se nos domínios prioritários em que a UE pode gerar valor acrescentado para ajudar os Estados-Membros a reforçar a segurança de todas as pessoas que vivem na Europa. Desde a sua adoção, foram abordadas todas as ações previstas, tendo sido incorporadas novas ações para dar resposta aos desafios em matéria de segurança.

Globalmente a Comissão já apresentou 36 iniciativas legislativas no âmbito da Estratégia para a União da Segurança. Em relação a mais de metade destas propostas, as negociações interinstitucionais já foram concluídas com a adoção de nova legislação reforçada, como se descreve no quadro em anexo. Continuam, contudo, em negociação pelo Parlamento Europeu e pelo Conselho várias iniciativas fundamentais propostas pela Comissão. Indo a atual legislatura terminar com as eleições europeias de junho de 2024, torna-se necessário acelerar os trabalhos para concluir estes dossiês pendentes, de modo que os cidadãos possam beneficiar plenamente da União da Segurança. O presente sexto relatório intercalar sobre a Estratégia da UE para a União da Segurança centra-se, por conseguinte, na definição dos dossiês legislativos

---

1 COM(2020) 605.

2 Ataques distribuídos de negação de serviço (DDoS): ver o relatório Spotlight da Europol intitulado *Cyber-attacks: the apex of crime-as-a-service*, 13 de setembro de 2023.

3 Durante o conflito na Ucrânia tem sido utilizado *software* malicioso para destruir dados e sistemas, afetando, por exemplo, o acesso à Internet de milhares de assinantes na UE, bem como uma importante empresa de energia alemã que perdeu o acesso à monitorização remota de mais de 5 800 turbinas eólicas. *The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict* (não traduzido para português), Estudo do Parlamento Europeu, setembro de 2023 – PE 702.594.

e não legislativos cruciais sobre a União da Segurança adotados pela Comissão, em relação aos quais é necessário envidar mais esforços para a sua finalização e aplicação efetiva.

No caso da legislação da UE já acordada, os seus benefícios só se farão sentir quando forem postos em prática. Os esforços devem concentrar-se na sua transposição correta e integral, bem como na sua execução e aplicação pelos Estados-Membros. Em 2023, a Comissão continuou a assegurar a concretização da Estratégia da UE para a União da Segurança, utilizando os seus poderes institucionais para instaurar processos por infração sempre que os Estados-Membros não transpuseram ou transpuseram incorretamente a legislação da UE.

O presente relatório resume igualmente as áreas em que a ação dos Estados-Membros e/ou das agências da UE é essencial para a execução. As agências da UE desempenham um papel crucial no apoio à execução das iniciativas da União da Segurança e as suas responsabilidades têm vindo a desenvolver-se nos últimos anos. O relatório descreve algumas das novas tarefas principais que lhes foram atribuídas para prestar um maior apoio aos Estados-Membros na execução de iniciativas fundamentais no âmbito da União da Segurança.

Além disso, a situação geopolítica veio evidenciar a importância da segurança externa para a nossa segurança interna. Um quadro interno da UE mais forte no domínio da segurança está intrinsecamente ligado ao reforço das parcerias e da cooperação com países terceiros. A UE deve continuar a explorar ativamente formas de participação a nível mundial que contribuam para garantir a segurança dos seus cidadãos.

II. Um ambiente de segurança adequado às exigências do futuro

Cibersegurança e resiliência das infraestruturas

No âmbito da União da Segurança, a UE está empenhada em assegurar que todos os cidadãos e empresas europeus estejam bem protegidos, tanto na Internet como fora dela, e em promover um ciberespaço aberto, seguro e estável. A dimensão, a frequência e o impacto crescentes dos incidentes de cibersegurança representam uma grave ameaça para o funcionamento das redes e sistemas de informação, assim como para o mercado interno. A guerra de agressão da Rússia contra a Ucrânia exacerbou ainda mais esta ameaça e as atuais tensões geopolíticas são agravadas por intervenções de uma multiplicidade de intervenientes associados a Estados, criminosos e «hacktivistas». A sabotagem, no outono passado, dos gasodutos Nord Stream veio evidenciar como setores essenciais como a energia, as infraestruturas digitais, os transportes e o espaço, estão dependentes da existência de infraestruturas críticas resilientes. O recente incidente envolvendo um gasoduto submarino e um cabo de dados na Estónia e na Finlândia ilustra a necessidade de um elevado nível de preparação para enfrentar este tipo de situações. Embora a causa dos danos continue por esclarecer e investigações ainda se encontrem em curso, a partilha de informações a diferentes níveis entre os Estados-Membros e a Comissão tem sido encorajadora. As perturbações em causa não tiveram efeitos imediatos em termos de conectividade à Internet ou de segurança do aprovisionamento de gás a nível europeu ou local, o que demonstra os progressos realizados e a intensificação dos esforços de preparação dos últimos meses.

Por conseguinte, é essencial dispor de um quadro jurídico claro e sólido para assegurar a proteção e a resiliência das infraestruturas críticas. Neste contexto, registou-se um avanço crucial com a adoção paralela da Diretiva revista relativa a medidas destinadas a garantir um

elevado nível comum de cibersegurança na União (SRI 2)[4], e da Diretiva relativa à resiliência das entidades críticas (REC)[5], que entraram em vigor em 16 de janeiro de 2023. Os Estados-Membros foram instados a transpor estes atos legislativos fundamentais de forma célere e integral, o mais tardar até 17 de outubro de 2024, de modo a criar um quadro da União suficientemente sólido para proteger as infraestruturas críticas contra ameaças físicas e ciberameaças.

Em julho de 2023, através de um regulamento delegado, a Comissão definiu serviços essenciais nos 11 setores abrangidos pela Diretiva REC[6]. A próxima etapa consiste na realização de avaliações de risco sobre estes serviços pelos Estados-Membros. Na sequência da Recomendação do Conselho[7] de 8 de dezembro de 2022, intensificaram-se os trabalhos sobre os testes de resistência das infraestruturas críticas, começando pelo setor da energia, e sobre o reforço da cooperação com a OTAN e com os principais países parceiros. Em junho de 2023, este trabalho deu origem a um relatório do grupo de trabalho UE-OTAN sobre a resiliência das infraestruturas críticas, que delineia os atuais desafios em matéria de segurança para as infraestruturas críticas em quatro setores fundamentais (energia, transportes, infraestruturas digitais e espaço) e formula recomendações para reforçar a resiliência. As referidas recomendações, nomeadamente sobre o reforço da coordenação, da partilha de informações e dos exercícios, estão a ser implementadas pessoal da UE e da OTAN no contexto do diálogo estruturado UE-OTAN sobre resiliência.

Paralelamente, em 6 de setembro de 2023, a Comissão adotou uma proposta[8] de recomendação do Conselho relativa a um plano de ação destinado a reforçar a coordenação da resposta a nível da UE a tentativas de perturbação de infraestruturas críticas com importante relevância transfronteiriça. Em 4 de outubro de 2023, foi organizado um exercício sob a forma de um debate sobre o plano baseado em cenários, a fim de testar a forma como este se aplicaria na prática e de fundamentar as negociações em curso sobre a proposta no âmbito do Conselho.

Na sequência dos apelos do Conselho[9], a Comissão, o alto representante e o grupo de cooperação Segurança das Redes e da Informação (SRI) têm vindo a realizar avaliações de risco e a elaborar cenários de risco do ponto de vista da cibersegurança. Este trabalho incide inicialmente nos setores das telecomunicações e da eletricidade. A participação de todos os organismos e redes pertinentes, civis ou militares, dá origem, pela primeira vez, a uma avaliação abrangente e inclusiva à escala da União. Além disso, irá complementar as avaliações coordenadas dos riscos de segurança das cadeias de aprovisionamento críticas realizadas no âmbito da Diretiva SRI 2, bem como as avaliações de risco e os testes de resistência das infraestruturas críticas nos setores da energia, das infraestruturas digitais de comunicação, dos transportes e do espaço. A fim de assegurar a coordenação e a coerência, estas atividades devem apoiar-se reciprocamente para ajudar a estabelecer uma abordagem normalizada e orientar o desenvolvimento de exercícios futuros. O êxito destas ações dependerá agora da participação ativa dos Estados-Membros.

---

4 Diretiva (UE) 2022/2555, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União e Diretiva (UE) 2018/1972 (Diretiva SRI 2).

5 Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho.

6 C(2023) 4878.

7 Recomendação do Conselho de 8 de dezembro de 2022 relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas.

8 COM(2023) 526.

9 Conclusões do Conselho, de 23 de maio de 2022, sobre o desenvolvimento da postura da União Europeia no ciberespaço e Apelo de Nevers, de 9 de março de 2022, para reforçar as capacidades da UE em matéria de cibersegurança.

O funcionamento das economias e das sociedades depende cada vez mais de serviços e dados relacionados com o espaço, especialmente no domínio da segurança e da defesa. O espaço é um domínio estratégico cada vez mais disputado e a sua importância para a segurança tem vindo a aumentar, em especial na sequência da invasão russa da Ucrânia. A Estratégia Espacial da UE para a Segurança e a Defesa foi adotada em março de 2023 com o objetivo de reforçar a nossa postura estratégica e a nossa autonomia no espaço. Enquanto medida fundamental decorrente desta estratégia, a Comissão Europeia irá propor, em 2024, um ato legislativo da UE sobre o espaço que regule a segurança, a sustentabilidade e a resiliência das atividades espaciais na UE.

Tendo em conta a dimensão externa, as infraestruturas seguras sustentam a resiliência da economia e das cadeias de aprovisionamento mundiais[10], razão pela qual a Estratégia Global Gateway da UE incorpora uma forte dimensão de segurança. De igual modo, dadas as interligações entre as infraestruturas da UE e as de países parceiros, é essencial uma maior cooperação internacional para reforçar a ciber-resiliência mundial e apoiar um ciberespaço livre, aberto, seguro e protegido.

Ato legislativo sobre a ciber-resiliência europeia

A garantia de que os consumidores e as empresas podem contar com produtos digitais seguros é crucial para a cibersegurança europeia. A Comissão procurou dar resposta a esta necessidade na sua proposta de ato legislativo sobre a ciber-resiliência europeia[11], adotada em 15 de setembro de 2022. Esta introduziria requisitos transversais de cibersegurança obrigatórios para os produtos com elementos digitais durante cinco anos ou para todo o seu ciclo de vida (consoante o que for mais curto). Criaria as condições para a conceção e o desenvolvimento de produtos com elementos digitais seguros, assegurando que o *hardware* e o *software* são colocados no mercado com o menor número possível de vulnerabilidades. Seria um marco fundamental no reforço das normas de cibersegurança da Europa em todos os domínios e é provável que se torne um ponto de referência internacional, proporcionando vantagens claras para a indústria de cibersegurança da União nos mercados mundiais. O Parlamento Europeu e o Conselho adotaram as respetivas posições em julho de 2023 e as negociações deverão avançar rapidamente.

A certificação da cibersegurança também desempenha um papel crucial no aumento da confiança nos produtos e serviços de tecnologias da informação e comunicação, permitindo que os consumidores, as empresas e as autoridades façam escolhas informadas com um nível adequado de cibersegurança. Os trabalhos sobre a certificação da cibersegurança continuam a avançar, assentando o sistema de certificação da cibersegurança em critérios comuns da UE que estão a ser avaliados no âmbito da comitologia. O projeto de Sistema de Certificação da Segurança da Nuvem (EUCS) está atualmente em fase de preparação pela Agência da União Europeia para a Cibersegurança (ENISA) e está a ser discutido no âmbito do Grupo Europeu para a Certificação da Cibersegurança. O intenso trabalho com peritos de vários setores, consumidores e fornecedores deverá conduzir a uma abordagem jurídica e técnica sólida que proporcione as garantias de segurança necessárias compatíveis com o direito da União, os compromissos internacionais e as obrigações da OMC. Além disso, a ENISA está a preparar o projeto de sistema EU5G e a carteira de identidade digital da UE (EUIDW). Serão essenciais esforços concertados de todos os Estados-Membros para reforçar a segurança global dos produtos, serviços e processos das tecnologias da informação e comunicação.

---

[10] JOIN(2021) 30.
[11] COM(2022) 454.

Regulamentos em matéria de segurança da informação e cibersegurança para as instituições, órgãos e organismos da UE

Os regulamentos propostos em conjunto, em março de 2022, para reger a cibersegurança e a segurança da informação para as próprias instituições da União evoluíram a ritmos diferentes. No passado mês de junho, foi alcançado um acordo político sobre o Regulamento Cibersegurança, que permite reforçar a postura em matéria de cibersegurança de todas as instituições, órgãos e organismos da UE e reflete a importância que a UE atribui à rápida aplicação desta proposta. Nesta situação, suscita especial preocupação que a proposta paralela relativa à segurança da informação, essencial para completar um quadro legislativo sólido para as instituições, órgãos e organismos da UE, tenha registado progressos inesperadamente lentos. Ambas as propostas devem ser adotadas antes das eleições para o Parlamento Europeu, a fim de tornar a administração europeia credível e resiliente no atual contexto geopolítico. Um conjunto mínimo de regras e normas de segurança da informação para todas as instituições, órgãos e organismos da UE criaria segurança para todas as partes envolvidas e asseguraria uma proteção coerente contra a evolução das ameaças às suas informações, tanto classificadas como não classificadas. No seu conjunto, estas novas regras proporcionariam uma base estável para o intercâmbio seguro de informações entre as instituições, órgãos e organismos da UE e com os Estados-Membros, com práticas e medidas normalizadas para proteger os fluxos de informação. Nesse sentido, respondem a múltiplos apelos do Conselho no sentido de reforçar a resiliência das instituições, órgãos e organismos da UE e proteger melhor o processo de tomada de decisões da União contra interferências mal-intencionadas.

Ato legislativo sobre a cibersolidariedade

Com base no quadro estratégico e legislativo sólido já em vigor, a proposta de ato legislativo sobre a cibersolidariedade[12] adotada em 18 de abril de 2023 pela Comissão, contribuirá para melhorar a deteção de ciberameaças e reforçar a resiliência e a preparação a todos os níveis do ecossistema de cibersegurança da UE. Estes objetivos seriam concretizados através de três ações principais:

(1) A implantação de um ***escudo de cibersegurança da UE*** para criar e reforçar capacidades comuns de deteção e conhecimento da situação, que consistiria em centros de operações de segurança nacionais («SOC nacionais») e transfronteiriços («SOC transfronteiriços»).
(2) A criação de um ***mecanismo de ciberemergência*** para apoiar os Estados-Membros na preparação, resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande escala. O apoio à resposta a incidentes incluiria a reserva da UE para a cibersegurança, que também estaria disponível para as instituições, órgãos e organismos europeus da União, bem como para os países terceiros associados ao Programa Europa Digital, desde que o seu acordo de associação ao Programa Europa Digital assim o preveja.
(3) A criação de um ***mecanismo europeu de análise de incidentes de cibersegurança*** para analisar e avaliar incidentes significativos ou em grande escala específicos O relatório de análise pós-incidente seria coordenado e preparado pela ENISA.

Já tiveram início os debates no Conselho e no Parlamento Europeu. A finalização das negociações antes do final do atual mandato do Parlamento Europeu daria um impulso significativo aos esforços para proteger os cidadãos e as empresas em toda a União.

[12] COM(2023) 209.

Academia de Competências de Cibersegurança

Embora as ciberameaças estejam a aumentar, a UE necessita urgentemente de profissionais com as aptidões e competências necessárias para prevenir, detetar, dissuadir e defender a UE contra ciberataques. As suas necessidades de efetivos no domínio da cibersegurança estão atualmente estimadas em 883 000 profissionais, ao passo que as vagas por preencher variavam entre 260 000 e 500 000 em 2022. Todos os setores da sociedade devem ser incentivados a contribuir para colmatar esta lacuna, mas cumpre notar, em especial, que em 2022 as mulheres representavam apenas 20 % dos licenciados em cibersegurança e 19 % dos especialistas em tecnologias da informação e comunicação. No âmbito do Ano Europeu das Competências 2023, a Comissão adotou, em 18 de abril de 2023[13], uma iniciativa acolhida favoravelmente pelos Estados-Membros[14] para criar uma Academia de Competências de Cibersegurança com vista a colmatar o défice de talentos neste domínio. A Academia de Competências de Cibersegurança reuniria as iniciativas existentes em matéria de competências de cibersegurança e melhoraria a coordenação A Comissão incentiva os Estados-Membros, as autoridades regionais e locais, bem como as entidades públicas europeias, a adotar estratégias ou iniciativas específicas em matéria de competências de cibersegurança ou a integrar competências de cibersegurança em estratégias ou iniciativas pertinentes de âmbito mais vasto (por exemplo, cibersegurança, competências digitais, emprego, etc.). A participação das partes interessadas do setor privado será também essencial para reduzir o défice de competências de cibersegurança e a escassez de mão de obra associada na Europa.

Aeronaves não tripuladas

Uma outra ameaça crescente para os espaços públicos e as infraestruturas críticas é a utilização maliciosa de aeronaves não tripuladas (*drones*). Os incidentes envolvendo drones tornaram-se mais frequentes dentro e fora da União e as soluções de combate a estas aeronaves são um instrumento fundamental para as autoridades policiais e outras autoridades públicas na União, bem como para os operadores privados de infraestruturas críticas. Ao mesmo tempo, a utilização legítima de aeronaves não tripuladas está a dar um contributo importante para a dupla transição ecológica e digital[15]. Tal como anunciado na Estratégia Drone 2.0, adotada em novembro de 2022, a Comissão adota hoje uma comunicação sobre como combater potenciais ameaças suscitadas por aeronaves não tripuladas, apoiada por dois manuais com orientações práticas sobre aspetos técnicos fundamentais[16]. Essa iniciativa visa proporcionar um quadro político abrangente e harmonizado, com um entendimento comum das regras em vigor para combater as eventuais ameaças colocadas pelas aeronaves não tripuladas e adaptar-se, na medida do necessário, à rápida evolução tecnológica. Os Estados-Membros e os operadores privados pertinentes são convidados a trabalhar em estreita colaboração com a Comissão para assegurar a sua plena aplicação.

Segurança marítima e da aviação

As atividades ilícitas, como a pirataria, os assaltos à mão armada no mar, a introdução clandestina de migrantes e o tráfico de seres humanos, armas e estupefacientes, bem como o terrorismo, continuam a constituir um desafio para a segurança marítima e são agravadas pela evolução das ameaças, incluindo os ataques híbridos e os ciberataques. A Comissão e o alto representante adotaram, em 10 de março de 2023, uma comunicação conjunta que atualiza a

[13] COM(2023) 207.
[14] Conclusões do Conselho de 22 de maio de 2023 sobre a política de ciberdefesa da UE.
[15] COM(2022) 652.
[16] COM(2023) 659.

Estratégia de Segurança Marítima da UE[17], a qual deve agora ser executada em conformidade com o plano de ação atualizado.

No domínio da segurança da aviação, a Comissão adotou, em 2 de fevereiro de 2023, um documento de trabalho dos serviços da Comissão intitulado *Working towards an enhanced and more resilient aviation security policy* [Trabalhar rumo a uma política de segurança da aviação reforçada e mais resiliente][18], que contém um programa ambicioso para: 1) modernizar a arquitetura regulamentar para a segurança da aviação, 2) promover o desenvolvimento e a adoção de soluções mais inovadoras, e 3) atualizar a base de referência em matéria de segurança da aviação, de modo que os aeroportos da União possam beneficiar plenamente de tecnologias novas e de ponta para fazer face às ameaças mais prioritárias. É necessário implementar catorze ações emblemáticas no prazo de dois anos.

A Comissão insta o Parlamento Europeu e o Conselho a concluírem urgentemente as negociações interinstitucionais e, em qualquer caso, antes do final do mandato do atual Parlamento Europeu, quanto aos seguintes dossiês ainda pendentes:

- a proposta de ato legislativo sobre a ciber-resiliência,
- a proposta de ato legislativo sobre a cibersolidariedade,
- a proposta de regulamento relativo à segurança da informação para as instituições, órgãos e organismos da UE.

A Comissão insta os Estados-Membros a:

- prosseguir a transposição da Diretiva Resiliência das Entidades Críticas como uma prioridade, bem como os testes de resistência das infraestruturas críticas no setor da energia,
- adotar a recomendação do Conselho sobre um plano de ação para a coordenação da resposta a nível da UE a perturbações em infraestruturas críticas com importante relevância transfronteiriça,
- transpor a Diretiva SRI 2 para reforçar a cibersegurança de entidades essenciais e importantes,
- participar ativamente na realização de avaliações dos riscos de cibersegurança e na elaboração de cenários de risco das infraestruturas críticas e das cadeias de aprovisionamento,
- dar seguimento à Academia de Competências em Cibersegurança, com uma forte participação a nível europeu e estratégias ou iniciativas nacionais específicas em matéria de competências de cibersegurança, reunindo as principais partes interessadas, nomeadamente os órgãos de poder local e regional,
- colaborar com os operadores privados pertinentes e com a Comissão com vista a assegurar a execução de todas as ações enumeradas na comunicação sobre o combate às potenciais ameaças resultantes dos *drones*,
- aplicar o Plano de Ação da Estratégia de Segurança Marítima da UE e comunicar regularmente informações sobre os resultados alcançados,
- implementar as 14 ações emblemáticas identificadas para reforçar a segurança da aviação.

[17] JOIN(2023) 8.
[18] SWD(2023) 37.

III. Fazer face à evolução das ameaças

As novas tensões geopolíticas têm demonstrado drasticamente como o desafio de segurança para a UE não só tem vindo a aumentar, como é cada vez mais volátil e agravado pela natureza híbrida de muitas ameaças. A segurança também tem de responder à evolução da sociedade e da tecnologia. A pandemia de COVID-19 aumentou as oportunidades para os cibercriminosos, tendo-se assistido, em especial, a uma ameaça crescente da pornografia infantil em linha. Os criminosos e os intervenientes mal-intencionados estão sempre prontos a explorar a evolução tecnológica. Perante estas ameaças, muitas vezes complexas e multidimensionais, torna-se necessária uma ação decisiva e coerente da UE.

Regulamento relativo ao combate ao abuso sexual de crianças em linha

A avaliação da ameaça da criminalidade organizada dinamizada pela Internet, conduzida pela Europol, concluiu que, em 2022, a exploração e o abuso sexual de crianças tinham aumentado ainda mais em termos de frequência e gravidade, continuando os criminosos a tirar partido das possibilidades técnicas para ocultar as suas ações e identidades[19]. O atual sistema baseado na deteção e denúncia voluntárias por parte das empresas tem-se revelado insuficiente para proteger as crianças. Um regulamento provisório permite a deteção e comunicação voluntárias por parte das empresas, desde que tal seja lícito ao abrigo do Regulamento Geral sobre a Proteção de Dados (RGPD). Esse regulamento caduca em agosto de 2024. Em maio de 2022, a Comissão propôs um regulamento[20] para combater a utilização abusiva de serviços em linha para efeitos de abuso sexual de crianças. O quadro proposto coloca uma forte ênfase na prevenção. As empresas seriam obrigadas a avaliar o risco de abuso sexual de crianças através dos respetivos sistemas e a tomar medidas preventivas. Como medida de último recurso, apenas em caso de risco significativo, os tribunais nacionais ou as autoridades administrativas independentes podem emitir ordens de deteção específicas aos prestadores de serviços. A criação de um novo centro independente da UE facilitaria os esforços dos prestadores de serviços, funcionando como plataforma de conhecimentos especializados, fornecendo informações fiáveis sobre o material identificado, recebendo e analisando denúncias de abusos sexuais de crianças em linha facultadas pelos prestadores de serviços em linha a fim de identificar denúncias incorretas e prestar apoio às vítimas. É essencial que as novas regras sejam adotadas e aplicadas o mais rapidamente possível, a fim de proteger as crianças contra futuros abusos, impedir que os materiais em causa voltem a aparecer na Internet e levar os criminosos a julgamento. Estão em curso negociações no Conselho e no Parlamento com o objetivo de se chegar a acordo sobre o dossiê antes do final do mandato do Parlamento.

Diretiva relativa ao combate à violência contra as mulheres e à violência doméstica

A ciberviolência contra as mulheres, incluindo no contexto da violência doméstica, surgiu como uma nova forma deste tipo de violência, que se propaga para além dos diferentes Estados-Membros através da Internet e de outras ferramentas informáticas. Em março de 2022, a Comissão propôs uma diretiva para combater a violência contra as mulheres e a violência doméstica, incluindo regras específicas em matéria de ciberviolência e medidas para colmatar as lacunas em matéria de proteção, acesso à justiça e prevenção. A sua adoção e aplicação precoces proporcionariam aos Estados-Membros instrumentos adicionais para combater esta forma de criminalidade. Os colegisladores encetaram negociações interinstitucionais em julho de 2023, que pretendem concluir antes do final do atual mandato do Parlamento Europeu.

---

[19] Europol (2023), Avaliação da ameaça da criminalidade organizada dinamizada pela Internet (iOCTA) 2023.
[20] COM(2022) 209.

Cibersegurança das redes 5G

A segurança das redes 5G é uma das principais prioridades da Comissão e uma componente essencial da sua Estratégia para a União da Segurança. As redes 5G são uma infraestrutura central que constitui a base de uma vasta gama de serviços essenciais para o funcionamento do mercado interno e para desempenhar funções sociais e económicas vitais. Em 15 de junho de 2023, as autoridades dos Estados-Membros da UE representadas no grupo de cooperação SRI, com o apoio da Comissão e da ENISA, publicaram um segundo relatório intercalar sobre a aplicação do conjunto de instrumentos da UE para a cibersegurança das redes 5G. De acordo com o relatório, 24 Estados-Membros adotaram ou estão a preparar medidas legislativas que conferem às autoridades nacionais poderes para realizar uma avaliação dos fornecedores e impor restrições, e dez Estados-Membros impuseram-nas efetivamente. No entanto, serão necessárias novas medidas para evitar vulnerabilidades para a União no seu conjunto, com impactos negativos potencialmente graves na segurança dos utilizadores individuais e das empresas em toda a União e das infraestruturas críticas da União. Todos os Estados-Membros devem aplicar sem demora este conjunto de instrumentos. No mesmo dia, a Comissão adotou uma comunicação sobre a aplicação do conjunto de instrumentos pelos Estados-Membros e sobre as suas próprias atividades de comunicação institucional e de financiamento da União, em que salientou fortes preocupações quanto aos riscos para a segurança da UE colocados pelos fornecedores de equipamentos de comunicações em redes móveis Huawei e ZTE. Neste contexto, a Comissão está a tomar medidas para evitar a exposição das suas comunicações institucionais às redes móveis que utilizam a Huawei e a ZTE como fornecedores. Os contratos públicos excluirão novos serviços de conectividade que dependam de equipamentos desses fornecedores e a Comissão irá trabalhar com os Estados-Membros e os operadores de telecomunicações para garantir que esses fornecedores sejam progressivamente excluídos dos serviços de conectividade existentes nas instalações da Comissão. A Comissão está também a estudar a forma de refletir esta decisão nos programas e instrumentos de financiamento pertinentes da União, em plena conformidade com o direito da União.

Acesso aos dados para efeitos de repressão policial

Na era digital dos dias de hoje, quase todos os crimes têm uma componente digital. As tecnologias e os instrumentos estão também a ser utilizados para fins criminosos, incluindo os indispensáveis para garantir a necessidade de cibersegurança, proteção de dados e privacidade da nossa sociedade. Isto torna cada vez mais difícil exercer a repressão policial em toda a UE, a fim de salvaguardar a segurança pública e prevenir, detetar, investigar e agir penalmente contra a criminalidade. Embora tenham sido envidados esforços significativos a nível da União e a nível nacional, nomeadamente através da adoção de legislação, bem como de iniciativas de reforço das capacidades e de inovação, persistem desafios jurídicos e técnicos neste domínio. A Comissão, em associação com a Presidência do Conselho, criou um grupo de alto nível sobre o acesso aos dados para uma repressão policial eficaz, a fim de proporcionar uma plataforma colaborativa para um vasto conjunto de partes interessadas e peritos, com vista a avaliar os desafios que os forças policiais e as autoridades judiciais enfrentam (por exemplo, cifragem, conservação de dados, redes 5G e normalização). A Comissão espera que o grupo de alto nível formule recomendações equilibradas, sólidas e exequíveis até junho de 2024, refletindo a complexidade destas questões, nomeadamente do ponto de vista da cibersegurança e da proteção de dados. Os Estados-Membros e os peritos que integram o grupo são, por conseguinte, incentivados a participar ativamente neste processo e a trabalhar no sentido de encontrar soluções eficazes, lícitas e consensualmente aceites.

Ameaças híbridas

Num contexto geopolítico em que as ameaças híbridas têm vindo a aumentar em complexidade e sofisticação, a Bússola Estratégica da UE para a Segurança e a Defesa[21] proporcionou uma avaliação comum das ameaças e dos desafios que se colocam à União, bem como um plano de ação estratégico. O aumento dos comportamentos maliciosos no ciberespaço por parte de Estados e intervenientes não estatais, nomeadamente no contexto da guerra contra a Ucrânia, pôs ainda mais em evidência o ciberespaço como um domínio de política externa e de segurança. Os riscos potenciais de ações maliciosas e de desinformação exigem uma vigilância especial durante os períodos eleitorais, nomeadamente durante o período que antecede as eleições europeias de 2024.

Tendo em conta os elevados riscos de efeitos colaterais, a UE continuou a desenvolver atividades de reforço das capacidades cibernéticas e a promover parcerias com países terceiros, nomeadamente através de ciberdiálogos específicos, a fim de contribuir ativamente para a resiliência global. Foram desenvolvidos, revistos e reforçados vários instrumentos para melhorar a capacidade da União para enfrentar eficazmente ameaças híbridas, como descrito no 7.º relatório intercalar sobre as ameaças híbridas, publicado em 14 de setembro de 2023[22]. Estas incluem:

- o conjunto de instrumentos da UE contra as ameaças híbridas, a fim de assegurar um quadro para uma resposta coordenada e bem informada às ameaças e campanhas híbridas;
- os trabalhos em curso para criar equipas de resposta rápida às ameaças híbridas da UE, capazes de prestar apoio adaptado a curto prazo aos Estados-Membros, aos países parceiros e às missões e operações da política comum de segurança e defesa (PCSD);
- o protocolo revisto da UE para a luta contra as ameaças híbridas («manual tático da UE»)[23] que descreve os processos e as estruturas da União que lidam com as ameaças e campanhas híbridas;
- as orientações de execução revistas do quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas[24](«conjunto de instrumentos de ciberdiplomacia»), que permite o desenvolvimento de estratégias sustentadas, adaptadas, coerentes e coordenadas contra ciberameaças persistentes;
- o conjunto de instrumentos relativos à manipulação da informação e ingerência por parte de agentes estrangeiros (FIMI), a fim de reforçar os instrumentos existentes da União para prevenir, dissuadir e responder a essa ameaça;
- a política de ciberdefesa da UE[25], a fim de intensificar as capacidades de ciberdefesa da UE, reforçar o conhecimento da situação e coordenar toda a gama de opções defensivas disponíveis, a fim de reforçar a resiliência, responder aos ciberataques e assegurar a solidariedade e a assistência mútua.

Por conseguinte, os Estados-Membros são incentivados a prosseguir e a reforçar a sua cooperação neste domínio, assegurando a aplicação efetiva dos instrumentos acima referidos, nomeadamente através de exercícios regulares, e chegando a acordo sobre o conceito de equipas de resposta rápida às ameaças híbridas, que fornecerá orientações para novas medidas com vista à criação das equipas.

[21] Documento do Conselho 7371/22.
[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23 de 8 de junho de 2023.
[25] JOIN(2022) 49.

A inteligência artificial no contexto da aplicação coerciva da lei

A inteligência artificial (IA) tornou-se rapidamente uma característica comum da vida quotidiana. Os efeitos da utilização da IA na cibercriminalidade e na cibersegurança ainda não são plenamente conhecidos, mas é evidente que virão colocar novos desafios. Embora possa trazer benefícios quando utilizada de forma segura e controlada, a IA pode ter suscitar riscos nas mãos de intervenientes mal-intencionados, nomeadamente ajudando os criminosos a ocultar as suas identidades em crimes como o terrorismo e o abuso sexual de crianças. Por conseguinte, é fundamental que as autoridades se mantenham a par das evoluções, a fim de prevenir abusos e dar resposta a utilizações abusivas[26]. As negociações sobre a proposta de Regulamento Inteligência Artificial visam abordar estas questões e entraram numa fase crucial, em que os colegisladores estão agora a debater questões técnicas e políticas que determinarão as interações com esta tecnologia nos próximos anos. Será essencial encontrar soluções equilibradas, especialmente no que diz respeito às aplicações de alto risco, nomeadamente no domínio da aplicação coerciva da lei.

A Comissão insta o Parlamento Europeu e o Conselho a concluírem urgentemente as negociações interinstitucionais e, em qualquer caso, antes do final do mandato do atual Parlamento Europeu, sobre os seguintes dossiês pendentes:

- a proposta de regulamento relativo à luta contra o abuso sexual de crianças em linha,
- a proposta de diretiva relativa ao combate à violência contra as mulheres e à violência doméstica,
- a proposta de regulamento que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial).

A Comissão insta os Estados-Membros a:

- concretizar sem demora a plena aplicação do conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G,
- apoiar o trabalho do grupo de alto nível sobre o acesso aos dados para uma aplicação coerciva eficaz da lei, com vista a formular recomendações claras, sólidas e exequíveis que respondam de forma proporcionada aos desafios atuais e expectáveis,
- tomar medidas, em cooperação com o alto representante, para assegurar a aplicação efetiva do conjunto de instrumentos da UE contra as ameaças híbridas, do conjunto revisto de instrumentos de ciberdiplomacia e do conjunto de instrumentos FIMI, nomeadamente através de exercícios regulares e tendo em conta a dinâmica mundial,
- chegar a acordo sobre o conceito de equipas de resposta rápida a ameaças híbridas.

IV. Proteger os europeus do terrorismo e da criminalidade organizada

O risco de acontecimentos mundiais ou locais desencadearem novos surtos de terrorismo está sempre presente. Paralelamente, a criminalidade organizada e o tráfico de droga figuram entre as ameaças mais graves à segurança da UE. A fim de intensificar os esforços coletivos da União na luta contra essas ameaças, estão em curso trabalhos coletivos sobre a aplicação da Estratégia

[26] Ver, por exemplo, o relatório da Europol publicado em 17 de abril de 2023: *ChatGPT - the impact of Large Language Models on Law Enforcement.*

da UE para Lutar contra a Criminalidade Organizada[27], da Estratégia da UE em matéria de Luta contra o Tráfico de Seres Humanos[28], da Agenda da UE de Luta contra a Droga[29] e da Agenda da UE de Luta contra o Terrorismo[30]. No entanto, para dar resposta à preocupante deterioração da situação em termos de criminalidade organizada e tráfico de droga, importa intensificar o trabalho dos Estados-Membros e da UE para reforçar a resposta coletiva às redes criminosas e proteger melhor as vítimas da criminalidade. Será publicado, em simultâneo com o presente relatório, um roteiro da UE para combater o tráfico de droga e a criminalidade organizada[31].

No domínio da luta contra o terrorismo, a UE tem vindo igualmente a reforçar o seu conjunto de instrumentos externos[32], tirando pleno partido dos diálogos de alto nível em matéria de luta contra o terrorismo e da rede de peritos em matéria de luta contra o terrorismo/segurança nas delegações da UE, bem como através da participação em fóruns multilaterais, nomeadamente na qualidade de copresidente do Fórum Mundial contra o Terrorismo.

Tráfico de droga

Com o novo mandato da Agência da UE para a Droga, que será aplicável a partir de julho de 2024, a UE ficará mais bem equipada para fazer face a um complexo problema de segurança e de saúde que afeta milhões de pessoas na UE e a nível mundial. A Comissão tem estado igualmente a rever[33] os regulamentos relativos aos precursores de drogas[34], a fim de fazer face aos principais desafios identificados na avaliação de 2020[35], que salientou a necessidade de dar resposta aos desafios colocados pelos pré-precursores[36] para reduzir a oferta de drogas ilegais.

No entanto, face ao aumento sem precedentes das drogas ilícitas disponíveis na Europa, é imperativo intensificar a luta contra o tráfico de droga, em cooperação com os parceiros internacionais. São necessárias medidas adicionais por parte dos Estados-Membros e da UE para desmantelar as redes criminosas e assegurar uma maior proteção das vítimas da criminalidade. A Comissão apresenta hoje um roteiro da UE para combater o tráfico de droga e a criminalidade organizada, que define 17 ações em quatro domínios prioritários: reforçar a resiliência dos centros logísticos com uma Aliança Europeia dos Portos; desmantelar as redes criminosas; intensificar os esforços de prevenção e reforçar a cooperação com os parceiros internacionais. Estas ações deverão ser levadas a cabo em 2024 e em 2025.

Armas de fogo

O tráfico de armas de fogo alimenta a criminalidade organizada na UE e na sua vizinhança. Estima-se que cerca de 35 milhões de armas de fogo ilícitas estejam nas mãos de civis na UE e cerca de 630 000 estão referenciadas como roubadas ou perdidas no Sistema de Informação Schengen. Com o desenvolvimento da entrega rápida de encomendas e das novas tecnologias,

---

27 COM(2021) 170.
28 COM(2021) 171.
29 COM(2020) 606.
30 COM(2020) 795.
31 COM(2023) 641.
32 Tal como preconizado no âmbito da Bússola Estratégica e das Conclusões do Conselho sobre a abordagem da dimensão externa da ameaça terrorista e extremista violenta em constante evolução, adotadas em junho de 2022.
33 Precursores de drogas – legislação da UE (regras revistas) (europa.eu)
34 Regulamento (CE) n.º 273/2004 relativo aos precursores de drogas e Regulamento (CE) n.º 111/2005 do Conselho, que estabelece regras de controlo do comércio de precursores de drogas entre a Comunidade e países terceiros.
35 COM(2020) 768.
36 Ação 23 do plano de ação antidroga, COM(2020) 606.

como a impressão 3D, o tráfico de armas de fogo tem assumido novas formas para escapar aos controlos. A guerra de agressão da Rússia contra a Ucrânia aumentou igualmente o risco de proliferação de armas de fogo. Em outubro de 2022, a Comissão adotou uma proposta para atualizar a legislação em vigor em matéria de importação, exportação e trânsito de armas de fogo civis, a fim de colmatar as lacunas existentes nas regras em vigor suscetíveis de aumentar o número de armas de fogo introduzidas ilegalmente e desviadas para a UE[37]. A médio prazo, as novas regras ajudarão a reduzir o risco de evasão aos embargos no caso das exportações de armas de fogo para uso civil e a aumentar os controlos da importação deste tipo de armas de fogo de países terceiros. Ambos os colegisladores ainda terão de adotar as suas posições sobre este dossiê a fim de de chegar a acordo sobre o mesmo antes do final do mandato do Parlamento.

Tráfico de seres humanos

O tráfico de seres humanos constitui uma forma particularmente séria de criminalidade organizada e uma grave violação dos direitos fundamentais. As vítimas são traficadas na UE, principalmente para fins de exploração sexual e laboral, mas também de mendicidade forçada, de criminalidade e não só. Em dezembro de 2022, a Comissão propôs alterar a Diretiva relativa à luta contra o tráfico de seres humanos[38] com regras atualizadas para suprir as carências do enquadramento jurídico em vigor. Uma vez adotada, a diretiva revista acrescentará o casamento forçado e a adoção ilegal ao seu âmbito de aplicação e introduzirá uma referência explícita à dimensão em linha do tráfico de seres humanos. Incluirá igualmente um regime obrigatório de sanções para os autores dos crimes e formalizará a criação de mecanismos de referenciação nacionais para melhorar a identificação precoce e o reenvio para assistência e apoio às vítimas a nível transnacional. O recurso, com conhecimento de causa, a serviços prestados por vítimas de tráfico será criminalizado e a recolha anual de dados sobre o tráfico de seres humanos, a publicar pelo Eurostat, passará a ser obrigatória. O Conselho adotou a sua orientação geral em junho de 2023, embora o Parlamento Europeu ainda tenha de adotar a sua posição. É necessária uma ação rápida para chegar a acordo antes do final do mandato deste Parlamento.

Criminalidade ambiental

A criminalidade ambiental tornou-se uma ameaça mundial, crescendo a uma taxa anual estimada de 5 % a 7 %. Os lucros avultados que podem ser gerados, as lacunas jurídicas entre os Estados-Membros e o baixo risco de deteção atraem a criminalidade organizada. Segundo a Europol, há indícios de que o produto destas atividades é utilizado para financiar o terrorismo. Em dezembro de 2021, a Comissão adotou uma proposta para substituir a Diretiva de 2008 relativa à proteção do ambiente através do direito penal. A proposta centra-se no aperfeiçoamento e atualização das definições de categorias de criminalidade ambiental e na definição de tipos e níveis de sanções eficazes, dissuasivas e proporcionadas para as pessoas singulares e coletivas. Os novos crimes incluem infrações relacionadas com a desflorestação ilegal, com violações da legislação da UE em matéria de produtos químicos, com a extração ilegal de águas superficiais ou subterrâneas e com a reciclagem ilegal de navios. A proposta visa reforçar significativamente a cadeia de combate ao crime e a cooperação transnacional entre as autoridades dos Estados-Membros e as agências e organismos da UE. O Parlamento Europeu e o Conselho adotaram as respetivas posições sobre a proposta e encontram-se num processo de negociação que deverão poder concluir até ao final do ano. Será necessário executar um plano de ação revisto[39] contra o tráfico de espécies selvagens para reforçar ainda mais a prevenção e a repressão do crime.

---

37 COM(2022) 480.
38 COM(2022) 732.
39 COM(2022) 581.

Recuperação e perda de bens

Privar os criminosos de receitas ilícitas é fundamental para desmantelar a criminalidade organizada. É por esta razão que, para além da proposta que prevê o acesso das autoridades policiais a informações sobre contas bancárias em toda a UE[40] (para a qual foi alcançado um acordo político em junho de 2023), a Comissão apresentou, em maio de 2022, uma proposta sobre a recuperação e a perda de bens[41], a fim de reforçar as capacidades de deteção, identificação, congelamento, perda e administração de bens. As principais disposições dessa proposta dizem respeito aos requisitos aplicáveis às investigações financeiras e aos poderes e instrumentos adicionais dos gabinetes de recuperação de ativos, bem como a medidas de congelamento e perda mais eficazes aplicáveis a um conjunto alargado de crimes. Uma das novas infrações penais às quais estas medidas passariam a ser aplicáveis é a violação de medidas restritivas da União. Em dezembro de 2022, a Comissão adotou uma proposta distinta para harmonizar as definições penais de violação de medidas restritivas da União, bem como as sanções que lhe são aplicáveis. A aplicação eficaz e a fiscalização do cumprimento das medidas restritivas da União continuam a ser uma das principais prioridades da Comissão, reforçada pelo trabalho do Grupo de Missão Congelar e Apreender criado pela Comissão em resposta à guerra de agressão da Rússia contra a Ucrânia. Em relação a ambas as propostas, o Parlamento Europeu e o Conselho adotaram as respetivas posições com o objetivo de chegar a acordo até ao final do corrente ano.

Pacote legislativo em matéria de luta contra o branqueamento de capitais

O branqueamento de capitais está associado a praticamente todas as atividades criminosas que geram receitas criminosas na UE[42], constituindo o pacote proposto, por conseguinte, um instrumento fundamental para combater a criminalidade na UE. Em julho de 2021, a Comissão apresentou propostas ambiciosas para reforçar as medidas da UE para prevenir o branqueamento de capitais e o financiamento do terrorismo[43], com quatro propostas legislativas destinadas a reforçar a prevenção e a deteção de tentativas de branqueamento de receitas ilícitas ou de financiamento por parte de criminosos de atividades terroristas através do sistema financeiro. Em maio de 2023, os colegisladores adotaram uma das quatro iniciativas do pacote legislativo com vista a assegurar a rastreabilidade das transferências de criptoativos[44]. O regulamento será aplicável a partir de 30 de dezembro de 2024, data a partir da qual todos os prestadores de serviços de criptoativos terão de recolher e conservar informações sobre o ordenante e o destinatário das transferências de criptoativos. As três propostas restantes têm por objetivo i) criar uma nova autoridade da UE em matéria de luta contra o branqueamento de capitais, a fim de assegurar uma fiscalização coerente e de elevada qualidade em todo o mercado interno, incluindo das entidades transnacionais de maior risco, apoiando e coordenando o trabalho das unidades de informação financeira, ii) estabelecer regras harmonizadas para o setor privado, incluindo a introdução de um limite de 10 000 EUR a nível da UE para pagamentos de grandes montantes em numerário em troca de serviços e bens, e iii) reforçar os poderes e os instrumentos de cooperação das autoridades competentes. Espera-se que o pacote legislativo reforce significativamente a capacidade da UE para combater o branqueamento de capitais e proteger os cidadãos da UE do terrorismo e da criminalidade organizada. As três propostas

[40] COM(2021) 429.
[41] COM(2022) 245.
[42] Europol, *Enterprising criminals – Europe's fight against the global networks of financial and economic crime*, 2020.
[43] COM(2021) 420.
[44] Regulamento (UE) 2023/1113 do Parlamento Europeu e do Conselho, de 31 de maio de 2023, relativo às informações que acompanham as transferências de fundos e de determinados criptoativos e que altera a Diretiva (UE) 2015/849.

pendentes encontram-se em fase de negociação pelos colegisladores com vista a chegar a acordo sobre este dossiê antes do final do mandato do Parlamento.

A Comissão insta o Parlamento Europeu e o Conselho a concluírem urgentemente as negociações interinstitucionais e, em qualquer caso, antes do final do mandato do atual Parlamento Europeu, quanto aos seguintes dossiês pendentes:

- a proposta de diretiva relativa à recuperação e perda de bens,
- a proposta de diretiva para harmonizar as definições penais de violação de medidas restritivas da União, bem como as sanções que lhe são aplicáveis,
- a proposta de diretiva relativa à luta contra o tráfico de seres humanos,
- a proposta de diretiva relativa à melhoria da proteção do ambiente através do direito penal,
- a proposta de um pacote legislativo em matéria de luta contra o branqueamento de capitais,
- a proposta de atualização da legislação em vigor em matéria de importação, exportação e trânsito de armas de fogo civis.

A Comissão insta os Estados-Membros e as agências e organismos da UE a:

- trabalharem em conjunto com vista à execução das 17 ações do roteiro da UE de luta contra o tráfico de droga e a criminalidade organizada em 2023 e 2024.

V. Um sólido ecossistema europeu de segurança

Nos últimos anos, as ameaças à segurança têm assumido cada vez mais uma dimensão transnacional, exigindo mais sinergias e uma cooperação mais estreita a todos os níveis. Desde a adoção da Estratégia para a União da Segurança, foram tomadas iniciativas importantes para maximizar a cooperação transnacional, racionalizar e modernizar os instrumentos e procedimentos disponíveis, tanto nas fronteiras externas como no interior do espaço Schengen, bem como para reforçar o intercâmbio de informações entre as autoridades policiais e judiciárias, a fim de melhor combater a criminalidade organizada. Neste contexto, a aplicação efetiva do quadro de interoperabilidade para o intercâmbio de dados é um pilar importante para reforçar a segurança e dar uma resposta europeia eficaz às ameaças transnacionais, garantindo simultaneamente a liberdade de circulação interna.

Reforço do intercâmbio de informações no espaço Schengen: informação antecipada sobre passageiros (API), registo de identificação dos passageiros (PNR) e Prüm II

As duas propostas API adotadas pela Comissão em dezembro de 2022[45] reforçariam a segurança interna da União ao disponibilizar às autoridades policiais dos Estados-Membros instrumentos adicionais para combater a criminalidade grave e o terrorismo. Mais concretamente, as informações antecipadas sobre os voos intra-UE, utilizadas juntamente com o PNR dos passageiros aéreos, permitiriam às autoridades policiais dos Estados-Membros aumentar significativamente a eficácia das respetivas investigações graças a intervenções mais bem direcionadas. É importante que as regras propostas sejam adotadas o mais rapidamente

[45] COM(2022) 729, COM(2022) 73.

possível, o que não só apoiaria a luta contra a criminalidade organizada e o terrorismo, mas reduziria também consideravelmente a necessidade de controlos sistemáticos de todos os passageiros em caso de reintrodução temporária de controlos nas fronteiras internas, facilitando as viagens aéreas e a liberdade de circulação. Em 6 de setembro de 2023, a Comissão Europeia recomendou ao Conselho que autorizasse o início de negociações com a Suíça, a Islândia e a Noruega tendo em vista a celebração de acordos sobre a transferência de dados PNR. A adoção destas três recomendações contribuiria para uma política externa coerente e eficaz da UE em matéria de PNR.

Os intercâmbios no âmbito do mecanismo de Prüm são utilizados diariamente pela polícia para combater a criminalidade organizada, a droga, o terrorismo, a exploração sexual e o tráfico de seres humanos. A proposta de regulamento relativo ao intercâmbio automatizado de dados para efeitos de cooperação policial («Prüm II»)[46] revê o atual quadro jurídico de Prüm com vista a colmatar as lacunas de informação e a reforçar a prevenção, deteção e investigação de infrações penais na UE. As regras revistas em matéria de intercâmbio automatizado de dados para efeitos de cooperação policial completam as propostas relativas à cooperação policial no presente mandato, juntamente com a recomendação do Conselho, já adotada, que reforça a cooperação operacional transfronteiras e a diretiva relativa ao intercâmbio de informações entre as autoridades de aplicação da lei. A rápida adoção e aplicação destes instrumentos conexos melhoraria, facilitaria e aceleraria o intercâmbio de dados entre as autoridades policiais e ajudaria a identificar os criminosos.

Sistema plenamente interoperável de gestão das fronteiras para um espaço Schengen seguro, forte, digital e unido

O bom funcionamento do espaço Schengen sem fronteiras internas depende da confiança mútua entre os Estados-Membros, o que, por sua vez, assenta em controlos eficazes, quer nas fronteiras externas da União, quer como medidas alternativas no território dos Estados-Membros. A alteração do Código das Fronteiras Schengen[47] proposta pela Comissão define a forma como os Estados-Membros podem utilizar melhor as alternativas aos controlos nas fronteiras internas que podem proporcionar um elevado nível de segurança. É importante que a alteração do Código das Fronteiras Schengen seja adotada e aplicada na íntegra, a fim de assegurar um nível elevado e proporcionado de segurança no espaço Schengen. Continua igualmente a ser desenvolvida a nova arquitetura dos sistemas de informação da UE para apoiar melhor o trabalho das autoridades nacionais, de modo a garantir a gestão da segurança e das fronteiras. Esta inclui o Sistema de Informação Schengen renovado, o Sistema Europeu de Informação e Autorização de Viagem, o Sistema de Entrada/Saída, a atualização do Sistema de Informação sobre Vistos e o quadro de interoperabilidade para ligar os sistemas em plena segurança. Uma vez plenamente concluída, esta nova arquitetura facultará às autoridades nacionais informações de segurança mais abrangentes e fiáveis. Todas as componentes do quadro de interoperabilidade são essenciais, o que significa que um atraso num aspeto ou num Estado-Membro resulta na implantação tardia de todas elas. Os atrasos no desenvolvimento técnico do Sistema de Entrada/Saída devem ser reduzidos ao mínimo, para que o sistema possa começar a funcionar o mais rapidamente possível e possam ser implementados todos os elementos fundamentais do quadro de interoperabilidade.

[46] COM(2021) 784.
[47] COM(2021) 891.

A proposta de triagem[48] reforçaria a segurança no espaço Schengen, ao criar regras uniformes relativas à identificação dos nacionais de países terceiros que não preenchem as condições de entrada referidas no Código das Fronteiras Schengen, submetendo-os aos controlos sanitários e de segurança nas fronteiras externas. O sistema Eurodac proposto apoiaria estes objetivos, identificando, após a triagem, qualquer pessoa que possa constituir uma potencial ameaça para a segurança interna. Essa identificação facilitaria, por sua vez, a aplicação da proposta de Regulamento Gestão do Asilo e da Migração. A Comissão insta os colegisladores a concluírem rapidamente as negociações sobre estes dossiês antes do final da atual legislatura.

Luta contra a corrupção

A corrupção é extremamente prejudicial para as nossas democracias, para a economia e para a nossa segurança, uma vez que funciona como um viabilizador da criminalidade organizada e da ingerência estrangeira hostil. A prevenção e o combate bem-sucedidos da corrupção são essenciais para salvaguardar os valores da UE e a eficácia das suas políticas, bem como para defender o Estado de direito e a confiança nos governantes e nas instituições públicas. Tal como anunciado pela presidente Ursula von der Leyen no discurso sobre o estado da União de 2022, a Comissão adotou, em 3 de maio de 2023, um pacote de medidas de combate à corrupção[49]**.** A proposta da Comissão de uma nova diretiva relativa à luta contra a corrupção inclui regras reforçadas que criminalizam a corrupção e harmonizam as sanções que lhe saõ aplicáveis em toda a UE. Por outro lado, possibilita investigações e procedimentos penais eficazes e coloca a tónica na prevenção e criação de uma cultura de integridade em que não é tolerada a corrupção . Os debates sobre essa proposta no Parlamento Europeu e no Conselho já tiveram início. Além disso, os Estados-Membros são convidados a aplicar as recomendações decorrentes do pilar anticorrupção do relatório de 2023 sobre o Estado de direito, adotado em 5 de julho de 2023. Uma proposta do alto representante, apoiada pela Comissão, criaria igualmente um regime de sanções específico da política externa e de segurança comum (PESC) para combater atos graves de corrupção em todo o mundo.

Reforço dos direitos das vítimas

Em 12 de julho de 2023, a Comissão propôs introduzir alterações na Diretiva Direitos das Vítimas, a fim de reforçar o acesso das vítimas à informação, ao apoio e à proteção, à participação em processos penais e ao acesso a indemnização. Um dos objetivos gerais da revisão é contribuir para um elevado nível de segurança mediante a criação de um ambiente mais seguro para as vítimas, que incentive as denúncias de crimes e diminua o receio de represálias.

A Comissão insta o Parlamento Europeu e o Conselho a concluírem urgentemente as negociações interinstitucionais e, em qualquer caso, antes do final do mandato do atual Parlamento Europeu, sobre os seguintes dossiês pendentes:

- a proposta de regulamento Prüm II,
- as propostas relativas às informações antecipadas sobre passageiros (API),
- as propostas em matéria de luta contra a corrupção e, em particular, de criação de um regime de sanções específico da política externa e de segurança comum: (PESC),
- a proposta de alteração do Código das Fronteiras Schengen,
- a proposta de diretiva relativa aos direitos das vítimas,
- a proposta relativa à triagem.

[48] COM(2020) 612.
[49] COM(2023) 234.

A Comissão insta os Estados-Membros a:

- assegurarem a entrada em vigor do Sistema de Entrada/Saída o mais rapidamente possível, a fim de concluir a implementação da arquitetura da UE em matéria de intercâmbio de informações.

VI. Aplicação

Garantir a segurança da Europa no seu conjunto é uma responsabilidade comum, em que cada interveniente deve dar o seu contributo, desde a adoção, pela Comissão e pelos colegisladores, de regras novas, sólidas, abrangentes e práticas até à transposição e aplicação tempestivas dessas regras pelos Estados-Membros e ao trabalho operacional realizado no terreno por uma multiplicidade de autoridades, organizações e partes interessadas. Os organismos competentes da UE nos domínios da justiça, dos assuntos internos e da cibersegurança também desempenham um papel fundamental, que assume uma importância cada vez maior com o alargamento recente das suas responsabilidades.

Reforço da análise dos beneficiários do financiamento da UE

Ao executar o orçamento da UE, a Comissão tem a responsabilidade de assegurar que os beneficiários de financiamento da UE respeitem os valores da União. Os mecanismos e os sistemas de controlo que determinam quem pode beneficiar de financiamento da UE já são sólidos e a atual negociação da reformulação do Regulamento Financeiro visa dotar a Comissão de meios jurídicos de intervenção reforçados, quando necessário. Além disso, a Comissão está atualmente a trabalhar sobre formas de reforçar a análise dos atuais e potenciais beneficiários de financiamento da UE, melhorando as orientações sobre as obrigações relativas ao respeito pelos valores da UE e as consequências que devem advir de uma violação desses valores. Tal permitirá clarificar as responsabilidades tanto dos beneficiários como das pessoas que asseguram o controlo a nível da UE, podendo servir de inspiração a nível nacional. Em caso de incumprimento das condições de financiamento, a Comissão não hesita nem hesitará em suspender a cooperação com os beneficiários do projeto em causa e em recuperar os fundos, se necessário. É importante que os Estados-Membros partilhem proativamente informações com a Comissão sempre que tomem conhecimento de riscos no que diz respeito às organizações que se candidatam a financiamento da UE.

Infrações

No domínio da segurança, a Comissão instaurou um grande número de processos por infração. Em 2023, por exemplo, foi instaurado um elevado número de processos por infração decorrentes do incumprimento das obrigações decorrentes do Regulamento de 2021 relativo à difusão de conteúdos terroristas em linha (16 Estados-Membros)[50] e, ao longo de 2022 e 2023, 20 Estados-Membros receberam cartas de notificação formal adicionais por aplicação incorreta da Diretiva de 2011 relativa à luta contra o abuso sexual de crianças[51]. Continua em aberto um número significativo de processos por infração por não conformidade da legislação nacional com a Diretiva de 2017 relativa à luta contra o terrorismo[52] e por não transposição das normas

[50] Regulamento (UE) 2021/784 relativo à difusão de conteúdos terroristas em linha.

[51] Diretiva (UE) 2011/93 relativa à luta contra o abuso sexual de crianças.

[52] Diretiva (UE) 2017/541 do Parlamento Europeu e do Conselho, de 15 de março de 2017, relativa à luta contra o terrorismo e que substitui a Decisão-Quadro 2002/475/JAI do Conselho e altera a Decisão 2005/671/JAI do Conselho.

destinadas a facilitar a utilização de informações financeiras e de outro tipo para efeitos de prevenção, deteção, investigação ou repressão de determinadas infrações penais[53]. Outros domínios em que se encontram em curso processos por infração incluem a legislação em matéria de armas de fogo, as regras relativas às substâncias psicoativas utilizadas na droga, a luta contra a fraude e a contrafação de meios de pagamento que não em numerário, a luta contra o branqueamento de capitais, o intercâmbio de registos criminais entre os Estados-Membros da UE e a Diretiva Direitos das Vítimas. Foi disponibilizado apoio técnico e financeiro aos Estados-Membros que executam iniciativas e ações acordadas, continuando a Comissão disponível para trabalhar com os Estados-Membros a fim de otimizar a essa execução.

Monitorização através de avaliações Schengen e do seu novo sistema de governação

O mecanismo de avaliação e de monitorização de Schengen continuou a contribuir para a aplicação efetiva das regras de Schengen destinadas a reforçar a segurança dentro do espaço sem controlos internos. Em 2023, foram realizadas as primeiras avaliações no âmbito do mecanismo reforçado de avaliação e monitorização de Schengen, que permitiram identificar e corrigir atempadamente vulnerabilidades estratégicas com impacto transnacional na segurança interna da UE. Além disso, em 2023, a Comissão lançou uma avaliação temática Schengen para examinar as práticas dos Estados-Membros que enfrentam desafios semelhantes na luta contra o tráfico de droga para a UE, com especial incidência no tráfico de elevados volumes de droga. Estas avaliações colocaram uma ênfase maior e mais abrangente nos elementos de segurança de Schengen. Com base nos resultados das avaliações Schengen periódicas, temáticas e sem aviso prévio, o Conselho estabeleceu, em junho de 2023, as prioridades do ciclo Schengen de 2023-2024, definindo domínios de incidência que exigem um impulso adicional para um espaço Schengen mais seguro e mais forte. Uma aplicação rápida e eficaz destas prioridades, juntamente com uma maior coordenação política do Conselho Schengen, reforçará ainda mais a luta contra a criminalidade organizada e maximizará a cooperação operacional transnacional.

Papel das agências e organismos da UE

As parcerias são fundamentais para a execução das iniciativas da União da Segurança, uma vez que o trabalho das diferentes autoridades e organismos nacionais e europeus é necessário para se obter resultados concretos. Por exemplo, a EMPACT (Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas) permite uma cooperação multidisciplinar estruturada dos Estados-Membros, apoiada por todas as instituições, órgãos e organismos da UE (nomeadamente a Europol, a Frontex, a Eurojust, a CEPOL, o OLAF e a eu-LISA). As operações realizadas pela EMPACT, nomeadamente através de unidades operacionais específicas, coordenam os esforços dos Estados-Membros e dos parceiros operacionais na luta contra as redes criminosas e a criminalidade grave. Só em 2022, a EMPACT deu origem a um total de 9 922 detenções, mais de 180 milhões de EUR em bens e dinheiro apreendidos, 9 263 investigações iniciadas, 4 019 vítimas identificadas, mais de 62 toneladas de droga apreendidas, 51 alvos de elevado valor identificados e 12 detidos, bem como a operações no contexto da guerra de agressão contra a Ucrânia, nomeadamente para combater o tráfico de seres humanos e as ameaças relacionadas com armas de fogo[54].

---

[53] Diretiva (UE) 2019/1153 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, que estabelece normas destinadas a facilitar a utilização de informações financeiras e de outro tipo para efeitos de prevenção, deteção, investigação ou repressão de determinadas infrações penais e que revoga a Decisão 2000/642/JAI do Conselho.

[54] Ficha informativa com os resultados da EMPACT em 2022: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf.

A Frontex, a Agência Europeia da Segurança Marítima (EMSA) e a Agência Europeia de Controlo das Pescas (AECP) continuam a reforçar a sua cooperação em matéria de funções de guarda costeira, a fim de apoiar as autoridades nacionais no reforço da segurança no mar. Estas agências contribuirão de forma significativa para a execução da estratégia de segurança marítima da UE.

Várias iniciativas da União da Segurança requerem novas responsabilidades e funções para as agências competentes, por vezes com implicações em termos de recursos humanos.

Agência da União Europeia para a Cibersegurança (ENISA)

No que diz respeito à preparação e resposta a incidentes para reforçar a cibersegurança, a Comissão instituiu uma ação a curto prazo para apoiar os Estados-Membros, transferindo fundos do Programa Europa Digital para a **Agência da União Europeia para a Cibersegurança (ENISA)**, a fim de reforçar a preparação e as capacidades de resposta a ciberincidentes graves. A proposta de Regulamento Cibersolidariedade, adotada em abril de 2023, baseia-se nesta ação e, uma vez adotada pelos colegisladores, poderão ser confiadas à ENISA atribuições adicionais, como o funcionamento e a administração da futura reserva de cibersegurança da União ou a elaboração de um relatório de avaliação de incidentes de cibersegurança em grande escala. A proposta de Regulamento Ciber-Resiliência incumbiria a ENISA de receber notificações, da parte dos fabricantes, de vulnerabilidades de produtos com elementos digitais e de incidentes com impacto na segurança desses produtos, que a ENISA deverá transmitir às CSIRT competentes ou aos pontos únicos de contacto pertinentes dos Estados-Membros. A ENISA deverá também elaborar um relatório técnico bienal sobre as tendências emergentes em matéria de riscos de cibersegurança em produtos com elementos digitais e apresentá-lo ao grupo de cooperação SRI.

Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança

O **Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança**, juntamente com a Rede de Centros Nacionais de Coordenação, é o novo organismo da União de apoio à inovação e à política industrial no domínio da cibersegurança. Este ecossistema reforçará as capacidades da comunidade tecnológica da cibersegurança, manterá a excelência da investigação e reforçará a competitividade da indústria da União neste domínio. O Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação tomarão decisões estratégicas de investimento e reunirão recursos da União, dos seus Estados-Membros e, indiretamente, da indústria, a fim de melhorar e reforçar as capacidades tecnológicas e industriais no domínio da cibersegurança. Por conseguinte, o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança tem um papel fundamental a desempenhar na consecução dos ambiciosos objetivos em matéria de cibersegurança dos programas Europa Digital e Horizonte Europa.

O Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança já recrutou mais de metade do seu pessoal e, em breve, recrutará o seu diretor executivo. Os trabalhos em curso incluem a vertente relativa à cibersegurança do programa DIGITAL e uma nova agenda estratégica[55] para o desenvolvimento e a implantação de tecnologias, que define ações prioritárias para apoiar as PME no desenvolvimento e utilização

[55] https://cybersecurity-centre.europa.eu/strategic-agenda_en.

de tecnologias, serviços e processos estratégicos de cibersegurança, apoiar e aumentar a mão de obra profissional e reforçar os conhecimentos especializados em matéria de investigação, desenvolvimento e inovação no ecossistema europeu mais vasto da cibersegurança.

Europol

Com um novo mandato, a **Europol** estará mais bem equipada para apoiar os Estados-Membros na luta contra a criminalidade organizada. A luta contra o tráfico de droga é uma prioridade fundamental, tendo em conta a importância cada vez maior deste problema e o crescente impacto negativo na segurança dos cidadãos da UE. Na sequência da autorização do Conselho da União Europeia, em 15 de maio de 2023, a Comissão tem vindo a trabalhar ativamente no sentido da celebração de acordos internacionais com a Bolívia, o Brasil, o Equador, o México e o Peru sobre o intercâmbio de dados pessoais com a Europol, com o objetivo de prevenir e combater a criminalidade grave e o terrorismo.

Eurojust

Com mais de 20 anos de experiência na prestação de apoio judiciário às autoridades nacionais para combater um vasto conjunto de crimes transnacionais graves e complexos, a **Eurojust** consolidou a sua posição no espaço de liberdade, segurança e justiça da UE. A fim de reforçar a cooperação a todos os níveis, a Comissão está a negociar acordos internacionais para facilitar a cooperação entre a Eurojust e 13 países terceiros com vista ao intercâmbio de dados pessoais para combater a criminalidade organizada e o terrorismo[56]. As negociações com a Arménia e o Líbano já foram concluídas, encontram-se em curso negociações com a Argélia e a Colômbia e já foram iniciadas as negociações com a Bósnia-Herzegovina. A Comissão incentiva o Parlamento Europeu e o Conselho a finalizarem a celebração de acordos com estes países antes do final da legislatura, de modo a reforçar a cooperação judiciária transnacional e a alargar a luta contra a criminalidade transfronteiras.

Procuradoria Europeia

Desde o início das suas atividades operacionais, em junho de 2021, a **Procuradoria Europeia** tem-se revelado um instrumento poderoso do conjunto de instrumentos da União para investigar e reprimir infrações lesivas do orçamento da União, incluindo as relacionadas com a participação em organizações criminosas, sempre que se trate de crimes contra o orçamento da União. A Comissão incentiva os Estados-Membros que ainda não participam na cooperação reforçada da Procuradoria Europeia a fazê-lo o mais rapidamente possível, a fim de concretizar todo o potencial da mesma para proteger o dinheiro dos contribuintes da UE.

Agência da União Europeia para a Droga

Com um novo mandato adotado pelos colegisladores em junho de 2023, o atual Observatório Europeu da Droga e da Toxicodependência (OEDT) transformar-se-á numa agência de pleno direito – a **Agência da União Europeia para a Droga** – com funções reforçadas. A agência terá capacidade para avaliar os novos desafios em matéria de saúde e segurança suscitados pelas drogas ilícitas de uma forma mais abrangente e contribuir mais eficazmente para o trabalho a nível dos Estados-Membros e a nível internacional. A recolha, análise e divulgação de dados continuarão a ser a principal atribuição da agência, mas o novo mandato reforçado permitir-lhe-á igualmente desenvolver capacidades gerais de avaliação das ameaças para a saúde e a segurança, a fim de identificar ameaças emergentes, incluindo o policonsumo de substâncias, reforçar a sua cooperação através de pontos focais nacionais e criar uma rede de laboratórios

[56] Argélia, Argentina, Arménia, Bósnia-Herzegovina, Brasil, Colômbia, Egito, Israel, Jordânia, Líbano, Marrocos, Tunísia e Turquia.

que forneça à agência informações forenses e toxicológicas. A agência poderá, deste modo, emitir alertas sempre que surgirem no mercado substâncias particularmente perigosas e aumentar a sensibilização.

A Comissão insta o Parlamento Europeu e o Conselho a concluírem urgentemente as negociações interinstitucionais e, em qualquer caso, antes do final do mandato do atual Parlamento Europeu, quanto aos seguintes dossiês pendentes:

- a proposta de reformulação do Regulamento Financeiro.

A Comissão insta os Estados-Membros a:

- partilhar proativamente informações com a Comissão sempre que tomem conhecimento de eventuais riscos relacionados com as organizações que se candidatam a financiamento da UE,
- implementar com celeridade as prioridades do ciclo de Schengen 2023-2024 para um espaço Schengen mais seguro e mais forte,
- resolver os processos por infração de que sejam objeto, a fim de assegurar a correta transposição da legislação em causa.

VII. Conclusão

Os últimos três anos foram marcados por um esforço constante e determinado para concretizar a ambição de criar uma União da Segurança para a UE. Os progressos realizados em todo o espetro da política de segurança foram muito significativos. Atualmente, a realidade de ameaças em constante evolução exige esforços contínuos com uma motivação renovada. Os trabalhos sobre o quadro legislativo devem ser concluídos em tempo útil antes do final da legislatura, na primavera de 2024. Os Estados-Membros têm responsabilidades permanentes em matéria de transposição, execução e aplicação da nova legislação. A execução exige esforços concertados, nomeadamente com o apoio das agências da UE, e, o mais das vezes, uma cooperação cada vez mais forte com os nossos parceiros internacionais.

Só com os esforços coletivos e determinados de todas as partes interessadas poderemos alcançar os níveis de segurança na UE ambicionados pelos cidadãos, impondo-se, nas circunstâncias atuais, como uma prioridade, que todos os intervenientes deem o seu contributo para o reforço da segurança da UE.