Jornal Oficial
da União Europeia

PT
Série L

2024/2659

16.10.2024

RECOMENDAÇÃO (UE) 2024/2659 DA COMISSÃO

de 11 de outubro de 2024

relativa às orientações sobre a exportação de produtos de cibervigilância nos termos do artigo 5.º do Regulamento (UE) 2021/821 do Parlamento Europeu e do Conselho

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 292.º,

Considerando o seguinte:

(1) O Regulamento (UE) 2021/821 do Parlamento Europeu e do Conselho ([1]) cria um regime da União de controlo das exportações, corretagem, assistência técnica, trânsito e transferências de produtos de dupla utilização:

(2) O Regulamento (UE) 2021/821 tem por objeto o risco de utilização de produtos de cibervigilância no contexto da repressão interna e/ou da prática de violações graves dos direitos humanos e do direito internacional humanitário.

(3) Nos termos dos artigos 5.º, n.º 2, e 26.°, n.º 1, do Regulamento (UE) 2021/821, a Comissão e o Conselho disponibilizam orientações aos exportadores no que diz respeito aos produtos de cibervigilância não incluídos na lista, tendo em conta a necessidade de garantir a eficiência do regime de controlo das exportações da União no que diz respeito à cibersegurança e a coerência da aplicação do Regulamento (UE) 2021/821.

(4) A presente recomendação e as orientações em anexo visam apoiar os exportadores na aplicação dos controlos dos produtos de cibervigilância não incluídos na lista, incluindo, entre outras, medidas de diligência devida que avaliem os riscos relacionados com a exportação desses produtos.

(5) As orientações anexas à presente recomendação foram objeto de amplas consultas no âmbito do Grupo de Peritos em Tecnologia de Vigilância em 2022 e 2023 e tiveram em conta as observações recebidas durante uma consulta pública ([2]) realizada no segundo trimestre de 2023.

(6) Importa recordar que a presente recomendação e as orientações em anexo não são vinculativas. Por conseguinte, os exportadores devem manter a responsabilidade de cumprir as obrigações que lhes incumbem por força do Regulamento (UE) 2021/821, ao passo que a Comissão deve assegurar que a presente recomendação mantém a sua pertinência ao longo do tempo,

([1]) Regulamento (UE) 2021/821 do Parlamento Europeu e do Conselho, de 20 de maio de 2021, que cria um regime da União de controlo das exportações, corretagem, assistência técnica, trânsito e transferências de produtos de dupla utilização (JO L 206 de 11.6.2021, p. 1, ELI: http://data.europa.eu/eli/reg/2021/821/oj).

([2]) https://policy.trade.ec.europa.eu/consultations/guidelines-export-cyber-surveillance-items-under-article-5-regulation-eu-no-2021821_en.

ADOTOU A PRESENTE RECOMENDAÇÃO:

Recomenda-se que as autoridades competentes e os exportadores dos Estados-Membros tenham em conta as orientações constantes do anexo da presente recomendação, a fim de cumprirem as obrigações que lhes incumbem por força do artigo 5.º, n.º 2, do Regulamento (UE) 2021/821.

Feito em Bruxelas, em 11 de outubro de 2024.

Pela Comissão
Valdis DOMBROVSKIS
Vice-Presidente Executivo

ANEXO

ÍNDICE

Página

Introdução 4

1. Disposições jurídicas, definições e conceitos-chave pertinentes 4

1.1. Panorâmica das disposições jurídicas pertinentes 4

1.2. Definições-chave 5

1.2.1. «Especialmente concebidos» 5

1.2.2. «Vigilância encoberta» 6

1.2.3. «Pessoas singulares» 6

1.2.4. «Monitorização, extração, recolha, análise de dados» 6

1.2.5. «De sistemas de informação e de telecomunicações» 7

1.2.6. «Conhecimento» e «destinam-se a» 7

1.3. Repressão interna, violações graves dos direitos humanos e do direito internacional humanitário 7

1.3.1. Repressão interna 8

1.3.2. Prática de violação grave dos direitos humanos 8

1.3.3. Prática de violação grave do direito internacional humanitário 9

2. Âmbito de aplicação técnico 9

2.1. Produtos de cibervigilância incluídos na lista 9

2.2. Potenciais produtos de cibervigilância não incluídos na lista 9

2.2.1. Tecnologia de reconhecimento facial e das emoções 10

2.2.2. Dispositivos de rastreamento da localização 10

2.2.3. Sistemas de videovigilância 10

3. Medidas de diligência devida 10

Requisitos previstos no artigo 5.º, n.º 2, do Regulamento (UE) 2021/821 12

4. Apêndice 12

Produtos de cibervigilância incluídos na lista sujeitos a controlo nos termos do anexo I do Regulamento (UE) 2021/821 12

Sistemas de interceção de telecomunicações (5A001.f.) 12

Sistemas de vigilância da Internet (5A001.j.) 13

«*Software* de intrusão» (4A005, 4D004 e controlos conexos no âmbito de 4E001.a. e 4E001.c.) 13

Software de monitorização das comunicações (5D001.e.) 14

Produtos utilizados para efetuar criptoanálise (5A004.a.) 14

Ferramentas forenses/de investigação (5A004.b., 5D002.a.3.b. e 5D002.c.3.b.) 14

INTRODUÇÃO

O quadro de controlo das exportações da União instituído pelo Regulamento (UE) 2021/821 («Regulamento») visa garantir o cumprimento das obrigações e dos compromissos internacionais da União e dos seus Estados-Membros, nomeadamente em matéria de paz, segurança e estabilidade regionais e respeito pelos direitos humanos e pelo direito internacional humanitário. Por conseguinte, a União e os seus Estados-Membros aplicaram as decisões tomadas no âmbito dos regimes multilaterais de controlo das exportações e atualizaram em conformidade a lista de controlo da União constante do anexo I do regulamento ([1]). Além disso, antes de o artigo 5.º do regulamento ser aplicável, as autoridades competentes dos Estados-Membros já controlavam a exportação de determinados produtos constantes da lista que podem ter aplicações de vigilância ([2]), tendo em conta os riscos de utilização indevida em determinadas circunstâncias específicas. Perante circunstâncias excecionalmente graves, a União impôs sanções que restringem a exportação de determinados equipamentos de vigilância ([3]).

O regulamento reflete o compromisso da União de combater eficazmente o risco de utilização de produtos de cibervigilância no contexto da repressão interna e/ou da prática de violações graves dos direitos humanos e do direito internacional humanitário. Em especial, o regulamento introduz novas disposições para o controlo das exportações de produtos de cibervigilância não incluídos na lista, incluindo a obrigação de os exportadores notificarem a autoridade competente quando tiverem conhecimento, de acordo com as suas averiguações em matéria de diligência devida, de que os produtos de cibervigilância não incluídos na lista que os exportadores se propõem exportar se destinam, total ou parcialmente, a ser utilizados no contexto da repressão interna e/ou da prática de violações graves dos direitos humanos e do direito internacional humanitário. O regulamento insta ainda a Comissão e o Conselho a disponibilizarem orientações aos exportadores para apoiar a aplicação efetiva dos novos controlos dos produtos de cibervigilância não incluídos na lista.

Por conseguinte, as presentes orientações visam apoiar os exportadores na aplicação dos controlos dos produtos de cibervigilância não incluídos na lista, incluindo, entre outras, medidas de diligência devida que avaliem os riscos relacionados com a exportação desses produtos para utilizadores finais e utilizações finais abrangidas pelas novas disposições do regulamento.

1. DISPOSIÇÕES JURÍDICAS, DEFINIÇÕES E CONCEITOS-CHAVE PERTINENTES

1.1. Panorâmica das disposições jurídicas pertinentes

O regulamento introduz novas disposições que preveem especificamente o controlo das exportações de produtos de cibervigilância não enumerados no anexo I do regulamento, que se destinem ou possam destinar-se, total ou parcialmente, a ser utilizados no âmbito da repressão interna e/ou da prática de violações graves dos direitos humanos e do direito internacional humanitário. Os considerandos e os artigos pertinentes são os seguintes:

a) considerando 8: «Para fazer face ao risco de determinados produtos de cibervigilância não listados exportados a partir do território aduaneiro da União poderem ser utilizados de forma abusiva por pessoas implicadas ou responsáveis pela direção ou pela realização de graves violações dos direitos humanos ou do direito internacional humanitário, é conveniente controlar a exportação desses produtos. Os riscos associados dizem respeito, em particular, aos casos em que os produtos de cibervigilância sejam especialmente concebidos para permitir a intrusão ou a inspeção profunda de

([1]) Ver, em especial, os controlos relacionados com os sistemas de interceção de telecomunicações (5A001.f), os sistemas de vigilância da Internet (5A001.j.), o *software* de intrusão (4A005, 4D004 e controlos conexos no âmbito de 4E001.a e 4E001.c) e o *software* de vigilância para fins policiais (5D001.e). Ver ainda, com base numa avaliação caso a caso, os controlos relativos a determinadas ferramentas forenses/de investigação (5A004.b, 5D002.a.3.b e 5D002.c.3.b).

([2]) Em especial, os sistemas de segurança da informação.

([3]) Ver Regulamento (CE) n.º 765/2006 do Conselho, de 18 de maio de 2006, que impõe medidas restritivas tendo em conta a situação na Bielorrússia e o envolvimento da Bielorrússia na agressão russa contra a Ucrânia (JO L 134 de 20.5.2006, p. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj); Regulamento (UE) n.º 359/2011 do Conselho, de 12 de abril de 2011, que impõe medidas restritivas contra determinadas pessoas, entidades e organismos tendo em conta a situação no Irão (JO L 100 de 14.4.2011, p. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj); Regulamento (UE) n.º 36/2012 do Conselho, de 18 de janeiro de 2012, que impõe medidas restritivas tendo em conta a situação na Síria e que revoga o Regulamento (UE) n.º 442/2011 (JO L 16 de 19.1.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj); Regulamento (UE) n.º 401/2013 do Conselho, de 2 de maio de 2013, relativo a medidas restritivas tendo em conta a situação em Mianmar/Birmânia e que revoga o Regulamento (CE) n.º 194/2008 (JO L 121 de 3.5.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj); e Regulamento (UE) 2017/2063 do Conselho, de 13 de novembro de 2017, que impõe medidas restritivas tendo em conta a situação na Venezuela (JO L 295 de 14.11.2017, p. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

pacotes de sistemas de informação e de telecomunicações, a fim de proceder à vigilância encoberta de pessoas singulares através da monitorização, extração, recolha ou análise de dados, incluindo dados biométricos, provenientes desses sistemas. Os produtos utilizados para aplicações puramente comerciais, designadamente faturação, comercialização, serviços de qualidade, satisfação dos utilizadores ou segurança da rede, são geralmente considerados como não implicando tais riscos»;

b) considerando 9: «Com vista a reforçar o controlo efetivo das exportações de produtos de cibervigilância não listados, é essencial continuar a harmonizar a aplicação de controlos «*catch-all*» nesse domínio. Para o efeito, os Estados-Membros estão empenhados em apoiar esses controlos partilhando informações entre si e com a Comissão, em particular no que diz respeito à evolução tecnológica de produtos de cibervigilância, e exercendo vigilância na aplicação de tais controlos para promover um intercâmbio a nível da União.»;

c) O artigo 2.º, ponto 20, que define os produtos de cibervigilância como produtos de dupla utilização especialmente concebidos para permitir a vigilância encoberta de pessoas singulares através da monitorização, extração, recolha e análise de dados de sistemas de informação e de telecomunicações»;

d) O artigo 5.º introduz um requisito de autorização para a exportação de produtos de cibervigilância não listados se o exportador tiver sido informado pela autoridade competente de que os produtos em questão se destinam ou se podem destinar, total ou parcialmente, a ser utilizados no contexto da repressão e/ou da prática de graves violações dos direitos humanos ou do direito internacional humanitário (artigo 5.º, n.º 1). Exige ainda que os exportadores notifiquem a autoridade competente se, com base nas averiguações em matéria de diligência devida, tiverem conhecimento de que os produtos se destinam, total ou parcialmente, a ser utilizados no contexto da repressão interna e/ou da prática de violações graves dos direitos humanos ou do direito internacional humanitário (artigo 5.º, n.º 2). Essa autoridade competente decide se sujeita ou não a exportação em causa a uma autorização. e

e) O artigo 5.º, n.º 2, estabelece ainda que «[a] Comissão e o Conselho disponibilizarão diretrizes aos exportadores, tal como referido no artigo 26.º, n.º 1.»

1.2. **Definições-chave**

O regulamento contém considerandos e disposições específicos que clarificam termos específicos pertinentes para os controlos das exportações de produtos de cibervigilância não incluídos na lista e que são importantes para os exportadores compreenderem claramente, a fim de exercerem a diligência devida e aplicarem os controlos de forma eficaz. De particular relevância, o artigo 2.º, ponto 20, oferece a seguinte definição precisa de «produtos de cibervigilância»: «produtos de dupla utilização especialmente concebidos para permitir a vigilância encoberta de pessoas singulares através da monitorização, extração, recolha e análise de dados de sistemas de informação e de telecomunicações».

Para efeitos das presentes orientações, devem ser clarificados aspetos específicos dessa definição.

1.2.1. *«Especialmente concebidos»*

Um artigo é concebido para vigilância encoberta quando as suas características técnicas são adequadas para o efeito e permitem objetivamente a vigilância encoberta de pessoas singulares. Por conseguinte, o termo «especialmente concebidos» significa que a vigilância encoberta de pessoas singulares deve ter sido o principal objetivo do desenvolvimento e da conceção do produto. Tal termo não exige, porém, que o produto só possa ser utilizado para a vigilância encoberta de pessoas singulares.

Tal como esclarece o considerando n.º 8 do regulamento, os produtos utilizados para aplicações puramente comerciais, designadamente faturação, comercialização, serviços de qualidade, satisfação dos utilizadores ou segurança da rede, não são especialmente concebidos para a vigilância encoberta de pessoas singulares e, como tal, não se enquadram na definição de produtos de cibervigilância. Por exemplo, se bem que possam ser utilizados para efeitos de vigilância, os produtos concebidos para a vigilância dos sistemas operativos na indústria ou a monitorização do tráfego dos utilizadores não são produtos de cibervigilância na aceção da definição, porque não são especialmente concebidos para permitir a vigilância encoberta de pessoas singulares.

1.2.2. *«Vigilância encoberta»*

Os produtos permitem uma vigilância encoberta, em especial quando a vigilância não é manifestamente percetível para a pessoa singular afetada. Seria este o caso quando as pessoas em causa não têm conhecimento da presença e/ou da ação de produtos de cibervigilância e, por conseguinte, não têm a oportunidade de se subtraírem à vigilância ou, pelo menos, de ajustar o seu comportamento em conformidade. Ainda que a vigilância seja efetuada através de elementos instalados ou em funcionamento no espaço público, a aquisição de dados pode, em certos casos, ser considerada relevante para a vigilância encoberta, nomeadamente os dados recolhidos podem ser desviados, avaliados ou tratados para outros fins diversos daqueles de que a pessoa singular afetada tem conhecimento. Por outras palavras, quando uma pessoa singular não pode objetivamente esperar estar sob vigilância, a vigilância pode ser considerada encoberta nos termos do artigo 2.º, ponto 20, do regulamento.

1.2.3. *«Pessoas singulares»*

O termo «pessoa singular» refere-se a um ser humano vivo por oposição a uma pessoa coletiva ou uma entidade, as quais, por conseguinte, não são abrangidas pelas disposições. O termo não abrange a vigilância de objetos, locais ou máquinas propriamente ditos.

1.2.4. *«Monitorização, extração, recolha, análise de dados»*

Segundo diversos dicionários de referência da língua portuguesa, as palavras monitorização, extração, recolha e análise têm o seguinte significado linguístico:

— «monitorização»: supervisão; controlo, acompanhamento e avaliação;

— «extração»: ato ou efeito de extrair;

— «recolha»: reunir; compilar;

— «análise»: decomposição de um todo ideal nos seus constituintes; processo de raciocínio que parte do geral para o particular ou das causas para os efeitos; examinar com atenção; exame minucioso de uma coisa em cada uma das suas partes. submeter a uma análise crítica ou computacional.

Estes termos implicam que os elementos utilizados na vigilância devem ter capacidades técnicas precisas para o tratamento de dados, a fim de monitorizar, recolher, extrair ou analisar dados, tais como, por exemplo, os seguintes elementos:

a) Elementos utilizados para monitorizar dados de sistemas de informação e de telecomunicações ([4]) (por exemplo, dimensão do ficheiro ou tráfego de pacotes dos dados transmitidos nesse sistema);

b) Os produtos que extraem dados de sistemas de informação e de telecomunicações realizando intrusão e extração (por exemplo, *software* de intrusão);

c) Os produtos que permitem uma análise de dados extraídos de sistemas de informação e de telecomunicações, incluindo os que podem tratar imagens obtidas por câmaras armazenadas nesses sistemas (por exemplo, certos tipos de tecnologias de análise de dados utilizadas como parte dos sistemas de reconhecimento facial).

Os produtos utilizados simplesmente para monitorizar sistemas de informação ou para vigiar a população através de câmaras de videovigilância e que permitem captar conversas, intercâmbios de dados, movimentos e comportamentos individuais não seriam produtos de cibervigilância na aceção do regulamento, uma vez que não são especialmente concebidos para este efeito e necessitam de outras tecnologias, como a inteligência artificial ou os megadados. No entanto, o sistema na sua globalidade (funcionando em conjunto com outras tecnologias, como a inteligência artificial ou as tecnologias dos megadados) pode potencialmente ser um produto de cibervigilância na aceção do artigo 2.º, ponto 20, do regulamento.

Importa salientar que, embora forneçam alguns exemplos úteis para fins ilustrativos, a definição e o âmbito dos produtos de cibervigilância não são limitados por esses exemplos, uma vez que o objetivo do artigo 5.º é permitir um controlo eficaz das exportações de produtos não incluídos na lista.

([4]) Ver o ponto 1.2.5 *infra* para a definição.

Tal como demonstrado pela utilização da conjunção «ou» na definição, as capacidades técnicas enumeradas devem ser consideradas como alternativas, não sendo necessário que um produto possua todas essas capacidades técnicas para monitorizar, extrair, recolher ou analisar dados. Por outras palavras, é suficiente que um produto tenha uma dessas capacidades técnicas para ser abrangido pela definição de produto de cibervigilância do artigo 2.º, ponto 20.

1.2.5. *«De sistemas de informação e de telecomunicações»*

Estes termos referem-se a sistemas que processam eletronicamente informações, por exemplo, programação/codificação, operações do sistema dos computadores pessoais (*hardware*) e outras formas de administração da informação, incluindo tecnologias de *software*, tecnologias Web, tecnologias informáticas, tecnologias de armazenamento, etc., e a alguns sistemas que transmitem informações à distância, por exemplo, sistemas técnicos que transmitem sons, sinais, texto, outros símbolos, imagens através de canais com e sem fios, através de fibras óticas, rádio e outros sistemas eletromagnéticos. Em conjunto, estes dois conceitos incluem uma vasta gama de sistemas de transmissão ou de tratamento de informações. Note-se que o termo se refere a sistemas e não a equipamentos.

1.2.6. *«Conhecimento» e «destinam-se a»*

Nos termos do artigo 5.º, n.º 2, do regulamento, o exportador deve notificar a autoridade competente se «tiver conhecimento […] de que os produtos de cibervigilância […] se destinam […] a ser utilizados no contexto da repressão e/ou da prática de graves violações dos direitos humanos ou do direito humanitário».

O termo «conhecimento» não é um conceito jurídico novo, mas tem sido utilizado em ligação com os requisitos de autorização relacionados com a utilização final (os chamados controlos «*catch-all*» ou «vassoura») nos termos dos artigos 4.º, 6.°, 7.° e 8.° do regulamento. Ter «conhecimento» implica que o exportador está efetivamente consciente da utilização indevida prevista. A mera possibilidade da existência de tal risco não é suficiente para concluir que existe conhecimento. No entanto, o termo «conhecimento» não pode ser equiparado a passividade: exige que o exportador tenha tomado medidas para obter conhecimento suficiente e adequado para avaliar os riscos relacionados com a exportação e assegurar o cumprimento do regulamento.

A indicação de que os produtos devem ser «destinados» a uma utilização final sensível relevante implica que o exportador deve avaliar a utilização final caso a caso, à luz das circunstâncias específicas desse caso. *A contrario*, um risco teórico, ou seja, não baseado numa apreciação factual do caso, de os artigos poderem ser utilizados de uma forma que viole os direitos humanos não seria suficiente para implicar que «se destinam» a uma utilização indevida específica na aceção do artigo 5.º.

1.3. **Repressão interna, violações graves dos direitos humanos e do direito internacional humanitário**

Nos termos do artigo 15.º do regulamento, que enuncia as considerações para a avaliação de uma autorização, os Estados-Membros devem ter em consideração todos os aspetos relevantes, incluindo os que são abrangidos pela Posição Comum 2008/944/PESC do Conselho ([5]).

O artigo 5.º do regulamento alarga os controlos à exportação de produtos de cibervigilância não incluídos na lista em função do risco de serem utilizados no âmbito da repressão interna e/ou da prática de violações graves dos direitos humanos e do direito internacional humanitário. A Posição Comum 2008/944/PESC e o Guia do Utilizador desta posição comum ([6]) oferecem orientações úteis a este respeito.

([5]) Posição Comum 2008/944/PESC do Conselho, de 8 de dezembro de 2008, que define regras comuns aplicáveis ao controlo das exportações de tecnologia e equipamento militares (JO L 335 de 13.12.2008, p. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Guia do Utilizador da Posição Comum 2008/944/PESC do Conselho que define regras comuns aplicáveis ao controlo das exportações de tecnologia e equipamento militares, https://www.consilium.europa.eu/media/40659/st12189-en19.pdf.

1.3.1. *Repressão interna*

Nos termos do artigo 2.º, n.º 2, da Posição Comum 2008/944/PESC, «[a] repressão interna inclui, designadamente, a tortura e outras penas ou tratamentos, desumanos ou degradantes, as execuções sumárias ou arbitrárias, os desaparecimentos, as detenções arbitrárias e outras violações graves dos direitos humanos e das liberdades fundamentais consignadas nos instrumentos internacionais pertinentes em matéria de direitos humanos, nomeadamente na Declaração Universal dos Direitos do Homem e no Pacto Internacional sobre os Direitos Civis e Políticos» (PIDCP). O Guia do Utilizador da Posição Comum 2008/944/PESC oferece orientações sobre os elementos a ter em conta na avaliação do exportador, incluindo os «antecedentes e o atual desempenho do utilizador final previsto em matéria de direitos humanos, bem como do país destinatário em geral».

1.3.2. *Prática de violação grave dos direitos humanos*

A utilização indevida de produtos de cibervigilância não incluídos na lista pode ter um impacto negativo num vasto leque de direitos humanos e interfere diretamente com o direito à vida privada e a proteção dos dados. A vigilância arbitrária ou ilegal pode também violar outros direitos humanos, nomeadamente os direitos à liberdade de expressão, de associação e de reunião, à liberdade de pensamento, de consciência e de religião, bem como os direitos à igualdade de tratamento ou à proibição da discriminação e ainda o direito a eleições livres, justas e por voto secreto. Em casos específicos, a vigilância, incluindo o seguimento ou a recolha de informações das pessoas singulares, tais como defensores dos direitos humanos, ativistas, figuras políticas, populações vulneráveis e jornalistas, pode conduzir à intimidação, à repressão, à detenção arbitrária, à tortura ou mesmo a execuções extrajudiciais. Por conseguinte, os exportadores devem incluir estes aspetos relacionados com violações graves dos direitos humanos nas suas avaliações.

A prática internacional mostra que quaisquer restrições aos direitos humanos devem ser «adequadas» e conformes com as normas internacionais em matéria de direitos humanos. Na prática, isto significa que existem garantias adequadas para assegurar que as restrições estão previstas na lei e preservam a essência dos direitos. Na observância do princípio da proporcionalidade, as restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a um fim legítimo — por exemplo, segurança nacional ou pública, ordem pública, proteção da saúde pública ou proteção dos direitos e liberdades de terceiros.

Os produtos de cibervigilância podem incluir instrumentos legítimos e regulamentados para aplicações policiais, como a prevenção, a investigação, a deteção ou a repressão de infrações penais, nomeadamente no domínio da luta contra o terrorismo ou na execução de sanções penais. Ao mesmo tempo, os produtos de cibervigilância também podem ser utilizados de forma indevida para cometer violações graves dos direitos humanos e do direito internacional humanitário quando exportados para regimes ou utilizadores finais privados repressores e/ou para zonas de conflito.

Isto exige uma avaliação caso a caso das circunstâncias, incluindo a aplicação da regulamentação pertinente à luz de quaisquer violações graves dos direitos humanos assinaladas pelos órgãos competentes de entidades como as Nações Unidas, a União ou o Conselho da Europa. O reconhecimento de violações dos direitos humanos em informações publicadas pelos órgãos competentes das Nações Unidas, pela União ou pelo Conselho da Europa é um primeiro indício da «gravidade» dessas violações. Tal reconhecimento explícito por parte desses organismos não constitui uma necessidade absoluta, mas é um fator importante para que os critérios estejam preenchidos.

Nos termos do artigo 5.º, a violação dos direitos humanos deve ser «grave». O Guia do Utilizador da Posição Comum 2008/944/PESC contém orientações úteis para classificar possíveis violações dos direitos humanos como «graves». Segundo este guia, a natureza e as consequências da violação são determinantes. As violações sistemáticas e/ou generalizadas dos direitos humanos são, por regra, consideradas graves; mas também as violações que não são sistemáticas ou generalizadas podem ser consideradas «graves» — por exemplo, devido à gravidade da intervenção para as pessoas afetadas.

O anexo II do Guia do Utilizador da Posição Comum 2008/944/PESC contém uma lista não exaustiva dos principais instrumentos internacionais e regionais em matéria de direitos humanos, incluindo o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), a Convenção contra a Tortura e Outras Penas ou Tratamentos Cruéis, Desumanos ou Degradantes, a Convenção Europeia dos Direitos Humanos (Convenção) e a Carta dos Direitos Fundamentais (Carta), os quais podem oferecer orientações importantes para a interpretação e a aplicação dos critérios para apoiar avaliações robustas em matéria de direitos humanos. Estes instrumentos e os respetivos protocolos adicionais constituem o acervo das principais normas e padrões internacionalmente vigentes nos domínios dos direitos humanos e das liberdades fundamentais.

1.3.3. *Prática de violação grave do direito internacional humanitário*

O direito internacional humanitário (também designado por «Direito de Genebra» ou «Direito dos Conflitos Armados») foi desenvolvido através de uma série de tratados internacionais, sobretudo o Regulamento da Haia, as Convenções de Genebra e os seus dois Protocolos Adicionais de 1977, e identifica regras que, em tempo de conflito armado, servem para proteger as pessoas que não participam ou deixaram de participar nas hostilidades (por exemplo, civis e combatentes feridos, doentes ou capturados) e impõem às partes beligerantes restrições em matéria de meios e métodos de guerra (Direito da Haia).

A utilização de produtos de cibervigilância não incluídos na lista deve respeitar o direito internacional humanitário quando esses produtos são utilizados como meios e métodos de guerra no contexto de um conflito armado. Nestas circunstâncias, o risco de violações graves do direito internacional humanitário é um aspeto a ter em consideração nos termos do regulamento e, no que se refere à prática de violações graves dos direitos humanos, deve ser avaliado à luz da utilização final prevista dos produtos no caso específico. O Guia do Utilizador da Posição Comum 2008/944/PESC oferece orientações sobre os elementos a ter em consideração, incluindo o historial passado e presente do destinatário em matéria de respeito do direito internacional humanitário, as intenções do destinatário expressas através de compromissos formais e a capacidade do destinatário para garantir que o equipamento ou a tecnologia transferidos são utilizados em conformidade com o direito internacional humanitário e não são desviados ou transferidos para outros destinos onde possam ser utilizados em violações graves deste direito.

Nos termos do artigo 5.º, a violação do direito internacional humanitário deve ser «grave». Podem encontrar-se orientações no Guia do Utilizador da Posição Comum 2008/944/PESC, que reconhece que «os incidentes isolados de violações do direito internacional humanitário não são necessariamente reveladores da atitude do país destinatário perante o direito internacional humanitário, mas «se emergir um certo padrão de violações, ou se o país destinatário não tiver tomado as medidas adequadas para punir as violações, haverá motivos para sérias preocupações». O Comité Internacional da Cruz Vermelha (CICV) formulou orientações sobre a avaliação das violações do direito internacional humanitário para efeitos do controlo das exportações. Segundo o CICV, «as violações do direito internacional humanitário são graves se colocarem em perigo pessoas protegidas (por exemplo, civis, prisioneiros de guerra, feridos e doentes) ou objetos protegidos (por exemplo, objetos ou infraestruturas civis) ou se violarem valores universais importantes». Os crimes de guerra, por exemplo, constituem violações graves do direito internacional humanitário. O CICV menciona ainda fatores semelhantes que devem ser considerados como o Guia do Utilizador da Posição Comum 2008/944/PESC, incluindo os compromissos formais para aplicar as regras do direito internacional humanitário, medidas adequadas que garantam a responsabilização pelas violações do direito internacional humanitário, formação em direito internacional humanitário para as forças militares e proibição de recrutar crianças para as forças armadas.

2. ÂMBITO DE APLICAÇÃO TÉCNICO

2.1. **Produtos de cibervigilância incluídos na lista**

O apêndice destas orientações oferece informações sobre os produtos de cibervigilância enumerados no anexo I do regulamento, a fim de ajudar os exportadores na identificação de potenciais produtos de cibervigilância não incluídos na lista.

2.2. **Potenciais produtos de cibervigilância não incluídos na lista**

Embora, por definição, seja impossível fornecer uma lista exaustiva dos produtos que podem ser controlados como «produtos não incluídos na lista» nos termos do artigo 5.º, os seguintes produtos podem ter um potencial de vigilância e podem justificar uma vigilância especial nos termos do regulamento.

Tal como esclarece o considerando n.º 8 do regulamento, considera-se, de um modo geral, que os produtos utilizados para aplicações puramente comerciais, designadamente faturação, comercialização, serviços de qualidade, satisfação dos utilizadores ou segurança da rede, não implicam riscos de utilização indevida, na medida em que sejam relevantes no âmbito de violações graves dos direitos humanos ou do direito internacional humanitário e, por conseguinte, não estão geralmente sujeitos a controlo nos termos do artigo 5.º. Muitos destes produtos têm funcionalidades de segurança da informação (criptográficas ou mesmo criptoanalíticas) que cumprem os parâmetros de controlo da categoria 5, parte 2, do texto de controlo constante do anexo I do regulamento. O equipamento para a segurança de redes — incluindo encaminhadores, comutadores ou relés, em que a funcionalidade de segurança da informação se limita às funções de «exploração, administração ou manutenção» aplicando apenas normas criptográficas comerciais ou publicadas — também não é abrangido pela definição de «produtos de cibervigilância», embora os exportadores devam permanecer vigilantes tendo em conta vários relatos de utilização indevida desses produtos para violações dos direitos humanos.

2.2.1. *Tecnologia de reconhecimento facial e das emoções*

As tecnologias de reconhecimento facial e das emoções têm múltiplas utilizações para além da cibervigilância — por exemplo, para identificação ou autenticação —, pelo que não são automaticamente abrangidas pela definição. No entanto, em determinadas circunstâncias, as tecnologias de reconhecimento facial e das emoções podem ser abrangidas pelo âmbito de aplicação do artigo 2.º, ponto 20, do regulamento.

As tecnologias de reconhecimento facial e das emoções que podem ser utilizadas para monitorizar ou analisar imagens de vídeo armazenadas poderão ser abrangidas pela definição de produto de cibervigilância. No entanto, mesmo que os critérios acima referidos estejam preenchidos, há que examinar cuidadosamente se o *software* é especialmente concebido para a vigilância encoberta.

2.2.2. *Dispositivos de rastreamento da localização*

Os dispositivos de rastreamento da localização permitem rastrear a localização física de um dispositivo ao longo do tempo e algumas tecnologias de rastreamento da localização há já algum tempo que têm vindo a ser utilizadas pelas forças policiais e pelos serviços de informações. O seu potencial para a vigilância dirigida e em larga escala tem evoluído consideravelmente, à medida que os progressos das tecnologias de rastreamento — incluindo o rastreamento da localização por satélite, o rastreamento da localização com base nas torres de telecomunicações móveis e nos dispositivos emissores-recetores Wi-Fi e Bluetooth — e os «dispositivos de rastreamento», como telemóveis inteligentes e outros dispositivos eletrónicos (por exemplo, sistemas de bordo dos veículos), têm vindo a generalizar-se.

Os dispositivos de rastreamento da localização são utilizados pelas forças policiais e pelos serviços de informações, por exemplo, para recolher elementos de prova no decurso de uma investigação ou para localizar suspeitos, mas também por empresas para fins comerciais, por exemplo comunicando padrões de movimento agregados nas ruas comerciais, rastreando trabalhadores que trabalham fora das instalações das empresas, ou para publicidade assente na localização.

2.2.3. *Sistemas de videovigilância*

A fim de ajudar os exportadores a identificar cibervigilância potencial, é igualmente útil clarificar quais os produtos que não são abrangidos pela definição. Neste sentido, por exemplo, os sistemas e as câmaras de videovigilância — incluindo as câmaras de alta resolução — utilizados para filmar pessoas em espaços públicos não são abrangidos pela definição de produtos de cibervigilância, uma vez que não monitorizam nem recolhem dados de sistemas de informação e de telecomunicações.

3. MEDIDAS DE DILIGÊNCIA DEVIDA

De acordo com o considerando 7 do regulamento, «o contributo de exportadores […] para o objetivo global dos controlos comerciais é crucial. Para que estes possam atuar em conformidade com o presente regulamento, a avaliação dos riscos relacionados com as transações abrangidas pelo presente regulamento deverá ser feita através de medidas de análise das transações, também conhecidas por princípio da diligência devida, enquanto parte de um Programa Interno de Conformidade (ICP)».

O artigo 2.º, ponto 21, define «Programa interno de conformidade» ou «ICP», como «políticas e procedimentos em curso eficazes, adequados e proporcionados, adotados por exportadores para facilitar o cumprimento das disposições e dos objetivos do presente regulamento e dos termos e das condições das autorizações aplicados ao abrigo do presente regulamento, nomeadamente as medidas de diligência devida que avaliam os riscos relacionados com a exportação dos produtos para utilizadores finais e utilizações finais».

A Recomendação (UE) 2019/1318 da Comissão ([7]) proporciona um quadro para ajudar os exportadores a identificar, gerir e atenuar os riscos associados aos controlos do comércio de produtos de dupla utilização e a assegurar o cumprimento das disposições legislativas e regulamentares da União e nacionais que são aplicáveis.

Estas orientações podem apoiar os exportadores na execução de medidas de análise das transações, também conhecidas por princípio da diligência devida, enquanto parte de um ICP.

Nos termos do artigo 5.º, n.º 2, do Regulamento (UE) 2021/821, os exportadores de produtos de cibervigilância não incluídos na lista são obrigados a exercer a diligência devida através de medidas de análise das transações, ou tomar medidas relativas à classificação dos produtos e à avaliação do risco das transações. Na prática, os exportadores são incentivados a examinar o seguinte:

([7]) Recomendação (UE) 2019/1318 da Comissão, de 30 de julho de 2019, relativa aos programas de conformidade interna para os controlos do comércio de produtos de dupla utilização ao abrigo do Regulamento (CE) n.º 428/2009 do Conselho (JO L 205 de 5.8.2019, p. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Examinar se o produto não incluído na lista a exportar pode ser um «produto de cibervigilância», ou seja especialmente concebido para permitir a vigilância encoberta de pessoas singulares através da monitorização, extração, recolha ou análise de dados de sistemas de informação e de telecomunicações.**

Esta etapa diz respeito à determinação da natureza do produto nos termos das disposições aplicáveis aos produtos de cibervigilância. Inclui uma análise das características técnicas dos produtos, com base nos parâmetros técnicos estabelecidos no anexo I do regulamento para os produtos constantes da lista e à luz dos termos e conceitos específicos da definição de produtos de cibervigilância para produtos não incluídos na lista, bem como da subsequente classificação do produto (produtos, tecnologia ou *software*).

3.2. **Examinar as capacidades do produto em questão para determinar o potencial de utilização indevida no âmbito da repressão interna e/ou da prática de violações graves dos direitos humanos e do direito internacional humanitário por utilizadores finais estrangeiros.**

Os exportadores devem realizar uma avaliação para determinar se o produto pode ser utilizado de forma indevida para a prática de repressão interna, violação ou abuso dos direitos humanos, nomeadamente o direito à vida, a não ser objeto de tortura nem de tratamentos desumanos e degradantes, o direito à vida privada, o direito à liberdade de expressão, o direito de associação e de reunião, o direito à liberdade de pensamento, de consciência e de religião, o direito à igualdade de tratamento ou à proibição da discriminação ou o direito a eleições livres, justas e por voto secreto.

Inclui igualmente uma avaliação para determinar se o produto pode ser utilizado como parte ou componente de um sistema suscetível de resultar nas mesmas violações e/ou utilizações indevidas.

Na sua avaliação, os exportadores devem utilizar os chamados sinais de alerta que se referem a quaisquer circunstâncias anormais numa transação que indiquem que a exportação pode destinar-se a uma utilização final, a um utilizador final ou a um destino inadequados.

Sinais de alerta:

a) o produto é comercializado com informações sobre a sua potencial utilização para vigilância encoberta;

b) informações que indiquem que um produto semelhante foi utilizado indevidamente no âmbito de repressão interna e/ou da prática de violações graves dos direitos humanos e do direito internacional humanitário (ver secção 1.3);

c) informações que indiquem que o produto foi utilizado ilegalmente em atividades de vigilância dirigidas contra um Estado-Membro ou relacionadas com a vigilância ilegal de um cidadão da UE;

d) informações que indiquem que a transação inclui produtos que podem ser utilizados para criar, personalizar ou configurar um sistema que se sabe ser utilizado de forma indevida no âmbito de repressão interna e/ou da prática de violações graves dos direitos humanos e do direito internacional humanitário (ver secção 1.3);

e) o produto, ou um produto semelhante, consta da lista publicada na série C do *Jornal Oficial da União Europeia*, em conformidade com o artigo 5.º, n.º 6, do regulamento.

3.3. **Em apoio das autoridades competentes, examinar as partes interessadas envolvidas na transação (incluindo os utilizadores finais e os destinatários, nomeadamente distribuidores e revendedores).**

Os exportadores devem, a fim de apoiar as autoridades competentes, e na medida do possível:

a) antes e durante qualquer transação, analisar a forma como os destinatários e/ou os utilizadores finais tencionam utilizar o produto ou serviço, com base em declarações de utilização final;

b) familiarizar-se com a situação no destino pertinente dos produtos, especialmente com a situação geral dos direitos humanos, uma vez que este elemento constitui um indicador importante do risco de violações graves dos direitos humanos e do direito internacional humanitário associado a uma exportação;

c) analisar os riscos de o produto ou serviço ser desviado para um utilizador final diferente e não autorizado, com base nos sinais de alerta enumerados a seguir.

Sinais de alerta:

a) o utilizador final tem uma relação óbvia com um governo estrangeiro que tem um historial de repressão interna e/ou violações graves dos direitos humanos e do direito internacional humanitário;

b) o utilizador final faz parte estrutural das forças armadas ou de outro grupo envolvido num conflito armado no passado em que se registaram medidas de repressão interna e/ou violações graves dos direitos humanos e do direito internacional humanitário;

c) o utilizador final exportou no passado produtos de cibervigilância para países onde a utilização desses produtos deu origem a medidas de repressão interna e/ou a violações graves dos direitos humanos e do direito internacional humanitário.

3.4. **Utilizar as averiguações em matéria de diligência devida para elaborar planos destinados a prevenir e atenuar os potenciais impactos negativos futuros.**

Os exportadores devem, com base nas suas averiguações em matéria de diligência devida, cessar as atividades que causam ou contribuem para efeitos negativos relacionados com os direitos humanos, bem como elaborar e aplicar um plano de medidas corretivas. Essas ações podem incluir o seguinte:

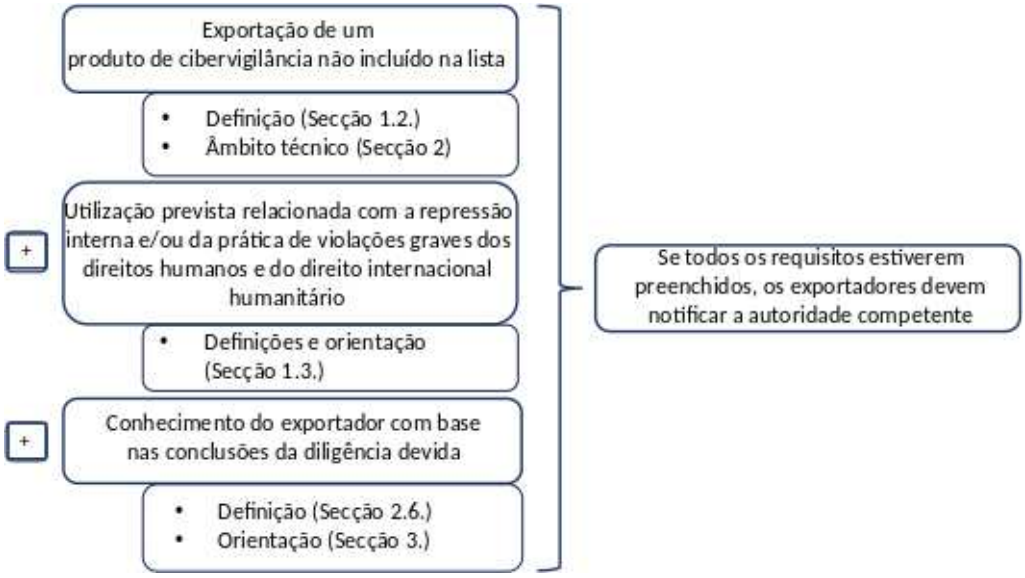
a) atualizar as políticas da empresa para fornecer orientações sobre a forma de evitar e fazer face aos efeitos negativos no futuro e assegurar a sua aplicação;

b) utilizar as conclusões da avaliação dos riscos para atualizar e reforçar os sistemas de gestão, a fim de rastrear melhor as informações e assinalar os riscos antes da ocorrência de impactos negativos;

c) recolher informações para compreender os riscos de alto nível colocados por impactos negativos relacionados com o setor;

d) notificar as autoridades competentes dos Estados-Membros das averiguações de diligência devida, a fim de facilitar o fluxo de informações no que diz respeito a determinados produtos, utilizadores finais e destinos.

Requisitos previstos no artigo 5.º, n.º 2, do Regulamento (UE) 2021/821



4. **APÊNDICE**

Produtos de cibervigilância incluídos na lista sujeitos a controlo nos termos do anexo I do Regulamento (UE) 2021/821

— **Sistemas de interceção de telecomunicações (5A001.f.)**

Na maioria dos países, incluindo os Estados-Membros, a confidencialidade das comunicações é protegida por lei, mas a vigilância eletrónica encoberta das comunicações pelas autoridades públicas pode ser autorizada no âmbito de um quadro jurídico (a chamada interceção legal). No entanto, a era digital trouxe consigo a possibilidade de utilizar tecnologias de interceção em larga escala. A utilização de ferramentas de interceção pelo regime líbio trouxe à luz o potencial de uso destas tecnologias em grande escala e promoveu a introdução de controlos das exportações de sistemas de interceção de telecomunicações em 2012.

Este controlo aplica-se a equipamentos concebidos para a extração do conteúdo de uma comunicação (voz ou dados), bem como a identificadores de assinante ou a outros metadados transmitidos por via hertziana através de comunicações sem fios, e a equipamentos de monitorização de radiofrequências. Este controlo aplica-se, por exemplo, aos intercetores IMSI (International Mobile Subscriber Identity) que intercetam o tráfego de telemóveis e rastreiam o movimento dos utilizadores de telemóveis ou ao equipamento que cria pontos de acesso Wi-Fi falsos que podem extrair números IMSI de um telefone, bem como a certos tipos de produtos especialmente concebidos para permitirem uma «inspeção profunda de pacotes» nos sistemas de telecomunicações. O equipamento de empastelamento de telecomunicações móveis não é abrangido pelo âmbito de aplicação dos produtos de cibervigilância, uma vez que não recolhe dados.

Embora esses sistemas possam ser criados com tecnologia de aplicação geral, as suas capacidades de interceção em larga escala dependerão de elementos e componentes específicos, incluindo, por exemplo, *software* específico, circuitos integrados avançados ou específicos para aplicações (por exemplo, matrizes de portas lógicas programáveis pós-fabrico, circuitos integrados de aplicação específica, etc.) com vista a aumentar o número de pacotes ou de sessões de comunicação que podem ser processadas por segundo.

— **Sistemas de vigilância da Internet (5A001.j.)**

Se bem que hoje em dia muitas comunicações através da Internet são normalmente cifradas por omissão, a interceção de dados de tráfego (metadados) sobre comunicações — tais como endereços IP e frequência e dimensões dos intercâmbios de dados — ainda pode ser utilizada para identificar ligações entre pessoas e nomes de domínio. Os Estados podem utilizar estes sistemas de forma lícita e com controlo judicial para fins legítimos, como a identificação de pessoas que visitam domínios associados a conteúdos criminosos ou terroristas. A monitorização e a análise do tráfego da Internet com base na caracterização étnica, religiosa, política ou social podem, no entanto, conduzir a uma cartografia humana e social completa de um país com vista ao controlo e à repressão da população, bem como a outros fins, por exemplo para identificar dissidentes políticos. Para além das questões relativas aos direitos humanos e à repressão interna, estes produtos podem também contribuir para o reforço das capacidades militares e de segurança.

O controlo previsto no ponto 5A001.j aplica-se aos sistemas de controlo da Internet que operam numa «rede dorsal com protocolo Internet (IP) (por exemplo, rede dorsal IP nacional)» para efetuar análise, extração e indexação de conteúdos de metadados transmitidos (voz, vídeo, mensagens, anexos) com base em «seletores concretos» e cartografar a rede relacional de pessoas. Trata-se de produtos que efetuam «vigilância encoberta» porque as pessoas visadas não têm conhecimento da interceção das comunicações. Em contrapartida, os controlos não visam sistemas em que existe uma ação ou uma interação com um utilizador ou um assinante e que, por exemplo, não se aplicam às redes sociais ou aos motores de pesquisa comerciais. Além disso, os controlos aplicam-se aos sistemas que tratam dados provenientes da rede principal de um fornecedor de Internet e não às redes sociais ou aos motores de pesquisa comerciais que tratam dados fornecidos pelos utilizadores.

— «***Software* de intrusão» (4A005, 4D004 e controlos conexos no âmbito de 4E001.a. e 4E001.c.)**

O *software* de intrusão permite ao seu operador obter, de forma encoberta, acesso remoto a um dispositivo eletrónico, como um telefone inteligente, um computador portátil, um servidor ou um dispositivo da Internet das coisas, obter dados armazenados no dispositivo, espiar através de uma câmara ou de um microfone incorporado no dispositivo ou a ele ligado e utilizar o dispositivo como rampa para efetuar ataques ao equipamento a que o dispositivo se liga, ou contra contactos do utilizador («pirataria informática através de dispositivos de terceiros»). Embora existam utilizações legítimas ([8]) de *software* de intrusão, por exemplo o «*software* de acesso remoto» utilizado pelos serviços informáticos para dar assistência à distância, a natureza encoberta da vigilância e a magnitude das informações que podem ser recolhidas representam um elevado risco de violação do direito à vida privada e à proteção dos dados pessoais e podem comprometer gravemente o direito à liberdade de expressão.

([8]) Por uma questão de clareza, os produtos de cibervigilância sujeitos a controlo por força da sua inclusão na lista do anexo I do Regulamento Dupla Utilização necessitam de uma autorização para serem exportados para países terceiros, independentemente de a utilização do produto ser legítima.

O controlo no âmbito de 4A005 *et al*. inclui *software*, bem como sistemas, equipamentos, componentes e tecnologia conexa, especialmente concebidos ou modificados para a geração, o comando e o controlo ou a distribuição de «*software* de intrusão», mas não se aplica ao próprio «*software* de intrusão», tal como definido no anexo I do regulamento. Estas ciberferramentas são objeto de controlo tendo em conta as potenciais perturbações e danos que podem causar se a sua utilização e execução tiver êxito, mas os controlos não se destinam a afetar a atividade dos investigadores e da indústria no domínio da cibersegurança, por exemplo, uma vez que estes necessitam de partilhar informações relacionadas com *software* de intrusão para poderem desenvolver correções para os seus produtos e instalá-las antes da divulgação pública de uma vulnerabilidade.

— ***Software* de monitorização das comunicações (5D001.e.)**

Este *software* foi concebido para a monitorização e a análise, pelas autoridades policiais autorizadas, dos dados recolhidos através de medidas de interceção dirigidas solicitadas a um prestador de serviços de comunicações. Este *software* permite pesquisas com base em «seletores concretos» dos conteúdos ou metadados das comunicações, utilizando uma interface para interceção legal, e cartografando a rede relacional ou rastreando o movimento das pessoas visadas com base nos resultados das pesquisas. Este *software* destina-se a «vigilância encoberta», uma vez que utiliza dados recolhidos a partir da interceção de comunicações sem o conhecimento das pessoas. Além disso, «analisa» os dados recolhidos através de «sistemas de telecomunicações». O *software* está instalado na autoridade pública (por exemplo, instalações de controlo do cumprimento da lei) e o controlo não se aplica aos sistemas de conformidade da interceção legal (por exemplo, sistemas de gestão da interceção legal e dispositivos de mediação) que são desenvolvidos comercialmente e instalados no espaço do prestador de serviços de comunicações (por exemplo, integrados na rede de comunicações), e que o prestador de serviços opera e mantém. Tal como clarificado no texto de controlo, os controlos não se aplicam ao «*software*» especialmente concebido ou modificado para fins puramente comerciais, como faturação, qualidade do serviço da rede (QoS), qualidade da experiência (QoE), dispositivos de mediação ou pagamento móvel ou utilização bancária.

— **Produtos utilizados para efetuar criptoanálise (5A004.a.)**

Este controlo aplica-se a produtos concebidos para contornar mecanismos criptográficos a fim de obter variáveis confidenciais ou dados sensíveis, incluindo texto transparente, senhas ou chaves criptográficas. A criptografia é utilizada para salvaguardar a confidencialidade das informações em trânsito e em repouso. A criptoanálise é utilizada para contrariar esta confidencialidade, dado que esta tecnologia «permite» a vigilância encoberta mediante monitorização, extração, recolha ou análise de dados de sistemas de informação e de telecomunicações.

— **Ferramentas forenses/de investigação (5A004.b., 5D002.a.3.b. e 5D002.c.3.b.)**

As ferramentas forenses/de investigação são concebidas para extrair dados brutos de um dispositivo (por exemplo, de computação ou de comunicação), de modo que os dados não sejam adulterados ou corrompidos e possam ser utilizados para fins judiciais, ou seja numa investigação criminal ou num tribunal. Estes produtos contornam os controlos de «autenticação» ou de autorização de um dispositivo, de modo que os dados brutos possam ser extraídos do dispositivo. Estes produtos são utilizados pelas autoridades públicas e pelos serviços e forças responsáveis pelo cumprimento da lei, mas também por forças militares para extrair e analisar dados de dispositivos apreendidos. Embora tenham utilizações legítimas, podem, no entanto, ser utilizados de forma indevida e, por conseguinte, representar um risco para dados sensíveis ou comerciais.

No entanto, as ferramentas forenses/de investigação que não sejam «especialmente concebidas» para a vigilância encoberta não são abrangidas pela definição de produtos de cibervigilância constante do artigo 2.º, ponto 20. Além disso, as ferramentas forenses/de investigação que apenas extraem dados dos utilizadores ou em que os dados não estão protegidos no dispositivo não são abrangidas pelas disposições de controlo de 5A004.b. *et al*. Do mesmo modo, os controlos não se aplicam aos equipamentos de produção ou ensaio dos fabricantes, às ferramentas de administração dos sistemas ou aos produtos exclusivamente destinados ao setor retalhista comercial, por exemplo produtos de desbloqueamento de telemóveis. Por conseguinte, tendo em conta a variedade destes tipos de tecnologia, a aplicação dos controlos depende de uma avaliação caso a caso de cada produto.

Por último, note-se que existem outros produtos relacionados com a vigilância enumerados no anexo I do regulamento que não devem ser considerados abrangidos pela definição de produtos de cibervigilância, como o equipamento de empastelamento de telecomunicações móveis (5A001.f.) concebido para danificar ou perturbar comunicações ou sistemas, *software* de intrusão que altera um sistema (4D004) e o equipamento de deteção acústica *laser* (6A005.g.) que recolhe dados áudio com um *laser* ou permite ouvir conversas à distância (por vezes designado por «microfone *laser*»). Do mesmo modo, a utilização para efeitos de vigilância de veículos aéreos não tripulados enumerados na lista não faz esses produtos entrar na definição de produtos de cibervigilância.