Journal officiel
de l'Union européenne

FR
Série L

2024/2659

16.10.2024

RECOMMANDATION (UE) 2024/2659 DE LA COMMISSION

du 11 octobre 2024

concernant des orientations pour l'exportation de biens de cybersurveillance au titre de l'article 5 du règlement (UE) 2021/821 du Parlement européen et du Conseil

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 292,

considérant ce qui suit:

(1) Le règlement (UE) 2021/821 du Parlement européen et du Conseil ([1]) institue un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage.

(2) Le règlement (UE) 2021/821 traite la question du risque que des biens de cybersurveillance fassent l'objet d'une utilisation impliquant la répression interne et/ou la commission de violations graves des droits de l'homme et du droit humanitaire international.

(3) Conformément à l'article 5, paragraphe 2, et à l'article 26, paragraphe 1, du règlement (UE) 2021/821, la Commission et le Conseil doivent formuler des orientations à l'intention des exportateurs concernant les biens de cybersurveillance non répertoriés, dans le but d'assurer l'efficacité du régime de contrôle des exportations de l'Union pour ce qui est de la cybersécurité et la cohérence de la mise en œuvre du règlement (UE) 2021/821.

(4) La présente recommandation et les orientations qui y sont jointes visent à soutenir les exportateurs dans l'application des contrôles concernant les biens de cybersurveillance non répertoriés, y compris, entre autres, dans l'application des mesures de vigilance visant à évaluer les risques liés à l'exportation de ces biens.

(5) Les orientations jointes à la présente recommandation ont fait l'objet de vastes consultations au sein du groupe d'experts sur les technologies de surveillance en 2022 et 2023 et il a été tenu compte des observations reçues lors d'une consultation publique ([2]) organisée au cours du deuxième trimestre de 2023.

(6) Il convient de rappeler que la présente recommandation et les orientations qui y sont jointes ne sont pas contraignantes. Les exportateurs devraient donc conserver la responsabilité de respecter les obligations qui leur incombent en vertu du règlement (UE) 2021/821, tandis que la Commission devrait veiller à ce que la présente recommandation reste pertinente au fil du temps,

([1]) Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (JO L 206 du 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.

A ADOPTÉ LA PRÉSENTE RECOMMANDATION:

Il est recommandé que les autorités compétentes des États membres et les exportateurs tiennent compte des orientations figurant à l'annexe de la présente recommandation en vue de remplir les obligations qui leur incombent en vertu de l'article 5, paragraphe 2, du règlement (UE) 2021/821.

Fait à Bruxelles, le 11 octobre 2024.

Par la Commission
Valdis DOMBROVSKIS
Vice-président exécutif

ANNEXE

TABLE DES MATIÈRES

INTRODUCTION

Le cadre de contrôle des exportations de l'Union établi par le règlement (UE) 2021/821 (ci-après le «règlement») vise à garantir le respect des obligations et engagements internationaux de l'Union et de ses États membres, y compris en ce qui concerne la paix, la sécurité et la stabilité régionales et le respect des droits de l'homme et du droit humanitaire international. C'est pourquoi l'Union et ses États membres ont mis en œuvre les décisions prises dans le cadre des régimes multilatéraux de contrôle des exportations et actualisé en conséquence la liste de contrôle de l'Union figurant à l'annexe I du règlement ([1]). En outre, avant l'entrée en application de l'article 5 du règlement, les autorités compétentes des États membres contrôlaient déjà l'exportation de certains biens répertoriés susceptibles d'avoir des applications en matière de surveillance ([2]), en tenant compte des risques d'utilisation abusive dans certaines circonstances spécifiques. Dans des circonstances exceptionnellement graves, l'Union a imposé des sanctions limitant l'exportation de certains équipements de surveillance ([3]).

Le règlement témoigne de la volonté de l'Union de lutter efficacement contre le risque que des biens de cybersurveillance fassent l'objet d'une utilisation impliquant la répression interne et/ou la commission de violations graves des droits de l'homme et du droit humanitaire international. Le règlement introduit, en particulier, de nouvelles dispositions relatives au contrôle des exportations de biens de cybersurveillance non répertoriés, y compris l'obligation pour les exportateurs d'informer l'autorité compétente lorsqu'ils ont connaissance, d'après les résultats des procédures de vigilance, de ce que des biens de cybersurveillance qui ne sont pas répertoriés et qu'ils entendent exporter sont destinés, en tout ou partie, à une utilisation impliquant la répression interne et/ou la commission de violations graves des droits de l'homme et du droit humanitaire international. Le règlement invite en outre la Commission et le Conseil à mettre à la disposition des exportateurs des orientations pour soutenir la mise en œuvre effective des nouveaux contrôles portant sur les biens de cybersurveillance non répertoriés.

Les présentes orientations visent par conséquent à aider les exportateurs lors de l'application des contrôles sur les biens de cybersurveillance non répertoriés, y compris les mesures de vigilance en ce qui concerne l'exportation de ces biens vers les utilisateurs finaux et aux fins des utilisations finales, en vertu des nouvelles dispositions du règlement.

1. DISPOSITIONS JURIDIQUES PERTINENTES, DÉFINITIONS ET CONCEPTS ESSENTIELS

1.1. Aperçu des dispositions juridiques pertinentes

Le règlement introduit de nouvelles dispositions prévoyant spécifiquement le contrôle des exportations de biens de cybersurveillance non énumérés à l'annexe I du règlement qui sont ou peuvent être destinés, entièrement ou en partie, à une utilisation impliquant la répression interne et/ou la commission de violations graves des droits de l'homme et du droit humanitaire international. Les considérants et articles pertinents sont les suivants:

a) le considérant 8: «Afin de lutter contre le risque que certains biens de cybersurveillance non répertoriés exportés au départ du territoire douanier de l'Union puissent être utilisés abusivement par des personnes complices ou responsables d'avoir ordonné ou commis des violations graves des droits de l'homme ou du droit humanitaire international, il y a lieu de contrôler l'exportation de ces biens. Les risques associés concernent notamment les cas où des biens de cybersurveillance sont conçus spécifiquement pour permettre l'intrusion ou l'inspection approfondie des

([1]) Voir en particulier les contrôles relatifs aux systèmes d'interception des télécommunications (5A001.f.), aux systèmes de surveillance de l'internet (5A001.j.), aux logiciels d'intrusion (4A005, 4D004 et contrôles connexes visés aux alinéas 4E001.a et 4E001.c.) et aux logiciels pour le suivi par les forces de l'ordre (5D001.e.). Voir en outre, sur la base d'une évaluation au cas par cas, les contrôles relatifs à certains outils de criminalistique/d'investigation (5A004.b., 5D002.a.3.b. et 5D002.c.3.b.).

([2]) En particulier les systèmes assurant la sécurité de l'information.

([3]) Voir le règlement (CE) nº 765/2006 du Conseil du 18 mai 2006 concernant des mesures restrictives en raison de la situation en Biélorussie et de l'implication de la Biélorussie dans l'agression russe contre l'Ukraine (JO L 134 du 20.5.2006, p. 1, ELI: http://data.europa.eu/eli/reg/2006/765/oj), le règlement (UE) nº 359/2011 du Conseil du 12 avril 2011 concernant des mesures restrictives à l'encontre de certaines personnes, entités et organismes au regard de la situation en Iran (JO L 100 du 14.4.2011, p. 1, ELI: http://data.europa.eu/eli/reg/2011/359/oj), le règlement (UE) nº 36/2012 du Conseil du 18 janvier 2012 concernant des mesures restrictives en raison de la situation en Syrie et abrogeant le règlement (UE) nº 442/2011 (JO L 16 du 19.1.2012, p. 1, ELI: http://data.europa.eu/eli/reg/2012/36/oj), le règlement (UE) nº 401/2013 du Conseil du 2 mai 2013 concernant des mesures restrictives instituées en raison de la situation au Myanmar/en Birmanie et abrogeant le règlement (CE) nº 194/2008 (JO L 121 du 3.5.2013, p. 1, ELI: http://data.europa.eu/eli/reg/2013/401/oj) et le règlement (UE) 2017/2063 du Conseil du 13 novembre 2017 concernant des mesures restrictives en raison de la situation au Venezuela (JO L 295 du 14.11.2017, p. 21, ELI: http://data.europa.eu/eli/reg/2017/2063/oj).

paquets dans des systèmes d'information et de télécommunication afin de procéder à une surveillance discrète de personnes physiques par la surveillance, l'extraction, la collecte et l'analyse des données provenant de ces systèmes, y compris des données biométriques. Les biens utilisés à des fins purement commerciales, comme la facturation, la commercialisation, les services de qualité, la satisfaction des utilisateurs ou la sécurité des réseaux, sont généralement considérés comme n'entraînant pas de tels risques»;

b) le considérant 9: «En vue de renforcer l'efficacité du contrôle des exportations de biens de cybersurveillance non répertoriés, il est essentiel d'harmoniser davantage l'application des contrôles "attrape-tout" dans ce domaine. À cette fin, les États membres s'engagent à soutenir ces contrôles en procédant à un échange d'informations entre eux et avec la Commission, notamment en ce qui concerne les évolutions technologiques relatives aux biens de cybersurveillance, et en faisant preuve de vigilance dans l'application de ces contrôles afin de promouvoir un échange au niveau de l'Union»;

c) l'article 2, point 20), qui définit de la manière suivante les biens de cybersurveillance: «les biens à double usage conçus spécifiquement pour permettre la surveillance discrète de personnes physiques par la surveillance, l'extraction, la collecte ou l'analyse de données provenant de systèmes d'information et de télécommunications»;

d) l'article 5 soumet à autorisation l'exportation des biens de cybersurveillance non répertoriés si l'autorité compétente a informé l'exportateur que les produits en question sont ou peuvent être destinés, entièrement ou en partie, à une utilisation impliquant la répression interne et/ou la commission de violations graves des droits de l'homme et du droit humanitaire international (article 5, paragraphe 1). Cet article prévoit en outre que les exportateurs doivent informer l'autorité compétente lorsqu'ils ont connaissance, d'après les résultats des procédures de vigilance, de ce que ces biens sont destinés, en tout ou partie, à une utilisation impliquant la répression interne et/ou la commission de violations graves des droits de l'homme et du droit humanitaire international (article 5, paragraphe 2). Il incombe à l'autorité compétente de décider de soumettre ou non l'exportation concernée à autorisation; et

e) l'article 5, paragraphe 2, dispose en outre ce qui suit: «La Commission et le Conseil formulent des orientations à l'intention des exportateurs, conformément à l'article 26, paragraphe 1».

1.2. **Définitions essentielles**

Le règlement contient des considérants et des dispositions spécifiques qui clarifient des termes particuliers pertinents pour le contrôle des exportations de biens de cybersurveillance non répertoriés, termes dont il est important que les exportateurs aient une bonne compréhension pour exercer leur devoir de vigilance et pour que les contrôles soient mis en œuvre efficacement. L'article 2, point 20), revêt une importance particulière, puisqu'il définit de manière précise les «biens de cybersurveillance»: «les biens à double usage conçus spécifiquement pour permettre la surveillance discrète de personnes physiques par la surveillance, l'extraction, la collecte ou l'analyse de données provenant de systèmes d'information et de télécommunications».

Aux fins des présentes orientations, il y a lieu de clarifier certains éléments spécifiques de cette définition.

1.2.1. *«Conçus spécifiquement»*

Un bien est conçu pour la surveillance discrète lorsque ses caractéristiques techniques sont adaptées à la surveillance discrète des personnes physiques et permettent objectivement de la réaliser. Par conséquent, l'expression «conçus spécifiquement» signifie que la surveillance discrète de personnes physiques doit avoir été la finalité principale du développement et de la conception du produit. Cette expression n'implique cependant pas que le bien doit uniquement pouvoir servir à la surveillance discrète de personnes physiques.

Comme précisé au considérant 8 du règlement, les biens utilisés à des fins purement commerciales, comme la facturation, la commercialisation, les services de qualité, la satisfaction des utilisateurs ou la sécurité des réseaux, ne sont pas conçus spécifiquement pour la surveillance discrète des personnes physiques et ne relèvent donc pas de la définition des biens de cybersurveillance. Par exemple, même si des biens destinés à la surveillance des systèmes d'exploitation dans l'industrie ou au suivi du trafic des utilisateurs peuvent être utilisés à des fins de surveillance, ils ne sont pas des biens de cybersurveillance au sens de la définition puisqu'ils ne sont pas conçus spécifiquement pour permettre la surveillance discrète des personnes physiques.

1.2.2. *«Surveillance discrète»*

Les biens permettent une surveillance discrète, en particulier, lorsque la surveillance n'est pas perceptible de manière évidente par la personne physique qui en fait l'objet. Tel est le cas lorsque les personnes concernées n'ont pas conscience de la présence et/ou de l'action de biens de cybersurveillance et n'ont donc pas la possibilité de se soustraire à cette surveillance ou, à tout le moins, d'adapter leur comportement en conséquence. Même si la surveillance est effectuée au moyen d'éléments installés ou fonctionnant dans l'espace public, l'acquisition de données peut, dans certains cas, être considérée comme relevant d'une surveillance discrète, notamment lorsque les données recueillies peuvent être détournées, évaluées ou traitées à des fins autres que celles dont la personne physique concernée a connaissance. En d'autres termes, lorsqu'une personne physique ne peut objectivement pas s'attendre à être sous surveillance, la surveillance peut être considérée comme discrète au sens de l'article 2, point 20), du règlement.

1.2.3. *«Personnes physiques»*

L'expression «personnes physiques» désigne les êtres humains, par opposition aux personnes morales ou aux entités, qui ne sont donc pas visées par les dispositions. Elle ne s'applique pas à la surveillance d'objets, de sites ou de machines en tant que tels.

1.2.4. *«Surveillance, extraction, collecte, analyse des données»*

Les termes «surveillance», «extraction», «collecte» et «analyse» sont généralement définis de la manière suivante dans les dictionnaires:

— «surveillance»: le fait de surveiller; ensemble des actes par lesquels on exerce un contrôle suivi,

— «extraction»: action d'extraire,

— «collecte»: action de réunir, de recueillir,

— «analyse»: différencier ou déterminer les éléments d'un objet (complexe) afin d'établir sa structure ou sa nature, et donc de l'expliquer ou de le comprendre; étude minutieuse et méthodique en vue d'une interprétation; action de soumettre à une analyse critique ou informatique.

Ces termes impliquent que les biens utilisés pour la surveillance doivent avoir des capacités techniques précises permettant le traitement des données dans le but de réaliser une surveillance, une extraction, une collecte ou une analyse de données. Tel est notamment le cas des biens suivants:

a) les biens qui sont utilisés pour surveiller les données provenant des systèmes d'information et de télécommunications ([4]) (par exemple la taille des fichiers ou le trafic groupé des données qui sont transmises dans de tels systèmes);

b) les biens qui permettent d'extraire des données des systèmes d'information et de télécommunications en effectuant des intrusions et des extractions (par exemple les logiciels d'intrusion);

c) les biens qui permettent d'analyser les données extraites des systèmes d'information et de télécommunications, y compris ceux qui peuvent traiter les images de caméras stockées dans ces systèmes (par exemple certains types de technologies d'analyse de données utilisés dans le cadre de systèmes de reconnaissance faciale).

Les biens utilisés simplement pour surveiller les systèmes d'information ou pour observer la population au moyen de caméras de vidéosurveillance et qui permettent de capter les conversations, les échanges de données, les mouvements et les comportements individuels ne seraient pas des biens de cybersurveillance au sens du règlement, étant donné qu'ils ne sont pas spécialement conçus à cette fin et doivent être utilisés avec d'autres technologies, telles que l'intelligence artificielle ou les mégadonnées. Toutefois, le système dans son ensemble (fonctionnant avec d'autres technologies telles que l'intelligence artificielle ou les technologies des mégadonnées) pourrait potentiellement être un bien de cybersurveillance au sens de l'article 2, point 20), du règlement.

Il est important de noter que, même si quelques exemples sont fournis à titre d'illustration, la définition et le champ d'application des biens de cybersurveillance ne sont pas limités par ces exemples, étant donné que l'objectif de l'article 5 est de permettre un contrôle efficace des exportations de biens non répertoriés.

([4]) Voir le point 1.2.5 ci-dessous pour la définition.

Comme l'indique l'emploi de la conjonction «ou» dans la définition, les capacités techniques énumérées doivent être considérées comme des alternatives, et il n'est pas nécessaire qu'un bien possède toutes ces capacités techniques de surveillance, d'extraction, de collecte ou d'analyse de données. Autrement dit, il suffit qu'un bien dispose d'une de ces capacités techniques pour rentrer dans la définition des biens de cybersurveillance figurant à l'article 2, point 20).

1.2.5. *«Provenant de systèmes d'information et de télécommunications»*

Cette expression désigne les systèmes qui traitent électroniquement des informations, par exemple les systèmes de programmation/de codage, les opérations du système d'ordinateur personnel (matériel) et d'autres systèmes d'administration de l'information, y compris la technologie logicielle, la technologie web, la technologie informatique, la technologie de stockage, etc., ainsi que certains systèmes qui communiquent des informations à distance, par exemple les systèmes techniques transmettant des sons, des signaux, du texte, d'autres signes ou des images, par des canaux filaires et sans fil, par fibre optique, par radio et par d'autres systèmes électromagnétiques. Ensemble, ces deux concepts recouvrent un large éventail de systèmes de transmission ou de traitement de l'information. Il convient de noter que cette expression fait référence à des systèmes et non à des équipements.

1.2.6. *«Connaissance» et «sont destinés à»*

L'article 5, paragraphe 2, du règlement prévoit qu'un exportateur est tenu d'informer l'autorité compétente lorsqu'il «a connaissance […] de ce que des biens de cybersurveillance […] sont destinés» à une utilisation impliquant la répression interne et/ou la commission de violations graves des droits de l'homme et du droit humanitaire international.

Le terme «connaissance» n'est pas un nouveau concept juridique, mais a été utilisé dans le cadre des exigences en matière d'autorisation liées à l'utilisation finale (les contrôles «attrape-tout») en vertu des articles 4, 6, 7 et 8 du règlement. Avoir «connaissance» implique le fait, pour l'exportateur, de savoir effectivement qu'une utilisation abusive est envisagée. La simple possibilité d'un tel risque ne suffit pas à établir une telle connaissance. La «connaissance» ne saurait toutefois être assimilée à une attitude passive: elle exige que l'exportateur ait agi pour obtenir des informations suffisantes et adéquates permettant d'évaluer les risques liés à l'exportation et de garantir le respect du règlement.

L'indication selon laquelle les biens doivent être «destinés à» une utilisation finale sensible pertinente implique que l'exportateur doit évaluer l'utilisation finale au cas par cas, à la lumière des circonstances spécifiques de l'espèce. À contrario, un risque théorique, c'est-à-dire non fondé sur une appréciation factuelle de la situation, que les biens puissent être utilisés d'une manière contraire aux droits de l'homme ne suffirait pas à impliquer qu'ils «sont destinés à» une utilisation abusive spécifique au sens de l'article 5.

1.3. **Répression interne, violations graves des droits de l'homme et du droit humanitaire international**

Conformément à l'article 15 du règlement, les États membres doivent tenir compte de tous les éléments pertinents énumérés audit article pour décider de l'octroi d'une autorisation, y compris les considérations qui relèvent de la position commune 2008/944/PESC du Conseil ([5]).

L'article 5 du règlement étend les contrôles à l'exportation de biens de cybersurveillance non répertoriés, compte tenu du risque qu'ils soient utilisés dans le cadre de la répression interne et/ou de la commission de violations graves des droits de l'homme et du droit humanitaire international. La position commune 2008/944/PESC et le guide d'utilisation correspondant ([6]) fournissent des orientations utiles à cet égard.

([5]) Position commune 2008/944/PESC du Conseil du 8 décembre 2008 définissant des règles communes régissant le contrôle des exportations de technologie et d'équipements militaires (JO L 335 du 13.12.2008, p. 99, ELI: http://data.europa.eu/eli/compos/2008/944/oj).

([6]) Guide d'utilisation de la position commune 2008/944/PESC du Conseil définissant des règles communes régissant le contrôle des exportations de technologie et d'équipements militaires (https://data.consilium.europa.eu/doc/document/ST-12189-2019-INIT/fr/pdf).

1.3.1. *Répression interne*

Aux termes de l'article 2, paragraphe 2, de la position commune 2008/944/PESC, la «répression interne comprend, entre autres, la torture et autres traitements ou châtiments cruels, inhumains et dégradants, les exécutions sommaires ou arbitraires, les disparitions, les détentions arbitraires et les autres violations graves des droits de l'homme et des libertés fondamentales que mentionnent les instruments internationaux pertinents en matière de droits de l'homme, dont la déclaration universelle des droits de l'homme et le pacte international relatif aux droits civils et politiques». Le guide d'utilisation relatif à la position commune 2008/944/PESC contient des orientations sur les éléments à prendre en considération lors de l'évaluation réalisée par l'exportateur, y compris la «réputation actuelle et passée de l'utilisateur final proposé pour ce qui est du respect des droits de l'homme ainsi que celle du pays destinataire en général».

1.3.2. *Commission de violations graves des droits de l'homme*

L'utilisation abusive de biens de cybersurveillance non répertoriés peut avoir une incidence négative sur un large éventail de droits de l'homme et porte directement atteinte au droit au respect de la vie privée et à la protection des données. Une surveillance arbitraire ou illégale peut également violer d'autres droits de l'homme, tels que le droit à la liberté d'expression, d'association et de réunion, la liberté de pensée, de conscience et de religion, ainsi que le droit à l'égalité de traitement ou l'interdiction de la discrimination, de même que le droit à des élections libres, équitables et à bulletin secret. Dans des cas particuliers, la surveillance, y compris le suivi ou la collecte d'informations sur des personnes physiques telles que des défenseurs des droits de l'homme, des militants, des personnalités politiques, des membres de groupes vulnérables ou des journalistes, peut conduire à des intimidations, à la répression, à des détentions arbitraires, à des actes de torture, voire à des exécutions extrajudiciaires. Par conséquent, les exportateurs devraient inclure ces aspects relatifs aux violations graves des droits de l'homme dans leurs évaluations.

La pratique internationale montre que toute restriction des droits de l'homme doit être «appropriée» et conforme aux normes internationales en matière de droits de l'homme. Concrètement, cela signifie que des garanties adéquates doivent être en place pour faire en sorte que les restrictions soient autorisées par la législation et préservent la substance des droits. Dans le respect du principe de proportionnalité, des restrictions ne peuvent être opérées que si elles sont nécessaires et répondent effectivement à un objectif légitime, par exemple la sécurité nationale ou publique, l'ordre public, la protection de la santé publique ou des droits et libertés d'autrui.

Les biens de cybersurveillance peuvent comprendre des outils légitimes et réglementés servant à assurer le respect du droit, utilisés par exemple à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, y compris dans le domaine de la lutte contre le terrorisme, ou d'exécution de sanctions pénales. À l'inverse, les biens de cybersurveillance peuvent être utilisés abusivement pour commettre de graves violations des droits de l'homme et du droit humanitaire international lorsqu'ils sont exportés vers des régimes répressifs ou des utilisateurs finaux privés et/ou vers des zones de conflit.

Il est donc nécessaire de réaliser une évaluation au cas par cas des circonstances de l'espèce, y compris l'application de la réglementation pertinente, à la lumière de tout constat de violations graves des droits de l'homme émanant des organismes compétents des Nations unies, de l'Union ou du Conseil de l'Europe, par exemple. La «gravité» des violations des droits de l'homme peut découler de la reconnaissance de l'existence de ces violations dans les informations publiées par les organismes compétents des Nations unies, par l'Union ou par le Conseil de l'Europe. Une telle reconnaissance explicite de la part de ces organismes n'est pas absolument nécessaire, mais constitue un facteur important indiquant que ce critère est rempli.

Selon les termes de l'article 5, la violation des droits de l'homme doit être «grave». Le guide d'utilisation relatif à la position commune 2008/944/PESC fournit des orientations utiles quant aux violations des droits de l'homme pouvant être qualifiées de «graves». D'après ce guide, la nature et les conséquences de la violation ont un caractère déterminant. Les violations des droits de l'homme systématiques et/ou nombreuses sont généralement considérées comme graves; cependant, des violations qui ne sont ni systématiques ni nombreuses peuvent être considérées comme «graves», par exemple en raison de la gravité de l'acte pour les personnes concernées.

L'annexe II du guide d'utilisation relatif à la position commune 2008/944/PESC contient une liste non exhaustive des principaux instruments internationaux et régionaux en matière de droits de l'homme, y compris le pacte international relatif aux droits civils et politiques (PIDCP), la convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants, la convention européenne des droits de l'homme (ci-après la «convention») et la charte des droits fondamentaux (ci-après la «charte»), qui peuvent fournir des orientations importantes pour l'interprétation et l'application des critères à l'appui d'évaluations solides au regard des droits de l'homme. Ces instruments ainsi que leurs protocoles additionnels respectifs constituent les principales normes internationales dans les domaines des droits de l'homme et des libertés fondamentales.

1.3.3. *Commission de violations graves du droit humanitaire international*

Le droit humanitaire international (également appelé «droit de Genève» ou «droit des conflits armés») a été élaboré au moyen d'une série de traités internationaux, dont les plus importants sont les règlements de La Haye, les conventions de Genève et leurs deux protocoles additionnels de 1977. Il définit des règles qui, en période de conflit armé, servent à protéger les personnes qui ne participent pas ou ne participent plus aux hostilités (par exemple les civils et les combattants blessés, malades ou capturés) et imposent aux parties belligérantes des limitations en ce qui concerne les moyens et les méthodes de guerre (droit de La Haye).

L'utilisation de biens de cybersurveillance non répertoriés devrait être conforme au droit humanitaire international lorsque ces biens sont déployés en tant que moyens et méthodes de guerre dans le contexte d'un conflit armé. Dans de telles circonstances, le risque de violations graves du droit humanitaire international est un élément à prendre en considération au titre du règlement et, comme pour les violations graves des droits de l'homme, devrait être évalué à la lumière de l'utilisation finale prévue des biens dans le cas d'espèce. Le guide d'utilisation relatif à la position commune 2008/944/PESC donne des orientations quant aux éléments à prendre en considération; ainsi, il convient de savoir si le pays destinataire a toujours été respectueux du droit humanitaire international et s'il continue de l'être, de voir quelles intentions il a exprimées au travers d'engagements officiels et de déterminer s'il est en mesure de veiller à ce que la technologie ou les équipements transférés soient utilisés dans le respect du droit humanitaire international et qu'ils ne soient pas détournés ou transférés vers d'autres destinations où ils pourraient servir à commettre des violations graves de ce droit.

L'article 5 indique que la violation du droit humanitaire international doit être «grave». Des orientations figurent dans le guide d'utilisation relatif à la position commune 2008/944/PESC, qui considère que les «cas isolés de violations du droit humanitaire international ne sont pas nécessairement révélateurs de l'attitude du pays destinataire à l'égard de ce droit», tout en précisant qu'il «y aurait lieu de s'inquiéter vivement si une certaine constance était observée dans les violations ou si le pays destinataire ne prenait pas les dispositions voulues pour sanctionner de tels actes». Le Comité international de la Croix-Rouge (CICR) a fourni des lignes directrices concernant l'évaluation des violations du droit humanitaire international à des fins de contrôle des exportations. Selon le CICR, les violations du droit humanitaire international sont graves si elles mettent en danger des personnes protégées (par exemple des civils, des prisonniers de guerre, des blessés et des malades) ou des objets protégés (par exemple des objets ou infrastructures civils) ou si elles violent des valeurs universelles importantes. Les crimes de guerre, par exemple, constituent des violations graves du droit humanitaire international. Le CICR mentionne en outre des facteurs à prendre en considération qui sont semblables à ceux cités dans le guide d'utilisation relatif à la position commune 2008/944/PESC, y compris les engagements formels d'appliquer les règles du droit humanitaire international, les mesures appropriées garantissant l'obligation de rendre des comptes en cas de violation du droit humanitaire international, la formation des militaires au droit humanitaire international et l'interdiction de recruter des enfants dans les forces armées.

2. **CHAMP D'APPLICATION TECHNIQUE**

2.1. **Biens de cybersurveillance répertoriés**

L'appendice des présentes orientations contient des informations sur les biens de cybersurveillance énumérés à l'annexe I du règlement, afin d'aider les exportateurs à identifier les biens de cybersurveillance non répertoriés potentiels.

2.2. **Biens de cybersurveillance non répertoriés potentiels**

S'il est par définition impossible de fournir une liste exhaustive des produits susceptibles d'être contrôlés au titre de l'article 5 dès lors qu'il s'agit de «biens non répertoriés», les biens décrits ci-après pourraient nécessiter une surveillance et justifier une vigilance particulière au titre du règlement.

Comme précisé au considérant 8 du règlement, les biens utilisés à des fins purement commerciales, comme la facturation, la commercialisation, les services de qualité, la satisfaction des utilisateurs ou la sécurité des réseaux, sont généralement considérés comme n'entraînant pas de risque d'utilisation abusive dans le cadre de violations graves des droits de l'homme ou du droit humanitaire international, et ne sont donc généralement pas soumis à un contrôle au titre de l'article 5. Nombre de ces biens possèdent des fonctionnalités de sécurité de l'information (cryptographie, voire cryptoanalyse) qui répondent aux paramètres de contrôle établis dans le texte explicatif se rapportant à la catégorie 5, partie 2, et figurant à l'annexe I du règlement. Les équipements de réseau relatifs à la sécurité — y compris les routeurs, les commutateurs ou les relais, dont la fonctionnalité de sécurité de l'information est limitée aux tâches «opération, administration ou maintenance» mettant en œuvre uniquement des normes cryptographiques publiées ou commerciales — ne sont pas non plus couverts par la définition des «biens de cybersurveillance» mais les exportateurs devraient rester vigilants car plusieurs cas d'utilisation abusive de ces biens dans le cadre de violations des droits de l'homme ont été rapportés.

2.2.1. *Technologie de reconnaissance faciale et de reconnaissance des émotions*

Les technologies de reconnaissance faciale et de reconnaissance des émotions ont de nombreuses utilisations en dehors de la cybersurveillance (par exemple l'identification ou l'authentification) et ne relèvent pas automatiquement de la définition. Elles peuvent toutefois, dans certaines circonstances, entrer dans le champ d'application de l'article 2, point 20), du règlement.

Lorsqu'elles peuvent être utilisées pour surveiller ou analyser des images vidéo stockées, ces technologies pourraient relever de la définition des biens de cybersurveillance. En tout état de cause, même lorsque les critères susmentionnés sont remplis, il convient d'examiner attentivement si le logiciel est spécialement conçu pour la surveillance discrète.

2.2.2. *Dispositifs de localisation*

Les dispositifs de localisation permettent de suivre dans l'espace et dans le temps l'emplacement physique d'un dispositif et, depuis un certain nombre d'années, certaines technologies de localisation sont utilisées par les services chargés de l'application de la loi et les services de renseignement. Les possibilités qu'ils offrent pour une surveillance ciblée et une surveillance de masse ont considérablement évolué avec les progrès des technologies de suivi — y compris la localisation par satellite, la localisation grâce aux antennes-relais, les émetteurs-récepteurs Wi-Fi et Bluetoooth — et la large diffusion des «dispositifs de suivi» tels que les smartphones et autres appareils électroniques (par exemple les systèmes embarqués dans les voitures).

Les services chargés de l'application de la loi et les services de renseignement utilisent des dispositifs de localisation, par exemple pour recueillir des éléments de preuve au cours d'une enquête ou pour suivre des suspects, mais les entreprises y ont également recours, à des fins commerciales, par exemple pour obtenir des schémas de déplacement agrégés dans les rues commerciales, suivre des employés travaillant hors site ou à des fins de publicité géolocalisée.

2.2.3. *Systèmes de surveillance vidéo*

Afin d'aider les exportateurs à identifier les biens de cybersurveillance potentiels, il est également utile de préciser quels biens sont exclus de la définition. En ce sens, par exemple, les systèmes de vidéosurveillance et les caméras — y compris les caméras à haute résolution — utilisés pour filmer des personnes dans les espaces publics n'entrent pas dans la définition des biens de cybersurveillance, étant donné qu'ils ne surveillent pas ni ne collectent de données provenant de systèmes d'information et de télécommunications.

3. **MESURES DE VIGILANCE**

Conformément au considérant 7 du règlement, «[l]a contribution des exportateurs […] à l'objectif général des contrôles effectués sur les échanges est essentielle. Afin de leur permettre d'agir conformément au présent règlement, l'évaluation des risques liés aux transactions concernées par le présent règlement doit être effectuée au moyen de mesures d'examen analytique des transactions, également connues sous le nom de principe de diligence raisonnable, dans le cadre d'un programme interne de conformité (PIC)».

Conformément à la définition figurant à l'article 2, point 21), le programme interne de conformité (PIC) correspond aux «politiques et procédures permanentes efficaces, appropriées et proportionnées, qui sont adoptées par les exportateurs pour favoriser le respect des dispositions et des objectifs du présent règlement ainsi que des conditions d'octroi des autorisations prévues par le présent règlement, et notamment les mesures de vigilance en ce qui concerne l'exportation des biens vers les utilisateurs finaux et aux fins des utilisations finales».

La recommandation (UE) 2019/1318 de la Commission ([7]) établit un cadre afin d'aider les exportateurs à détecter, à gérer et à atténuer les risques associés au contrôle des échanges de biens à double usage ainsi qu'à assurer la conformité avec la législation et la réglementation pertinentes des États membres et de l'Union.

Les présentes orientations peuvent aider les exportateurs à mettre en œuvre des mesures d'examen analytique des transactions, également connues sous le nom de principe de diligence raisonnable, dans le cadre d'un PIC.

Conformément à l'article 5, paragraphe 2, du règlement (UE) 2021/821, les exportateurs de biens de cybersurveillance non répertoriés doivent appliquer des procédures de vigilance au moyen de mesures d'examen analytique des transactions, c'est-à-dire qu'ils doivent prendre des mesures concernant la classification des biens et l'évaluation des risques liés aux transactions. En pratique, les exportateurs sont encouragés à effectuer les vérifications décrites ci-dessous.

([7]) Recommandation (UE) 2019/1318 de la Commission du 30 juillet 2019 relative aux programmes internes de conformité aux fins du contrôle des échanges de biens à double usage en vertu du règlement (CE) nº 428/2009 du Conseil (JO L 205 du 5.8.2019, p. 15, ELI: http://data.europa.eu/eli/reco/2019/1318/oj).

3.1. **Vérifier si le bien non répertorié destiné à l'exportation pourrait être un «bien de cybersurveillance», c'est-à-dire s'il est conçu spécifiquement pour permettre la surveillance discrète de personnes physiques par la surveillance, l'extraction, la collecte ou l'analyse de données provenant de systèmes d'information et de télécommunications**

Cette mesure concerne la détermination du type de bien en vertu des dispositions applicables aux biens de cybersurveillance. Il s'agit notamment d'examiner les caractéristiques techniques du bien sur la base des paramètres techniques énoncés à l'annexe I du règlement pour les biens répertoriés et à la lumière des termes et concepts spécifiques figurant dans la définition des biens de cybersurveillance pour les biens non répertoriés, et de classifier le bien en conséquence (bien matériel, technologie ou logiciel).

3.2. **Examiner les capacités du bien en question afin de déterminer le potentiel d'utilisation abusive dans le cadre d'une répression interne et/ou de violations graves des droits de l'homme et du droit humanitaire international par des utilisateurs finals étrangers**

Les exportateurs devraient procéder à une évaluation afin de déterminer si le produit pourrait être utilisé abusivement pour commettre des actes de répression interne, violer les droits de l'homme ou y porter atteinte, y compris le droit à la vie, l'interdiction de la torture et des traitements inhumains ou dégradants, le droit au respect de la vie privée, le droit à la liberté d'expression, le droit à la liberté d'association et de réunion, le droit à la liberté de pensée, de conscience et de religion, le droit à l'égalité de traitement, l'interdiction de la discrimination ou le droit à des élections libres, équitables et à bulletin secret.

Il convient également, dans le cadre de cette évaluation, de déterminer si le produit pourrait être utilisé comme partie ou composant d'un système susceptible de conduire aux mêmes violations et/ou utilisations abusives.

Les exportateurs devraient fonder leur évaluation sur des «signaux d'alerte», à savoir l'existence de toute circonstance anormale dans une transaction qui indique que l'exportation est peut-être destinée à une utilisation finale, à un utilisateur final ou à une destination inappropriés.

Signaux d'alerte:

a) le bien est commercialisé avec des informations relatives à son utilisation potentielle à des fins de surveillance discrète;

b) informations indiquant qu'un bien similaire a été utilisé abusivement à des fins de répression interne et/ou dans le cadre de violations graves des droits de l'homme et du droit humanitaire international (voir partie 1.3);

c) informations indiquant que le bien a été utilisé illégalement dans le cadre d'activités de surveillance dirigées contre un État membre ou dans le cadre d'une surveillance illégale d'un citoyen de l'Union;

d) informations indiquant que la transaction comprend des biens qui pourraient être utilisés pour mettre en place, personnaliser ou configurer un système dont on sait qu'il est utilisé abusivement à des fins de répression interne et/ou dans le cadre de violations graves des droits de l'homme et du droit humanitaire international (voir partie 1.3);

e) le bien ou un bien similaire figure sur la liste publiée au *Journal officiel de l'Union européenne*, série C, conformément à l'article 5, paragraphe 6, du règlement.

3.3. **Examiner les acteurs participant à la transaction (y compris les utilisateurs finals et les destinataires tels que les distributeurs et les revendeurs), afin de soutenir les autorités compétentes**

Les exportateurs devraient, afin de soutenir les autorités compétentes, et dans la mesure du possible:

a) avant et pendant toute transaction, vérifier, sur la base des déclarations relatives à l'utilisation finale, la manière dont les destinataires et/ou les utilisateurs finals ont l'intention d'utiliser le produit ou le service;

b) se renseigner sur la situation applicable dans la région de destination, en particulier en ce qui concerne la situation générale des droits de l'homme, car cela constitue un indicateur important du risque de violations graves des droits de l'homme ou du droit humanitaire international dans le cadre d'une exportation;

c) examiner les risques de détournement du produit ou service vers un autre utilisateur final non autorisé, sur la base des signaux d'alerte ci-dessous.

Signaux d'alerte:

a) l'utilisateur final a des liens manifestes avec un gouvernement étranger ayant des antécédents en matière de répression interne et/ou de violations graves des droits de l'homme et du droit humanitaire international;

b) l'utilisateur final fait structurellement partie des forces armées ou d'un autre groupe ayant participé par le passé à un conflit armé impliquant des mesures de répression interne et/ou des violations graves des droits de l'homme et du droit humanitaire international;

c) l'utilisateur final a exporté par le passé des biens de cybersurveillance vers des pays où l'utilisation de ces biens a donné lieu à des mesures de répression interne et/ou à de graves violations des droits de l'homme et du droit humanitaire international.

3.4. Utiliser les résultats des procédures de vigilance pour élaborer des plans visant à prévenir et à atténuer les incidences négatives potentielles à l'avenir

Les exportateurs devraient, sur la base des résultats de leurs procédures de vigilance, mettre un terme aux activités qui ont des incidences négatives sur les droits de l'homme ou y contribuent, et élaborer et mettre en œuvre un plan de mesures correctives. Ces mesures peuvent notamment être les suivantes:

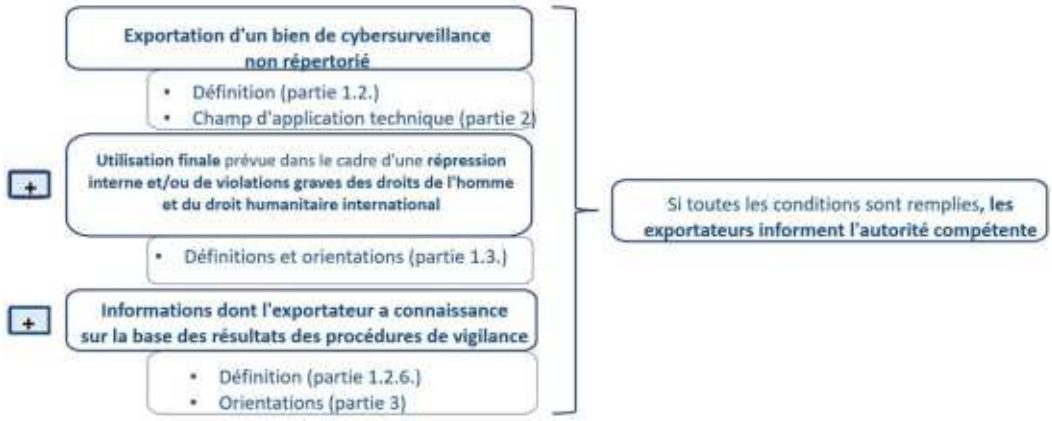
a) mettre à jour la stratégie de l'entreprise afin de fournir des orientations sur la manière d'éviter et de traiter les incidences négatives à l'avenir, et veiller à sa mise en œuvre;

b) exploiter les conclusions de l'évaluation des risques pour mettre à jour et renforcer les systèmes de gestion afin de mieux suivre les informations et de mettre en évidence les risques avant que des incidences négatives ne se produisent;

c) recueillir des informations afin de comprendre les risques élevés d'incidences négatives liés au secteur;

d) notifier les résultats des procédures de vigilance aux autorités compétentes des États membres afin de faciliter les flux d'informations en ce qui concerne certains biens, certains utilisateurs finals et certaines destinations.

Exigences énoncées à l'article 5, paragraphe 2, du règlement (UE) 2021/821



4. APPENDICE

Biens de cybersurveillance mentionnés à l'annexe I du règlement (UE) 2021/821

— **Systèmes d'interception des télécommunications (5A001.f.)**

Dans la plupart des pays, y compris les États membres, la confidentialité des communications est protégée par la loi, mais la surveillance électronique discrète des communications par les autorités gouvernementales peut être autorisée à l'intérieur d'un cadre juridique [«interception légale» (LI)]. L'ère numérique a toutefois rendu possible l'utilisation de technologies d'interception à grande échelle. L'utilisation d'outils d'interception par le régime libyen a mis en évidence le potentiel de déploiement de ces technologies à grande échelle et a conduit, en 2012, à l'introduction de contrôles à l'exportation sur les systèmes d'interception des télécommunications.

Ces contrôles portent sur les équipements conçus pour extraire le contenu d'une communication (voix ou données), ainsi que les identifiants d'abonnés ou autres métadonnées transmis par voie aérienne via une communication sans fil, et sur les équipements de surveillance des radiofréquences. Ils s'appliquent notamment aux intercepteurs d'IMSI (identité internationale de l'abonné mobile) qui interceptent le trafic de téléphones mobiles et suivent les mouvements des utilisateurs de téléphones mobiles, aux équipements générant de faux points d'accès Wi-Fi capables d'extraire les numéros IMSI d'un téléphone, ainsi qu'à certains types de biens spécialement conçus pour permettre une «inspection approfondie des paquets» dans les systèmes de télécommunications. Le matériel de brouillage des télécommunications mobiles ne relève pas du champ d'application des biens de cybersurveillance car il ne collecte pas de données.

Bien que les technologies à usage général puissent être utilisées pour mettre en place de tels systèmes, leurs capacités d'interception à grande échelle dépendent de pièces et de composants spécifiques, tels que des logiciels spécifiques ou des circuits intégrés avancés ou spécifiques à une application (FGPA, ASIC, etc.), qui permettent d'augmenter le nombre de paquets ou de sessions de communication pouvant être traités par seconde.

— **Systèmes de surveillance de l'internet (5A001.j.)**

Bien que les communications sur l'internet soient désormais généralement cryptées par défaut, il est encore recouru à l'interception des données de trafic (métadonnées) relatives aux communications — telles que les adresses IP et la fréquence et le volume des échanges de données — pour établir les liens entre les personnes et les noms de domaine. Les gouvernements peuvent utiliser ces systèmes de manière légale et moyennant un contrôle judiciaire à des fins légitimes, par exemple pour identifier les visiteurs de domaines associés à des contenus criminels ou terroristes. Le suivi et l'analyse du trafic internet sur la base de caractéristiques ethniques, religieuses, politiques ou sociales peuvent toutefois servir à dresser une vaste cartographie humaine et sociale d'un pays dans le but de contrôler et de réprimer la population, ou à d'autres fins, par exemple pour identifier les dissidents politiques. En dehors des questions relatives aux droits de l'homme et à la répression interne, ces biens peuvent également contribuer au renforcement des capacités militaires et de sécurité.

Le contrôle prévu à l'alinéa 5A001.j. s'applique aux systèmes de contrôle de l'internet qui fonctionnent sur un «réseau IP de classe opérateur» (par exemple réseau de transport IP au niveau national) pour effectuer l'analyse, l'extraction et l'indexation du contenu des métadonnées transmises (voix, vidéo, messages, pièces jointes) sur la base de «sélecteurs stricts» et cartographier le réseau relationnel des personnes. Il s'agit de biens permettant d'effectuer une «surveillance discrète» parce que les personnes visées n'ont pas connaissance de l'interception de leurs communications. En revanche, les contrôles ne portent pas sur les systèmes dans lesquels il existe une action ou une interaction avec un utilisateur ou un abonné; ainsi, ils ne s'appliquent pas aux réseaux sociaux ou aux moteurs de recherche commerciaux. De plus, les contrôles s'appliquent aux systèmes qui traitent des données provenant d'un réseau central d'un fournisseur d'internet et ne s'appliquent pas aux réseaux sociaux ou aux moteurs de recherche commerciaux qui traitent les données communiquées par les utilisateurs.

— **«Logiciels d'intrusion» (4A005, 4D004 et contrôles connexes au titre des alinéas 4E001.a. et 4E001.c.)**

Les logiciels d'intrusion permettent à leur opérateur d'obtenir discrètement un accès à distance à un appareil électronique, tel qu'un smartphone, un ordinateur portable, un serveur ou un dispositif de l'internet des objets, afin d'obtenir des données stockées sur l'appareil, de réaliser une écoute au moyen d'une caméra ou d'un microphone intégré à l'appareil ou connecté à celui-ci, et d'utiliser l'appareil pour attaquer les équipements auxquels l'appareil se connecte ou les contacts de l'utilisateur («piratage par l'intermédiaire d'appareils tiers»). Il existe certes des utilisations légitimes ([8]) de logiciels d'intrusion, par exemple les «logiciels d'accès à distance» utilisés pour le support à distance par les services informatiques mais, en raison de la nature discrète de la surveillance et du volume des informations pouvant être recueillies, ces logiciels présentent un risque élevé de violation du droit à la vie privée et à la protection des données à caractère personnel et d'atteinte grave au droit à la liberté d'expression.

([8]) Il est utile de préciser ici que tous les biens de cybersurveillance mentionnés à l'annexe I du règlement sur les biens à double usage nécessitent une autorisation pour être exportés vers des pays tiers, que l'utilisation du bien soit légitime ou non.

Le contrôle au titre du paragraphe 4A005 et des autres rubriques citées inclut les logiciels ainsi que les systèmes, équipements, composants et technologies connexes spécialement conçus ou modifiés pour la génération, la commande et le contrôle ou la livraison de «logiciels d'intrusion», mais ne s'applique pas aux «logiciels d'intrusion» eux-mêmes tels que définis à l'annexe I du règlement. Ces cyberoutils sont contrôlés en raison des perturbations et dommages potentiels qu'ils peuvent causer s'ils sont utilisés et mis en œuvre avec succès mais le but n'est pas d'entraver, par exemple, l'activité des chercheurs et de l'industrie de la cybersécurité car ceux-ci ont besoin de partager des informations concernant les logiciels d'intrusion pour mettre au point des solutions pour leurs produits et les mettre en place avant la divulgation publique d'une vulnérabilité.

— **Logiciels de surveillance des communications (5D001.e.)**

Ces logiciels sont conçus pour permettre le suivi et l'analyse, par les autorités autorisées chargées de l'application de la loi, des données collectées au moyen de mesures d'interception ciblées demandées à un fournisseur de services de communications. Ils permettent d'effectuer des recherches à partir de «sélecteurs stricts» de contenu de la communication ou de métadonnées, à l'aide d'une interface pour l'interception légale, et de cartographier le réseau relationnel ou de suivre les mouvements des personnes ciblées sur la base des résultats des recherches. Ils sont destinés à la «surveillance discrète» parce qu'ils utilisent des données collectées lors de l'interception de communications à l'insu des personnes concernées. En outre, ils «analysent» les données collectées au moyen de «systèmes de télécommunications». Les logiciels sont installés dans les locaux de l'autorité gouvernementale (par exemple une installation de surveillance des services autorisés) et les contrôles ne s'appliquent pas aux systèmes de conformité de l'interception légale (par exemple systèmes de gestion de l'interception légale et dispositifs de médiation) qui sont développés commercialement et installés chez le fournisseur de services de communications (par exemple intégrés dans le réseau de communications) et exploités et gérés par le fournisseur de services. Comme précisé dans le texte explicatif, les contrôles ne s'appliquent pas aux logiciels spécialement conçus ou modifiés à des fins purement commerciales, telles que la facturation, la qualité de service du réseau de (QoS), la qualité de l'expérience (QoE), les dispositifs de médiation ou le paiement mobile ou l'usage bancaire.

— **Biens utilisés pour l'analyse cryptographique (5A004.a.)**

Ce contrôle s'applique aux biens conçus pour déjouer les mécanismes cryptographiques afin d'obtenir des variables confidentielles ou des données sensibles, y compris du texte en clair, des mots de passe ou des clés cryptographiques. La cryptographie est utilisée pour préserver la confidentialité des informations en transit et au repos. L'analyse cryptographique est utilisée pour déjouer cette confidentialité et «permet» donc une surveillance discrète par la surveillance, l'extraction, la collecte ou l'analyse de données provenant de systèmes d'information et de télécommunications.

— **Outils de criminalistique/d'investigation (5A004.b., 5D002.a.3.b. et 5D002.c.3.b.)**

Les outils de criminalistique/d'investigation sont conçus pour extraire des données brutes d'un dispositif (par exemple informatique ou de communication) de telle sorte que les données ne soient pas altérées ou corrompues et puissent être utilisées à des fins judiciaires, c'est-à-dire dans le cadre d'une enquête pénale ou devant une juridiction. Ces produits contournent les contrôles d'«authentification» ou d'autorisation d'un dispositif afin que les données brutes puissent être extraites de celui-ci. Ces produits sont utilisés par le gouvernement et les services chargés de l'application de la loi, mais aussi par les forces militaires pour extraire et analyser des données provenant d'appareils saisis. Bien qu'ils aient des utilisations légitimes, ils peuvent être utilisés abusivement et donc présenter un risque pour les données sensibles ou commerciales.

Toutefois, les outils de criminalistique/d'investigation qui ne sont pas «spécialement conçus» pour la surveillance discrète ne relèvent pas de la définition des biens de cybersurveillance figurant à l'article 2, point 20). En outre, les outils de criminalistique/d'investigation qui extraient uniquement les données de l'utilisateur ou qui sont utilisés alors que les données ne sont pas protégées sur le dispositif ne sont pas visés par le texte explicatif de l'alinéa 5A004.b. et des autres alinéas cités. De même, les contrôles ne s'appliquent pas aux équipements de production ou d'essai du fabricant, aux outils de l'administrateur du système ou aux produits destinés exclusivement au secteur de la vente au détail, par exemple les produits de déverrouillage de téléphones mobiles. Par conséquent, étant donné la diversité de ces types de technologies, l'application des contrôles dépend d'une évaluation au cas par cas de chaque produit.

Enfin, il convient de noter qu'il existe d'autres biens liés à la surveillance, énumérés à l'annexe I du règlement, qui ne devraient pas être considérés comme relevant de la définition des biens de cybersurveillance, tels que les équipements de brouillage de télécommunications mobiles (5A001.f.) conçus pour détériorer ou perturber des communications ou des systèmes, les logiciels d'intrusion qui modifient un système (4D004) et les équipements laser de détection acoustique (6A005.g.) qui recueillent des données audio au moyen d'un laser ou permettent d'écouter des conversations à distance (parfois appelés «microphones laser»). De même, le fait d'utiliser à des fins de surveillance des véhicules aériens sans équipage (UAV) répertoriés ne ferait pas entrer ces biens dans la définition des biens de cybersurveillance.